Goldstein · Schappacher · Schwermer

The Shaping of Arithmetic after C. F. Gauss's Disquisitiones Arithmeticae

Catherine Goldstein
Norbert Schappacher
Joachim Schwermer *Editors*

The Shaping of Arithmetic

after C. F. Gauss's Disquisitiones Arithmeticae

With 36 Figures

Springer

Catherine Goldstein
Histoire des sciences mathématiques
Institut de mathématiques de Jussieu
175 rue du Chevaleret
75013 Paris, France
E-mail: cgolds@math.jussieu.fr

Joachim Schwermer
Fakultät für Mathematik
Universität Wien
Nordbergstraße 15
1090 Wien, Austria
E-mail: joachim.schwermer@univie.ac.at

Norbert Schappacher
UFR de mathématique
et d'informatique / IRMA
7 rue René Descartes
67084 Strasbourg Cedex, France
E-mail: schappa@math.u-strasbg.fr

Library of Congress Control Number: 2006932291

ISBN 978-3-540-20441-1 Springer Berlin Heidelberg New York

Springer is a part of Springer Science+Business Media

springer.com

Typeset by the editors
Production: LE-TEX Jelonek, Schmidt & Vöckler GbR, Leipzig
Cover design: WMXDesign GmbH, Heidelberg

Printed on acid-free paper 44/3100/YL 5 4 3 2 1 0

In memoriam

Martin Kneser
1928 – 2004

Foreword

In 1998, the editors convinced themselves that it was the right time to take stock of recent research concerning the modern history of number theory, and to evaluate in its light our comprehension of the development of this discipline as a whole. One issue at stake was to bring together historiographical results coming from different disciplines and linguistic domains which, we felt, had remained too often unaware of each other.

We organized two meetings at the *Mathematisches Forschungsinstitut Oberwolfach* : first a small RIP-workshop held June 14–19, 1999, among historians of number theory and historians of related topics, and then a larger conference which took place June 17–23, 2001, two hundred years after the publication of Carl Friedrich Gauss's *Disquisitiones Arithmeticae*. The latter brought together historians and philosophers of mathematics with number theorists interested in the recent history of their field. Two further meetings, organized by one of us in Vienna and Zürich the following years, continued our venture.

Two concrete projects arose from these activities. One concerned the creation of resources, for scholars and students: we initiated a bibliography of secondary literature on the History of Number Theory since 1800.[1]

The present volume is the second result of our work. It aims at answering the question, already raised during the first workshop, on the role of Gauss's *Disquisitiones Arithmeticae* in the definition and evolution of number theory. This role is here appraised in a comparative perspective, with attention both to the mathematical reception of the treatise, and to its role as a model for doing mathematics. The volume is the result of a collective work. Although all authors have kept their proper voices, they have also accepted quite a bit of editorial interference with a view to making the volume as coherent as possible. We have nonetheless left room for original analyses and results, including newly discovered documents.

[1] A preliminary version of this bibliography has been kindly put on line by Franz Lemmermeyer on a website hosted by the University of Heidelberg (http://www.rzuser.uni-heidelberg.de/~hb3/HINTbib.html).

During its rather long elaboration, the present book has greatly profited from the help of many individuals and institutions which we here gratefully acknowledge: the *Mathematisches Forschungsinstitut Oberwolfach* and its director at the time of the meetings, Matthias Kreck; the *Erwin-Schroedinger International Institute for Mathematical Physics* at Vienna; the ETH at Zürich, and special encouragement provided by Urs Stammbach; the CIRM at Luminy, which gave us a week's refuge for our editorial work in the summer of 2003; the *Laboratoire de mathématiques de l'Université Paris-Sud*, the *Institut de mathématiques de Jussieu*, as well as the *Institut de la recherche mathématique avancée* at Strasbourg which actively supported our joint work for the preparation of this book. Special thanks go to the *Abteilung Handschriften und Alte Drucke der Niedersächsischen Staats- und Universitätsbibliothek Göttingen*, and in particular to Jürgen Rohlfing, for the expert collaboration which made so many documents available to us, some of them as high quality scans. We also express our sincere gratitude to Springer-Verlag and their associated staff at Heidelberg and Leipzig, especially to Joachim Heinze, who believed in this project at an early stage. Our warmest thanks go to Frazer Jarvis for linguistic work on the texts, and to Jim Ritter for constant technical and moral support.

And last but not least, we thank all the participants of the Oberwolfach meetings who have shared their insights and knowledge with us for the benefit of the project: besides the authors of this book, Leo Corry, Hélène Gispert, Jeremy Gray, Ralf Haubrich, Helmut Koch, Martina Schneider, Takase Masahito, Erhard Scholz, Urs Stammbach, and Hans Wussing.

One of the participants at the 2001 conference was Martin Kneser. Despite his serious illness, his intense, visible passion for number theory and its history was a challenging inspiration to all of us, historians and mathematicians alike. Martin Kneser died on February 16, 2004. We dedicate this book to his memory.

July 2006

Catherine Goldstein
Norbert Schappacher
Joachim Schwermer

Table of Contents

Editions of Carl Friedrich Gauss's *Disquisitiones Arithmeticae*

The *Disquisitiones Arithmeticae* has been omitted from the list of references of the individual chapters: we list underneath its various editions. Throughout this book, passages from Gauss's *Disquisitiones Arithmeticae* are referred to only by the article number. The title of Gauss's work is routinely abbreviated as "D.A." For all works, a mention of [Author 1801a] refers to the item "Author. 1801a" in the bibliography, a mention of [Author 1801/1863] refers to the 1863 edition in this item.

1801. *Disquisitiones Arithmeticae.* Leipzig: Fleischer. Repr. Bruxelles: Culture et civilisation, 1968. Repr. Hildesheim: Olms, 2006. Rev. ed. in *Werke*, vol. 1, ed. Königliche Gesellschaft zu Göttingen [E. Schering]. Göttingen: Universitäts-Druckerei, 1863; 2nd rev. ed., 1870; repr. Hildesheim: Olms, 1973.

http://gallica.bnf.fr
http://dz-srv1.sub.uni-goettingen.de/cache/toc/D137206.html

1807. *Recherches arithmétiques.* French transl. A.-C.-M. Poullet-Delisle. Paris: Courcier. Repr. Sceaux: Gabay, 1989.

http://gallica.bnf.fr

1889. *Arithmetische Untersuchungen.* German transl. H. Maser. In *Untersuchungen über höhere Arithmetik*, pp. 1–453. Berlin: Springer. Repr. New York: Chelsea, 1965; 2nd ed., 1981.

http://dz-srv1.sub.uni-goettingen.de/cache/toc/D232699.html

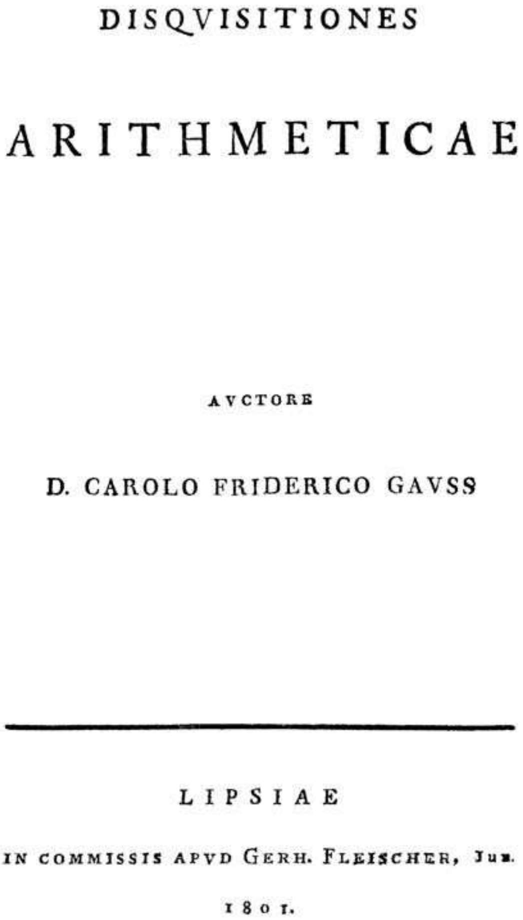
1959. *Arifmetičeskie issledovaniya.* Russian transl. V. B. Dem'yanov. In *Trudi po teorii čisel* [Works on number theory], ed. I. M. Vinogradov, B. N. Delone, pp. 7–583. Moscow: Academy of Sciences USSR.

1966. *Disquisitiones Arithmeticae.* English transl. A. A. Clarke. New Haven: Yale University Press. Rev. ed. W. C. Waterhouse. New York: Springer, 1986.

1995. *Disquisitiones Arithmeticae.* Spanish transl. H. Barrantes Campos, M. Josephy, A. Ruiz Zùñiga. Colección Enrique Pérez Arbelaez 10. Santa Fe de Bogotá: Academia Colombiana de Ciencias Exactas, Fisicas y Naturales.

1995. *Seisuu ron.* Japanese transl. Takase Masahito. Tokyo: Asakura-Shoten.

1996. *Disquisicions aritmètiques.* Catalan transl. G. Pascual Xufré. Barcelona: Institut d'Estudis Catalans, Societat Catalana de Matemàtiques.



DISQVISITIONES

ARITHMETICAE

AVCTORE

D. CAROLO FRIDERICO GAVSS

LIPSIAE

IN COMMISSIS APVD GERH. FLEISCHER, Iun.

1801.

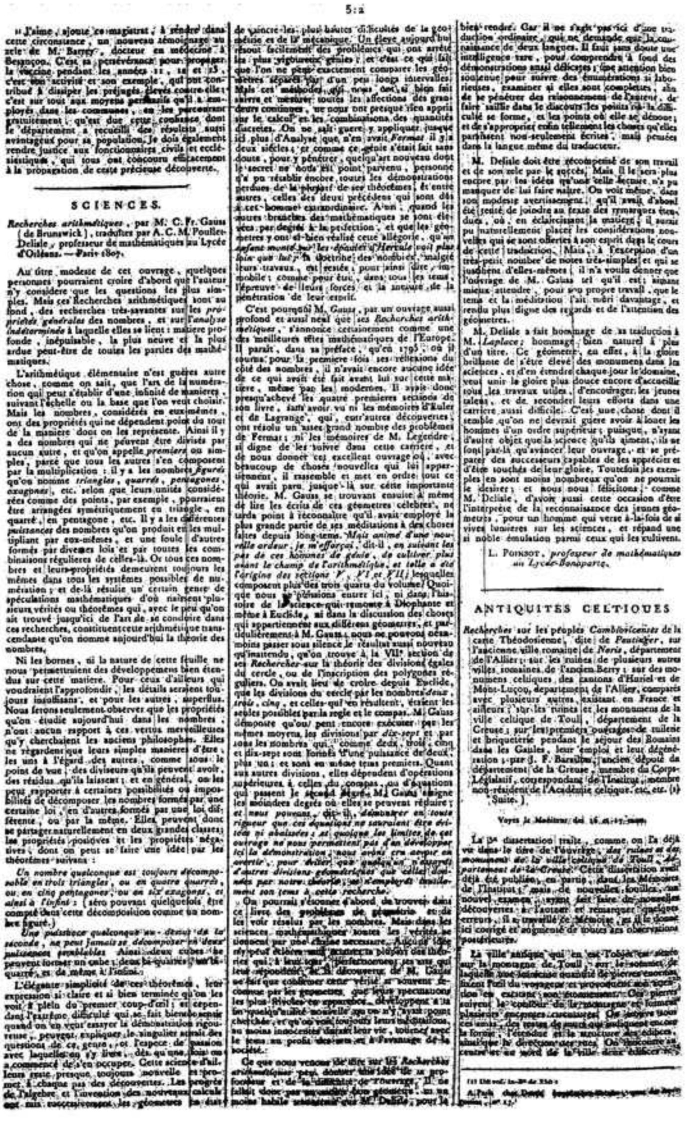
Fig. I. Title page of *Disquisitiones Arithmeticae*, 1801 edition
(Private copy)

Part I

A Book's History

Welche Wichtigkeit Gauß: *Disquisitiones Arithmeticae für die Entwicklung der Mathematik gehabt haben, darüber existiert wohl kein Zweifel. Es ist ein Werk, das ungefähr in der Mathematik dieselbe Stellung einnimmt, wie die Kritik der reinen Vernunft von* Kant *in der Philosophie.*

Carl Itzigsohn, March 23, 1885



» J'aime, ajoute ce magistrat, à rendre dans cette circonstance, un nouveau témoignage au zele de M. Barrey, docteur en médecine à Besançon. C'est sa persévérance pour propager la vaccine pendant les années 11, 12 et 13, c'est son activité et son exemple, qui ont contribué à dissiper les préjugés élevés contre elle; c'est sur tout aux moyens persuasifs qu'il a employés dans les communes, en les parcourant gratuitement, qu'est due cette confiance dont le département a recueilli des résultats aussi avantageux pour sa population. Je dois également rendre justice aux fonctionnaires civils et ecclésiastiques, qui tous ont concouru efficacement à la propagation de cette précieuse découverte.

SCIENCES.

Recherches arithmétiques, par M. C. Fr. Gauss (de Brunswick), traduites par A. C. M. Poullet-Delisle, professeur de mathématiques au Lycée d'Orléans. — Paris 1807.

Au titre modeste de cet ouvrage, quelques personnes pourraient croire d'abord que l'auteur n'y considere que les questions les plus simples. Mais ces Recherches arithmétiques sont au fond, des recherches très-savantes sur les *propriétés générales* des nombres, et sur l'*analyse indéterminée* à laquelle elles se lient : matiere profonde, inépuisable, la plus neuve et la plus ardue peut-être de toutes les parties des mathématiques.

L'arithmétique élémentaire n'est guères autre chose, comme on sait, que l'art de la numération qui peut s'établir d'une infinité de manieres, suivant l'échelle ou la base que l'on veut choisir. Mais les nombres, considérés en eux-mêmes, ont des propriétés qui ne dépendent point du tout de la maniere dont on les représente. Ainsi il y a des nombres qui ne peuvent être divisés par aucun autre, et qu'on appelle *premiers* ou simples, parce que tous les autres s'en composent par la multiplication : il y a les nombres *figurés* qu'on nomme *triangles*, *quarrés*, *pentagones*, *exagones*, etc. selon que leurs unités considérées comme des points, par exemple, pourraient être arrangées symétriquement en triangle, en quarré, en pentagone, etc. Il y a les différentes *puissances* des nombres qu'on produit en les multipliant par eux-mêmes, et une foule d'autres formés par diverses lois et par toutes les combinaisons régulieres de celles-là. Or tous ces nombres et leurs propriétés demeurent toujours les mêmes dans tous les systêmes possibles de numération; et de-là résulte un certain genre de spéculations mathématiques d'où naissent plusieurs vérités ou théorêmes qui, avec le peu qu'on ait trouvé jusqu'ici de l'art de se conduire dans ces recherches, constituent cette arithmétique transcendante qu'on nomme aujourd'hui la théorie des nombres.

Ni les bornes, ni la nature de cette feuille ne nous permettraient des développemens bien étendus sur cette matiere. Pour ceux d'ailleurs qui voudraient l'approfondir, les détails seraient toujours insuffisans, et pour les autres, superflus. Nous ferons seulement observer que les propriétés qu'on étudie aujourd'hui dans les nombres, n'ont aucun rapport à ces vertus merveilleuses qu'y cherchaient les anciens philosophes. Elles ne regardent que leurs simples manieres d'être, les uns à l'égard des autres, comme sous le point de vue des diviseurs qu'ils peuvent avoir, des résidus qu'ils laissent; et en général, on les peut rapporter à certaines possibilités ou impossibilités de décomposer les nombres formés par une certaine loi, en d'autres formés par une loi différente, ou par la même. Elles peuvent donc se partager naturellement en deux grandes classes; les propriétés positives et les propriétés négatives, dont on peut se faire une idée par les théorêmes suivans :

Un nombre quelconque est toujours décomposable en trois triangles, ou en quatre quarrés, ou en cinq pentagones, ou en six exagones, et ainsi à l'infini : (zéro pouvant quelquefois être compté dans cette décomposition comme un nombre figuré.)

Une puissance quelconque au-dessus de la seconde, ne peut jamais se décomposer en deux puissances semblables. Ainsi deux cubes ne peuvent former un cube; deux bi-quarrés, un bi-quarré, et de même à l'infini.

L'élégante simplicité de ces théorêmes, leur expression si claire et si bien terminée qu'on les voit à plein du premier coup-d'œil; et cependant l'extrême difficulté qui se fait bientôt sentir quand on en veut essayer la démonstration rigoureuse, peuvent expliquer le singulier attrait des questions de ce genre, et l'espece de passion avec laquelle on s'y livre, dès qu'une fois on a commencé de s'en occuper. Cette science d'ailleurs reste presque toujours nouvelle et promet, à chaque pas des découvertes. Les progrès de l'algebre, et l'invention des nouveaux calculs ont mis successivement les géomètres en état de vaincre les plus hautes difficultés de la géométrie et de la mécanique. Un éleve aujourd'hui résout facilement des problêmes qui ont arrêté les plus vigoureux génies; et c'est ce qui fait que l'on ne peut exactement comparer les géomètres séparés par d'un peu longs intervalles. Mais ces méthodes, qui nous ont si bien fait suivre et mesurer toutes les affections des grandeurs continues, ne nous ont presque rien appris sur le calcul et les combinaisons des quantités discretes. On ne sait guere y appliquer jusqu'ici plus d'Analyse que n'en avait *Fermat* il y a deux siècles; et comme ce génie s'était fait sans doute, pour y pénétrer, quelqu'art nouveau dont le secret ne nous est point parvenu, personne n'a pu rétablir encore toutes les démonstrations perdues de la plupart de ses théorêmes, et entre autres, celles des deux précédens qui sont dûs à cet homme extraordinaire. Ainsi, quand les autres branches des mathématiques se sont élevées par degrés à la perfection, et que les géomètres y ont si bien réalisé cette allégorie, qu'*un enfant monté sur les épaules d'Hercule voit plus loin que lui*; la doctrine des nombres, malgré leurs travaux, est restée, pour ainsi dire, immobile; comme pour être, dans tous les tems, l'épreuve de leurs forces et la mesure de la pénétration de leur esprit.

C'est pourquoi M. *Gauss*, par un ouvrage aussi profond et aussi neuf que ses *Recherches arithmétiques*, s'annonce certainement comme une des meilleures têtes mathématiques de l'Europe. Il paraît, dans sa préface, qu'en 1795, où il tourna pour la premiere fois ses réflexions du côté des nombres, il n'avait encore aucune idée de ce qui avait été fait avant lui sur cette matiere, même par les modernes. Il avait donc presqu'achevé les quatre premieres sections de son livre, sans avoir vu ni les mémoires d'Euler et de Lagrange, qui, entr'autres découvertes, ont résolu un assez grand nombre des problêmes de Fermat; ni les mémoires de M. Legendre, si digne de les suivre dans cette carriere, et de nous donner cet excellent ouvrage où, avec beaucoup de choses nouvelles qui lui appartiennent, il rassemble et met en ordre tout ce qui avait paru jusque-là sur cette importante théorie. M. Gauss se trouvant ensuite à même de lire les écrits de ces géomètres célèbres, ne tarda point à reconnaître qu'il avait employé la plus grande partie de ses méditations à des choses faites depuis long-tems. *Mais animé d'une nouvelle ardeur, je m'efforçai*, dit-il, *en suivant les pas de ces hommes de génie, de cultiver plus avant le champ de l'arithmétique, et telle a été l'origine des sections V, VI et VII*; lesquelles composent plus des trois quarts du volume. Quoique nous ne puissions entrer ici, ni dans l'histoire de la science qui remonte à Diophante et même à Euclide, ni dans la discussion des choses qui appartiennent aux différens géomètres, et particulièrement à M. Gauss; nous ne pourons néanmoins passer sous silence le résultat aussi nouveau qu'inattendu, qu'on trouve à la VII^e section de ses *Recherches* sur la théorie des divisions égales du cercle, ou de l'inscription des polygones réguliers. On avait lieu de croire depuis Euclide, que les divisions du cercle par les nombres *deux*, *trois*, *cinq*, et celles qui en résultent, étaient les seules possibles par la regle et le compas. M. Gauss démontre qu'on peut encore exécuter par les mêmes moyens, les divisions par *dix-sept* et par tous les nombres qui, comme deux, trois, cinq et dix-sept sont formés d'une puissance de deux, plus un; et sont en même tems premiers. Quant aux autres divisions, elles dépendent d'opérations supérieures à celles du compas, ou d'équations qui passent le second degré. M. Gauss assigne les moindres degrés où elles se peuvent réduire; *et nous pouvons*, dit-il, *démontrer en toute rigueur que ces équations ne sauraient être divisées ni abaissées; et quoique les limites de cet ouvrage ne nous permettent pas d'en développer ici la démonstration, nous avons cru devoir en avertir, pour éviter que quelqu'un n'essayât d'autres divisions géométriques que celles données par notre théorie, ou n'employât inutilement son tems à cette recherche.*

» On pourrait s'étonner d'abord de trouver dans ce livre des problêmes de géométrie et de les voir résolus par les nombres. Mais dans les sciences mathématiques toutes les vérités se tiennent par une chaîne nécessaire. Aucune idée n'y peut éclore sans [illegible] la plupart des théories qui, à leur tour, perfectionnent les arts qui leur répondent. Et la découverte de M. Gauss ne fait que confirmer cette vérité si souvent reconnue par les géomètres, que leurs spéculations les plus frivoles en apparence, développent à la fin quelqu'utilité nouvelle qu'on n'y avait point cherchée, et qu'on voit toujours leurs méditations, au moins innocentes durant leur vie, tourner avec le tems au profit des arts et à l'avantage de la société.

Ce que nous venons de dire sur les *Recherches arithmétiques* peut donner une idée de sa profondeur et de la difficulté de l'ouvrage. Il ne fallait donc pas un [illegible] géomètre, ou au moins habile [illegible] que M. Delisle, pour la bien rendre. Car il ne s'agit pas ici d'une traduction ordinaire, qui ne demande que la connaissance de deux langues. Il faut sans doute une intelligence rare, pour comprendre à fond des démonstrations aussi délicates; une attention bien soutenue pour suivre des énumérations si laborieuses, examiner si elles sont complettes, afin de se pénétrer des raisonnemens de l'auteur, de faire saillir dans le discours les points où la difficulté se forme, et les points où elle se dénoue; et de s'approprier enfin tellement les choses qu'elles paraissent non-seulement écrites, mais pensées dans la langue même du traducteur.

M. Delisle doit être récompensé de son travail et de son zele par le succès. Mais il le sera plus encore par les idées qu'une telle lecture n'a pu manquer de lui faire naître. On voit même, dans son modeste avertissement, qu'il avait d'abord été tenté de joindre au texte des remarques étendues, où, en éclaircissant la matiere, il aurait pu naturellement placer les considérations nouvelles qui se sont offertes à son esprit dans le cours de cette traduction. Mais, à l'exception d'un très-petit nombre de notes très-simples et qui se justifient d'elles-mêmes, il n'a voulu donner que l'ouvrage de M. Gauss tel qu'il est; aimant mieux attendre, pour son propre travail, que le tems et la méditation l'ait mûri davantage, et rendu plus digne des regards et de l'attention des géomètres.

M. Delisle a fait hommage de sa traduction à M. *Laplace*; hommage bien naturel à plus d'un titre. Ce géomètre, en effet, à la gloire brillante de s'être élevé des monumens dans les sciences, et d'en étendre chaque jour le domaine, veut unir la gloire plus douce encore d'accueillir tous les travaux utiles, d'encourager les jeunes talens, et de seconder leurs efforts dans une carriere aussi difficile. C'est une chose dont il semble qu'on ne devrait guere avoir à louer les hommes d'un ordre supérieur; puisque, n'ayant d'autre objet que la science qu'ils aiment, ils ne font par-là qu'avancer leur ouvrage, et se préparer des successeurs capables de les apprécier et d'être touchés de leur gloire. Toutefois les exemples en sont moins nombreux qu'on ne pourrait le desirer; et nous nous félicitons, comme M. Delisle, d'avoir aussi cette occasion d'être l'interprête de la reconnaissance des jeunes géomètres, pour un homme qui verse à-la-fois de si vives lumieres sur les sciences, et répand une si noble émulation parmi ceux qui les cultivent.

L. Poinsot, *professeur de mathématiques au Lycée-Bonaparte.*

ANTIQUITES CELTIQUES

Recherches sur les peuples *Cambiovicenses* de la carte Théodosienne, dite de *Peutinger*, sur l'ancienne ville romaine de *Neris*, département de l'Allier; sur les ruines de plusieurs autres villes romaines de l'ancien Berry; sur des monumens celtiques des cantons d'Huriel et de Mont-Luçon, département de l'Allier, comparés avec plusieurs autres, existant en France et ailleurs; sur les ruines et les monumens de la ville celtique de Toull, département de la Creuse; sur les premiers ouvrages de tuilerie et briqueterie pendant le séjour des Romains dans les Gaules, leur emploi et leur dégénération; par J. F. Baraillon, ancien député du département de la Creuse, membre du Corps-Législatif, correspondant de l'Institut, membre non-résident de l'Académie celtique, etc. etc. (1) (Suite.)

Voyez le Moniteur des 16 et 17 mars.

La 3^e dissertation traite, comme on l'a déjà vu dans le titre de l'ouvrage, *des ruines et des monumens de la ville celtique de Toull, département de la Creuse*. Cette dissertation avait déjà été publiée, en partie, dans les Mémoires de l'Institut; mais de nouvelles fouilles, un nouvel examen, ayant fait faire de nouvelles découvertes à l'auteur et remarquer quelques erreurs, il a travaillé ce Mémoire, et il le donne ici corrigé et augmenté de toutes ses observations postérieures.

La ville antique qui en est l'objet est située sur la montagne de Toull, sur le sommet de laquelle une immense quantité de pierres énormes fixent l'œil du voyageur et provoquent son attention en excitant son étonnement. Ces pierres suivent le contour de la montagne et forment plusieurs enceintes circulaires. On trouve sous ces amas, des restes de murs qui indiquent encore la forme, l'étendue et la structure des édifices, ainsi que la direction des rues. On rencontre au centre et au nord de la ville deux édifices [illegible]

(1) Un vol. in-8° de 350 p.
A Paris, chez Dentu, imprimeur-libraire, quai des Augustins, n° 17.

Fig. I.1. A newspaper review of the *Disquisitiones Arithmeticae*
Gazette nationale, ou le Moniteur universel, March 21, 1807

I.1

A Book in Search of a Discipline (1801–1860)

Catherine Goldstein and Norbert Schappacher

Carl Friedrich Gauss's *Disquisitiones Arithmeticae* of 1801 has more than one claim to glory: the contrast between the importance of the book and the youth of its author; the innovative concepts, notations, and results presented therein; the length and subtlety of some of its proofs; and its role in shaping number theory into a distinguished mathematical discipline.

The awe that it inspired in mathematicians was displayed to the cultured public of the *Moniteur universel ou Gazette nationale*[1] as early as March 21, 1807, when Louis Poinsot, who would succeed Joseph-Louis Lagrange at the Academy of Sciences six years later, contributed a full page article about the French translation of the *Disquisitiones Arithmeticae*:

> The doctrine of numbers, in spite of [the works of previous mathematicians] has remained, so to speak, immobile, as if it were to stay for ever the touchstone of their powers and the measure of their intellectual penetration. This is why a treatise as profound and as novel as his *Arithmetical Investigations* heralds M. Gauss as one of the best mathematical minds in Europe.[2]

[1] This French newspaper, created by Charles-Joseph Panckoucke in the first months of the French Revolution, had the goal of informing its readers of administrative, political, and cultural events and of promoting French achievements. It opened its columns regularly to reviews of books recommended by the *Institut national des sciences et des arts.*

[2] *Gazette nationale ou Le Moniteur universel* 80 (1807), 312: *La doctrine des nombres malgré leurs travaux [antérieurs] est restée, pour ainsi dire, immobile ; comme pour être dans tous les tems, l'épreuve de leurs forces et la mesure de la pénétration de leur esprit. C'est pourquoi Monsieur Gauss, par un ouvrage aussi profond et aussi neuf que ses* Recherches arithmétiques *s'annonce certainement comme une des meilleures têtes mathématiques de l'Europe.*

A long string of declarations left by readers of the book, from Niels Henrik Abel to Hermann Minkowski, from Augustin-Louis Cauchy to Henry Smith, bears witness to the profit they derived from it. During the XIX$^{\text{th}}$ century, its fame grew to almost mythical dimensions. In 1891, Edouard Lucas referred to the *Disquisitiones Arithmeticae* as an "imperishable monument [which] unveils the vast expanse and stunning depth of the human mind,"[3] and in his Berlin lecture course on the concept of number, Leopold Kronecker called it "the Book of all Books."[4] In the process, new ways of seeing the *Disquisitiones* came to the fore; they figure for instance in the presentation given by John Theodore Merz in his celebrated four-volume *History of European Thought in the Nineteenth Century*:

> Germany … was already an important power in the Republic of exact science which then had its centre in Paris. Just at the beginning of the nineteenth century two events happened which foreboded for the highest branches of the mathematical sciences a revival of the glory which in this department Kepler and Leibniz had already given to their country. … The *first* was the publication of the 'Disquisitiones Arithmeticae' in Latin in 1801.[5] … [Gauss] raised this part of mathematics into an independent science of which the 'Disquisitiones Arithmeticae' is the first elaborate and systematic treatise.… It was … through Jacobi, and still more through his contemporary Lejeune-Dirichlet … that the great work of Gauss on the theory of numbers, which for twenty years had remained sealed with seven seals, was drawn into current mathematical literature… The seals were only gradually broken. Lejeune-Dirichlet did much in this way, others followed, notably Prof. Dedekind, who published the lectures of Dirichlet and added much of his own.[6]

Gauss's book (hereafter, we shall often use the abbreviation "the D.A." to designate it) is now seen as having created number theory as a systematic discipline in its own right, with the book, as well as the new discipline, represented as a landmark of German culture. Moreover, a standard history of the book has been elaborated. It stresses the impenetrability of the D.A. at the time of its appearance and integrates it into a sweeping narrative, setting out a continuous unfolding of the book's content, from Johann Peter Gustav Lejeune-Dirichlet and Carl Gustav Jacob Jacobi on.

In this history modern algebraic number theory appears as the natural outgrowth of the discipline founded by the *Disquisitiones Arithmeticae*. Historical studies have accordingly focused on the emergence of this branch of number theory, in particular on the works of Dirichlet, Ernst Eduard Kummer, Richard Dedekind, Leopold Kronecker, and on the specific thread linking the D.A. to the masterpiece of algebraic number theory, David Hilbert's *Zahlbericht* of 1897. In addition, they have also explored the fate of specific theorems or methods of the D.A. which are relevant for number theorists today.

Yet a full understanding of the impact of the *Disquisitiones Arithmeticae*, at

[3] [Lucas 1891], p. vi: *Ce livre, monument impérissable dévoile l'immense étendue, l'étonnante profondeur de la pensée humaine.*

[4] [Kronecker 1891/2001], p. 219: *das Buch aller Bücher.*

[5] The second event alluded to by Merz is the computation of Ceres's orbit, also by Gauss.

[6] [Merz 1896–1914], vol. I, pp. 181, 181–182 (footnote), 187–188 and 721.

all levels, requires more than just a "thicker description"[7] of such milestones; it requires that light be shed on other patterns of development, other readers, other mathematical uses of the book – it requires a change in our questionnaire. We need to answer specific questions, such as: What happened to the book outside Germany? What were the particularities, if any, of its reception in Germany? Which parts of it were read and reworked? And when? Which developments, in which domains, did it stimulate – or hamper? What role did it play in later attempts to found mathematics on arithmetic?

Such questions suggest narrower foci, which will be adopted in the various chapters of the present volume. In this first part, however, we take advantage of the concrete nature of our object of inquiry – a book – to draw a general map of its tracks while sticking closely to the chronology. That is to say, instead of going backwards, seeking in the *Disquisitiones Arithmeticae* hints and origins of more recent priorities, we will proceed forwards, following Gauss's text through time with the objective of surveying and periodizing afresh its manifold effects.[8]

But let us start, first, at the beginning of all beginnings…

1. The Writing and the Architecture of the *Disquisitiones Arithmeticae*

Gauss began to investigate arithmetical questions, at least empirically, as early as 1792, and to prepare a number-theoretical treatise in 1796 (i.e., at age 19 and, if we understand his mathematical diary correctly, soon after he had proved both the constructibility of the 17-gon by ruler and compass and the quadratic reciprocity law). An early version of the treatise was completed a year later.[9] In November 1797, Gauss started rewriting the early version into the more mature text which he would give to the printer bit by bit. Printing started in April 1798, but proceeded very slowly for technical reasons on the part of the printer. Gauss resented this very much, as his letters show; he was looking for a permanent position from 1798. But he did use the delays to add new text, in particular to sec. 5 on quadratic forms, which had roughly doubled in length by the time the book finally appeared in the summer of 1801.[10]

[7] The reference is to Gilbert Ryle and Clifford Geertz, in particular [Geertz 1973].

[8] We have systematically tracked mentions of the D.A. in the main nineteenth-century journals, and then in the complete works – if published – of the mathematicians encountered. For want of space (in the text or in the margin …), only part of the evidence used to establish our main claims can be presented here.

[9] Parts of the manuscript, known as *Analysis residuorum*, were published posthumously in Gauss's *Werke*; other parts were identified as such in 1980 by Uta Merzbach in different German archives; see [Merzbach 1981], also for a global comparison of the early version with the printed book; for detailed comparisons of specific parts, in particular sec. 2, see [Bullynck 2006a] and [Bullynck 2006b], appendices A and B. See also [Schlesinger 1922], sec. III.

[10] Basic data on the genesis of the *Disquisitiones* can be derived from Gauss's mathematical diary, [Gauss 1796–1814], and from his correspondence. Our quick summary here is based on [Merzbach 1981]. What exactly Gauss found in his predecessors and how he was influenced by them remains a difficult question, in spite of his own historical

1.1. The First Sections: Congruences to the Fore

Let us skim through the contents of the *Disquisitiones Arithmeticae* as they appeared in 1801.[11] Although it may make somewhat tedious reading, we think it useful to indicate the full variety of matters treated by Gauss. The 665 pages and 355 articles of the main text are divided unevenly into seven sections. The first and smallest one (7 pp., 12 arts.) establishes a new notion and notation which, despite its elementary nature, modified the practice of number theory:

> If the number a measures[12] the difference of the numbers b, c, then b and c are said to be *congruent according to* a; if not, *incongruent*; this a we call the *modulus.* Each of the numbers b, c are called a *residue* of the other in the first case, a *nonresidue* in the second.[13]

The corresponding notation $b \equiv c \pmod{a}$ is introduced in art. 2. The remainder of sec. 1 contains basic observations on convenient sets of residues modulo a and on the compatibility of congruences with the arithmetic operations. To consider numbers or equations up to a given integer was not new with Gauss.[14] His innovation was to turn this occasional computational device into a topic in its own right.

Section 2 (33 pp., 32 arts.) opens with several theorems on integers including the unique prime factorization of integers (in art. 16), and then treats linear congruences in arts. 29–37, including the Euclidean algorithm and what we call the Chinese remainder theorem. At the end of sec. 2, Gauss added a few results for future reference which had not figured in the 1797 manuscript, among them: (i) properties

remarks. We do not go into it here, referring for a first orientation and survey of Gauss's obvious predecessors, in particular Euler, Lagrange and Legendre, to [Weil 1984]; the less-expected tradition of German arithmetical textbooks and the more general impact of Lambert's and Hindenburg's works are explored in the original thesis of Maarten Bullynck, [Bullynck 2006b].

[11] The reader is invited to go back and forth between our rough summary and Gauss's original detailed table of contents which we reproduce on the double page 10–11. In the present section, expressions in quotation marks, with no explicit reference attached, are the English translations of key words from this Latin table of contents. The table is copied from the 1801 edition of the D.A. except that, for the sake of readability, we have modified the letters "u" and "v" according to current Latin spelling. Other surveys of the book are proposed in [Bachmann 1911], [Rieger 1957], [Neumann 1979–1980], [Bühler 1981], chap. 3, [Neumann 2005].

[12] Along with this classical Euclidean term "to measure" (*metiri*), which, as well as "modulus" (small measure), reminds us of the additive flavour of Euclidean division, Gauss also used "to divide" (*dividere*) as of sec. 2, art. 13, in the context of a product of natural integers. This diversity of expressions was not always maintained in translations.

[13] Our translation of the opening paragraph of D.A., art. 1: *Si numerus a numerorum b, c differentiam metitur, b et c* secundum *a* congrui *dicuntur, sin minus,* incongrui*: ipsum a* modulum *appellamus. Uterque numerorum b, c, priori in casu alterius* residuum*, in posteriori vero* nonresiduum *vocatur.*

[14] Gauss acknowledged this fact in the footnote to art. 2, noticing that Legendre had used a simple equality in such situations, and pleading at the same time for his own, unequivocal notation. Other authors are discussed in [Bullynck 2006b], appendix A.

of the number $\varphi(A)$ of prime residues modulo A (arts. 38–39); (ii) in art. 42, a proof that the product of two polynomials with leading coefficient 1 and with rational coefficients that are not all integers cannot have all its coefficients integers;[15] and (iii) in arts. 43 and 44, a proof of Lagrange's result that a polynomial congruence modulo a prime cannot have more zeros than its degree.[16]

Section 3 (51 pp., 49 arts.) is entitled "On power residues." As Gauss put it, it treats "geometric progressions" $1, a, a^2, a^3, \ldots$ modulo a prime number p (for a number a not divisible by p), discusses the "period" of a modulo p and Fermat's theorem, contains two proofs for the existence of "primitive roots" modulo p, and promotes the use of the "indices" of $1, \ldots, p-1$ modulo p with respect to a fixed primitive root, in analogy with logarithm tables.[17] After a discussion, in arts. 61–68, of n^{th} roots mod p from the point of view of effective computations, the text returns to calculations with respect to a fixed primitive root, and gives in particular in arts. 75–78 two proofs – and sketches a third one due to Lagrange – of Wilson's theorem, $1 \cdot 2 \cdots (p-1) \equiv -1 \pmod{p}$. The analogous constructions and results for an odd prime power are discussed in arts. 82–89, the exceptional case of the powers of $p = 2$ in arts. 90–91. Finally, integers n for which there exists a primitive root modulo n are characterized in art. 92.

Section 4 (73 pp., 59 arts.), "On congruences of degree 2," develops a systematic theory of "quadratic residues" (i.e., residues of perfect squares). It culminates in the "fundamental theorem" of this theory, from which "can be deduced almost everything that can be said about quadratic residues,"[18] and which Gauss stated as:

> If p is a prime number of the form $4n+1$, then $+p$, if p is of the form $4n+3$, then $-p$, will be a [quadratic] residue, resp. nonresidue, of any prime number which, taken positively, is a residue, resp. nonresidue of p.[19]

Gauss motivated this *quadratic reciprocity law* experimentally, gave the general statement and formalized it in tables of possible cases (arts. 131 and 132), using the notation aRa', resp. aNa', to mean that a is a quadratic residue, resp. nonresidue, modulo a'.[20] He also gave here the first proof of the law, an elementary one by

[15] This is one of several results known today as "Gauss's lemma."

[16] See [Bullynck 2006a], for a closer study of sec. 2 in comparison to Gauss's earlier manuscript of the D.A.

[17] In modern terms, the period is the order of the element a in the multiplicative group $(\mathbf{Z}/p\mathbf{Z})^*$, Fermat's theorem states that this order divides $p-1$, a primitive root is a generator of the group and the index of an element is the corresponding exponent with respect to the chosen generator.

[18] D.A., art. 131: ... *omnia fere quae de residuis quadraticis dici possunt, huic theoremati innituntur.*

[19] Our translation of D.A., art. 131: *Si p est numerus primus formae* $4n+1$, *erit* $+p$, *si vero p formae* $4n+3$, *erit* $-p$ *residuum vel non residuum cuiusuis numeri primi qui positive acceptus ipsius p est residuum vel non residuum.* The supplementary theorems about the quadratic residue behaviour of -1 and 2 are treated in parallel.

[20] Today one usually sees this quadratic reciprocity law written in terms of Legendre's symbol. It is defined, for any integer a and p a prime number not dividing a, by

induction.[21] A crucial nontrivial ingredient (used in art. 139) is a special case of a theorem stated in art. 125, to the effect that, for every integer which is not a perfect square, there are prime numbers modulo which it is a quadratic nonresidue.[22]

1.2. Quadratic Forms

The focus changes in sec. 5 of the D.A., which treats "forms and indeterminate equations of the second degree," mostly binary forms, in part also ternary. With its 357 pp. and 156 arts., this section occupies more than half of the whole *Disquisitiones Arithmeticae*. Leonhard Euler, Joseph-Louis Lagrange, and Adrien-Marie Legendre had forged tools to study the representation of integers by quadratic forms. Gauss, however, moved away from this Diophantine aspect towards a treatment of quadratic forms as objects in their own right, and, as he had done for congruences, explicitly pinpointed and *named* the key tools. This move is evident already in the opening of sec. 5:

> The form $axx + 2bxy + cyy$,[23] when the indeterminates x, y are not at stake, we will write like this, (a, b, c).[24]

Gauss then immediately singled out the quantity $bb - ac$ which he called the "determinant"[25] – "on the nature of which, as we will show in the sequel, the prop-

$\left(\frac{a}{p}\right) = \pm 1 \equiv a^{\frac{p-1}{2}}$ (mod p), that is, 1 if a is quadratic residue modulo p, -1 if not; see [Legendre 1788], p. 186, and D.A., art. 106, for the last congruence. Given distinct odd prime numbers p, q, the quadratic reciprocity law then says that $\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}\left(\frac{q}{p}\right)$. Notwithstanding Dirichlet's criticism (published after Gauss's death) of the D.A. as lacking a notational calculus for quadratic residues, [Dirichlet 1889–1897], vol. 2, p. 123, one may point out that Gauss's formulation stresses the normalization of $\pm p$, a phenomenon that would recur with higher reciprocity laws; see [Neumann 2005], p. 308.

[21] In the late 1960s, John Tate "lifted directly from the argument which was used by Gauss in his first proof of the quadratic reciprocity law" his determination of the second K-group of the field of rational numbers $K_2(\mathbf{Q})$; see [Milnor 1971], p. 102. More generally, Gauss's argument is seen to provide an inductive procedure to determine successively the local factors at all primes p of a given Steinberg symbol on $\mathbf{Q}^* \times \mathbf{Q}^*$, and the decomposition of the universal continuous Steinberg symbol with values in $\{\pm 1\}$ is tantamount to the reciprocity law. See [Milnor 1971], p. 101–107; cf. [Tate 1971], § 3.

[22] This follows easily from the reciprocity law; Gauss does not even bother to give the details. The difficulty is to prove it *directly* (arts. 125–129) in a special case which then makes the proof by complete induction of the reciprocity law work: that every $\pm p$, for a prime p of the form $4n + 1$, is a quadratic nonresidue modulo some prime $q < p$.

[23] Gauss's convention that the coefficient of the mixed term be even is original and its advantages and drawbacks have been much in debate; see J. Schwermer's chap. VIII.1.

[24] D.A., art. 153: *Formam $axx + 2bxy + cyy$, quando de indeterminatis x, y non agitur, ita designabimus* (a, b, c). In [Kronecker 1891/2001], p. 235, this move is heralded as the first time in history that a system of three discrete quantities was introduced.

[25] Nowadays called, sometimes up to a constant, the *discriminant* of the form. For the various normalizations and names of this quantity in the XIX$^{\text{th}}$ century, see [Dickson 1919–1923], vol. 3, p. 2. We will usually employ Gauss's word in this chapter.

erties of the form chiefly depend"[26] – showing that it is a quadratic residue of any integer primitively represented[27] by the form (art. 154).

The first part of sec. 5 (arts. 153–222, 146 pp.) is devoted to a vast enterprise of a finer classification of the forms of given determinant, to which the problem of representing numbers by forms is reduced. Gauss defined two quadratic forms (art. 158) to be equivalent if they are transformed into one another under substitutions of the indeterminates, changing (x, y) into $(\alpha x + \beta y, \gamma x + \delta y)$, for integral coefficients $\alpha, \beta, \gamma, \delta$, with $\alpha\delta - \beta\gamma = +1$ or $= -1$.[28] Two equivalent forms represent the same numbers. If $\alpha\delta - \beta\gamma = +1$, the equivalence is said to be "proper," if $\alpha\delta - \beta\gamma = -1$, "improper." While integral invertible substitutions were already used by Lagrange, this finer distinction is due to Gauss and greatly exploited by him. After generalities relating to these notions and to the representation of numbers by forms – in particular (art. 162), the link between the problem of finding *all* transformations between two, say, properly equivalent forms, when one is known, and the solutions of the equation $t^2 - Du^2 = m^2$, where D is the determinant of the forms and m the greatest common divisor of their coefficients – the discussion then splits into two very different cases according to whether the determinant is negative or positive. In each case, Gauss showed that any given form is properly equivalent to a so-called "reduced" form (art. 171 for negative, art. 183 for positive discriminants), not necessarily unique, characterized by inequalities imposed on the coefficients.[29] The number of reduced forms – and thus also the number of equivalence classes of forms – of a given determinant is finite. Equivalence *among reduced forms* is studied – in particular, the distribution of the reduced forms of given positive determinant into "periods" of equivalent reduced forms, art. 185 – and a general procedure is given to determine if two binary quadratic forms with the same determinant are (properly or improperly) equivalent and to find all transformations between them. Using this, Gauss settled the general problem of representing integers by quadratic forms (arts. 180–181, 205, 212), as well as the resolution in integers of quadratic equations with two unknowns and integral coefficients (art. 216). The first half of sec. 5 closes with a brief historical reminder (art. 222).

The classification of forms also ushers the reader into the second half of sec. 5, entitled "further investigations on forms." Art. 223 fixes an algorithm to find a good representative for every (proper equivalence) class of quadratic forms of a given determinant. Representing classes by reduced forms avoids working with the infinite classes abstractly, just as Gauss never worked with our field $\mathbf{Z}/p\mathbf{Z}$, the elements of which are infinite sets of integers, but with conveniently chosen residues modulo p.

[26] D.A., art. 154: *Numerum bb − ac, a cuius indole proprietates formae* (a, b, c) *imprimis pendere, in sequentibus docebimus,* determinantem *huius formae vocabimus.*

[27] I.e., which can be written as $axx + 2bxy + cyy$, for two *coprime* integers x and y.

[28] Gauss also handled the general case of arbitrary substitutions with integral coefficients transforming a form into another one which is then said to be "contained" in the first.

[29] A reduced form (A, B, C) of determinant $D < 0$ is such that $A \leq 2\sqrt{-D/3}$, $B \leq A/2$, $C \geq A$. A reduced form of determinant $D > 0$ is such that $0 \leq B < \sqrt{D}$, $\sqrt{D} - B \leq |A| \leq \sqrt{D} + B$.

Original Table of Contents of the *Disquisitiones Arithmeticae*

Dedicatio. Praefatio.

Sectio prima. De numerorum congruentia in genere.

Numeri congrui, moduli, residua et non residua, art. 1 sq. Residua minima, 4. Propositiones elementares de congruis, 5. Quaedam applicationes, 12.

Sectio secunda. De congruentiis primi gradus.

Theoremata praeliminaria de numeris primis, factoribus etc. 13. Solutio congruentiarum primi gradus, 26. De inveniendo numero secundum modulos datos residuis datis congruo 32. Congruentiae lineares quae plures incognitas implicant 37. Theoremata varia 38.

Sectio tertia. De residuis potestatum.

Residua terminorum progressionis geometricae ab unitate incipientis constituunt seriem periodicam, 45. *Considerantur primo moduli qui sunt numeri primi.* Ponendo modulum $= p$, multitudo terminorum in periodo metitur numerum $p - 1$ art. 49. Fermatii theorema, 50. Quot numeris respondeant periodi, in quibus terminorum multitudo est divisor datus numeri $p - 1$ art. 52. Radices primitivae, bases, indices, 57. Algorithmus indicum, 58. De radicibus congruentiae $x^n \equiv A$, art. 60. Nexus indicum in systematibus diversis, 69. Bases usibus peculiaribus accommodatae, 72. Methodus radices primitivas assignandi, 73. Theoremata varia de periodis et radicibus primitivis, 75. (Theorema Wilsonianum, 76). *De modulis qui sunt numerorum primorum potestates, 82. Moduli qui sunt potestates binarii, 90. Moduli e pluribus primis compositi, 92.*

Sectio quarta. De congruentiis secundi gradus.

Residua et nonresidua quadratica art. 94. Quoties modulus est numerus primus, multitudo residuorum ipso minorum multitudini nonresiduorum aequalis, 96. Quaestio, utrum numerus compositus residuum numeri primi dati sit an nonresiduum, ab indole factorum pendet, 98. De modulis, qui sunt numeri compositi, 100. Criterium generale, utrum numerus datus numeri primi dati residuum sit an nonresiduum, 106. *Disquisitiones de numeris primis quorum residua aut non residua sint numeri dati* 107 sqq. Residuum -1 art. 108. Residua $+2$ et -2, art. 112. Residua $+3$ et -3, art. 117. Residua $+5$ et -5 art. 121. De ±7 art. 124. Praeparatio ad disquisitionem generalem, 125. Per inductionem theorema generale (*fundamentale*) stabilitur, conclusionesque inde deducuntur 130. Demonstratio rigorosa huius theorematis, 135. Methodus analoga, theorema art. 114 demonstrandi, 145. Solutio problematis generalis 146. De formis linearibus omnes numeros primos continentibus, quorum vel residuum vel non residuum est numerus quicunque datus 147. De aliorum laboribus circa has investigationes 151. De congruentiis secundi gradus non puris 152.

Sectio quinta. De formis aequationibusque indeterminatis secundi gradus.

Disquisitionis propositum; formarum definitio et signum 153. Numerorum repraesentatio; determinans 154. Valores expr. $\sqrt{(bb - ac)}$ (mod. M) ad quos repraesentatio numeri M per formam (a, b, c) pertinet, 155. Forma aliam implicans, sive sub alia contenta; transformatio, propria et impropria, 157. Aequivalentia, propria et impropria 158. Formae oppositae 159, contiguae 160. Divisores communes coëfficientium formarum 161. Nexus omnium transformationum similium formae datae in formam datam 162. Formae ancipites 163. Theorema circa casum ubi forma sub alia simul proprie et improprie contenta est 164. Generalia de repraesentationibus numerorum per formas, earumque nexu cum transformationibus 166. *De formis determinantis negativi* 171. Applicationes speciales ad discerptionem numerorum in quadrata duo, in quadratum simplex et duplex, in simplex et triplex 182. *De formis determinantis positivi non-quadrati* 183. *De formis determinantis quadrati* 206. Formae sub aliis contentae quibus tamen non aequivalent 213. *Formae determinantis* 0 art. 215. Solutio generalis omnium aequationum indeterminatarum secundi gradus duas incognitas implicantium per numeros integros 216. Annotationes historicae 222.

Disquisitiones ulteriores de formis. Distributio formarum determinantis dati in classes 223; classium in ordines 226. Ordinum partitio in genera 228. *De compositione formarum* 238. Compositio ordinum 245, generum 246, classium 249. Pro determinante dato in singulis generibus eiusdem ordinis classes aeque multae continentur 252. Comparantur multitudines classium in singulis generibus ordinum diversorum contentarum 253. De multitudine classium ancipitum 257. Certe semissi omnium characterum pro determinante dato assignabilium genera proprie primitiva (positiva pro det. neg.) respondere nequeunt 261. Theorematis fundamentalis et reliquorum theorematum ad residua -1, $+2$, -2 pertinentium demonstratio secunda 262. Ea characterum semissis, quibus genera respondere nequeunt, propius determinantur 263. Methodus peculiaris, numeros primos in duo quadrata decomponendi 265. Digressio continens tractatum de formis ternariis 266 sqq. *Quaedam applicationes ad theoriam formarum binariarum.* De invenienda forma e cuius duplicatione forma binaria data generis principalis oriatur 286. Omnibus characteribus, praeter eos, qui in artt. 262, 263 impossibiles inventi sunt, genera revera respondent 287, III. Theoria decompositionis tum numerorum tum formarum binariarum in tria quadrata 288. Demonstratio theorematum Fermatianorum, quemvis integrum in tres numeros trigonales vel quatuor quadrata discerpi posse 293. Solutio aequationis $axx + byy + czz = 0$ art. 294. De methodo per quam ill. Le Gendre theorema fundamentale tractavit 296. Repraesentatio cifrae per formas ternarias quascunque 299. Solutio generalis aequationum indeterminatarum secundi gradus duas incognitas implicantium per quantitates rationales 300. De multitudine mediocri generum 301, classium 302. Algorithmus singularis classium proprie primitivarum; determinantes regulares et irregulares etc. art. 305.

Sectio sexta. Variae applicationes disquisitionum praecedentium.

Resolutio fractionum in simpliciores 309. Conversio fractionum communium in decimales 312. Solutio congruentiae $xx \equiv A$ per methodum exclusionis 319. Solutio aequationis indeterminatae $mxx + nyy = A$ per exclusiones 323. Alia methodus congruentiam $xx \equiv A$ solvendi pro eo casu ubi A est negativus 327. Duae methodi, numeros compositos a primis dignoscendi, illorumque factores investigandi, 329.

Sectio septima. De aequationibus, circuli sectiones definientibus.

Disquisitio reducitur ad casum simplicissimum, ubi multitudo partium, in quas circulum secare oportet, est numerus primus 336. Aequationes pro functionibus trigonometricis arcuum qui sunt pars aut partes totius peripheriae; reductio functionum trigonometricarum ad radices aequationis $x^n - 1 = 0$ art. 337. *Theoria radicum huius aequationis* (ubi supponitur, n esse numerum primum). Omittendo radicem 1, reliquae (Ω) continentur in aequatione $X = x^{n-1} + x^{n-2} + \text{etc.} + x + 1 = 0$. Functio X resolvi nequit in factores inferiores, in quibus omnes coëfficientes sint rationales 341. Propositum disquisitionum sequentium declaratur 342. Omnes radices Ω in certas classes (periodos) distribuuntur 343. Varia theoremata de his periodis 344 sqq. His disquisitionibus superstruitur solutio aequationis $X = 0$ art. 352. Exempla pro $n = 19$, ubi negotium ad duas aequationes cubicas unamque quadraticam, et pro $n = 17$, ubi ad quatuor quadraticas reducitur artt. 353, 354. *Disquisitiones ulteriores de hoc argumento.* Aggregata, in quibus terminorum multitudo par, sunt quantitates reales 355. De aequatione, per quam distributio radicum Ω in *duas* periodos definitur 356. Demonstratio theorematis in sect. IV commemorati 357. De aequatione pro distributione radicum Ω in *tres* periodos 338. Aequationum, per quas radices Ω inveniuntur reductio ad puras 359. *Applicatio disquisitionum praecedentium ad functiones trigonometricas.* Methodus, angulos quibus singulae radices Ω respondeant dignoscendi 361. Tangentes, cotangentes, secantes et cosecantes e sinubus et cosinubus absque divisione derivantur 362. Methodus, aequationes pro functionibus trigonometricis successive deprimendi 363. Sectiones circuli, quas per aequationes quadraticas sive per constructiones geometricas perficere dicet 365.

Additamenta.

Tabulae.

In art. 226, certain classes are grouped together into an "order" according to the divisibility properties of their coefficients.[30] There follows (arts. 229–233) a finer grouping of the classes within a given order according to their "genus." Gauss showed that, for every odd prime divisor p of the determinant of a form (with coprime coefficients), integers prime to p that can be represented by the form (and thus by all forms of its class) are either all quadratic residues, or all nonresidues modulo p: recording this information, as well as similar information at $p = 2$ for even discriminants, defines the "character" of the form (or of the class of the form). Classes with the same character are put into the same genus. The principal genus for a determinant D is that of the principal form $(1, 0, -D)$.[31]

In art. 235, Gauss defined a form $F(X, Y) = AXX+2BXY+CYY$ to be a "composite" of $f(x, y) = axx + 2bxy + cyy$ and $f'(x', y') = a'x'x' + 2b'x'y' + c'y'y'$, if $F(B_1, B_2) = f(x, y) \cdot f'(x', y')$, for certain transformations of the indeterminates $B_i(x, y; x', y')$, bilinear, as we would say, in x, y and x', y'. While this definition generalizes time-honoured relations like the following,[32] with $F = f = f'$:

$$(xx' - Nyy')^2 + N(xy' + yx')^2 = (x^2 + Ny^2) \cdot (x'^2 + Ny'^2),$$

the generality of the concept allowed Gauss to enter uncharted territory, for instance, to check – by elaborate computations – formal properties like the commutativity and associativity of the operation, as far as it is defined on the level of forms (arts. 240–241). In the end, the concept yields a multiplicative structure on the set of orders (art. 245) and of genera, with the principal genus acting like a neutral element (arts. 246–248), and indeed of classes (art. 239 and art. 249) of the same determinant.[33]

This rich new structure gave Gauss a tremendous leverage: to answer new questions, for instance, on the distribution of the classes among the genera (arts. 251–253); to come back to his favourite theorem, the quadratic reciprocity law, and derive a second proof of it from a consideration of the number of characters that actually correspond to genera of a given discriminant (arts. 261–262); to solve a long-standing conjecture of Fermat's (art. 293) to the effect that every positive integer is the sum of three triangular numbers. For this last application, as well as for deeper insight into the number of genera, Gauss quickly generalized (art. 266 ff.) the basic theory of reduced forms, classes etc., from binary to ternary quadratic forms. This

[30] It is with explicit reference to this terminology that Richard Dedekind would later introduce the notion of order into algebraic number theory in [Dedekind 1930–1932], vol. 1, pp. 105–158.

[31] See also §2 of F. Lemmermeyer's chap. VIII.3 below. Such classificatory schemes, then part and parcel of the natural sciences, already existed in mathematics, with variants, see Hindenburg's classification in [Bullynck 2006b], pp. 259–260. Note, however, that Gauss put classes below genera and orders.

[32] [Weil 1986]. Cf. the blackboard in [Weil 1979], vol. III, p. ii.

[33] This particularly difficult theory of the composition of forms has been reformulated several times by Gauss's successors; two different perspectives, emphasizing different aspects of its history and of its current relevance, are proposed in chaps. II.2 and II.3 below, by H.M. Edwards and by D. Fenster and J. Schwermer.

gave him in particular explicit formulae for the number of representations of binary quadratic forms, and of integers, by ternary forms, implying especially that every integer $\equiv 3 \pmod 8$ can be written as the sum of three squares, which is tantamount to Fermat's claim.[34] Sec. 5 closes (arts. 305–307) by open-ended reflections on the analogy between the multiplicative structure of the prime residue classes modulo an integer and of the classes of quadratic forms.[35]

Sec. 5 sometimes displays, and often hides, a tremendous amount of explicit computations performed by Gauss,[36] of numbers of classes, genera, or representations. To mention just one striking example of such extensive computations, which had an intriguing long term history, Gauss observed that any given "classification," that is, any given pair of numbers, one for the number of genera (which Gauss wrote as a Roman numeral) and one for the number of classes contained in a single genus (Arabic numeral), is realized by at most finitely many negative determinants:

> It seems beyond doubt that the sequences written down do indeed break off, and by analogy the same conclusion may be extended to any other classification. For instance, since in the whole tenth thousand of determinants there is none corresponding to a class number less than 24, it is highly probable that the classifications I.23, I.21 etc.; II.11; II.10 etc.; IV.5; IV.4; IV.3; IV.2 stop already before -9000, or at least that they contain extremely few determinants beyond -10000. However, *rigorous* proofs of these observations appear to be most difficult.[37]

[34] The entry in Gauss's mathematical diary about this problem is the only one accompanied by Archimedes's exclamation "EYPHKA"; see [Gauss 1796–1814], July 10, 1796.

[35] This as well as the composition of orders and genera alluded to above would provide one of the sources for the later development of the abstract concept of group, see [Wussing 1969], I, § 3.3, and [Wussing 2001].

[36] Examples relative to the composition of forms are displayed in H.M. Edwards's chap. II.2 below, who argues that such computations play a crucial role in Gauss's conception of a well-founded theory. See also Gauss's addition to art. 306 at the end of the 1801 edition and the tables in [Gauss 1863/1876], pp. 399–509. Gauss discussed how much numerical material on quadratic forms ought to be published *in extenso* in an 1841 letter to H. C. Schumacher, translated in [Smith 1859–1865], §119. Cf. [Maennchen 1930] and [Neumann 1979–1980], p. 26.

[37] Our translation of D.A., art. 303: *Nullum dubium esse videtur, quin series adscriptae revera abruptae sint, et per analogiam conclusionem eandem ad quasuis alias classificationes extendere licebit. E.g. quum in tota milliade decima determinantium nullus se obtulerit, cui multitudo classium infra 24 responderit: maxime est verisimile, classificationes I.23, I.21 etc.; II.11; II.10 etc.; IV.5; IV.4; IV.3; IV.2 iam ante* -9000 *desiisse, aut saltem perpaucis determinantibus ultra* -10000 *comprendere. Demonstrationes autem* rigorosae *harum observationum perdifficiles esse videntur.* Indeed, for one of the simplest constellations of numbers of classes and genera (corresponding to "orders of class number one" in imaginary quadratic fields, in Richard Dedekind's terminology of 1877), the proof that the list of determinants found by Gauss (art. 303) is actually complete was given by Kurt Heegner only in 1954 – and at first not accepted – by a method which subsequently would greatly enrich the arithmetic of elliptic curves. A book on Heegner by H. Opolka, S.J. Patterson, and N. Schappacher is in preparation.

1.3. Applications

Explicit calculations had evidently been part and parcel of number theory for Gauss ever since he acquired a copy of [Lambert 1770] at age 15, and launched into counting prime numbers in given intervals in order to guess their asymptotic distribution.[38] In these tables, Johann Heinrich Lambert made the memorable comment:

> What one has to note with respect to all factorization methods proposed so far, is that primes take longest, yet cannot be factored. This is because there is no way of knowing beforehand whether a given number has any divisors or not.[39]

The whole D.A. is illustrated by many non-trivial examples and accompanied by numerical tables. Section 6 (52 pp., 27 arts.) is explicitly dedicated to computational applications. In the earlier part of sec. 6, Gauss discussed explicit methods for partial fraction decomposition, decimal expansion, and quadratic congruences. Its latter part (arts. 329–334) takes up Lambert's problem and proposes two primality tests: one is based on the fact that a number which is a quadratic residue of a given integer M is also a quadratic residue of its divisors and relies on results of sec. 4; the second method uses the number of values of $\sqrt{-D}$ mod M, for $-D$ a quadratic residue of M, and the results on forms of determinant $-D$ established in sec. 5.

The final Section 7 on cyclotomy (74 pp., 31 arts.) is probably the most famous part of the *Disquisitiones Arithmeticae*, then and now, because it contains the conditions of constructibility of regular polygons with ruler and compass. After a few reminders on circular functions – in particular (art. 337), the fact that trigonometric functions of the angles kP/n, for a fixed integer n and for $k = 0, 1, 2, \ldots n - 1$, where $P = 2\pi$ denotes "the circumference of the circle," are roots of equations of degree n – Gauss focused on the prime case and the irreducible[40] equation

$$X = 0, \quad \text{where } X = \frac{x^n - 1}{x - 1} = x^{n-1} + x^{n-2} + \cdots + x + 1\ ;\ n > 2 \text{ prime},$$

which his aim is to "decompose *gradually* into an increasing number of factors in such a way that the coefficients of these factors can be determined by equations of as

[38] See Gauss's letter to Johann Franz Encke of December 24, 1849 in [Gauss 1863/1876], pp. 444–447. In [Biermann 1977], pp. 7–18, it is established that the page of Gauss's mathematical diary which follows the last entry of July 9, 1814, records the dates when Gauss counted prime numbers in certain intervals. On the influence of Lambert's and Hindenburg's tables on Gauss's sec. 6, see [Bullynck 2006b]. See also [Maennchen 1930], in particular pp. 27–35.

[39] [Lambert 1770], pp. 29–30: *Was übrigens bey allen bißher erfundenen Methoden, die Theiler der Zahlen aufzusuchen, zu bemerken ist, besteht darinn, daß man bey Primzahlen am längsten aufsuchen muß, und zuletzt doch nichts findet, weil man nicht voraus weiß, ob eine forgegebene Zahl Theiler hat oder nicht.* Lambert went on to propose Fermat's Little Theorem as a first necessary criterion for primality.

[40] D.A., art. 341. The word "irreducible" was established a few decades later. Cf. O. Neumann's chap. II.1 below.

low a degree as possible, until one arrives at simple factors, i.e., at the roots Ω of X."[41] Art. 353 illustrates the procedure for $n = 19$, which requires solving two equations of degree three and one quadratic equation (because $n - 1 = 3 \cdot 3 \cdot 2$); art. 354 does the same for $n = 17$ which leads to four quadratic equations ($n - 1 = 2 \cdot 2 \cdot 2 \cdot 2$).[42]

All roots of $X = 0$ are powers r^i of one of them, but to solve the equation, Gauss replaced the natural sequence of the exponents i, that is $1, 2, \ldots, n - 1$, by the more efficient bookkeeping provided by sec. 3:

> But in this [natural] form of the roots there is presented no means of distributing them into cyclical periods, nor even of ascertaining the existence of such periods or of determining their laws. It was the happy substitution of a geometrical series formed by the successive powers of a primitive root of n in place of the arithmetical series of natural numbers, as the indices [i.e., exponents] of r, which enabled [Gauss] to exhibit not merely all the different roots of the equation $\frac{x^n-1}{x-1}$, but which also made manifest the cyclical periods which existed among them. Thus if α was a primitive root of n and $n - 1 = mk$, then in the series $r, r^\alpha, r^{\alpha^2}, \ldots, r^{\alpha^{k-1}}, \ldots, r^{\alpha^{mk-1}}$ the m successive series which are formed by the selection of every k^{th} term, beginning with the first, the second … are periodical.[43]

Complementary results on the auxiliary equations, i.e., those satisfied by the sums over all the roots of unity in a given period, are given in art. 359, applications to the division of the circle in the final arts. 365 and 366. As a byproduct of his resolution of $X = 0$, Gauss also initiated a study of what are today called "Gauss sums," i.e., certain (weighted) sums of roots of unity, like the sum of a period, or of special values of circular functions. For instance, he proved (art. 356) that, for an odd prime n and an integer k not divisible by n,

$$\sum_R \cos \frac{kRP}{n} - \sum_N \cos \frac{kNP}{n} = \pm\sqrt{n} \quad \text{or} \quad 0,$$

according to whether $n \equiv 1$ or $n \equiv 3 \bmod 4$. Here, R varies over the quadratic residues, N over the quadratic non-residues modulo n.[44]

1.4. The Disquisitiones Arithmeticae as a System

In the preface of the D.A., Gauss explicitly restricted the objects of arithmetic to be the rational integers; he wrote:

[41] Our translation of D.A., art. 342: *Propositum disquisitionum sequentium … eo tendit, ut X in factores continuo plures* GRADATIM *resolvatur, et quidem ita, ut horum coëfficientes per aequationes ordinis quam infimi determinentur, usque dum hoc modo ad factores simplices sive ad radices Ω ipsas perveniatur.*

[42] For Gauss's early annoucements of these results and details on the case of the 17-gon, see [Reich 2000]. The impact on the theory of equations is discussed in O. Neumann's chap. II.1.

[43] [Peacock 1834], p. 316. Gauss described his view in his letter to Christian Gerling of January 6, 1819; see [Gauss & Gerling 1927/1975], p. 188.

[44] The sign of $\sqrt{n}$ depends on whether k is or is not a quadratic residue modulo n, but Gauss did not succeed in proving this fact in the D.A. See S.J. Patterson's chap. VIII.2 below.

> The theory of the division of the circle ... which is treated in sec. 7 does not belong *by itself* to arithmetic, but its *principles* can only be drawn from higher arithmetic.[45]

In sec. 7 itself, he promised that the "intimate connection" of the topic with higher arithmetic "will be made abundantly clear by the treatment itself."[46] There is of course the technical link mentioned above, that is, the bookkeeping of the roots of unity via sec. 3. But the "intimate connection" that Gauss announced goes further and also concerns the systemic architecture of the treatise.

Despite the impressive theoretical display of sec. 5, one cannot fully grasp the systemic qualities of the D.A. from the torso that Gauss published in 1801. At several places in the D.A. and in his correspondence a forthcoming volume II is referred to. The only solid piece of evidence we have is what remains of Gauss's 1796–1797 manuscript of the treatise. This differs from the structure of the published D.A. in that it contains an (incomplete) 8th chapter (*caput octavum*), devoted to higher congruences, i.e., polynomials with integer coefficients taken modulo a prime and modulo an irreducible polynomial.[47] Thus, according to Gauss's original plan, sec. 7 would not have been so conspicuously isolated, but would have been naturally integrated into a greater, systemic unity. The division of the circle would have provided a model for the topic of the *caput octavum*, the theory of higher congruences; it would have appeared as part of a theory which, among many other insights, yields two entirely new proofs of the quadratic reciprocity law.[48]

The treatise would thus have come full circle in several respects: beginning with ordinary congruences and ending with higher congruences; encountering various periodic structures along the way: prime residues, periods of reduced quadratic forms of positive discriminant, classes of quadratic forms which are all multiples of one class, cyclotomic periods and their analogues mod p; and proving quadratic reciprocity four separate times in the process.

That scientificity ought to be expressed by way of a system was a widespread idea in Germany in the second half of the XVIIIth century. Lambert, whose works were well represented in Gauss's library, wrote, besides his scientific *œuvre*, several philosophical texts developing this idea, at least two of which Gauss owned personally.[49] German idealist philosophers from Immanuel Kant to Georg Wilhelm Friedrich Hegel, for instance Johann Gottlieb Fichte, Friedrich Wilhelm Joseph von

[45] Our translation of D.A., *praefatio: Theoria divisionis circuli ..., quae in Sect. VII tractatur,* ipsa *quidem* per se *ad Arithmeticam non pertinet, attamen eius* principia *unice ex Arithmetica Sublimiori petenda sunt.*

[46] D.A., art. 335: *tractatio ipsa abunde declarabit, quam intimo nexu hoc argumentum cum arithmetica sublimiori coniunctum sit.*

[47] We summarize in this paragraph G. Frei's analysis, in chap. II.4 below, of the *caput octavum* and its importance for the economy of the whole treatise that Gauss originally planned.

[48] Gauss published them later independently; see G. Frei's chap. II. 4 below.

[49] Maarten Bullynck has drawn our attention to [Lambert 1764] and [Lambert 1771]; see [Bullynck 2006b], p. 278. Unfortunately, the dates of acquisition for these items are not known.

Schelling, Karl Leonhard Reinhold, and Jakob Friedrich Fries, cultivated various systemic programmes. Starting with Fichte, a system with a circular instead of linear architecture – returning to its initial point which thereby receives its higher justification – is called upon to provide a self-justifying foundation for the unfolding of self-consciousness. With Hegel this would become the unfolding of reason; in his first philosophical publication, which appeared in the same year as Gauss's D.A., Hegel wrote that "the method of the system, which may be called neither analytical nor synthetical, is realized most purely if it appears as the development of reason itself."[50]

The systemic design of Gauss's original plan for his arithmetic fits those ambient ideas remarkably well.[51] It makes it possible, for instance, to appreciate the four proofs of the quadratic reciprocity law originally planned for the treatise in a dual way: deducing a theorem at a certain place of the systemic development endows it with a specific theoretical meaning;[52] on the other hand, the various proofs of the same result connect these theoretical frameworks into a system which is not simply a deduction of increasingly complicated theorems from initial axioms. In Gauss's words,

> It is the insight into the marvellous interlinking of the truths of higher arithmetic which constitutes the greatest appeal of these investigations.[53]

Another systemic cyclicity is created precisely by the already mentioned recurrence of periodic structures throughout the treatise. Gauss himself insisted on the analogy between what we call cyclic components of class groups and the multiplicative structure of residues modulo a prime number:

> The proof of the preceding theorem will be found to be completely analogous to the proofs of arts. 45, 49, and the theory of the multiplication of classes actually has a very great affinity in every respect with the argument of sec. 3.[54]

[50] [Hegel 1801], p. 35: *Am reinsten gibt sich die weder synthetisch noch analytisch zu nennende Methode des Systems, wenn sie als eine Entwicklung der Vernunft selbst erscheint.* For a general orientation about the philosophical ideas alluded to in this paragraph, see [Ritter, Gründer 1998], art. "System," pp. 835–843.

[51] In spite of Gauss's philosophical interests – e.g., he is said to have read Kant's *Critique of Pure Reason* several times; see [Dunnington 1955], p. 315; cf. J. Ferreirós's chap. III.2 and J. Boniface's chap. V.1 below – we have no evidence of a direct and conscious inspiration; later mentions of Hegel by Gauss are rather critical; see for instance [Gauss & Schumacher 1862], vol. 4, n° 944, p. 337. A reference to Gauss's idea of science as a system in the not very reliable biographical essay [Waltershausen 1856], p. 97, suggests only a banal deductive structure.

[52] From the philosophical point of view, cf. [Hartmann 1972], p. 106: "The point easily lost sight of is that the [systemic] methodological structure provides a new meaning to categories that already have a meaning."

[53] Our translation of [Gauss 1817], p. 160: *Dann ist gerade die Einsicht in die wunderbare Verkettung der Wahrheiten der höhern Arithmetik dasjenige, das einen Hauptreiz dieses Studiums ausmacht, und nicht selten wiederum zur Entdeckung neuer Wahrheiten führt.*

[54] Our translation of D.A., art. 306: *Demonstratio theor. praec. omnino analoga invenietur*

Gauss thus drew the attention of the reader to the fact that sec. 3 was not only instrumental for decomposing the cyclotomic equation in sec. 7 but also linked the theory of forms to the rest. He also significantly called "irregular" a determinant whose principal genus was not cyclic, i.e., not constituted by the multiples of a single class of forms.

Half a century later, the mathematician Ernst Eduard Kummer reflected upon a suitable system for "the more recent mathematics," and concluded that it should not be linear but

> rather like the system of the universe; its goal would be to give not just the deduction of the mathematical truths, but an insight into all the essential relations among them.[55]

As mentioned above, the subject of the *Disquisitiones Arithmeticae* was natural numbers and Gauss's proofs were anchored in intricate computations, both formal (as in the sec. 5) and numerical, ultimately based on integers. The tension between this anchorage of the book and the striving towards a wider theoretical scope, as illustrated in the last section of the D.A., will be a recurring theme in what follows. It explains why the question of the reception of the book is tightly linked to the shaping of number theory as a specific discipline.

2. The Early Years of the *Disquisitiones Arithmeticae*

Gauss's own impressions of the early reception of the *Disquisitiones Arithmeticae* are scattered in his correspondence. A letter of June 16, 1805, to Antoine-Charles Marcel Poullet-Delisle, his French translator,[56] summarizes them well:

> It is for me as sweet as it is flattering that the investigations contained in my Work, to which I devoted the best part of my youth, and which were the source of my sweetest pleasures, have acquired so many friends in France; a fate quite different from what

demonstrationibus in arts. 45, 49, reveraque theoria multiplicationis classium cum argumento in Sect. III tractato permagnam undique affinitatem habet. Cf. the note on D.A., art. 306.IX: "Démonstration de quelques théorèmes concernant les périodes des classes des formes binaires du second degré," [Gauss 1863/1876], pp. 266–268, where Gauss used, of course informally, the word "group" (*groupe*) referring to all classes of forms of given determinant.

[55] [Kummer 1975], vol. 2, p. 697: *die neuere Mathematik ... wird sich erst später ihr eigenthümliches System schaffen, und zwar wol nicht mehr nur ein in einer Linie fortlaufendes, dessen Vollkommenheit allein darin liegt, dass das Folgende überall durch das Vorhergehende begründet werde, sondern ein dem Weltsysteme ähnlicheres, dessen Aufgabe es sein wird, über die blosse Begründung der mathematischen Wahrheiten hinausgehend, eine allseitige Erkenntnis der wesentlichen Beziehungen derselben zueinander zu geben.* In [Kummer 1975], vol. 2, p. 687, the parallel is made explicit between Hegel's principle of the systemic "self-interpretation of content" (*Sichselbstauslegen des Inhalts*) and the system required for the new mathematics since Gauss.

[56] On his life, see [Boncompagni 1882].

> they found in Germany where a taste for the most difficult parts of pure mathematics is the property of a very small number of persons.[57]

The *Disquisitiones Arithmeticae* had in fact been mentioned at the French Academy at least as early as January 1802:

> Citizen Legendre communicates a geometrical discovery, made in Germany by M. Charles Frédéric Bruce [sic], from Brunswick, and published by him in his work entitled *Disquisitiones arithmeticae*, Leipsik, 1801,[58]

and was commented upon very positively from all quarters.[59] The project of a French translation was supported by arguably the most prominent mathematician of the time, Pierre-Siméon Laplace, and on May 31, 1804, Joseph-Louis Lagrange wrote to Gauss:

> Your *Disquisitiones* have put you at once among the first mathematicians, and I consider the last section as one which contains the most beautiful analytic discovery made in a long time. Your work on planets will moreover have the merit of the importance of its topic.[60]

The beginning of this praise is often quoted, but taken in its entirety, the citation provides important clues about the early reception of the D.A. First, attention focused on the last section, the resolution of $x^n - 1 = 0$ through auxiliary equations and its consequences for the constructibility of regular polygons; this is the part of the book which borders both on the general theory of equations and on geometry. Second, Gauss's innovation was described as "analytical." Finally, number theory (and more generally pure mathematics) was considered a subsidiary subject compared to astronomy or mathematical physics.

[57] Letter published by Ernest Fauque de Jonquières in 1896, *Comptes rendus de l'Académie des sciences* 122, p. 829: *Il m'est aussi doux que flatteur que les recherches contenues dans mon Ouvrage, auxquelles j'avais dévoué la plus belle partie de ma jeunesse, et qui ont été la source de mes plus douces jouissances, aient acquis tant d'amis en France; sort bien inégal à celui qu'elles ont trouvé en Allemagne où le goût pour les parties plus difficiles des mathématiques pures n'est la propriété que d'un fort petit nombre de personnes.* In the letter, Gauss also expressed his hopes to publish the sequel of the D.A., a project he described as delayed for lack of time and printer.

[58] *Procès verbaux de l'Académie des sciences*, registre 114, vol. II, séance du 6 pluviôse an 10 (26 janvier 1802), p. 457: *Le Citoyen Legendre communique une découverte géométrique, faite en Allemagne par M. Charles Frédéric Bruce, de Brunswick, et publiée par lui dans son ouvrage intitulé* Disquisitiones arithmeticae*, Leipsik, 1801.*

[59] Gauss's fame in France was decisive for his connection to Alexander von Humboldt (then in Paris), and for establishing on the German scene, through Humboldt, a place for himself and, afterwards, for other number theorists; see H. Pieper's chap. III.1 in this volume.

[60] [Lagrange 1867–1892], vol. 14, p. 299: *Vos Disquisitiones vous ont mis tout de suite au rang des premiers géomètres et je regarde la dernière section commme contenant la plus belle découverte analytique qui ait été faite depuis longtemps. Votre travail sur les planètes aura de plus le mérite de l'importance de son objet.* "Geometer" (*géomètre*) remains a standard terminology for "mathematician" in French during the XIX$^{\text{th}}$ century.

This challenges the disciplinary position of the *Disquisitiones Arithmeticae* both in its mathematical and cultural aspects. Two situations typified the first generation of its readers:[61] either their involvement with the book, even if significant and fruitful, occupied only a small part within all their mathematical activities, or they themselves occupied a marginal position in the mathematical community. Augustin-Louis Cauchy is a good example of the first category, and Sophie Germain of the second.[62] And Gauss himself, after all, turned to astronomy and geodesy to secure a position.

This does not mean, however, that the reading of the D.A. at the time was restricted to one section, nor that it remained superficial and did not lead at all to innovative work. Sophie Germain displayed in her papers a thorough knowledge of all the sections: those on congruences of course which she used freely in her work on Fermat's Last Theorem as well as in her new proof of the quadratic residue behaviour of the prime 2, but also the difficult sec. 5, and specifically the composition of forms and the theory of ternary forms.[63] In his memoir on symmetric functions, presented to the *Institut* on November 30, 1812, Cauchy relied on concepts and a notation which he borrowed directly from the D.A., such as the idea of an adjoint and the notion of determinant, to prove that if a function of n quantities takes less than p distinct values, where p is the greatest prime divisor of n, then it can take at most 2 values, and furthermore to develop his theory of combinations and of determinants, seen with hindsight as key steps towards the development of group theory.[64]

However, as Lagrange's quote suggested, the D.A. was first of all taken up for its treatment of $x^n - 1$ and therefore mostly in treatises on algebra. For instance, Sylvestre François Lacroix included in the third edition of his *Complément des Élemens d'algèbre* (1804) a discussion of Gauss's results in the section on binomial equations.[65] Lagrange's second edition of his *Traité de la résolution des équations*

[61] Different aspects of this early reception have been documented in [Neumann 1979–1980], [Reich 1996], [Reich 2000], [Goldstein 2003], and [Neumann 2005].

[62] On the shifting professional status of number theory and number theorists, and the characteristics of the craft at different moments, see [Goldstein 1989].

[63] See for instance Bibliothèque Nationale de France, Manuscripts f.fr 9118, pp. 40–41, 86; f.fr. 9114, pp. 92–94. On Germain's work, see [Edwards 1977], pp. 61–65, and [Laubenbacher, Pengelley 1998].

[64] See [Cauchy 1815], where Cauchy – perhaps significantly – refers to Gauss's "Recherches analytiques" [sic]; cf. [Belhoste 1991], pp. 32–35. Between 1813 and 1815, Cauchy also published, in [Cauchy 1813–1815], his proof of Fermat's general claim to the effect that each natural number is the sum of no more than n n-gonal numbers. Gauss had shown in passing how to reduce the case $n = 4$ (already proved by Lagrange) to his theorem for $n = 3$; see end of D.A., art. 293. Cauchy then managed to reduce the cases $n \geq 5$ to those proven by Gauss; the most original elements of this proof, however, seem quite independent of the D.A.

[65] [Lacroix 1804], p. 92: *M. Gauss, dans un ouvrage très-remarquable, intitulé Disquisitiones Arithmeticae, a fait voir que* toute équation à deux termes, dont l'exposant est un nombre premier, peut être décomposée rationnellement en d'autres équations dont les degrés sont marqués par les facteurs premiers du nombre qui précède d'une unité ce

numériques de tous les degrés [Lagrange 1770/1808] also includes, as a final note XIV, a simplification of D.A., art. 360 rendering "the consideration of auxiliary equations superfluous,"[66] thanks to what are called "Lagrangian resolvents," i.e., sums such as $r + \alpha r^a + \alpha^2 r^{a^2} + \cdots + \alpha^{\mu-2} r^{a^{\mu-2}}$, where α is a $(\mu - 1)^{\text{th}}$, r a μ^{th} root of unity, and a a primitive root modulo μ.

Gauss's treatment of the cyclotomic equation was mentioned many times, in various countries, during the first decades of the century: Peter Barlow, a mathematics teacher at the Royal Military Academy, Woolwich, better known for his chromatic telescope lens, his work on magnetism and as a royal commissioner for railways, devoted a chapter to it in his book on Diophantine analysis, [Barlow 1811]. Nikolai Ivanovič Lobačevskii, who had been introduced to Gauss's work by his teacher (and Gauss's friend) Martin Bartels at Kazan, published a note on it.[67] Charles Babbage included the D.A. among the small list of works he recommended to the members of the newly created Cambridge Analytical Society, mentioning in particular "that celebrated theorem of Gauss on the resolution of the equation of $x^n - 1 = 0$."[68] Hegel used it as a famous example in his *Wissenschaft der Logik* in a discussion of analytical versus synthetical proofs.[69] In April 1818, Poinsot explained to the Academy his ideas to develop simultaneously the theory of the resolution of $x^n - 1 = 0$ and that of $x^n - 1 = \mathfrak{M}(p)$, in Legendre's notation.[70] Mindful of a general view of the world and the sciences in which the notion of "order" (*ordre*) played a key role, Poinsot saw Gauss's reindexation of the roots of the cyclotomic equation as a paradigm of the fact that order was the natural source of the properties of numbers, and algebra the proper domain to express it, see [Poinsot 1819–1820].

These variegated allusions to "analytic" and "analysis" redirect our attention to the problem of the disciplinary landscape in which the *Disquisitiones Arithmeticae*

nombre premier. ..., *mais pour le démontrer il faut recourir à des propriétés des nombres, que je ne pourrai faire connaître qu'à la fin de cet ouvrage.* Indeed, on pp. 294–315, the required parts of D.A., sec. 3 are explained, and then applied to the discussion of $x^{17} - 1 = 0$ and, in less detail, of $x^{19} - 1 = 0$.

[66] [Poinsot 1808/1826], p. xviii: *de sorte que sa méthode rend superflue cette considération des équations auxiliaires.* Lagrange used Gauss's sec. 7 to "reduce the resolution of binomial equations to the same principle as that of cubic and quartic equations"; see [Lagrange 1867–1892], vol. 14, p. 300.

[67] See [Neumann 2005], p. 313.

[68] [Babbage 1813/1989], p. 32.

[69] [Hegel 1812–1816], vol. 2, p. 325. Hegel concluded that Gauss's method to resolve $x^m - 1 = 0$ (which he called "one of the most important extensions of analysis in recent times") is synthetic, not analytic (in the Kantian, philosophical sense), because it uses the residues modulo m and primitive roots, "which are not data of the problem itself."

[70] This notation was used in [Legendre 1798/1808] for what Gauss wrote as $x^n \equiv 1$ (mod p) (in other terms, $x^n - 1$ is a multiple of p). Barlow, in [Barlow 1811] replaced Gauss's triple bar by another symbol of his own device. On the other hand, Christian Kramp, a professor of mathematics in the then French towns of Strasbourg and Cologne, used Gauss's congruence notation in his *Élémens d'Arithmétique Universelle*, published in 1808; see [Cajori 1928–1929], vol. 2, p. 35.

was to be situated.[71] In the preface of the D.A., Gauss directly addressed this issue: as said above, he *defined* the domain of his book as that of general investigations of integers (and of fractions as expressed by integers),[72] more precisely their advanced part, as opposed to the elementary part which deals with the writing of numbers and the usual operations. Moreover, according to Gauss, this domain entertains with indeterminate (or Diophantine) analysis roughly the same relation that universal analysis – which investigates general quantities – entertains with ordinary algebra, i.e., the theory of algebraic equations. In other words, arithmetic provides the general theoretical framework for the investigation of equations in integers or fractions. Gauss thus claimed quite an important status for his domain, *parallel* to analysis and rich in its own applications, as illustrated by secs. 6 and 7 of the D.A.

However, this was markedly different from the usual contemporary point of view;[73] Legendre for instance, in the preface to his *Essai sur la théorie des nombres*, stated:

> I shall not distinguish the Theory of Numbers from Indeterminate Analysis, and I consider these two parts as making up one single branch of Algebraic Analysis.[74]

The report on the mathematical sciences presented to the emperor Napoléon on February 6, 1808 by Jean Baptiste Joseph Delambre, Secretary of the Academy, adopted a very similar view: the presentation moves from geometry to algebra, number theory, and calculus – the three of them seen as analytical investigations – and then on to mechanics, astronomy, physics and geography.[75] Barlow also referred to number theory as a "branch of analysis" in the preface of [Barlow 1811].

[71] One has to keep in mind that 1801 was in the middle of a transitional period for mathematics where one passes from a vision of analysis as a global approach to problems, opposed to the synthetic one associated with Euclid's geometry, to a vision of analysis as a specific mathematical domain dealing with functions and limits. The last decades of the XVIII$^{\text{th}}$ century saw the triumph of algebraic analysis, as promoted for example by Lagrange. See [Jahnke 1990], in particular chaps. 4–8.

[72] See also J. Boniface's chap. V.1 below.

[73] This does not mean that Gauss's point of view had no precedent. One may think of Pierre Fermat, for instance, advocating an autonomous theory of integers (opposed to general quantities) in his 1657 challenge, see *Œuvres de Pierre Fermat*, ed. P. Tannery, C. Henry, vol. 2, p. 334. Paris: Gauthier-Villars, 1894.

[74] [Legendre 1798/1808], p. xi: *Je ne sépare point la Théorie des Nombres de l'Analyse indéterminée et je regarde ces deux parties comme ne faisant qu'une seule et même branche de l'Analyse algébrique.*

[75] [Delambre 1810]. About 30 pages are allotted to analysis, as opposed to some 230 pages for the rest. Analysis gets about half the room devoted to astronomy, in accordance with Lagrange's point of view expressed in his 1804 letter. Gauss is mentioned several times, as one of the very rare foreigners in this report which concentrates mainly on the achievements of French scientists. Representing him as "one of the best minds in Europe," but also as a successor of Lagrange and Legendre, i.e., at the same time as European and as an heir and participant of French culture, is quite characteristic of the late French Enlightenment; see [Goldstein 2003].

Notwithstanding the attention paid to the D.A., the disciplinary *status quo* remained unchanged, as textbooks show. In Barlow's treatise for instance, theoretical arithmetic, including that inherited from Gauss's book, only serves as prolegomena to the solution of families of indeterminate equations. Legendre did not adopt Gauss's congruence notation, nor did he distinguish congruences as a topic worthy of a separate treatment. He did present a proof of the quadratic reciprocity law as well as a whole chapter on cyclotomic equations, after Gauss, in the second edition of his *Essai sur la théorie des nombres*, but commented:

> One would have wished to enrich this Essay with a greater number of the excellent materials which compose the work of M. Gauss: but the methods of this author are so specific to him that one could not have, without extensive detours and without reducing oneself to the simple role of a translator, benefited from his other discoveries.[76]

Thus, the *Disquisitiones Arithmeticae* had at first a strong effect, but in a direction *opposite* to that of establishing number theory as an autonomous research discipline, as defined by Gauss in the preface of the D.A., that is, focused on integers and congruences; the book contributed to, and sometimes even launched, developments in algebra (perceived as a branch of analysis), in the theory of equations and in the study of linear transformations, determinants, and substitutions, towards the theories of groups and of invariants.[77] This partial fusion with other domains could even be perceived as a valorization of number theory, in that this would overcome its isolation. In his report to the British Association for the Advancement of Science "on the recent progress and present state of certain branches of analysis," delivered at Cambridge in 1833, George Peacock, after an analysis of sec. 7 of the D.A., which "gave an immense extension to our knowledge of the theory and solution of such binomial equations" ([Peacock 1834], p. 316), comments on Poinsot's investigations on the cyclotomic equation and its analogue modulo p, mentioned above:

> These views of Poinsot are chiefly interesting and valuable as connecting the theory of indeterminates with that of ordinary equations. It has, in fact, been too much the custom of analysis to consider the theory of numbers as altogether separated from that of ordinary algebra. The methods employed have generally been confined to the specific problem under consideration and have been altogether incapable of application when the known quantities employed were expressed by general symbols and not by specific numbers. It is to this cause that we may chiefly attribute the want of continuity in the methods of investigation which have been pursued, and the great confusion which has been occasioned by the multiplication of insulated facts

[76] [Legendre 1798/1808], Avertissement, p. vi: *On aurait désiré enrichir cet Essai d'un plus grand nombre des excellens matériaux qui composent l'ouvrage de M. Gauss : mais les méthodes de cet auteur lui sont tellement particulières qu'on n'aurait pu, sans des circuits très étendus, et sans s'assujétir au simple rôle de traducteur, profiter de ses autres découvertes.*

[77] For instance, Jacobi in his paper on Pfaff's theory referred to the D.A. for the notion of determinant, see [Jacobi 1882–1891], vol. 4, p. 26. However, given that the D.A. was often not the only source of a mathematical development in those areas, gauging its precise effect is a delicate question.

> and propositions which were not referable to, nor deducible from any general and comprehensive theory.[78]

We will see that the following phase would be characterized by an even greater entwinement around the *Disquisitiones Arithmeticae* of several disciplinary orientations. Paradoxically enough, this would help to consolidate the status of number theory, particularly in Germany.

3. The *Disquisitiones* as the Core for Arithmetic Algebraic Analysis

Because of the already-established fame of the book, and because it did not require many prerequisites, the generations of mathematicians born after 1801 often read the D.A. early on: the Norwegian Niels Henrik Abel, born in 1802, studied it in his first year of university, the Italian Angelo Genocchi, born in 1817, perused it while he was still in law school, and the Englishman Arthur Cayley, born in 1821, quoted it in his first important paper on determinants presented to the Cambridge Philosophical Society. The publication of shorter articles focusing on new results, instead of books or long memoirs, began to spread as normal mathematical activity: these papers are strewn with references to the *Disquisitiones Arithmeticae* in the second quarter of the XIX$^{\text{th}}$ century, and witness engagement with several specific questions arising from the first sections. A small industry developed for example around the determination of primitive roots modulo a prime p, accompanied sometimes by the publication of extensive tables. Guglielmo Libri and especially Victor-Amédée Lebesgue also investigated at some length the number of solutions of various types of congruences, in particular $a_1x_1^m + \ldots + a_kx_k^m \equiv a \bmod p$, for $p = hm + 1$.[79]

However, the reception of the *Disquisitiones Arithmeticae* during the 1820s did not simply result from a closer, more systematic study of the book, in the continuation of the first decades: two new factors directly intervened in the 1820s, which would at the same time consolidate and diversify a fledgling domain of research emerging from the *Disquisitiones Arithmeticae*. One was cultural and institutional, the other had to do with mathematical content and technique.[80]

[78] [Peacock 1834], p. 322. We are indebted to M.J. Durand-Richard for drawing our attention to this text.

[79] See [Lebesgue 1837]. Lebesgue occupied several professorships in provincial towns and published numerous articles, mostly on number theory, including a new proof of the quadratic reciprocity law. He illustrates well the development of research activities and publications outside the main centres, i.e., outside Paris and far from the Academy in the case of France. Characteristically, he also published, in the same issue of the journal, "astronomical theses" whose real topic was in fact substitutions of forms. His counting of solutions for congruence equations is mentioned (rather dismissively) in André Weil's seminal article [Weil 1975], vol. 1, [1949b], which culminated in the statement of the general "Weil Conjectures" (and referred to art. 358 of the D.A. as the origin of the question).

[80] For more details on the two aspects, see respectively Parts III and IV of this book.

3.1. Mathematics in Berlin

The first aspect was the conscious renewal of German, and specifically Prussian, mathematics in the aftermath of the wars against Napoléon and the founding of Berlin University.[81] The values associated with mathematics as of the late 1820s and the corresponding efforts to hire adequate professors allowed Gauss's D.A. to play a prominent role in this development. As Abel wrote to Christoffer Hansteen on December 5, 1825: "The young mathematicians in Berlin and, as I hear, all over Germany almost worship Gauss; he is the epitome of all mathematical excellence."[82] Gauss's letter of recommendation for Dirichlet, for instance, explicitly stressed number theory as a significant topic on which to judge the value of a mathematician, as well as the patriotic aspect of the hiring.[83] August Crelle's foundation of the *Journal für die reine und angewandte Mathematik* in 1826 provided the new discipline with a crucial organ in Germany. A comparison of the papers published in Crelle's journal to those in, say, Joseph Gergonne's *Annales de mathématiques* or the memoirs of the Paris Academy in those years illuminates the new domains touched upon.

This orientation would be reinforced by the lectures offered on number theory at Berlin University and the production of textbooks. Ferdinand Minding, for example, *Privatdozent* at Berlin, published in 1832 an introduction to higher arithmetic, which presents a shortened and expurgated version of the D.A. focusing on the basic parts of the various sections, with the notable exception of sec. 7. Minding dropped the more delicate part of Gauss's theory of forms (genera, composition), but added things expected from the perspective of a textbook, for instance, linear Diophantine equations or continued fractions. He did, however, identify the quadratic reciprocity law as "the most remarkable theorem of higher arithmetic,"[84] and, in a historical endnote, stressed rigour:

> Gauss's *Disquisitiones Arithmeticae* offers a presentation of arithmetic conducted with ancient rigour and distinguished by new discoveries. Among other things an excellent merit of the work lies in the rigorous proof of the reciprocity theorem. Since then the science has been enriched by a non-negligible number of new proofs and results, some of which are to be found in the memoirs of various learned societies, others in mathematical journals, and especially in Crelle's Journal for mathematics.[85]

[81] This foundation goes back to 1810 and Wilhelm von Humboldt's neo-humanist reform (see [Vierhaus 1987]); but its strong impact on the development of mathematics mostly started after Alexander von Humboldt's return from Paris to Berlin in 1827. See [Biermann 1988], chap. 3.

[82] Quoted from [Ore 1957], p. 91.

[83] This letter to Encke and the hiring of number theorists is discussed in H. Pieper's chap. III.1, §2, below.

[84] [Minding 1832], p. 53. We heartily thank Ms. Bärbel Mund at the Göttingen university library for making Gauss's copy of this little book accessible to us. In the author's announcement of his book in Crelle's *Journal* (vol. 7, 1831, pp. 414–416), Minding described pure number theory as both a necessary foundation for algebra (whose basic notion is that of number) and a paradigm for a rigorously developed, autonomous branch of mathematics.

[85] [Minding 1832], p. 198: *Eine in antiker Strenge durchgeführte und durch neue Entdek-*

A comparison with Legendre's or Barlow's books mentioned above also reveals a change of focus: Minding's treatment makes congruences an important topic *per se*, instead of a mere prelude to the study of specific Diophantine equations.

3.2. Biquadratic Residues

The second new factor of change was paradoxically brought about by new developments in analysis, specifically analysis involving continuity. It eventually gave rise to an active, largely international, integrated domain of research, which blossomed in the middle of the century: for short, we shall refer to it as *arithmetic algebraic analysis*. It was rooted in XVIII$^{\text{th}}$ century algebraic analysis, onto which the *Disquisitiones Arithmeticae* grafted a potent arithmetical shoot which grew to be its central stem for a while. At least three new developments in analysis gave substance to arithmetic algebraic analysis: (1) the acceptance of complex numbers and Gauss's publications on biquadratic residues between 1825 and 1832; (2) the integration of Fourier analysis into number theory; and (3) the theory of elliptic functions. We shall discuss them in turn, although they were actually tightly interwoven in much of the production of those years.

Gauss's investigations on biquadratic (that is, quartic) residues[86] led him to complex numbers and their claim to enter the subject matter of higher arithmetic. Apparently conceived a few years after the publication of the D.A., his ideas on extending the domain of arithmetic were published only after 1825.[87] The goal of this work was to state and prove a biquadratic reciprocity law; while his first

kungen ausgezeichnete Darstellung der Arithmetik geben die disquisitiones arithmeticae *von Gauß... Unter andern macht der strenge Beweis des Satzes der Reciprocität ein vorzügliches Verdienst dieses Werkes aus. Seitdem ist die Wissenschaft durch eine nicht unbedeutende Anzahl neuer Beweise und Resultate bereichert worden, welche sich theils in den Denkschriften verschiedner gelehrten Gesellschaften, theils in mathematischen Zeitschriften, und namentlich in Crelle's Journal für Mathematik befinden.*

[86] He presented his results to the Göttingen Academy in two installments, the first in 1825, the second in 1831, and announced both presentations in the *Göttingische gelehrte Anzeigen* a few days later, some time before the papers themselves were published, see [Gauss 1863/1876], pp. 65–92, pp. 93–148, pp. 165–168, and pp. 169–178, respectively; an English translation of the second self-announcement is to be found in [Ewald 1996], vol. 1, pp. 306–313. During the first decades of the century, Gauss had also completed the D.A. on several points; see [Gauss 1863/1876].

[87] In [Gauss 1863/1876], pp. 165–168, Gauss dated the beginning of his work on cubic and biquadratic residues to 1805. This is compatible with material evidence about two of the early notes on cubic residues published in [Gauss 1900], pp. 5–11. However, his mathematical diary records on February 15, 1807: "Beginning of the theory of cubic and biquadratic residues" (*Theoria Residuorum cubicorum et biquadraticorum incepta*), and on October 23, 1813: "The foundation of a general theory of biquadratic residues, searched for during almost seven years with the greatest effort but always in vain, we have finally and happily discovered on the same day that a son was born to us" (*Fundamentum theoriae residuorum biquadraticorum generalis, per septem propemodum annos summa contentione sed semper frustra quaesitum tandem feliciter deteximus eodem die quo filius nobis natus est*); see [Gauss 1796–1814].

communication handled the results on -1 and 2 as biquadratic residues for any prime of the form $4n + 1$, the second got as far as stating the biquadratic law. However, its most original feature was elsewhere:

> As easily as all such special theorems are discovered by induction, so difficult it is to find a general law for these forms in the same way, even though several common features are obvious. And it is even more difficult to find the proofs of these theorems. … One soon recognizes that totally new approaches are necessary to enter this rich domain of higher arithmetic, … that for the true foundation of the theory of biquadratic residues the field of higher arithmetic, which before had only extended to the real integers, has to be extended to also include the imaginary ones and that exactly the same right of citizenship has to be given to the latter as to the former. As soon as one has understood this, that theory appears in a totally new light, and its results acquire a most surprising simplicity.[88]

Gauss then considered what are now called "Gaussian integers" $a+bi$ (with $i^2 = -1$ and rational integers a, b), and extended to them the concepts and results of arithmetic *as defined in the Disquisitiones Arithmeticae*: the units ± 1, $\pm i$; (complex) prime numbers and congruences; Fermat's Little Theorem; the quadratic reciprocity law, etc. In Gauss's words:

> Almost all the investigations of the first four sections of the *Disquisitiones Arithmeticae* find, with a few modifications, their place also in the extended arithmetic.[89]

He was then able to state a quartic reciprocity law for Gaussian integers.[90]

While we are now used to interpreting Gaussian integers arithmetically, as an instance of algebraic numbers,[91] the legitimacy of complex numbers inside analysis

[88] [Gauss 1863/1876], pp. 170–171: *So leicht sich aber alle dergleichen specielle Theoreme durch die Induction entdecken lassen, so schwer scheint es, auf diesem Wege ein allgemeines Gesetz für diese Formen aufzufinden, wenn auch manches Gemeinschaftliche bald in die Augen fällt, und noch viel schwerer ist es, für diese Lehrsätze die Beweise zu finden. … Man erkennt demnach bald, dass man in dieses reiche Gebiet der höhern Arithmetik nur auf ganz neuen Wegen eindringen kann, … dass für die wahre Begründung der Theorie der biquadratischen Reste das Feld der höhern Arithmetik, welches man sonst nur auf die reellen ganzen Zahlen ausdehnte, auch über die imaginären erstreckt werden, und diesen das völlig gleiche Bürgerrecht mit jenen eingeräumt werden muss. Sobald man diess einmal eingesehen hat, erscheint jene Theorie in einem ganz neuen Lichte, und ihre Resultate gewinnen eine höchst überraschende Einfachheit.*

[89] [Gauss 1863/1876], p. 172: *Fast die sämmtlichen Untersuchungen der vier ersten Abschnitte der* Disquisitiones Arithmeticae *finden mit einigen Modificationen, auch in der erweiterten Arithmetik ihren Platz.* Gauss also completed his purely arithmetical presentation with a geometric one, interpreting complex numbers as points in the plane, see §§ 38, 39 and pp. 174–178.

[90] For two distinct prime Gaussian integers α and β which are primary, that is, congruent to 1 modulo $2+2i$, one has $\left[\frac{\alpha}{\beta}\right]\left[\frac{\beta}{\alpha}\right] = (-1)^{\frac{N\alpha-1}{4}\frac{N\beta-1}{4}}$, where $\left[\frac{\alpha}{\beta}\right]$ is the quartic analogue of the Legendre symbol (which takes the four values, ± 1, $\pm i$) and $N\alpha$ designates the norm of the Gaussian integer α; see [Lemmermeyer 2000], chap. 6. As in the D.A., Gauss did not use any Legendre-like symbol.

[91] Several authors would later describe the inclusion of the Gaussian integers as the initial

was still very much in debate during these decades and contemporaries first perceived Gauss's move as establishing links inside analysis. The fact that Gauss announced a proof of the biquadratic reciprocity law, but never published it, provided additional incentive to work on reciprocity laws for small degrees, in particular cubic, quartic and sextic.[92] Jacobi was the first to make a proof of the biquadratic law at least semi-public through Johann Georg Rosenhain's notes of his 1836–1837 Königsberg lectures: "Gauss advertises these theorems very much in that they occupied him particularly, and they are indeed of the highest importance."[93] The proof relied on cyclotomy: Jacobi's point of departure was Gauss's work on biquadratic reciprocity as well as the D.A., reading the latter very much from the point of view of sec. 7. Thus, his emphasis is different from Minding's:

> Number Theory in its present state consists of two big chapters, one of which may be called the theory of the solution of pure equations, the other the theory of quadratic forms. Here I will deal mainly with the first part whose discovery we owe to Gauss.[94]

This description is interesting because it does not mention congruences as a part by itself; on the contrary, it suggests that congruences are a common theme underlying both "chapters," in agreement with the increasing importance of reciprocity laws as the core of number theory, and also with what we can guess about Gauss's original plan of his treatise. It also fits well with the idea of arithmetic algebraic analysis, the equations and forms (as algebraic core) providing the intermediary step between the arithmetical topic (congruences) and analytic tools, as we shall now see.

3.3. Infinite Series

Gauss apparently had long had his own ideas on the proper discipline of analysis. In 1812, he identified limiting processes as the "true soil on which the transcendental functions are generated."[95] This marks a cautious distance from the tradition of algebraic analysis, and Gauss would implicitly confirm this distance later in his

step in this direction; see for instance [Sommer 1907], p. i: *Seitdem Gauß die Arithmetik durch Aufnahme der komplexen Zahlen $a + b\sqrt{-1}$ erweitert hat, ist eine großartige Theorie der allgemeinen algebraischen Zahlen entstanden*. For a recent example of the same perspective, see the beginning of [Neukirch 1999]. Cf. chap. I.2 below.

[92] For detailed overviews, we refer to [Smith 1859–1865], §§28–38, and [Lemmermeyer 2000], chaps. 6–8. See also §3 of C. Houzel's chap. IV.2 below. We will briefly discuss Eisenstein below, who gave altogether five proofs of biquadratic reciprocity.

[93] [Jacobi 1836–1837], 35th course, p. 221: *Gauß preist diese Theoreme sehr an, indem sie ihn besonders beschäftigten, u. sie sind in der That von der größten Wichtigkeit.* Handwritten copies of these lectures circulated in Germany; see [Jacobi 1881–1891], vol. 6, 2nd footnote on pp. 261–262. Henry Smith, however, had apparently no access to them when he wrote his report in the 1860s; see [Smith 1859–1865], p. 78.

[94] [Jacobi 1836–1837], 1st course, p. 5: *Die Zahlentheorie auf ihrem jetzigen Standpunkte zerfällt in zwei große Kapitel, von denen das eine als die Theorie der Auflösung der reinen Gleichungen, das andere als die Theorie der quadratischen Formen bezeichnet werden kann. Ich werde hier hauptsächlich von dem ersten Theile handeln, dessen Erfindung wir Gauß verdanken.*

[95] [Gauss 1866], p. 198: ... *überhaupt die Annäherung an eine Grenze durch Operationen,*

positive reaction to Enno H. Dirksen's voluminous *Organon* [Dirksen 1845], a book which, while obviously rooted in this tradition, stresses "transcendental determinations" (*transzendente Bestimmungsformen*), phenomena lying outside the range of algebra:[96]

> I procrastinated from one week to the next, and it is only now that I have found the time to familiarize myself with the tendency of your work. It is of the kind that I have always held in high esteem. Already very early, a good deal more than 50 years ago, I considered everything I found in books on infinite series very unsatisfactory and abhorrent to the true mathematical spirit, and I recall that I made an attempt, in 1793 or 1794, to develop the basic concepts in a more satisfactory way which, as far as I can remember, was ... quite similar to yours.[97]

Infinite series and limits are central to the second aspect of arithmetic algebraic analysis at the time: the introduction of functions of a real variable and Fourier analysis as tools for higher arithmetic. The main actor here was Peter Gustav Lejeune-Dirichlet who, around 1821, left Germany for Paris to study higher mathematics with the *Disquisitiones Arithmeticae* under his arm. The topics and the spirit of Dirichlet's first papers – starting with the $n = 5$ case of Fermat's Last Theorem,[98] and divisors of forms, then calculus and Fourier series – show the strong influence of his Paris mathematical environment. But even there, the traces of his involvement with the D.A. are already obvious from the frequent explicit references to specific articles of it, very similar to the way early-modern authors referred to Euclid's *Elements*. He also reacted very quickly to Gauss's publications on biquadratic reciprocity, studying divisors of quartic forms in his 1828 dissertation *ad veniam docendi*, and completing Gauss's statements on *quadratic* reciprocity for Gaussian integers in 1832.

Back in Berlin from 1829 (professor at Berlin University from 1831), Dirichlet devoted numerous articles to arithmetical questions, typically beginning with some reference to Gauss. His German career indeed demonstrates the new possibilities given specifically to number theorists in Prussia: Gauss recommended him for this

die nach bestimmten Gesetzen ohne Ende fortgesetzt werden – dies ist der eigentliche Boden, auf welchem die transcendenten Functionen erzeugt werden.

[96] [Jahnke 1990], p. 413, with reference to [Dirksen 1845], p. 44.

[97] See the letter of Gauss to Dirksen of November 5, 1845 in [Folkerts 1983–1984], p. 73: *habe ich von einer Woche zur anderen procrastinirt, und erst jetzt habe ich dazu kommen können, mich etwas näher mit der Tendenz Ihres Werkes bekannt zu machen. Es ist eine solche die mir von jeher sehr werth gewesen ist. Schon sehr früh, das ist vor weit mehr als 50 Jahren, war mir alles was ich über unendliche Reihen in Büchern fand sehr unbefriedigend, und vom ächten mathematischen Geiste abhorrirend, und ich erinnere mich, daß ich etwa im Jahre 1793 oder 1794 einen Versuch anfing die Grundbegriffe auf eine genügendere Art zu entwickeln, die so weit mein Gedächtniß reicht mit Ihrem Wege ... viel Ähnlichkeit hatte.*

[98] Fermat's Last Theorem had been proposed as a prize subject by the Paris Academy for the year 1818. As is well-known, Gauss placed the general, theoretical development of higher arithmetic above this individual result. To the news about the prize communicated to him by Olbers, he replied on March 21, 1816 that this isolated statement had little interest for him; see [Gauss & Olbers 1900/1976], part 1, p. 629.

reason.[99] On July 37, 1837, Dirichlet announced at the Academy of Berlin a proof of the statement that "every infinite arithmetic progression whose first term and difference have no common divisor contains infinitely many primes." This fact had been noticed and studied by Legendre – whose arguments were criticized in one of the appendices of the D.A. – but Dirichlet commented:

> It was only after I left completely the path taken by Legendre that I hit upon a totally rigorous proof of the theorem on arithmetic progressions. The proof that I found … is not purely arithmetical but relies in part on the consideration of continuously varying quantities.[100]

Despite the difference in topics, we would like to underline the striking parallel with Gauss's 1831 description of his procedure for biquadratic reciprocity; Gauss also stressed how he was led outside the traditional framework of number theory in order to obtain satisfactory proofs.

To complete his proof on the distribution of primes, Dirichlet needed to establish another result which was interesting for its own sake and which illustrates well the mixture of arithmetic, algebra and analysis at work in this research area: he gave a formula to compute *a priori* the number of classes of quadratic forms of a given determinant. More specifically, for a prime q of the form $4n + 3$, say, he showed first, making Legendre's symbol explicit, that

$$\sum \frac{1}{n^s} \cdot \sum \left(\frac{n}{q}\right) \frac{1}{n^s} \cdot (\sum \frac{1}{n^{2s}})^{-1} = \sum \frac{2^\mu}{m^s},$$

where m varies over the odd positive numbers having only quadratic residues of q as prime factors, and μ is the number of distinct prime divisors of the corresponding m. Then he identified the right-hand sum as

$$\sum \frac{1}{(ax^2 + 2bxy + cy^2)^s} + \sum \frac{1}{(a'x^2 + 2b'xy + c'y^2)^s} + \dots,$$

where the quadratic forms in the denominators vary over a complete system of representatives, up to proper equivalence, of forms of determinant $-q$ and where the sums are taken over all integers x and y which make the value of the considered form odd and prime to q. Using results both of the D.A.[101] and of Joseph Fourier's *Théorie de la chaleur* to evaluate the sums for s close to 1, Dirichlet obtained the number h of classes of quadratic forms of discriminant $-q$ to be

$$h = 2\left[1 - \left(\frac{2}{q}\right)\frac{1}{2}\right] \frac{\sum b - \sum a}{q},$$

[99] See H. Pieper's chap. III.1 below. Note also that Dirichlet published a large number of his papers in Crelle's *Journal*.

[100] [Dirichlet 1889–1897], vol. 1, p. 316: *Erst nachdem ich den von Legendre eingeschlagenen Weg ganz verlassen hatte, bin ich auf einen völlig strengen Beweis des Theorems über die arithmetische Progression gekommen. Der von mir gefundene Beweis … ist nicht rein arithmetisch, sondern beruht zum Teil auf der Betrachtung stetig veränderlicher Grössen.*

[101] The paper "Sur l'usage des séries infinies dans la théorie des nombres," [Dirichlet 1889–1897], vol. 1, pp. 357–374, for instance contains 23 references to articles of the D.A.

with a and b varying respectively over the quadratic residues and non-residues of q which are smaller than q. For instance, Gauss's relation for $q \equiv 3 \bmod 4$, proved up to the sign in art. 356 of the D.A., and including the precise sign in [Gauss 1863/1876], pp. 9–45, 155–158,

$$\sum \sin \frac{2\pi an}{q} - \sum \sin \frac{2\pi bn}{q} = \left(\frac{n}{q}\right)\sqrt{q}$$

reduces the evaluation of $\sum \left(\frac{n}{q}\right)\frac{1}{n}$ to that of classical Fourier series of the type $\sum \frac{\sin nz}{n}$, for $0 < z < 2\pi$.

In a letter to Gauss of September 9, 1838, Dirichlet commented:

> I would almost like to conjecture that my method bears some analogy with the investigations alluded to in the final remark of the *disq. arith.*, in particular because you say about these investigations that they throw light on several parts of analysis, and my method is so intimately connected with the remarkable trigonometric series that represent discontinuous functions and whose nature was still completely mysterious at the time of the publication of the *disq. arith.*[102]

Dirichlet favoured this kind of *rapprochement* between the different branches of mathematics:

> The method I use seems to merit some attention above all because of the link it establishes between infinitesimal analysis and higher arithmetic.[103]

For a positive determinant, the formula for the number of classes contains a regulator, involving logarithms and a solution of the Pell equation. He wrote:

> [The expression of the law] is of a more composite nature, and somehow mixed, because, besides the arithmetic elements on which it depends, it contains others which have their origin in certain auxiliary equations appearing in the theory of binomial equations, and therefore belonging to Algebra. The last result is particularly remarkable and offers a new example of these hidden relations that a deep study of

[102] [Dirichlet 1889–1897], vol. 2, p. 382: *Ich möchte fast vermuthen, dass meine Methode mit den in der Schlussbemerkung der* disq. arith. *angedeuteten Untersuchungen einige Analogie hat, besonders deshalb, weil Sie von Ihren Untersuchungen sagen, dass sie über mehrere Theile der Analysis Licht verbreiten, und meine Methode in so innigem Zusammenhange mit den merkwürdigen trigonometrischen Reihen steht, welche discontinuierliche Funktionen darstellen, und deren Natur zur Zeit des Erscheinens der* disq. arith. *noch ganz unaufgeklärt war.* Later, Dirichlet would find alternative analytic means to handle the question.

[103] [Dirichlet 1889–1897], vol. 1, p. 360: *La méthode que j'emploie me paraît surtout mériter quelque attention par la liaison qu'elle établit entre l'Analyse infinitésimale et l'arithmétique transcendante.* To the French readers to whom this particular paper is addressed, Dirichlet added his hope of attracting in this way the attention of mathematicians who were not *a priori* interested in number theory.

> mathematical analysis allows us to discover between what appears to be completely disparate questions.[104]

He expressed such priorities not only in the production of new results, but also in his simplifications of Gauss's proofs, through continued rereading of the D.A., esp. in the 1840s: for instance, he would comment on his simplification of the theory of binary quadratic forms with positive determinant by saying that "the characteristic feature of this method is that it brings irrational numbers into the circle of our ideas."[105] The intervention of analysis reveals links and, paradoxically enough for an advanced subject, it simplifies and democratizes the *Disquisitiones Arithmeticae*:

> My work may also contribute to the advancement of science in establishing on new grounds and closer to the elements beautiful and important theories which until now had been accessible only to the small number of geometers who were capable of the concentration needed in order not to lose the thread of thought in a long series of computations and of very complicated reasonings.[106]

3.4. Elliptic Functions

We now turn to point (3) mentioned at the beginning of § 3.2: the theory of elliptic functions. At the beginning of sec. 7 of the D.A., Gauss put this section, and indeed higher arithmetic as a whole, in a much wider perspective by mentioning "many other transcendental functions" besides the circular functions, to which the methods and results of sec. 7 could be extended. But he gave only one example of such functions: "those which depend on the integral $\int dx/\sqrt{1-x^4}$,"[107] and never published the

[104] [Dirichlet 1889–1897], vol. 1, p. 536: *[L'expression de la loi] est d'une nature plus composée et en quelque sorte mixte, puisque, outre les éléments arithmétiques dont elle dépend, elle en renferme d'autres qui ont leur origine dans certaines équations auxiliaires qui se présentent dans la théorie des équations binômes, et appartiennent par conséquent à l'Algèbre. Ce dernier résultat est surtout remarquable et offre un nouvel exemple de ces rapports cachés que l'étude approfondie de l'Analyse mathématique nous fait découvrir entre les questions en apparence les plus disparates.*

[105] [Dirichlet 1863], § 72. We quote here J. Stillwell's English translation. Dirichlet associated to such a form $ax^2 + 2bxy + cy^2$ the roots of the equation $ax^2 + 2bx + c = 0$ and derived most of the facts about the reduction of the forms from these roots, and more specifically from their expansions as continued fractions.

[106] [Dirichlet 1889–1897], vol. 1, p. 414: *Mon travail pourra encore contribuer à l'avancement de la science en établissant sur de nouvelles bases et en rapprochant des éléments, de belles et importantes théories qui n'ont été jusqu'à présent à la portée du petit nombre de géomètres capables de la contention d'esprit nécessaire pour ne pas perdre le fil des idées dans une longue suite de calculs et de raisonnements très composés.* The context is that of arts. 234 ff in the D.A.

[107] D.A., art. 335: *Ceterum principia theoriae ... non solum ad functiones circulares, sed pari successu ad multas alias functiones transscendentes applicari possunt, e.g. ad eas quae ab integrali* $\int \frac{dx}{\surd(1-x^4)}$ *pendent.* In a letter to Schumacher (who would be the adressee of Jacobi's first notes on elliptic functions in 1827) dated September 17, 1808, Gauss called the functions which are not reducible to circular or logarithmic functions a "magnificent

"big treatise" (*amplum opus*) on these functions promised in 1801.[108] In a letter dated February 8, 1827, Jacobi tested Gauss on this announcement: "The application of higher arithmetic to the division of the elliptic transcendents is promised in the *Disquisitiones*; oh, may the promise be kept!"[109]

When Jacobi himself turned to elliptic functions,[110] he first studied transformations between various elliptic integrals, rather than the immediate analogue of sec. 7, i.e., the division of a single elliptic integral or function. But this division had then just been settled by Abel, who had also been inspired by Gauss's announcement in the D.A.[111] The story of Abel's and Jacobi's rival and parallel development of the theory of elliptic functions is well-known.[112] It was characterized by inverting elliptic integrals classified in [Legendre 1811] and [Legendre 1825–1828], such as $u = \int_0^{\varphi} \sqrt{(1-x^2)(1-\kappa^2x^2)}^{\,-1} dx$; by recognizing the double periodicity of the resulting complex functions $u \mapsto \varphi(u, \kappa)$; and by studying certain algebraic equations arising from the theory such as the *division equation* and the *modular equation*. The division equation of order $m > 1$ for a given elliptic function φ is that whose roots are the m^2 values $\varphi(\beta)$ such that $\varphi(m\beta) = \varphi(\alpha)$, for a given α; generalizing Gauss's sec. 7 from a cyclic to a bicyclic situation, Abel showed that it could be solved by radicals of rational expressions in $\varphi(\alpha)$. The *modular equation* is the one linking the $\sigma(n)$ possible moduli λ's to a given modulus κ, for which there exist transformations $y = U(x)V(x)^{-1}$, with relatively prime polynomials U, V, where U has odd degree

golden treasure" (*herrliche Goldgrube*), and gave as specific examples those relating to the rectification of the ellipse and the hyperbola; [Gauss & Schumacher 1860], vol. 1, n° 2, p. 3.

[108] See [Schlesinger 1922], secs. III–VI, for the most complete published survey of Gauss's unpublished papers on elliptic functions. See also C. Houzel's chap. IV.2 below as well as [Houzel 1978]. Moreover, Jacobi would recognize formulae related to the theory of elliptic functions in Gauss's article establishing the sign of Gauss sums; see [Jacobi 1836–1837], 35th course, p. 221: *die Formen enthält, welche auch in der Theorie der elliptischen Funktionen vorkommen.*

[109] [Jacobi 1881–1891], vol. 7, p. 400: *Die Anwendung der höheren Arithmetik auf die Theilung der elliptischen Transzendenten ist in den Disquisitiones versprochen; o würde doch das Versprechen erfüllt!* Gauss's reply to this, if any, is not known. At the time of the letter, Abelian functions were not yet public knowledge.

[110] See his letter to Schumacher of June 13, 1827 in [Jacobi 1881–1891], vol. 1, pp. 31–48, and his subsequent publications as well as the letters to Legendre in [Jacobi 1881–1891], vol. 1, pp. 185–461.

[111] [Schlesinger 1922], p. 183–184. See also [Abel 1881], vol. 1, pp. 263–388, no. 21: *Le procédé par lequel nous allons effectuer cette résolution est entièrement semblable à celui qui est dû à M.* Gauss *pour la résolution de l'équation* $\theta^{2^n+1} - 1 = 0$.

[112] See [Abel 1902], [Königsberger 1904], as well as the sources in [Abel 1881], [Jacobi 1881–1891], vols. 1 and 7. Dirichlet's obituary of Jacobi, in particular [Jacobi 1881–1891], vol. 1, pp. 7–18, offers a remarkably well written informal account. See also [Houzel 1978] and Houzel's chap. IV.2 below.

n and V degree $n-1$, such that $\dfrac{dy}{\sqrt{(1-x^2)(1-\lambda^2x^2)}} = \dfrac{dx}{M\cdot\sqrt{(1-x^2)(1-\kappa^2x^2)}}$ for an appropriate number M.[113] Linking M and κ gives rise to yet another algebraic equation of the same degree, Jacobi's *multiplier equation*.[114]

Let us explain why we see these developments as characteristic of a new domain of research, for which we have coined the name *arithmetic algebraic analysis*.

First, just as Jean-Baptiste le Rond d'Alembert, in his article on Diophantus in the *Encyclopédie* in 1784, found it natural to underline how useful Diophantus's method of solving his number problems was for the transformation of integrals, the new complex analytic theory of elliptic functions was at first derived directly from arithmetico-algebraic properties of the integrals at hand (with additional inspiration provided by Euler's treatment of the trigonometric and exponential functions), but *not* as the theory of a special type of complex functions within an existing general function theory. The double periodicity of the inverse functions, for instance, was deduced by Abel by defining very meticulously his function $\varphi(\alpha)$, first on a real interval, then on a purely imaginary one via the substitution $\alpha \mapsto \alpha i$, and finally on all complex numbers via the addition theorem; see [Abel 1881], vol. 1, pp. 263–388, secs. 1–5. We note that the same is true for the infinite series introduced by Dirichlet, of the general type $\sum \frac{a_n}{n^s}$, whose construction at first directly reflected arithmetical and algebraic properties.

Second, just like sec. 7 of the D.A., the new analysis of elliptic functions could be claimed by the theory of algebraic equations as well as by arithmetic.[115] Thus, the cyclotomic equations, the division equations of elliptic functions, and the modular equation all functioned as crucial model cases which oriented the general theory. Now, in all these cases, the roots come indexed in a way which permits linear operations on them by the integers taken with respect to a suitable modulus N. Évariste Galois is often described as having created a general, abstract theory which he then also applied to special classes of equations.[116] But we think that theory and examples were much more closely linked at the time, and that the examples we mentioned informed Galois about what he had to formulate in the general theory.

[113] See the first half of [Jacobi 1829]. Here, $\sigma(n)$ denotes the sum of all the divisors of n.

[114] [Jacobi 1881–1891], vol. 1, p. 261.

[115] Concerning relations between the theory of elliptic functions and geometry, Abel's construction of the division of the lemniscate is geometric in precisely the same sense as is Gauss's result of sec. 7. Jacobi's paper, in 1828, concerning Poncelet's closure theorem could be interpreted as a link with more recent geometrical works, see [Jacobi 1881–1891], vol. 1, pp. 277–293 and [Bos, Kers, Oort, Raven 1987]. But most of the time the geometry aimed at within the field during this period was more elementary, as in Kummer's paper on quadrilaterals with rational sides and diagonals, where the geometrical setting is only a gloss on the key issue, the link between elliptic functions and traditional Diophantine analysis; see [Kummer 1975], vol. I, pp. 253–273.

[116] For instance, [Kiernan 1971], p. 89, writes about Galois's *second mémoire* ([Galois 1962], pp. 129–147): "This paper was, in Galois' mind, not a development of his theory, but rather an application of it to a particular class of equations."

Sec. 7 of the D.A., or "*la méthode de M. Gauss*," as Galois says, and its elliptic analogues, are recurring signposts in Galois's writings. When he introduced his "number-theoretic imaginaries,"[117] i.e., the solutions of $x^{p^\nu} \equiv x \pmod{p}$, his chief application was to "the theory of permutations, where one constantly has to vary the form of the indices," and he showed how this indexing of the roots of an equation of prime power degree allowed one to recognize its solvability by radicals.[118] His mathematical testament, written to Auguste Chevalier on May 29, 1832, starts very plainly: "I have done several new things in analysis. Some concern the theory of equations, the others the functions given by integrals."[119] But it exactly delineates our domain: the last item in the first group of results was the determination of the groups of modular equations.

Let us note in passing that Abel's general approach to algebraic equations – contrary to Galois's – aimed at making explicit "the most general form of the solutions" to equations of a given type. This appears not to be linked to the D.A., but rather to the tradition of algebraic analysis. Among Abel's followers on this point, however, we find Jacobi and Kronecker who in their work would link this approach to arithmetic inspirations from the D.A.[120]

In the further development of Galois theory, the parallel between the general theory and the special examples continued to be evident for a while. Enrico Betti, for example, is famous for the first systematic account of Galois's theory in 1852 which established the model of organizing the material, with an abstract part on substitutions preceding the application to algebraic equations, see [Betti 1903], pp. 31–80. But he followed this up by a paper focused on the division and modular equations of

[117] The expression *les imaginaires de la théorie des nombres* is from Galois's letter to Chevalier; see [Galois 1962], p. 175. Note that Galois adopted in 1830 the approach to higher congruences that the young Gauss had systematically avoided in his *caput octavum* back in 1797; see § 4.2 of G. Frei's chap. II.4 below, with reference to Gauss's § 338.

[118] [Galois 1962], p. 125: *C'est surtout dans la théorie des permutations, où l'on a sans cesse besoin de varier la forme des indices, que la considération des racines imaginaires des congruences paraît indispensable. Elle donne un moyen simple et facile de reconnaître dans quel cas une équation primitive est soluble par radicaux.* In today's parlance, if one interprets the symmetric group S on p^ν letters as the group of permutations of the field $\mathbf{F}_{\mathbf{p}^\nu}$, a subgroup of S is solvable if and only if it is affine, i.e., if all its permutations are of the form $x \mapsto ax+b$. We recall incidentally that Poinsot – who wanted to treat in parallel the study of congruences and of equations – already advocated in his 1808 analysis of the 2nd edition of Lagrange's *Traité des équations* keeping to a theoretical description of the operations involved, in the presence of overwhelming numerical complexity: *Par la nature du problème, la longueur des calculs croit avec une telle rapidité que la question ne peut plus être aujourd'hui de chercher la formule, mais simplement de prédire la suite des opérations qui y conduirait à coup sûr.*

[119] [Galois 1962], p. 173: *J'ai fait en analyse plusieurs choses nouvelles. Les unes concernent la théorie des équations ; les autres, les fonctions intégrales.* On relating Galois to the D.A., see also O. Neumann's chap. II.1 below.

[120] For Abel and Kronecker, see [Petri, Schappacher 2004], §§ 1.4, 1.5, 2.1. Jacobi presented the "true form of the surds of the equation $x^p = 1$ which has never been given before" in his applications of cyclotomy to number theory, [Jacobi 1881–1891], vol. 6, pp. 254–274.

elliptic functions where he proved Galois's claim concerning the modular equation, see [Betti 1903], pp. 81–95. When he subsequently came back to the general subject of his 1852 article, it was to show (among other things) how to derive the substance of Gauss's method of sec. 7 "directly from the decomposition of the corresponding substitutions."[121] Again with reference to the modular equation, Kronecker noted in 1862 the

> altogether singular circumstance … that the progress of algebra and of its methods depends crucially on the material of equations which is delivered from outside, or if I may say so, on the variety of algebraic phenomena provided by the further development of analysis.[122]

An even later echo of the original unity may be seen in the strong presence of linear substitutions, and the treatment of the modular equation, in [Jordan 1870].

Another telling illustration of the influence of elliptic functions on the theory of algebraic equations is provided by Gotthold Eisenstein's well-known irreducibility criterion, which he introduced to show the irreducibility of the division equations of the lemniscatic elliptic function, and which he also used to give another proof of the irreducibility of $X^{p-1} + \cdots + X + 1$ first shown in D.A., art. 342.[123]

This being said, explicit references to the D.A. in the context of algebraic equations tended to evaporate after 1850 outside Germany. For instance, Joseph-Alfred Serret, in the first edition (1849) of his influential *Cours d'algèbre supérieure*, based on his lectures at the Sorbonne and devoted to the algebraic resolution of equations and "incident questions related to it," discussed congruences in the 23th and 24th lessons, cyclotomy in the 26th and 27th. The 25th presents "curious and useful theorems" derived from the principles explained before, for instance the decomposition of an integer as a sum of four squares; the name of Gauss is attached here to the notation of congruence and to the solvability of the cyclotomic equations, and the

[121] [Betti 1903], p. 123: *La decomposizione dei gruppi complessi di grado non primo forma la sostanza del metodo di Gauss per le equazioni binomie ; io ho mostrato come essa deriva direttamente dalla decomposizione delle sostituzioni che loro appartengono…*

[122] [Kronecker 1895–1930], vol. 4, p. 213: *Es liegt dieß an einem ganz eigenthümlichen Umstande, welcher bei den in Rede stehenden Gleichungen auftritt und welcher wiederum zeigt, daß … der Fortschritt der Algebra und ihrer Methoden wesentlich durch das ihr von Außen herzugebrachte Material an Gleichungen bedingt ist oder, wenn ich mich so ausdrücken darf, durch die Mannigfaltigkeit algebraischer Phänomene, welche die Analysis in ihrer weiteren Entwickelung darbietet.*

[123] See his letter to C.F. Gauss, August 18, 1847, [Eisenstein 1975], vol. 2, pp. 845–855, and [Eisenstein 1975], vol. 2, pp. 542–544. The footnote in [Lemmermeyer 2000], p. 254, led us to Theodor Schönemann's priority claim in [Schönemann 1850], and to [Schönemann 1846], p. 100, where a marginally more general criterion is derived in the context of higher congruences modulo p^2. This independent development of Gauss's unfulfilled promise of a sec. 8 on higher congruences, started in [Schönemann 1845], was continued in particular by Richard Dedekind and would finally merge, at the very end of the XIXth century, with the line of thought initiated by Galois's imaginaries and expanded in [Serret 1849/1854], pp. 343-370, into a theory of finite fields; see G. Frei's chap. II.4.

D.A. is proposed more specifically next to Legendre's *Théorie des nombres* as a general reference for the 25th lesson. Five years later in the second edition, this section has totally changed, and the arithmetical theorems are replaced by Galois's theory of imaginaries;[124] a supplementary note about quadratic reciprocity mentions only Legendre as its discoverer and then Jacobi as the author of the specific proof given in the book; see [Serret 1849/1854], pp. 533–537.

The conjunction of the theory of elliptic functions with arithmetic is not restricted to the D.A. Diophantine analysis is touched upon in Kummer's paper on quadrilaterals with rational sides and diagonals mentioned above (footnote 115) and is briefly promoted in very general terms by Jacobi in 1835; see [Jacobi 1881–1891], vol. 2, pp. 51–55. Jacobi was in fact actively promoting the introduction of elliptic functions "into all parts of mathematical analysis,"[125] blurring at the same time the direct connection with the *Disquisitiones Arithmeticae*. As far as it continued the D.A., however, the impact of elliptic functions went deeper and revolved around three interrelated topics: reciprocity laws, class numbers, and complex multiplication – we shall meet them again in the remainder of this chapter. These investigations, combined with the use of complex numbers and Dirichlet's analytical methods, constituted a solid ground for expanding Gauss's ideas, knit together by multiple links into what appeared to be a unified enterprise, though disruptive factors were also present.

In the summer of 1848, for his second term of teaching at Berlin University, Eisenstein offered two lecture courses which, taken together, would have constituted an introduction to arithmetic algebraic analysis: one on "the integral calculus as source of transcendental functions," and another one "explaining Gauss's *Disquisitiones Arithmeticae*, with special investigations on the divisions of the circle."[126]

We have already alluded in § 3.1 to Jacobi's proof of the biquadratic reciprocity law from his Königsberg lectures. One of Eisenstein's proofs is sketched in sec. 3

[124] The Gaussian roots of Galois's work are not mentioned in Serret's lectures. In the subsequent restructured editions of this mathematical bestseller, after 1866, properties of integers that are "necessary for the theory of the algebraic resolution of equations," in particular a study of congruences and higher congruences, are the topic of a third section (with several chapters); Gauss's name, like many others, is episodically mentioned on specific points with no particular emphasis.

[125] See his little 1831 paper presenting an application to continued fractions, [Jacobi 1881–1891], vol. 1, pp. 329–331, in particular p. 329: *j'ai avancé que les fonctions elliptiques doivent entrer dans toutes les parties de l'analyse mathématique et contribuer essentiellement à leur progrès.*

[126] [Eisenstein 1975], vol. 2, p. 902: *Integralrechnung als Quelle der transcendenten Functionen; Erläuterung der Disquisitiones Arithmeticae von Gauss mit speciellen Untersuchungen über die Kreisteilungen.* The second did not find enough interested students, though, so Eisenstein taught instead a class on the *einfachsten Principien der Mechanik.* For a useful quick survey of Eisenstein's life and work, which mentions in particular a few important papers – for instance, on cubic forms, and on ternary quadratic forms – that we do not go into here in spite of their direct connection with the D.A., see Weil's review of Eisenstein's *Mathematische Werke*; e.g., in [Weil 1979], vol. 3, pp. 398–402.

of C. Houzel's chap. IV.2 below. All five of his proofs can pass for showcase illustrations of arithmetic algebraic analysis. But some also contain special aspects which foreshadow the end of this amalgamated research field. For example, in his paper entitled "Applications of Algebra to Higher Arithmetic," after having neatly derived the classical quadratic reciprocity from the polynomial expression of sin pv in the variable $x = \sin v$, and the biquadratic law from an elliptic analogue, Eisenstein remarked:

> Maybe some readers do not approve of using circular or elliptic functions in arithmetic arguments; but one has to observe that these functions enter here only *symbolically*, so to speak, and that it would be possible to eliminate them altogether without changing the substance and the basis of the proof.[127]

He went on to replace, for instance, the division values of the sine function by any suitable geometric division of an arbitrary closed curve only assumed to be symmetric with respect to both coordinate axes.[128]

If arithmetic was allowed to distance itself from analysis here, Eisenstein later rewrote this proof within a long text where analysis clearly takes the lead, for he introduced there the circular and elliptic functions via his own original method of series summation.[129] Eisenstein was not the only author searching for a new analytical foundation of the theory initiated by Abel and Jacobi. The 1830s and 1840s witness a growing interest in elliptic functions, with publications by Joseph Liouville, Alfred Serret, William Roberts, Arthur Cayley, Joseph Raabe, Ludwig Schläfli, and Königsberg colleagues and students of Jacobi, like Friedrich Richelot, Ludwig Adolf Sohncke, and Christoph Gudermann (whose 1839–1840 course on elliptic functions was followed by the young Karl Weierstrass). Many of these authors belong to the tradition of arithmetic algebraic analysis (Richelot's doctoral dissertation was about $x^{257} - 1 = 0$), but they also began to propose alternative constructions of the functions on a purely analytic basis. From the beginning of the 1830s on, Jacobi would use the theory of theta functions as a foundation for the whole theory of elliptic functions in his lectures.[130] In long series of papers in Crelle's *Journal* starting in the late 1830s, Gudermann tried to build a systematic theory of elliptic functions on the

[127] [Eisenstein 1975], vol. 1, p. 297: *Il se pourrait qu'on n'approuvât pas l'usage des fonctions circulaires et elliptiques dans les raisonnements arithmétiques ; mais il y a à observer que ces fonctions n'y entrent que d'une manière pour ainsi dire* symbolique*, et qu'il serait possible de les en chasser complètement sans détruire la substance et le fond des démonstrations.*

[128] In his 1852 *Théorie des nombres*, focused on Diophantine problems, Eugène Desmarest complained that Gauss had mixed up arithmetic with analysis. We do not know whether Eisenstein reacted to somebody's opinion with his remark, or if it was just a truly Gaussian reflection on the specific merits of various proofs. Smith pointed out that Eisenstein also gave his first proof of the biquadratic law (via cyclotomy, like Jacobi's) "a purely arithmetical form" when he presented it a second time; see [Smith 1859–1865], p. 81, with reference to [Eisenstein 1975], vol. 1, pp. 141–163.

[129] [Eisenstein 1975], vol. 1, pp. 357–478. Cf. [Weil 1976].

[130] See his *Theorie der elliptischen Funktionen aus den Eigenschaften der Thetareihen abgeleitet*, published from notes taken by C.W. Borchardt in [Jacobi 1881–1891], vol. 1,

basis of expansions in infinite series. In France from 1847, Liouville and Hermite started to work out a general theory of doubly periodic complex functions.[131]

In the same way, Dirichlet later gave alternative proofs of some of his results, using simple calculus, see [Dirichlet 1863], § 103. While his formulas involving Gauss sums had at first tightly linked Fourier series, residues and classes of forms, these new proofs, although technically more direct, loosened the ties between analytical and arithmetical aspects. After the middle of the century, this emancipation of analytical techniques from their algebraic roots, as much as the wish to eliminate analysis from number-theoretical proofs, would contribute to tearing arithmetic algebraic analysis apart.

4. … And Pastures New

While keeping close to their connections with the *Disquisitiones Arithmeticae*, the investigations we described have the potential to launch autonomous lines of development. This phenomenon may also operate at a finer scale than those met in the preceding section. We will demonstrate it for a single, but remarkable, example of research which, while building directly on the D.A. and on developments discussed in the last section, ushered in several new lines of thought independent of Gauss's known and unknown work.

The mathematicians coming together here were Ernst Eduard Kummer (born in 1810), and his younger colleagues Charles Hermite, Gotthold Eisenstein, and Leopold Kronecker (all three born between December 1822 and December 1823). They all had studied the *Disquisitiones Arithmeticae* early on[132] and knew the works of the preceding generation we have just discussed. Complex numbers, elliptic functions (Kummer alone would hardly ever use them in his own work), and Dirichlet's series were part of their resources, and served in turn as filters for their reading of the D.A. and of Gauss's later work. Our point is that this wealth of resources would lead to differing uses of the D.A., and in due course to diverging developments, even though, for a few decades, these perspectives would still be seen as complementary to rather than exclusive of one another, and the main actors would continue to see themselves as taking part in the construction of a vast field of research combining arithmetic, algebra, and function theory.

The impulse for all the far-reaching and diverging developments we are about to sketch in this section was given by a programmatic 5-page note written by Jacobi, [Jacobi 1839]. Not much is proved there; results obtained are alluded to, as was still allowed in those days, and the paper is really about how to look at things,

pp. 497–538, and Weierstrass's editorial comment thereon in [Jacobi 1881–1891], vol. 1, p. 545. In his *Fundamenta nova*, on the contrary, Jacobi had deduced his theory from the properties of elliptic functions, which were defined by inverting elliptic integrals.

[131] See [Belhoste 1996].

[132] Kronecker studied the *Disquisitiones Arithmeticae* under Kummer's guidance; see [Kronecker 1891/2001], p. 219. Eisenstein bought the French translation in 1842 and read it while travelling with his family in the British Isles; see [Ullrich 2001], p. 205. As for Hermite, see chap. VI.1 below.

more specifically at "complex prime numbers." It starts by recalling Gauss's work on biquadratic reciprocity which called for generalizing the D.A. from rational to Gaussian integers, introducing "complex numbers of the form $a+b\sqrt{-1}$ as modules [of congruences] or divisors." In perfect coherence with the idea of arithmetic algebraic analysis, Jacobi speculated:

> I do not believe that arithmetic alone has led to such an arcane idea, but that it was drawn from the study of the elliptic transcendents, namely that special type which gives the rectification of the lemniscatic arc. For in the theory of multiplication and division of the lemniscatic arc, the complex numbers of the form $a + b\sqrt{-1}$ play precisely the role of ordinary integers.[133]

After an allusion to the analogous connection between cubic residues, complex integers $\frac{a+b\sqrt{-3}}{2}$ built from cubic roots of unity, and other elliptic functions, Jacobi turned to quadratic forms with Gaussian integer coefficients, thus resuming in a new way a theme alluded to before: the bringing together of what Jacobi saw as the two main parts of number theory, cyclotomy and the theory of forms.

He showed for instance that a Gaussian integer which divides the form $yy - \sqrt{-1}\,zz$ can be represented by it. Such is the case for any prime $p = aa+bb = 8n+1$ because, by Gauss's theory, $\sqrt{-1}$ is a quadratic residue of $a + b\sqrt{-1}$. From this it follows that $a+b\sqrt{-1} = \phi(\alpha)\phi(\alpha^5)$, where $\phi(\alpha)$ is a real linear combination of the powers of an 8th root of unity α. Also $a - b\sqrt{-1} = \phi(\alpha^3)\phi(\alpha^7)$. This shows that any prime $p = 8n + 1$ is the product of four complex numbers built from 8th roots of unity; the three ways in which one can order the four factors in two pairs give the three different representations of the prime p as $a^2 + b^2$, $c^2 + 2d^2$, $e^2 - 2f^2$, the main point being that all three now flow, as Jacobi put it, "from a common source." He then announced identical results for primes of the form $12n + 1$ with 12th roots of unity. More generally, Jacobi had previously noticed that a prime $p = 1+\lambda n$ can usually be represented in different ways as a product of two complex numbers[134] and had manipulated products and quotients of such complex numbers with surprising effects. He commented, allowing us a glimpse of the state of the art concerning "complex prime numbers" a few years before Kummer's work:

> A closer consideration ... convinced me that the complex factors of the prime number p are in general themselves composite, so that if one decomposes them into true complex prime numbers, the factors that make up the denominator will cancel one

[133] [Jacobi 1839], p. 275: *Ja ich glaube nicht, dass zu einem so verborgenen Gedanken die Arithmetik allein geführt hat, sondern dass er aus dem Studium der elliptischen Transcendenten geschöpft worden ist, und zwar der besonderen Gattung derselben, welche die Rectification von Bogen der Lemniscata giebt. In der Theorie der Vervielfachung und Theilung von Bogen der Lemniscata spielen nämlich die complexen Zahlen von der Form $a+b\sqrt{-1}$ genau die Rolle gewöhnlicher Zahlen.* (That Gauss was indeed aware of some such connection is supported by the last entry (July 9, 1814) of his mathematical diary [Gauss 1796–1814], a document discovered by Paul Stäckel only in 1898).

[134] For instance, $p = 8n + 1$ can be written as the product $(a + b\sqrt{-1})(a - b\sqrt{-1})$, or as $(c + \sqrt{-2}d)(c - \sqrt{-2}d)$ or as $(e + \sqrt{2}f)(e - \sqrt{2}f)$.

by one against the prime factors of the numerator.[135]

Jacobi thought that these "true complex prime numbers" might be precisely what he had just obtained for $p = 8n + 1$ or $p = 12n + 1$; he ended his paper by announcing similar results for primes $p = 5n + 1$ (relative to the 5th roots of unity), and hoped for a proof of higher reciprocity laws.[136]

These still mysterious and unproved statements clearly challenged younger mathematicians: we shall examine how four of them, equipped in particular with their different experience of the D.A., rose to the challenge.

4.1. Hermite's Minima of Forms

A French translation of Jacobi's article appeared in 1843, and at this point Hermite entered the scene. After a previous exchange with Jacobi about Abelian functions, Hermite wrote him in 1847 a letter proposing a proof of the decomposition of a prime $5m + 1$ (resp. $7m + 1$) into complex factors built from the 5th (resp. 7th) roots of unity. Hermite took up Jacobi's allusion to elliptic transcendents rather than the link with reciprocity laws; he even mentioned as his immediate starting point Jacobi's theorem that there is no complex analytic function with three independent periods.

The decompositions of prime numbers were deduced from Hermite's celebrated theorem on the minima of quadratic forms which he had proved by closely following Gauss's discussion of ternary forms in the D.A.[137] For a prime $p = 5N + 1$, for instance, Hermite considered linear forms

$$\varphi(\xi) = Nx_0 + (\xi - a)x_1 + (\xi^2 - a^2)x_2 + (\xi^3 - a^3)x_3 + (\xi^4 - a^4)x_4,$$

where ξ is a primitive 5th root of unity and a an integer different from 1, which verifies the congruence $a^5 \equiv 1 \bmod N$. For all integral values of the indeterminates x_i, the product $\mathcal{F} = \varphi(\xi)\varphi(\xi^2)\varphi(\xi^3)\varphi(\xi^4)$ is an integer multiple of N, say MN. Hermite then cleverly associated a quadratic form with real coefficients to this product of

[135] [Jacobi 1839], p. 279: *Eine genaue Betrachtung ... führte mich zu der Ueberzeugung, dass diese complexen Factoren der Primzahl p im Allgemeinen selbst wieder zusammengesetzt sein müssen, so dass, wenn man sie in die wahren complexen Primzahlen auflöst, die complexen Primzahlen, welche die Factoren des Nenners bilden, gegen die Primfactoren des Zählers sich einzeln aufheben lassen.*

[136] Cauchy also established a few of these results, and announced the possibility of proving higher reciprocity laws, in a memoir presented to the Paris Academy on May 31, 1830. Its publication was, however, delayed for ten years as Cauchy left France after the 1830 Revolution; see [Belhoste 1991], chaps. 9 and 10. A shorter version had already appeared in 1829. It ends with the remark that Jacobi told Cauchy he also had obtained the same results with basically the same approach. Via cyclotomy, Cauchy had also deduced results on the decomposition of primes in complex quadratic domains: "M. Jacobi's research on the quadratic forms of prime numbers," Cauchy wrote in [Cauchy 1840], "and one must say as much of mine, may be considered as offering new developments of M. Gauss's beautiful theory."

[137] Hermite's response to Jacobi's 1839 note and his derivation of Jacobi's statement are studied in detail in C. Goldstein's chap. VI.1 below.

linear forms: his result on the minima of forms applied to this quadratic form shows that there exist integers $(x_0, \ldots, x_4)$ such that the product $\mathcal{F}$ is strictly smaller than $2N$, and thus equals N. This provides the decomposition of N as a product of four complex numbers built from 5th roots of unity.

Hermite's further programme was to study algebraic complex numbers in general and to classify them in the spirit of Lagrange's and Gauss's classification of binary quadratic forms. But pursuing his own direction, he wanted to base this study on that of n-ary quadratic forms, and keep close to elliptic functions. This would lead him and a number of his followers to enter more deeply into general invariant theory and to promote general complex functions as a leading topic.

4.2. Kummer's Ideal Numbers

Meanwhile, Kummer's reaction to Jacobi's statements was more directly linked to reciprocity laws. His first mathematical works of the 1830s had mainly dealt with differential equations and series.[138] He turned seriously to number-theoretical questions in the following decade, in connection with his appointment at the University of Breslau. His letter to his friend and former pupil Kronecker on January 16, 1842, again documents the role of number theory in the Berlin sphere of influence:

> Since I noticed during my last stay in Berlin that the Breslau affair could get serious, I sat down at home and worked very hard in order to elaborate something like a habilitation thesis, and I started with something completely new to me, the cubic residues of the prime numbers $6n + 1$.[139]

In this letter, Kummer mentioned only the D.A. and Dirichlet. A month later, however, he had begun reading Jacobi's work on cubic residues[140] and, following Jacobi even further, getting involved with complex numbers and, with less conviction, elliptic functions. Until the mid-1860s, number theory, and more specifically, the study of "numbers built from roots of unity," would be at the centre of his activities.

Kummer's focus in this early work was what we now call Gauss sums for cubic residues,

$$\sum_0^{p-1} \cos \frac{2\alpha k^3 \pi}{p}, \quad \sum_0^{p-1} \cos \frac{2\beta k^3 \pi}{p}, \quad \sum_0^{p-1} \cos \frac{2\gamma k^3 \pi}{p},$$

for p a prime of the form $3n+1$, α denoting a cubic residue, β and γ representatives of the two kinds of cubic non-residues. These sums are the roots of the cubic equation $z^3 = 2pz + pt$, where t is a normalized solution of $4p = t^2 + 27u^2$. Kummer's

[138] Including his well-known paper on the hypergeometric series. An exception was a small 1835 paper on Fermat's Last Theorem for even exponents.

[139] [Kummer 1975], vol. 1, p. 46: *Seit ich bei meiner letzten Anwesenheit in Berlin merkte, es könne mit Breslau Ernst werden, so setzte ich mich zu Hause hin und arbeitete sehr fleißig um so etwas wie eine Dissertation zur Habilitirung zu arbeiten, und ich fing bei etwas mir ganz neuem an, nämlich bei den Cubischen Resten der Primzahlen* $6n + 1$.

[140] [Kummer 1975], vol. 1, p. 51: "I had also striven from the very beginning for a cubic reciprocity law," which Jacobi stated. (*Einem Reciprocitätsgesetze für cubische Reste habe ich ebenfalls ganz anfangs nachgestrebt.*)

aim was to determine completely which sum corresponds to which root, in analogy with Gauss's determination of the sign of the quadratic Gauss sums.[141] He failed,[142] but did find results allowing him to compute the Gauss sums up to $p = 100$, using in particular analytic techniques in Dirichlet's style.

Studying our paper of reference [Jacobi 1839] would redirect his research. During the autumn of 1844, Kummer obtained a rigorous proof of Jacobi's statement for 5 and extended it to 7. The proofs are based on a study of "complex numbers built from 5th roots of unity" (respectively 7th roots of 1), that is, complex numbers of the form $f(\alpha) = a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4$, for a primitive 5th root of unity α and integer coefficients a_i (or the analogue for 7); for simplicity, we shall call such numbers "5-cyclotomic (or 7-cyclotomic) numbers." The key point of Kummer's proof is that the norm $Nf(\alpha) = f(\alpha)f(\alpha^2)f(\alpha^3)f(\alpha^4)$ allows one to define a Euclidean division on 5-cyclotomic numbers, as was the case for Gaussian integers; adapting the Euclidean algorithm then shows that a prime $p = 5n + 1$ is the norm of a 5-cyclotomic integer, that is a product of four 5-cyclotomic numbers, as desired (with analogous results for 7). Kummer never published these results,[143] but this very same year, he devoted an article to related matters, fittingly published in a volume dedicated by Breslau University to the tercentenary celebration of the University of Königsberg, i.e., Jacobi's university. Here, Kummer studied λ-cyclotomic numbers, this time for an arbitrary prime λ: he showed in particular that the norm $Nf(\alpha) = f(\alpha)f(\alpha^2)\cdots f(\alpha)^{\lambda-1}$, for α a λth root of unity, is congruent to 0 or 1 modulo λ and gave an explicit criterion, based on computations with ordinary integers, to decide if one complex number divides another. But, above all, he produced the first example of a number having *different* decompositions into $\lambda - 1$ *irreducible* cyclotomic factors, for $\lambda = 23$. The stakes are clearly indicated in a communication to the Berlin Academy, on March 26, 1846:

> However, I have noticed that, even if $f(\alpha)$ can in no way be decomposed into complex factors, it yet does not have the true nature of a complex prime number, because it usually lacks the first and most important property of prime numbers: that is, that the product of two prime numbers is not divisible by any prime number different from them. These numbers $f(\alpha)$ thus have the nature of composite numbers even though they are not decomposable into complex factors; but the factors are then not actual, but *ideal complex numbers*.[144]

[141] See [Kummer 1975], vol. 1, pp. 143–144 and p. 145–163. For the normalizations of Gauss sums, and further results, see S.J. Patterson's chap. VIII.2 below. Kummer's point of departure is closely related to art. 358 of the D.A.

[142] It follows from [Heath-Brown, Patterson 1979] that it is not possible to determine the argument of cubic Gauss sums through local informations at a finite number of places (that is, by a finite number of congruences).

[143] Kummer's hitherto lost manuscript has been recovered by Reinhard Bölling; see his commentary and transcription in chap. IV.1 below.

[144] [Kummer 1975], vol. 1, p. 203: *Ich habe nun aber bemerkt, daß, wenn auch $f(\alpha)$ auf keine Weise in complexe Factoren zerlegt werden kann, sie deshalb noch nicht die wahre Natur einer complexen Primzahl hat, weil sie schon gewöhnlich der ersten und wichtigsten*

From then on, Kummer steadily elaborated his theory of ideal complex numbers, which he defined by a set of divisibility properties, in fact a set of congruences. They could be "multiplied" (more exactly: multiplicatively composed) and they provided a substitute for the decomposition of primes into ordinary complex numbers expected by Jacobi. The construction of the theory, its use in the decomposition of primes, the further applications to the proofs of higher reciprocity laws and of Fermat's Last Theorem for regular primes,[145] have been well documented and analyzed,[146] In particular, H. Edwards has reconstructed Kummer's heavy reliance on the "periods" used by Gauss in sec. 7 (which, as sums of roots of $x^\lambda - 1$, are in particular λ-cyclotomic numbers) to establish the properties of divisibility which his theory required; see [Edwards 1977], chap. 4. Kummer referred to the *Disquisitiones Arithmeticae* quite often: for instance, in a synthesis published in French in 1851, he referred to art. 52 (giving the multiplicative structure of the residues modulo a prime number), art. 306 (on cyclic properties of the classes of forms), and art. 358 on cubic residues and equations. The D.A. serves both as a model and as a source of problems to be taken up afresh. Another feature very much in the style of the D.A. is the use of induction and of numerical examples. Sometimes relying on already existing, extensive tables, like Jacobi's *Canon Arithmeticus*, the examples are highly non-trivial and thus do not serve as mere illustrations but, as in the D.A., as inspirations for the understanding of phenomena and the clarification of laws.[147]

Mathematically, Kummer decisively contributed to placing higher reciprocity laws at the center of attention. Reporting in 1850, through Dirichlet, to the Academy on his recent achievements, he said:

> Through my investigations on the theory of complex numbers and its applications to the proof of Fermat's Last Theorem … I succeeded in discovering the general reciprocity laws for arbitrarily high power residues, which are to be regarded, according to the present state of number theory, as the main task and the summit of this science.[148]

Eigenschaft der Primzahlen ermangelt: nämlich, daß das Product zweier Primzahlen durch keine von ihnen verschiedene Primzahl theilbar ist. Es haben vielmehr solche Zahlen $f(\alpha)$, wenn gleich sie nicht in complexe Factoren zerlegbar sind, dennoch die Natur der zusammengesetzten Zahlen; die Factoren aber sind alsdann nicht wirkliche, sondern ideale complexe Zahlen. Notice the distinction introduced here between what we call today "irreducibility" and "primality."

[145] Kummer defined an equivalence relation among ideal complex numbers associated to λ-cyclotomic numbers (more or less saying that two ideal numbers are equivalent if they differ multiplicatively by a usual cyclotomic number); the number of equivalence classes h_λ is finite. A prime λ is regular if it does not divide the class number h_λ. Kummer characterized this condition by an effective test in terms of Bernoulli numbers.

[146] See [Edwards 1975–1977], [Edwards 1977], chaps. 4 and 5, [Edwards 1980], [Neumann 1981], and [Haubrich 1992], chap. 3.

[147] See [Edwards 1977].

[148] [Kummer 1975], vol. 1, p. 346–347: *Bei meinen Untersuchungen über die Theorie der complexen Zahlen und den Anwendungen derselben auf den Beweis des Fermatschen Lehrsatzes … ist es mir gelungen die allgemeinen Reciprocitätsgesetze für beliebig hohe*

Kummer also made available a stock of images and stories concerning number theory. His national German tenor is quite pronounced in this context. In official discourses, but sometimes also in his mathematical papers and reviews, he would insist on what he saw as the German mathematical tradition. For instance, in his announcement of the first volume of Jacobi's *Mathematische Werke*, he described the changing scene of the 1820s like this:

> It was also at that time that Lejeune-Dirichlet returned from France … to Germany, and we proudly count him completely as one of us; for it is the German genius which pulled him back to his fatherland and which gives his works their admirable depth. … As Germans we are certain that we now have the creative force of the *Geist* on our side.[149]

Kummer was also at the origin of some famous anecdotes, like the description of Dirichlet's never putting the D.A. back on the shelf.[150] As we saw in Merz's quote at the beginning of this chapter,[151] later commentators would take their clue from such sources, even if they cut out the explicitly nationalistic component.

Kummer's work on ideal numbers ties together ideas coming particularly from the first sections of the D.A. on congruences and from the last on cyclotomy. Remembering Hermite's approach to Jacobi's problem, it is interesting to understand whether and how Kummer dealt with the sec. 5 on forms. On the one hand, this section operates as a decisive source of inspiration for the key question of equivalence among ideal numbers:

Potenzreste zu entdecken, welche nach dem gegenwärtigen Stande der Zahlentheorie als die Hauptaufgabe und die Spitze dieser Wissenschaft anzusehen sind. One may also recall his famous statement that Fermat's Last Theorem is a curiosity rather than a focal point of science. (*Der Fermatsche Satz ist zwar mehr ein Curiosum als ein Hauptpunkt der Wissenschaft*); see [Kummer 1975], vol. 1, p. 281.

[149] [Kummer 1975], vol. 2, p. 695: *Damals kehrte auch Lejeune-Dirichlet aus Frankreich … nach Deutschland zurück: und wir rechnen ihn mit Stolz ganz zu den Unserigen; denn es ist der deutsche Genius, welcher ihn in sein Vaterland zurückgezogen hat, und welcher seinen wissenschaftlichen Arbeiten ihre bewunderungswürdige Tiefe verleiht. … Wir [Deutschen] sind dessen gewiss, dass wir jetzt die schöpferische Macht des Geistes auf unserer Seite haben.* Another example is provided by his 1856 speech at a Leibniz ceremony.

[150] See [Dirichlet 1889–1897], vol. 2, p. 315, where Kummer also states that the D.A. had a "much more important influence on Dirichlet than his other, Parisian, studies." (*Dieses hat auf seine ganze mathematische Bildung und Richtung einen viel bedeutenderen Einfluß ausgeübt als seine anderen Pariser Studien.*)

[151] Compare for instance Merz with [Kummer 1875], vol. 2, p. 695, where Kummer writes: " the blossoming of the mathematical sciences in Germany dates back to the beginning of the century, when Gauss first appeared on the scene with his *Disquisitiones Arithmeticae*. It towered so much above everything done before in this discipline that at first only very few of the best mathematicians were capable of understanding it. … for a long time he remained in splendid isolation … until about 1826 a new life began in this science for our fatherland, for which Crelle's *Journal* was created as its chief organ. It was then that Jacobi started his investigations on elliptic functions."

> The general investigation of ideal complex numbers has the greatest analogy with the section "on the composition of forms," treated in such a difficult way by Gauss, and the main results which Gauss proved for quadratic forms starting in art. 234 are also valid for the composition of general ideal complex numbers.[152]

However, on the other hand, Kummer perceived his theory of ideal numbers as capable of throwing light in turn on the complicated concept of proper equivalence in Gauss's D.A. Elsewhere, ideal numbers helped him to find the key to the question of irregular determinants.[153] That is, while Hermite's solution was pushing him towards the study of higher forms in order to solve, among others, questions inherited from algebraic numbers and reciprocity laws, Kummer's solution was to develop "ideal complex numbers" to tackle them all. Both the alternative and Kummer's position are very explicit in his 1851 synthesis:

> If one considers the coefficients of a complex number as indeterminates, the norm will represent a homogeneous form of a certain degree, of the kind decomposable into linear factors. The theory of complex numbers amounts in essence to the theory of these forms, and thus belongs to one of the most beautiful branches of higher arithmetic… [But] the discussion of these forms seems to us less simple than that of the complex numbers themselves, which are their factors, their elements so to speak, and of which the analogy with integers is striking.[154]

4.3. Eisenstein and Kronecker on Complex Multiplication

In 1844, Gotthold Eisenstein wrote from Berlin to his friend Moritz Stern in Göttingen: "I am writing up the residues of the 8th, 12th, and also 5th powers, which are finished."[155] Four years later, he would explain that he had not pursued for some time the investigation of decompositions into complex primes, the main theme of

[152] [Kummer 1975], vol. 1, p. 209: *Die allgemeine Untersuchung über die idealen complexen Zahlen hat die größte Analogie mit dem bei* Gauß *sehr schwierig behandelten Abschnitte:* De compositione formarum, *und die Hauptresultate, welche* Gauß *für die quadratischen Formen pag. 337 sqq. bewiesen hat, finden auch für die Zusammensetzung der allgemeinen idealen complexen Zahlen Statt.*

[153] See his 1853 article on this issue, [Kummer 1975], vol. 1, pp. 539–545. Edwards convincingly shows how Kummer's innovative work can be interpretated as a conservative move with respect to the D.A., [Edwards 1977], pp. 152–154: "The Gaussian notion of proper equivalence is something which needs to be saved from [its] appearance of artificiality" and ideal numbers might be this saviour.

[154] [Kummer 1975], vol. 1, p. 363, 366: *Si l'on prend les coefficients du nombre complexe pour des indéterminés, la norme représentera une forme homogène d'un certain degré, du genre de celles qui sont décomposables en facteurs linéaires. La théorie des nombres complexes revient, au fond, à la théorie de ces formes, et à cet égard, elle fait partie d'une des plus belles branches de l'Arithmétique supérieure… [Mais] la discussion de ces formes nous paraît moins simple que celle des nombres complexes eux-mêmes, qui en sont les facteurs, les éléments pour ainsi dire, et dont l'analogie avec les nombres entiers est frappante.*

[155] [Eisenstein 1975], vol. 2, p. 793: *Die Reste der 8ten, 12ten, und auch 5ten Potenzen, welche fertig sind, arbeite ich jetzt aus.*

Jacobi's seminal note [Jacobi 1839], because of tensions with Jacobi. However, in Eisenstein's hands, Jacobi's note would help to kindle the *arithmetic theory of complex multiplication* of elliptic integrals and functions.

An elliptic integral like $u = \int\limits_0^{\varphi} \frac{dx}{\sqrt{(1-x^2)(1-\kappa^2x^2)}}$, or its inverse function, an elliptic function like $\varphi(u,\kappa) = \mathrm{sinam}(u,\kappa)$ (in Jacobi's notation), admits multiplications by rational integers in the sense that, for every integer m, $\mathrm{sinam}(mu,\kappa)$ is a rational function of $\mathrm{sinam}(u,\kappa)$ and its derivative, in the same way that $\sin(mu)$ is a polynomial in $\sin(u)$ and $\cos(u)$.[156] They are said to have *complex multiplication* if there exist multiplications besides those by rational integers. This happens precisely when the ratio of the two basic periods of the elliptic function is an imaginary quadratic irrationality $\sqrt{-n}$, and the transformations in question are then multiplications by complex integers of the form $a + b\sqrt{-n}$, or $a + b\frac{(1+\sqrt{-n})}{2}$, depending on n, with a and b integers.

Examples of such elliptic integrals and functions presented themselves from the very beginning: the integral $\int \frac{dx}{\sqrt{1-x^4}}$ measuring the lemniscatic arc has complex multiplication by Gaussian integers; other elliptic integrals such as $\int \frac{dx}{\sqrt{1 \pm x^3}}$ admit complex multiplications by numbers of the form $a + b\frac{(1+\sqrt{-3})}{2}$.[157] Eisenstein first studied elliptic functions with complex multiplication by the third (or sixth) roots of unity in the context of cubic reciprocity.[158] But while such examples of complex multiplication had been available for some time, their arithmetic theory – albeit inspired by Abel's[159] and Jacobi's works – only took shape after Kummer had introduced

[156] For odd m, the derivative of $\mathrm{sinam}(u,\kappa)$ does not intervene. These functions (or the integrals) admit also more general *transformations*, linking $\varphi(\frac{au+b}{cu+d}, \kappa_1)$ and $\varphi(u,\kappa)$, for different moduli κ_1 and κ, where a, b, c, d are integers with $ad - bc = n > 0$, the *order* of the transformation. Such transformations for integrals were alluded to in §3.4 above. In modern parlance, these transformations are the isogenies between the lattices, or the elliptic curves, associated to elliptic functions. Multiplication by m is obviously a particular case of transformation, with $\kappa_1 = \kappa$ and order m^2.

[157] See for instance [Gauss 1796–1814], September 9, 1796; cf. [Gauss 1900], pp. 93–95. Only these two types of complex multiplication are hinted at in [Jacobi 1839]; they are those for which the complex multipliers are generated by a root of unity.

[158] In the first volume of [Eisenstein 1975], this theme occurs on pp. 80; 89–94 (this 1844 paper picks up [Jacobi 1839] explicitly, and also envisages a possible generalization from elliptic to Abelian functions with complex multiplication by general rings of cyclotomic integers); 111; 389–394; and 454–461 (this last part containing a parallel treatment of complex multiplication by the 4th and the 6th roots of 1). The tension with Jacobi alluded to above is mentioned in [Eisenstein 1975], vol. 2, pp. 506–510, see also [Lemmermeyer 2000], pp. 270–275 and the footnote 74 of H. Pieper's chap. III.1 below.

[159] Beside his resolution of the division equation of the lemniscate mentioned above, Abel remarked in 1828 that the equations for the moduli κ of elliptic integrals with given complex multiplications are solvable by radicals, see [Abel 1881], vol. 1, p. 425–426, and § 1 of C. Houzel's chap. IV.2 below. Note that even Gauss's posthumously published papers did not explicitly anticipate the arithmetic theory of complex multiplication.

ideal numbers in the wake of Jacobi's paper.

A big stride was taken in a long and leisurely article published (in three parts) by Eisenstein in 1850, again in Crelle's journal; see [Eisenstein 1975], pp. 536–619. It starts with Eisenstein's irreducibility criterion, applied to the division equation for the inverse function φ of the integral measuring the lemniscatic arc; see §2 above. But the whole paper revolves around formulae such as

$$\varphi(mt) = \frac{\varphi(t)^{N(m)} + m \cdot P}{1 + m \cdot Q} \tag{1}$$

$$F(k)^{N(n)} = F(nk) + nT \tag{2}$$

The first line states that, for a Gaussian prime number $m \equiv 1 \pmod{2+2i}$, there exist P, Q, polynomials in $\varphi(t)$ with Gaussian integer coefficients, such that (1) holds; the second states that, for a Gaussian prime number $n \equiv 1 \pmod{2+2i}$, and different from m, and for F any polynomial with Gaussian integer coefficients, there exists T, a polynomial with Gaussian integer coefficients, such that (2) holds, when F and T are applied to the roots of the m^{th} division equation of φ; in both formulas, N denotes the norm.

Eisenstein read these identities in two ways: on the one hand, he took them as higher congruences (mod m), resp. (mod n), in the spirit of Gauss's unpublished eighth section[160] and Schönemann's theory, involving the natural, but fundamental, exponentiation ($\varphi(t)^{N(m)}$ and $F(k)^{N(n)}$) which we today view as the Frobenius automorphism with respect to the Gaussian integers modulo m, resp. n. On the other hand, Eisenstein recognized that Kummer's then recent invention of ideal numbers for the cyclotomic integers could be imitated precisely for the algebraic integers generated over the Gaussian numbers by the m^{th} division values of φ,[161] putting into practice his conviction, expressed to Stern in 1844, that the lemniscatic function plays with respect to the complex numbers exactly the same role as the circular and exponential for the real theory.[162]

[160] Like other readers of the D.A., Eisenstein wondered what exactly Gauss had intended to present there; see for instance a note in the margin of his copy of the D.A., art. 62 (in [Ullrich 2001], pp. 208–209, the editor erroneously corrects "Section VIII" into "Section VII"). In his 1850 article, [Eisenstein 1975], vol. 1, footnote on p. 550, he suggested that Gauss might also have wanted to allow certain infinite series to occur in higher congruences. See also the footnote on pp. 559–560, where he suggested improving on Kummer's theory of complex numbers from the point of view of higher congruences. At least today, it is not hard to prove the inductive observation recorded in the last entry of Gauss's mathematical diary using Eisenstein's formulae; cf. [Schappacher 1997], §6. But we have no evidence that anything like this was realized at the time.

[161] [Eisenstein 1975], vol. 1, pp. 574–575, where he wrote in particular that before learning of Kummer's theory, he had found these properties only in a rather clumsy form.

[162] [Eisenstein 1975], vol. 2, p. 797: *die Lemniscaten Funktionen, welche in Bezug auf die complexen Zahlen genau dieselbe Rolle spielen, als die Sinus für die reelle Theorie.* For an ordinary integer m, the roots of the cyclotomic equation over the rationals, $\frac{x^m-1}{x-1}$ are the m^{th} roots of unity, that is $e^{2ik\pi/m}$, i.e., the division values of the exponential.

The end of his paper presents applications to the theory of 8^{th} power residues. Eisenstein developed the Euclidean algorithm for the domain of 8^{th} roots of 1 and derived Jacobi's decomposition of prime numbers $N(m) = p = 8\lambda + 1$ in this domain (where m denotes a Gaussian prime number). He considerably refined the analysis of the factors of this decomposition with the help of polynomial expressions in the m-division values of the lemniscatic function φ and the 8^{th} roots of 1, which behave under permutations of the division values in a way closely analogous to the behaviour of certain resolvents studied by Kummer while trying to find actual complex numbers, in larger domains, which would represent the ideal factors found in the decomposition of primes in cyclotomic fields.[163]

Given Eisenstein's adoption of Kummer's ideal numbers, the continuity with Kronecker is particularly striking. In 1853, Kronecker conceived of what is now called the Kronecker-Weber Theorem – in his terms,[164] "the roots of any Abelian equation with integer coefficients can be expressed as rational functions of roots of unity" – as a direct application of precisely that same article of Kummer on ideal prime numbers that Eisenstein had transposed to the lemniscatic context. Kronecker thought at first that ideal numbers were needed to prove it, and he also generalized his statement immediately to equations abelian *over the Gaussian numbers*, linking them here to the lemniscatic theory.[165] But Kronecker did not stop there. "The subject itself," as he put it, pushed him to study not just the division equations of a particular elliptic function (the analogue over the Gaussian integers of the cyclotomic equation over the rational numbers), but "the arithmetic properties of those moduli" κ for which complex multiplication occurs.[166]

> The elliptic functions for which complex multiplication occurs are situated … between the circular functions and the other elliptic functions. … thus the values of the moduli of that special type of elliptic functions are characterized as limit values by the fact that only for them does the modular equation have multiple roots. Furthermore, while for circular functions there is only multiplication, and for general elliptic functions both multiplication and transformation, for that particular type of elliptic functions, transformation loses in part its peculiar character and turns into a sort of multiplication by ideal numbers. Indeed, as, for an integer p which is represented by the principal form $x^2 + ny^2$ of determinant $-n$, one of the transformations of order p is the multiplication by $x + y\sqrt{-n}$, i.e., $\sin^2 \operatorname{am}\,(x + y\sqrt{-n})u$ is expressed as rational function of $\sin^2 \operatorname{am}\, u$ and κ, one of the transformations of order q, where q is represented by one of the other forms of determinant $-n$, gives a transformed function: $\sin^2 \operatorname{am}(\mu \cdot u, \lambda)$ expressed as a rational function of $\sin^2 \operatorname{am}(u, \kappa)$ and κ, where λ is one of the other moduli for which multiplication by $\sqrt{-n}$ occurs, and μ belongs to a certain value of $\sqrt{-n}$ (mod. q) and thus represents an ideal factor

[163] See [Kummer 1975], vol. I, pp. 211–251.

[164] Kronecker coined this terminology "Abelian equation" in that paper. Today it means that the Galois group of the equation is commutative; but see O. Neumann's chap. II.1 below for the evolution of Kronecker's usage.

[165] [Kronecker 1895–1930], vol. 4, pp. 3–11; [Petri, Schappacher 2004], pp. 234–239 and pp. 252–255.

[166] [Kronecker 1895–1930], vol. 4, p. 209.

> of q. These multipliers: μ are explicit algebraic irrationalities and it is in many ways remarkable that this gives a first example where analysis provides the irrationalities for the representation of ideal numbers.[167]

Extending Kummer's usual cyclotomic frame of reference, Kronecker here, in 1858, thought of ideal numbers of the imaginary quadratic domain of complex multiplication. He remarked that the various classes are represented by (functions of) the various moduli for which complex multiplication by $\sqrt{-n}$ occurs, the so-called "singular moduli."[168] Kronecker came up on the one hand with a list of formulae involving class numbers of binary quadratic forms with negative discriminants, and on the other with an explicit resolution, related to the genera of corresponding quadratic forms, of the modular equations in the case of complex multiplication.[169] For instance, he stated that, if $n \equiv 3 \bmod 4$, $\phi(n)$ the sum of divisors of n which are greater than $\sqrt{n}$, $\psi(n)$ of the remaining divisors, one has $2F(n) + 4F(n-2^2) + 4F(n-4^2) + \ldots = \phi(n) - \psi(n)$, where $F(m)$ denotes the number of classes of binary quadratic forms which are either properly primitive (i.e., $(a, 2b, c)$ are coprime) of determinant $-m$ or a multiple of such forms, the sum on the left being stopped when $n - i^2 = 0$ or < 0. Such formulae would in turn be taken up by Hermite, which nicely closes up our circle of papers inspired by Jacobi's 1839 article, [Jacobi 1839].

[167] [Kronecker 1895–1930], vol. 4, p. 181: *Die elliptischen Functionen, für welche complexe Multiplication stattfindet, stehen ihren wesentlichen Eigenschaften nach zwischen den Kreisfunctionen einerseits und den übrigen elliptischen Functionen anderseits. … so werden auch die Werthe der Moduln jener besonderen Gattung von elliptischen Functionen dadurch als Grenzwerthe charakterisirt, daß nur für diese … die Modulargleichungen gleiche Wurzeln enthalten. Während ferner für die Kreisfunctionen nur Multiplication, für die allgemeinen elliptischen Functionen aber Multiplication und Transformation stattfindet, verliert die Transformation bei jener besondern Gattung elliptischer Functionen zum Theil ihren eigenthümlichen Charakter und wird selbst eine Art Multiplication, indem sie gewissermaaßen die Multiplication mit idealen Zahlen darstellt. Wie nämlich für eine Zahl p, welche sich durch die zur Determinante $-n$ gehörige Hauptform $x^2 + ny^2$ darstellen läßt, eine der Transformationen pter Ordnung die Multiplication mit $x + y\sqrt{-n}$ d.h. die Darstellung von* $\sin^2 \operatorname{am}(x + y\sqrt{-n})u$ *als rationale Function von* $\sin^2 \operatorname{am} u$ *und* κ *gewährt, so ergiebt eine der Transformationen qter Ordnung, wenn q durch eine der übrigen zur Determinante $-n$ gehörigen Formen darstellbar ist, eine transformirte Function:* $\sin^2 \operatorname{am}(\mu \cdot u, \lambda)$ *ausgedrückt als rationale Function von* $\sin^2 \operatorname{am}(u, \kappa)$ *und κ, in welcher λ einer der andern Moduln ist, für welche Multiplication mit $\sqrt{-n}$ stattfindet, in welcher ferner μ zu einem bestimmten Werthe von* $\sqrt{-n}$ (mod. q) *gehört und geradezu die Stelle eines idealen Factors von q vertritt. Diese Multiplicatoren: μ sind explicite algebraische Irrationalitäten und es ist in vielfacher Hinsicht bemerkenswerth, daß hier ein erstes Beispiel gegeben ist, in welchem die Analysis die Irrationalitäten zur Darstellung idealer Zahlen gewährt.*

[168] This sentence is compatible with the language of the 1850s and 1860s as well as with modern presentations of the theory; see for instance [Serre 1967], last theorem in §1.

[169] See [Kronecker 1895–1930], vol. 4, pp. 185–195, cf. [Smith 1859–1865], §§ 130–137, and § 2 (cf. also § 6) of C. Houzel's chap. IV.2 below. An explicit appeal to D.A., art. 227, occurs for instance in [Kronecker 1895–1930], vol. 4, p. 210; see also p. 237.

Kronecker, however, would come back to complex multiplication in a long series of papers from the 1880s,[170] and directly take up Eisenstein's work, and in particular the formulae (1) and (2), in the very context of the quote given above (footnote 167). His "main goal" (*Hauptzielpunkt*) then was to establish – which he does by giving three different proofs – the following vast generalization of (1) and (2)[171] :

$$(-1)^{\frac{1}{2}(n-1)}\sqrt{\lambda}\,\sin\mathrm{am}\,(\mu u,\lambda) \equiv \left(\sqrt{\kappa}\,\sin\mathrm{am}(u,\kappa)\right)^n \pmod{\mu}.$$

Commenting on this formula, Kronecker stressed the simultaneous presence of transformation (indicated by the two moduli: κ and λ) and multiplication (indicated by the multiplier μ).[172] This comment is actually presented as a praise of Jacobi's notation, underscoring the markedly traditional style of this whole series of notes. Contrary to modern reflexes,[173] Kronecker appreciated this formula, not in algebro-geometric terms, but as a quintessential result of arithmetic algebraic analysis: a congruence derived from an algebraic relation involving analytic functions. Already in the long quote above we saw him stress the role of analysis as being able to deliver to arithmetic what is hard or impossible to come by in a purely arithmetic way.[174]

5. In Search of a Discipline

By the middle of the XIX$^{\text{th}}$ century, the *Disquisitiones Arithmeticae* had left its imprint on several areas of mathematical research: in higher arithmetic and in the theory of equations, of course, but also, for instance, in all those domains where determinants or substitutions were used. It had also found new readers: mathematicians who had studied it closely, often early in their careers, who would devote an important part of their professional activities to developing it, and of whom several occupied key positions on the mathematical scene.

[170] They fill almost one third of vol. 4 of Kronecker's Collected Papers.

[171] [Kronecker 1895–1930], vol. 4, pp. 389–471, formula (64), p. 439. The letter n replaces what was called q in the long quote above.

[172] [Kronecker 1895–1930], vol. 4. This two-sidedness is one reason to reject the one-sided interpretation of *Kronecker's Jugendtraum* given in Hilbert's 12$^{\text{th}}$ problem; see Helmut Hasse's *Zusatz 35* in [Kronecker 1895–1930], vol. 5, pp. 510–515. Cf. [Schappacher 1998].

[173] Looked at from the second half of the XX$^{\text{th}}$ century, the formula appears as an ancestor of both the Shimura-Taniyama and the Eichler-Shimura congruence relations; see [Vlăduţ 1991], part I, chaps. 3, 4. Shimura and Taniyama alluded explicitly to Kronecker's formula in [Shimura, Taniyama 1961], sec. 13, p. 110.

[174] This is also a recurring thought in Kronecker's lectures [Kronecker 1901]. At the same time, as is well-known, Kronecker forcefully propagated a general arithmetic which was to actually contain analysis, and a foundational view of mathematics where rigour ultimately should be based only on natural integers, see chap. I.2 and §2.2 of B. Petri's and N. Schappacher's chap. V.2 below. At least the technical parts of his papers on elliptic functions seem unaffected by this creed.

5.1. A Research Field

More specifically, we have called arithmetic algebraic analysis the domain of research directly connected with the D.A. that knit together reciprocity laws, series with arithmetical interpretations, elliptic functions and algebraic equations. We argue that it constituted a (research) *field*, in the sense that "all the people who are engaged in [this] field have in common a certain number of fundamental interests, viz., in everything that is linked to the very existence of the field," and that one can uncover "the presence in the work of traces of objective relations … to other works, past or present, [of the field]."[175]

As we have noticed, its main actors were indeed linked by a dense communication network, both personal and mathematical. Their published papers would meet with prompt reactions; quite a number of these papers were in fact excerpts of letters adressed to another mathematician working in the domain. An interesting characteristic feature was the production of new proofs of the central results, a phenomenon of which we have seen several instances.[176]

A main motto was that of the unity of this specific area and of the strive toward unity of the mathematicians working in it. It is expressed for instance by Gauss himself in his preface to Eisenstein's *Mathematische Abhandlungen* in 1847:

> The higher arithmetic presents us with an inexhaustible store of interesting truths, of truths, too, which are not isolated, but stand in a close internal connexion, and between which, as our knowledge increases, we are continually discovering new and sometimes wholly unexpected ties.[177]

At Hermite's jubilee in 1892, Poincaré, discussing how Hermite "illuminated with a new light the admirable edifice raised by Gauss," added that the merit of his discoveries was increased by the "care that [Hermite] always took to make clearly evident the mutual support that all these sciences, apparently so diverse, provide to each other."[178] In the same way, Kummer emphasized that Dirichlet's "mind [was]

[175] [Bourdieu 1976/2002], p. 115: *tous les gens qui sont engagés dans un champ ont en commun un certain nombre d'intérêts fondamentaux, à savoir tout ce qui est lié à l'existence même du champ*, and p. 116: *Un des indices les plus sûrs de la constitution d'un champ est … la présence dans l'œuvre de traces de relations objectives … aux autres œuvres, passées ou contemporaines [du champ].*

[176] This could go beyond a deliberate attempt to prove a statement published without proof, as in the case of Jacobi's paper discussed above, § 4, or to provide a new perspective on a celebrated result such as the reciprocity law. Since similar results were elaborated independently by different persons, the feeling of an unconscious convergence or repetition of ideas was sometimes expressed: on April 6, 1853, Hermite wrote to Dirichlet about the transformations of an indefinite ternary form into itself, a subject that he had discussed in Berlin with both Eisenstein and Dirichlet: "[it seems] a law of my destiny that all I do in arithmetic is to rediscover some of the discoveries that you have made a long time ago" (Nachlass Dirichlet, Staatsbibliothek zu Berlin-Preussischer Kulturbesitz-Handschriftenabteilung).

[177] Quoted from the English translation offered by Smith at the beginning of his report, [Smith 1859–1865], part I, p. 228.

[178] [Hermite 1893], p. 6: *vous éclairiez d'une lumière nouvelle l'admirable édifice élevé*

always striving toward unity."[179]

This motto was supported by an actual circulation of concepts and methods; for instance, Dirichlet's analytic techniques were used by Kummer, ideal numbers by Eisenstein and Kronecker, while the study of forms along the lines of the section 5 of the D.A. was extended by Dirichlet and Hermite to forms with Gaussian integers as coefficients; Liouville, Charles Joubert, and Hermite took up Kronecker's relations on the number of classes of quadratic forms. Yet another famous connection between algebraic equations and elliptic functions was established in various ways by Hermite, Kronecker, and Francesco Brioschi: the analytic solution of the general quintic equation via suitable modular or multiplier equations.[180] It was also reinforced by translations and texts of a historical or biographical nature.[181] An example of this tight intertwinement is offered for instance by Jules Houël's letter to Dirichlet of April 30, 1857:

> I just finished the translation of your beautiful memoir *Vereinfachung der Theorie der binären quadratischen Formen von positiver Determinante*, the simplicity of which I admire all the more as I am just studying for the first time section 5 of the D.A. M. Lebesgue, who has volunteered to go over my translation, will send it to M. Liouville in a few days. I also translated and submitted to M. Liouville your obituary address on Jacobi which contains an interesting history of the contemporary development of mathematics, a development of which a considerable part is due to that great man.[182]

Specific media played an important role in this process: we have seen how that of

par Gauss.... Le prix de vos découvertes est encore rehaussé par le soin que vous avez toujours eu de mettre en évidence l'appui mutuel que se prêtent les unes aux autres toutes ces sciences en apparence si diverses. Poincaré specifically mentioned number theory, algebraic forms, elliptic functions, and modular equations.

[179] [Dirichlet 1889–1897], vol. 2, p. 327: *In seinem überall zur Einheit strebenden Geiste konnte er diese beiden Gedankensphären nicht neben einander bestehen lassen.* The two "spheres of thought" are analysis and number theory.

[180] See [Petri, Schappacher 2004], §§ 3, 4, and the literature and sources cited there.

[181] Cf. [Bourdieu 1976/2002], pp. 116–117: *Un des indices les plus surs de la constitution d'un champ est, avec la présence dans l'oeuvre de traces de relations objectives ... aux autres oeuvres, passées ou contemporaines [du champ], l'apparition d'un corps de conservateurs de vies ... ou des œuvres. ... Et un autre indice du fonctionnement en tant que champ est la trace de l'histoire du champ dans l'oeuvre.* In the case at hand, the mathematicians themselves served as their own historians and biographers.

[182] Nachlass Dirichlet, Staatsbibliothek zu Berlin, Preussischer Kulturbesitz, Handschriftenabteilung: *Je viens de terminer la traduction de votre beau Mémoire, intitulé: "Vereinfachung der Theorie der binären quadratischen Formen von positiver Determinante," dont j'admire d'autant plus la simplicité que je suis en train d'étudier pour la première fois la section V des Disq. arithm. M. Lebesgue, qui veut bien se charger de revoir ma traduction, l'enverra sous peu de jours à M. Liouville. J'ai également traduit et remis à M. Liouville l'Eloge de Jacobi, qui renferme une histoire intéressante du développement contemporain des mathématiques, développement dont une part bien considérable revient à ce grand homme.* Note that no more than 4 out of 26 pages of this obituary deal with works by Jacobi which lie outside of arithmetic algebraic analysis.

Crelle's *Journal* was recognized by several mathematicians; Genocchi's proof of the reciprocity law published as a memoir of the Belgian Academy in 1852, on the other hand, passed unnoticed until it was recalled in the Paris *Comptes rendus de l'Académie des sciences* thirty years later.[183]

However, we think that it would be misleading to interpret this situation as the establishment of a *discipline* based on the D.A., in the sense of an "object-oriented system of scholarly activities."[184] Indeed, the developments of different parts of the D.A. provided different key objects on which mathematicians could focus their investigations: congruences for some, algebraic integrals for others; ideal numbers or forms; integers or elliptic functions, etc. To each of them in turn divergent key problems were associated, from reciprocity laws to classification issues. While most references to the D.A. at that time would extol the quality of its proofs – their ancient rigour, in Minding's terms – and while some of these proofs constituted technical models to emulate and even mimic, Gauss's demonstrations were also criticized on several grounds, sometimes for their length and complexity, on other occasions for their synthetic nature. The very activity of proof analysis – reflecting on existing proofs in order to fathom their mechanism and simplify their presentation – which sometimes could effectively gather mathematicians of various orientations around the same statement, was not central for all. According to Jacobi,

> [Dirichlet] alone, not I, nor Cauchy, nor Gauss knows what a completely rigorous mathematical proof is, but we know it only from him. When Gauss says he *proved* something, I take it to be very likely, when Cauchy says it, one may bet as much for or against, when Dirichlet says it, it is *certain.* For myself, I prefer not to get involved in these subtleties.[185]

[183] On Genocchi's 1852 memoir and Kronecker's interest in it, see A. Brigaglia's chap. VII.1.

[184] [Guntau, Laitko 1987], p. 26: *gegenstandsorientiertes System wissenschaftlicher Tätigkeiten*. We owe this reference to Ralf Haubrich who, at the 2001 Oberwolfach Conference, suggested characterizing a mathematical discipline by a list of *internal* elements such as its subject matter, its core concepts and theorems, its systematization, its proof system, the mathematical values advocated in evaluating its results, etc. A word of caution may be appropriate here: Thomas Kuhn's description of a "disciplinary matrix," in the Postscript to the second edition of *The Structure of Scientific Revolutions*, could appear to be very similar; however, Kuhn's conception is deliberately anchored in the analysis of communities and groups of practitioners, which, by themselves and by their very existence, delineate the characteristics of this "matrix." For that matter, the cyclotomic equation, with its links to circular functions on the one hand, and to primitive roots modulo a prime on the other, is a perfect *paradigm* in Kuhn's sense (that is, a shared key-example), linking (although perhaps tacitly) the practitioners of arithmetic algebraic analysis. But we want to use the word "discipline" here in the more restricted sense indicated above, just as we have used above the sociologically better defined "field" (*champ*) instead of Kuhn's "community."

[185] See the letter of Jacobi to A.v. Humboldt, December 21, 1846, [Jacobi & Humboldt], p. 99: *Er allein, nicht ich, nicht Cauchy, nicht Gauss weiß, was ein vollkommen strenger mathematischer Beweis ist, sondern wir kennen es erst von ihm. Wenn Gauss sagt, er habe etwas* bewiesen, *ist es mir sehr wahrscheinlich, wenn Cauchy es sagt, ist ebensoviel pro als contra zu wetten, wenn Dirichlet es sagt, ist es* gewiß. Ich *lasse mich auf diese*

The close relation to the D.A. is of course a kind of trade-mark for all these works; but, as we have pointed out on several occasions, different sections, or even articles of the D.A., were privileged and pondered upon by different authors. We have also indicated moves towards giving a more prominent profile and greater independence to formerly amalgamated components of arithmetic algebraic analysis.

5.2. An Academic Discipline

Yet another perspective deserves consideration. The *Disquisitiones Arithmeticae* is a research monograph, but during the first half of the XIX$^{\text{th}}$ century, research results tended rather to be published in shorter papers, whereas the publication of books would be increasingly associated to other genres like, for instance, textbooks or syntheses. Following the thread of textbooks, say, from Minding's treatise on, rather convincingly reveals the constitution of a discipline based on the D.A. Two works, conceived at the end of the 1850s, would incarnate it in the following decades, serving as standard references for the numerous textbooks on number theory from the end of the century:[186] Henry John Smith's *Report on the Theory of Numbers* and Dedekind's first edition of Dirichlet's *Vorlesungen über Zahlentheorie*.

While Peacock in 1834 had integrated the D.A. in a report on analysis, twenty-five years later number theory received an extensive and detailed report by itself at the British Association for the Advancement of Science. Smith had begun to tackle number-theoretical questions in the mid-1850s essentially in Legendre's style. However, his report, published between 1857 and 1865, covered very thoroughly the research from Gauss to Kummer. Smith classified the material under two main headings, following more or less Gauss's table of contents:

> There are two principal branches of the higher arithmetic:– the Theory of Congruences, and the Theory of Homogeneous Forms. … It might, at first sight, appear as if there was not sufficient foundation for the distinction. But in the present state of our knowledge, the methods applicable to, and the researches suggested by these two problems, are sufficiently distinct to justify their separation from one another. … Those miscellaneous investigations, which do not properly come under either of them, we shall place in a third division by themselves.[187]

Richard Dedekind adopted roughly the same presentation when in 1863 he edited Dirichlet's Göttingen lectures of 1857–58 for the first time:[188] after a first chapter on general properties of integers, as in Minding, two chapters are devoted to congruences and two others to binary quadratic forms, while miscellanea, including results on the cyclotomic equation, are exiled into several supplements.

Delicatessen lieber gar nicht ein. On the idea of proof analysis and Dirichlet's importance for this issue, see [Haubrich 1992], p. 14.

[186] In his 1890 survey on number theory, for instance, Thomas Stieltjes would recognize his debts to both of them and two years later George Mathews would write in his own book that "he derived continual assistance" from them; for these examples and others, see the following chap. I.2.

[187] [Smith 1859–1865], pp. 39–40.

[188] On the *Vorlesungen über Zahlentheorie*, see [Goldstein 2005].

In both cases, novel developments were forced into this bipartite scheme, the D.A. giving the lead to the whole text. Smith is explicit about it:

> Instead of confining our attention exclusively to the most recent researches in the Theory of Quadratic Forms, we propose … to give a brief but systematic *résumé* of the theory itself, as it appears in the Disq. Arith., introducing in their proper places, notices, … of the results obtained by later mathematicians. We adopt this method, partly to render the later researches themselves more easily intelligible, by showing their connexion with the whole theory; but partly also in the hope of facilitating to some persons the study of the Fifth Section of the Disq. Arith.[189]

Similarly, Smith presented Kummer's ideal numbers in the section on higher congruences, in connection with reciprocity laws. Dirichlet's chapters on quadratic forms integrate his simplifications of the D.A. on this topic, as well as his class number formula. But several analytic lemmas and his theorem on primes in arithmetical progressions are relegated to the supplements, just as Smith relegated Jacobi's theta functions and their applications to quadratic forms to the end of his report.[190]

Gauss's strong impact on shaping survey publications can be measured *a contrario* by two other books on number theory published around 1850. That of Eugène Desmarest, a pharmacist and amateur number-theorist, [Desmarest 1852], is mostly devoted to exhibiting effective, "practical" solutions to quadratic Diophantine equations. Despite its Legendre-like appearance, it was only with respect to Gauss's D.A. that Desmarest felt the need in 1852 to justify the "foolhardiness," as he put it, of his encompassing title *Théorie des nombres*. And although he rejected Gauss's notation for congruences, he did organize his treatise into a first part on the resolution of binary quadratic equations modulo a prime number, a second part on the representation of numbers by binary quadratic forms (including proper and improper equivalence), finally applying them in a third part to his main problem.

As for Pafnuti L. Čebyšev, who published in 1849 a treatise on the theory of

[189] [Smith 1859–1865], p. 169.

[190] It is interesting to contrast the situation of analytic methods here with what Kummer said about them at the same time, in Dirichlet's obituary of 1860: "that in those applications, analysis would be made to serve number theory in such a way that it does not just yield coincidentally some isolated results, but is bound to yield with necessity the solutions to certain general types of problems of arithmetic as yet inaccessible in other ways," and thus that "these methods of Dirichlet's … would have to be recognized as the creation of a new mathematical discipline, if they extended not just to certain types of problems but uniformly to all problems of number theory" ([Dirichlet 1889–1897], vol. 2, p. 327: *in ihnen die Analysis der Zahlentheorie in der Art dienstbar gemacht wird, dass sie nicht mehr nur zufällig manche vereinzelte Resultate für dieselbe abwirft, sondern dass sie die Lösungen gewisser allgemeiner Gattungen, auf anderen Wegen noch ganz unzugänglicher Probleme der Arithmetik mit Notwendigkeit ergeben muss. … sie würden auch … als Schöpfung einer neuen mathematischen Disciplin anerkannt werden müssen, wenn sie sich nicht bloss auf gewisse Gattungen, sondern auf alle Probleme der Zahlentheorie gleichmässig erstreckten.*) A proper research discipline, centered around Dirichlet series, but encompassing neither all number theory, nor arithmetic algebraic analysis, would flourish in the second half of the century.

congruences based on his Saint-Petersburg dissertation, he was of course no marginal figure like Desmarest, but his keen regard for practical applications of mathematics put his own papers mostly outside of arithmetic algebraic analysis. In his number-theoretical papers from the 1850s,[191] he refers to Dirichlet, but not to the *Disquisitiones Arithmeticae*. At the same time, he was coediting Leonhard Euler's number theoretical memoirs with Viktor Yakovlevič Bunyakovski. In his own book, he elected neither Diophantus, nor Fermat, nor Gauss, but Euler as the father of number theory. He claimed in the preface not to follow Legendre or Gauss – implicitly, however, he used the *Disquisitiones Arithmeticae* to restructure Euler's results:

> Among Euler's numerous investigations in the domain of number theory, the memoirs which had the most important influence on the success of this science are those on the two following topics: (1) On the powers of numbers considered with respect to their residues when divided by a given number. (2) On numbers that are represented as a sum of two numbers, of which one is a square and the other is the product of a square by a given number. The memoirs on the first topic provided the basis of the theory of indices, of the theory of binomial congruences in general and of quadratic residues in particular; the memoirs on the second topic built the beginning of the theory of quadratic forms.[192]

His book focuses on the first part, congruences, quadratic forms appearing as a subsection in the chapter on quadratic congruences, while his own analytic results were put at the end and were eventually omitted from the German translation.

To summarize, the role of the *Disquisitiones Arithmeticae* in the constitution of number theory fifty years after its publication was two-fold. On the one hand, the D.A. provided number theory with the features of its self-organization[193] as an academic discipline. It shaped what number theory[194] was and ought to be: congruences

[191] Where he proved Bertrand's postulate, a result on the mean values of arithmetical functions, and the fact that if $\pi(x) \cdot \frac{\log x}{x}$, where $\pi(x)$ denotes the number of primes less than x, has a limit as x tends to ∞, then this limit has to be 1.

[192] From the preface of [Čebyšev 1849]: Между многими изысканиями Эйлера в теории чисел наиболее имели влияния на успех этой науки изыскания его по следующим двум предметам: 1) о степенях чисел в отношении остатков, получаемых при делении их на данное число, и 2) о числах, представляющих сумму двух чисел, из которых одно есть квадрат, а другое произведение квадрата на данное число. Первые положили основание теории указателей, сравнений двучленных вообще и в особенности теории квадратичных вычетов; вторые были началом теории квадратичных форм. Hearty thanks to Ilia Itenberg, Strasbourg, for finding this original citation, and advising us on the translation.

[193] Cf. Rudolf Stichweh, *Zur Entstehung des modernen Systems wissenschaftlicher Disziplinen. Physik in Deutschland 1740–1890.* Frankfurt: Suhrkamp, 1984, chap. I: "The differentiation of disciplines … is a mechanism of self-organization of the system."

[194] Ralf Haubrich has coined the expression "Gaussian Number Theory" to designate this core. We would like to stress that in the middle of the century, as the titles of books witness, it was intended to be seen as "Number Theory" *per se*. Even Diophantine analysis bore its marks. "Gaussian" thus is meant to allude to the role of the D.A. to

and forms with integer coefficients (with their possible generalizations). This image informed advanced textbooks and helped to structure them, and it would, for an even longer time, structure classifications of mathematics. On the other hand, the D.A. had launched an active research field, with a firm grasp on number theory, algebra and analysis, supported by close and varied readings of the book. It provided the field with technical tools, and a stock of proofs to scrutinize and adapt. It also provided concrete examples of the very links between different branches of mathematics that created the field, often articulated around richly textured objects and formulae, such as the cyclotomic equation or Gauss sums. The (meta)stability of the field was not guaranteed by any unicity of purpose or concept (individual mathematicians might have their own priorities, mix differently the resources available or disregard some of them), nor by a merging into a larger domain,[195] but by a constant circulation from one branch to another, a recycling of results and innovations. How certain branches emancipated themselves, and with which consequences for number theory and for the role of the D.A., will be the subject of the next chapter.

References

Abel, Niels Henrik. 1881. *Œuvres complètes*, ed. L. Sylow, S. Lie. 2 vols. Christiania: Grøndahl & Søn.

———. 1902. *Mémorial publié à l'occasion du centenaire de sa naissance*. Kristiania: Jacob Dybwad; Paris: Gauthier-Villars; Leipzig: Teubner; London: Williams & Norgate.

Babbage, Charles. 1813. Preface. *Memoirs of the Analytical Society* 1, i-xxii. Repr. in *Science and Reform. Selected Works of Charles Babbage*, ed. A. Hyman, pp. 11–34. Cambridge: Cambridge University Press, 1989.

Bachmann, Paul. 1911. *Über Gauß' zahlentheoretische Arbeiten*. Leipzig: Teubner. Repr. slightly revised in [Gauss 1922–1933], Abhandlung 1.

Barlow, Peter. 1811. *An Elementary Investigation of the Theory of Numbers, with its application to the indeterminate and diophantine analysis, the analytical and geometrical division of the circle and several other curious algebraical and arithmetical problems*. London: Johnson.

Belhoste, Bruno. 1991. *Augustin-Louis Cauchy. A Biography*. New York, etc.: Springer-Verlag.

———. 1996. Autour d'un mémoire inédit: la contribution d'Hermite au développement de la théorie des fonctions elliptiques. *Revue d'Histoire des mathématiques* 2, 1–66.

Betti, Enrico. 1903. *Opere matematiche,* vol. I, ed. Reale Accademia dei Lincei. Milano: Ulrico Hoepfli.

Biermann, Kurt-R. 1977. Aus unveröffentlichten Aufzeichnungen des jungen Gauß (zum 200. Geburtstag von C.F. Gauß). *Wissenschaftliche Zeitschrift der Technischen Hochschule Ilmenau* 4, 7–24.

———. 1988. *Die Mathematik und ihre Dozenten an der Berliner Universität 1810–1933*. Berlin: Akademie-Verlag.

shape, but not to qualify or restrict its domain.

[195] The situation is thus markedly different from the earlier period, see § 2 above, when some of the contents of the D.A. merged into algebra.

Boncompagni, Baldassare. 1882. Intorno alla vita ed ai lavori di Antonio Carlo Marcellino Poullet-Delisle. *Bullettino di Bibliografia e Storia delle Scienze Matematiche e Fisiche* 15, 670–678.

Bos, Henk J. M., Kers, Cees, Oort, Franz, Raven, Diederik W. 1987. Poncelet's Closure Theorem, its history, its modern formulation, a comparison of its modern proof with those by Poncelet and Jacobi, and some mathematical remarks inspired by these early proofs. *Expositiones Mathematicae* 5, 289–364.

Bourdieu, Pierre. 1976. Quelques propriétés des champs. Exposé à l'ENS, novembre 1976. In *Questions de sociologie*, pp. 113–120. Paris: Les Editions de Minuit, 2002.

Bühler, Walter Kaufmann. 1981. *Gauss. A Biographical Study.* Berlin, Heidelberg, etc.: Springer.

Bullynck, Maarten. 2006a. A Note on Article 36 in Gauss's *Disquisitiones Arithmeticae*. A Ramified Story in the Margin of the Re-Writing of Section II. *Bulletin of the Belgian Mathematical Society. Simon Stevin*, to appear.

———. 2006b. *Vom Zeitalter der Formalen Wissenschaften. Anleitung zur Verarbeitung von Erkenntnissen anno 1800, vermittelst einer parallelen Geschichte*. Thesis, Universiteit Ghent. Ghent.

Cajori, Florian. 1928–1929. *A History of Mathematical Notations*. 2 vols. Chicago: Open Court.

Cauchy, Augustin-Louis. 1813–1815. Démonstration du théorème général de Fermat sur les nombres polygones. *Mémoires des sciences mathématiques et physiques de l'Institut de France* 14, 1st ser., 177–220. Repr. in *Œuvres complètes*, ed. Académie des sciences, 2nd ser., vol. 6, pp. 320–353. Paris: Gauthier-Villars, 1887.

———. 1815. Mémoire sur les fonctions qui ne peuvent obtenir que deux valeurs égales et de signes contraires par suite des transpositions opérées entre les variables qu'elles renferment. *Journal de l'Ecole polytechnique* 17e cahier, 10, 29–97. Repr. in *Œuvres complètes*, ed. Académie des sciences, 2nd ser., vol. 1, pp. 91–169. Paris: Gauthier-Villars, 1905.

———. 1840. Mémoire sur la théorie des nombres. *Mémoires de l'Académie des Sciences* 17, 249–768. Repr. in *Œuvres complètes*, ed. Académie des sciences, Ist ser., vol. 3, pp. 5–449. Paris: Gauthier-Villars, 1911.

Čebyšev, Pafnuti Lvovič. 1849. *Teoria sravnenii.* Sanktpetersburg: Tipographia Akademii Nauk. German transl. by H. Schapira: *Theorie der Congruenzen. Elemente der Zahlentheorie*. Berlin: Mayer & Müller, 1889; repr. 1902.

Décaillot, Anne-Marie. 1999. *Edouard Lucas (1842–1891): le parcours original d'un scientifique français dans la deuxième moitié du XIXe siècle*. Thèse de l'université René Descartes. Paris.

Dedekind, Richard. 1930–1932. *Gesammelte mathematische Werke*, ed. E. Noether, R. Fricke, O. Ore. 3 vols. Braunschweig: Vieweg.

Delambre, Jean-Baptiste Joseph. 1810. *Rapport historique sur les progrès des sciences mathématiques depuis 1789, et sur leur état actuel.* Paris: Imprimerie impériale.

Desmarest, Eugène. 1852. Théorie des nombres, Traité de l'analyse indéterminée du second degré à deux inconnues, suivi de l'application de cette analyse à la recherche des racines primitives, avec une table de ces racines pour tous les nombres premiers compris entre 1 et 10000. Paris: Hachette.

Dickson, Leonard Eugene. 1919–1923. *History of the Theory of Numbers.* 3 vols. Washington: The Carnegie Institute. Repr. New York: Chelsea, 1956.

Dirichlet, Johann Peter Gustav Lejeune-. 1863. *Vorlesungen über Zahlentheorie*, ed. R. Dedekind. Braunschweig: Vieweg. English transl. J. Stillwell. History of Mathematics Sources 16. Providence: AMS, London: LMS, 1999.

———. 1889–1897. *Werke*, ed. L. Kronecker, L. Fuchs. 2 vols. Berlin: Reimer.

Dirksen, Enno Heeren. 1845. *Organon der gesammten transcendenten Analysis. Erster Theil. Transcendente Elementarlehre.* Berlin: Reimer.

Dunnington, Guy Waldo. 1955. *Carl Friedrich Gauss, Titan of Science. A Study of his Life and Work.* New York: Exposition Press. Repr. (with additional material by J. Gray and F.-E. Dohse). The Mathematical Association of America, 2004.

Edwards, Harold M. 1975–1977. The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes. *Archive for History of Exact Sciences* 14, 219–236. Postscript to "The Background of Kummer's Proof …." *Archive for History of Exact Sciences* 17, 381–394

———. 1977. *Fermat's Last Theorem. A Genetic Introduction to Algebraic Number Theory.* New York: Springer.

———. 1980. The Genesis of Ideal Theory. *Archive for History of Exact Sciences* 23, 321–378.

Eisenstein, Gotthold. 1975. *Mathematische Werke*. 2 vols. New York: Chelsea.

Ewald, William Bragg. 1996. *From Kant to Hilbert, A Source Book in the Foundations of Mathematics*. 2vols. Oxford: Clarendon Press.

Folkerts, Menso. 1983–1984. Der Mathematiker E.H. Dirksen und C.F. Gauß. *Mitteilungen der Gauß-Gesellschaft Göttingen* 20–21, 66–76.

Galois, Évariste. 1962. *Écrits et mémoires mathématiques*, ed. R. Bourgne, J.-P. Azra. Paris: Gauthier-Villars.

Gauss, Carl Friedrich. 1796–1814. [Mathematical Diary.] Original manuscript in Latin: Handschriftenabteilung Niedersächsische Staats- und Universitätsbibliothek Göttingen, Cod. Ms. Gauß Math. 48 Cim. 1st comm. ed. F. Klein: Wissenschaftliches Tagebuch 1796–1914. *Festschrift zur Feier des hundertfünfzigjährigen Bestehens der Königlichen Gesellschaft der Wissenschaften zu Göttingen.* Berlin: Weidmann, 1901. Repr. *Mathematische Annalen* 57 (1903), 1–34. 2nd comm. ed.: Abdruck des Tagebuchs (Notizenjournals) (with Fac-simile). In [Gauss 1917], pp. 483–575. Ed. with German transl. by E. Schuhmann, a historical introduction by K.-R. Biermann, and new annotations by H. Wußing und O. Neumann: *Mathematisches Tagebuch 1796–1814.* 5th ed. Ostwalds Klassiker der exakten Wissenschaften 256. Leipzig: Akademische Verlagsgesellschaft Geest & Portig; Frankfurt a.M., Thun: Harry Deutsch, 2005. French comm. transl. P. Eymard, J.-P. Lafon: Le journal mathématique de Gauss. *Revue d'histoire des sciences et de leurs applications* 9 (1956), 21–51.English comm. transl. J. Gray: A commentary on Gauss's mathematical diary, 1796-1814, with an English translation. *Expositiones Mathematicae* 2 (1984), 97–130. Repr. in [Dunnington 1855/2004], pp. 409-505.

———. 1863. *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universitäts-Druckerei. 2nd augm. ed., 1876.

———. 1866. *Werke*, vol. III, *Analysis*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universitäts-Druckerei.

———. 1900. *Werke*, vol. VIII, *Arithmetik und Algebra: Nachträge zu Band 1–3*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Leipzig: Teubner.

———. 1917. *Werke*, vol. X.1, *Nachtraege zur reinen Mathematik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Leipzig: Teubner.

———. 1922–1933. *Werke*, vol. X.2, *Abhandlungen über Gauß' wissenschaftliche Tätigkeit auf den Gebieten der reinen Mathematik und Mechanik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Berlin: Springer.

GAUSS, Carl Friedrich & GERLING, Christian Ludwig. 1927. *Briefwechsel zwischen Carl Friedrich Gauß und Christian Ludwig Gerling*, ed. C. Schäfer. Berlin: Elsner. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 3. Hildesheim: Olms, 1975.

GAUSS, Carl Friedrich & OLBERS, Wilhelm. 1900–1909. *Briefwechsel zwischen Olbers und Gauß*, ed. C. Schilling and I. Kramer. *Wilhelm Olbers, sein Leben und seine Werke*, ed. C. Schilling, vol. 2. Berlin: J. Springer. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 4. 2 parts. Hildesheim: Olms, 1976.

GAUSS, Carl Friedrich & SCHUMACHER, Heinrich C. 1860–1865. *Briefwechsel.* 6 vols, ed. C.A.F. Peters. Altona: Esch. Repr. Hildesheim: Olms, 1975.

GEERTZ, Clifford. 1973. Thick Description: Toward an Interpretative Theory of Culture. In *The Interpretation of Cultures: Selected Essays*, pp. 3–30. New York: Basic.

GOLDSTEIN, Catherine. 1989. Le métier des nombres aux 17^{e} et 19^{e} siècles. In *Éléments d'Histoire des Sciences*, ed. M. Serres, pp. 274–295. Bordas: Paris. English transl. in *A History of Scientific Thought*, pp. 344–371. Oxford: Blackwell, 1995.

———. 2003. Les *Disquisitiones Arithmeticae* en France: un parcours de recherche. *Revue de la Bibliothèque nationale de France* 14, 48–55.

———. 2005. The *Vorlesungen über die Zahlentheorie* by P. G. Dirichlet. In *Landmarks of the History of Mathematics*, ed. I. Grattan-Guinness, pp. 480–490. Amsterdam: Elsevier.

GUNTAU, Martin, LAITKO, Hubert. 1987. Entstehung und Wesen wissenschaftlicher Disziplinen. In *Der Urspung der modernen Wissenschaften. Studien zur Entstehung wissenschaftlicher Disziplinen*, ed. M. Guntau, H. Laitko, pp. 17-89. Berlin: Akademie-Verlag.

HARTMANN, Klaus. 1972. Hegel: A non-metaphysical view. In *Hegel. A collection of criticial essays*, ed. A. MacIntyre, pp. 101–124. Garden City, NY: Anchor Books, Doubleday.

HAUBRICH, Ralf. 1992. *Zur Entstehung der algebraischen Zahlentheorie Richard Dedekinds.* Dissertation, Georg-August-Universität Göttingen. Göttingen.

HEATH-BROWN, David Rodney, PATTERSON, Samuel James. 1979. The distribution of Kummer sums at prime arguments, *Journal für die Reine und Angewandte Mathematik* 310, 111–130.

HEGEL, Georg Wilhelm Friedrich. 1801. *Differenz des Fichte'schen und Schelling'schen Systems der Philosophie.* Jena: Seidler. Repr. Philosophische Bibliothek 62a. Hamburg: Meiner, 1962.

———. 1812–1816. *Wissenschaft der Logik.* 2 vols. in 3 books. Nürnberg: J.L. Schrag. Repr. Philosophische Bibliothek 377. Hamburg: Meiner, 1986–1994.

HERMITE. 1893. *1822–1892. Jubilé de M. Hermite.* Paris: Gauthier-Villars.

HOUZEL, Christian. 1978. Fonctions elliptiques et intégrales abéliennes. In *Abrégé d'histoire des mathématiques 1700–1900*, J. Dieudonné (ed.), vol. II, pp. 1–113. Paris: Hermann.

JACOBI, Carl Gustav Jacob. 1829. *Fundamenta nova theoriae functionum ellipticarum.* Königsberg: Gebrüder Borntraeger. Repr. in [Jacobi 1881–1891], vol. 1, pp. 49–239.

———. 1836–1837. *Theorie der Zahlen.* Lecture notes by J.G. Rosenhain, copied by hand.[196]

———. 1839. Über die complexen Prinzahlen, welche in der Theorie der Reste der 5$^{\text{ten}}$, 8$^{\text{ten}}$ und 12$^{\text{ten}}$ Potenzen zu betrachten sind. *Monatsbericht der Akademie der Wissenschaften zu Berlin* Mai 1839, pp. 86–91. Repr. in *Journal für die reine und angewandte Mathematik* 19 (1839), 314–318. Repr. in [Jacobi 1881–1891], vol. 6, pp. 275–280. French transl. *Journal de mathématiques pures et appliquées* 8 (1843), 268–272.

———. 1881–1891. *Gesammelte Werke,* ed. C.W. Borchardt, K. Weierstrass. 7 vols. Berlin: Reimer.

JACOBI & HUMBOLDT. 1987. *Briefwechsel zwischen Alexander von Humboldt und Carl Gustav Jacob Jacobi*, ed. H. Pieper. Berlin: Akademie-Verlag.

JAHNKE, Hans Niels. 1990. *Mathematik und Bildung in der Humboldtschen Reform.* Studien zur Wissenschafts-, Sozial- und Bildungsgeschichte der Mathematik 8. Göttingen: Vandenhoeck & Ruprecht.

JORDAN, Camille. 1870. *Traité des substitutions et des équations algébriques.* Paris: Gauthier-Villars.

KIERNAN, B. Melvin. 1971. The Development of Galois Theory from Lagrange to Artin. *Archive for History of Exact Sciences* 8, 40–154.

KÖNIGSBERGER, Leo. 1904. *Carl Gustav Jacob Jacobi. Festschrift zur Feier der hundertsten Wiederkehr seines Geburtstags.* Leipzig: Teubner.

KRONECKER, Leopold. 1891. Vorlesungen Sommersemester 1891. Manuscript: Strasbourg: Bibliothèque de l'IRMA. Ed. in J. Boniface & N. Schappacher, "Sur le concept de nombre dans la mathématique". Cours inédit de Leopold Kronecker à Berlin (1891). *Revue d'Histoire des mathématiques* 7 (2001), 207–275.

———. 1901. *Vorlesungen über Zahlentheorie*, vol. 1, ed. K. Hensel. Leipzig: Teubner. Repr. Berlin, Heidelberg, New York: Springer, 1978.

———. 1895–1930. *Werke*, ed. K. Hensel. 5 vols. Leipzig: Teubner. Repr. New York: Chelsea, 1968.

KUMMER, Ernst Eduard. 1975. *Collected Papers*, ed. A. Weil. 2 vols. Berlin, Heidelberg, etc.: Springer.

LACROIX, Sylvestre François. 1804. *Complément des Élemens d'algèbre, à l'usage de l'École centrale des quatre-nations.* 3$^{\text{rd}}$ ed. Paris: Courcier.

LAGRANGE, Joseph Louis. 1770 (an VI). *Traité de la résolution des équations numériques de tous les degrés.* Paris: Duprat. 2$^{\text{nd}}$ ed., Paris: Courcier, 1808. Repr. in [Lagrange 1867–1892], vol. 8, pp. 1-370. 3$^{\text{rd}}$ ed., with [Poinsot 1808], Paris: Bachelier, 1826.

———. 1867–1892. *Œuvres*, ed. J.-A Serret. 14 vols. Paris: Gauthier-Villars, 1879. Repr. Hildesheim, New York: Olms, 1973.

LAMBERT, Johann Heinrich. 1764. *Neues Organon oder Gedanken über die Erforschung und Bezeichnung des Wahren und dessen Unterscheidung vom Irrthum und Schein.* Leipzig: Johann Wendler.

[196] We have used the 2 copies kept at the library of IRMA, Strasbourg: n$^{\text{o}}$ L 2244 (former property of Hesse, Weierstrass) and n$^{\text{o}}$ L 3052 (former property of Kronecker, Hensel). Quotes follow the spelling and the page-by-page numbering of the former.

———. 1770. *Zusätze zu den logarithmischen und trigonometrischen Tabellen zur Erleichterung und Abkürzung der bey Anwendung der Mathematik vorfallenden Berechnungen*. Berlin: Haude und Spener. Repr. in *Opera mathematica*, ed. A. Speiser, vol. 2, pp. 1–111. Zürich: Orell Füssli, 1948.

———. 1771. *Anlage zur Architectonic, oder Theorie des Ersten und des Einfachen in der philosophischen und mathematischen Erkenntniß*. Riga: Hartknoch.

LAUBENBACHER, Reinhard, PENGELLEY, David. 1998. *Mathematical Expeditions: Chronicles by the Explorers*. New York: Springer.

LEGENDRE, Adrien-Marie. 1788. Recherches d'analyse indéterminée. *Histoire de l'Académie royale des sciences de Paris. Année 1785*, Mémoires, 465–559.

———. 1798. *Essai sur la théorie des nombres*. Paris: Duprat. Repr. with suppl., 1816. 2nd augm. ed. Paris: Courcier, 1808; supplements, 1825.

———. 1811. *Exercices de calcul intégral sur divers ordres de transcendantes et sur les quadratures*. Paris: Courcier.

———. 1825–1828. *Traité des fonctions elliptiques et des intégrales Euleriennes avec des tables pour en faciliter le calcul numérique*. 3 vols. Paris: Huzard-Courcier.

———. 1830. *Théorie des nombres*. 2 vols. Paris: Didot.

LEBESGUE, Victor-Amédée. 1837. Recherches sur les nombres. *Journal de mathématiques pures et appliquées* 2, 253-292.

LEMMERMEYER, Franz. 2000. *Reciprocity Laws from Euler to Eisenstein*. Berlin, etc.: Springer.

LUCAS, Edouard. 1891. *Théorie des nombres*. Paris: Gauthier-Villars.

MAENNCHEN, Philipp. 1930. *Gauß als Zahlenrechner*. In [Gauss 1922–1933], Abhandlung 6.

MERZ, John Theodor. 1896–1914. *A History of European Thought in the Nineteenth Century*. 4 vols. Edinburgh, London: Blackwood and sons.

MERZBACH, Uta C. 1981. An Early Version of *Disquisitiones Arithmeticae*. In *Mathematical Perspectives, Essays on mathematics and its historical development presented to Prof. Dr. Kurt-R. Biermann on the occasion of his 60th birthday*, ed. J. Dauben, pp. 167–177. New York etc.: Academic Press.

MILNOR, John. 1971. *Introduction to Algebraic K-Theory*. Annals of Mathematics Studies 72. Princeton: Princeton University Press.

MINDING, Ferdinand. 1832. *Anfangsgründe der höheren Arithmetik*. Berlin: Reimer.

NEUKIRCH, Jürgen. 1999. *Algebraic Number Theory*. Grundlehren der mathematischen Wissenschaften 322. Berlin, etc.: Springer.

NEUMANN, Olaf. 1979–1980. Bemerkungen aus heutiger Sicht über Gauss' Beiträge zu Zahlentheorie, Algebra und Funktionentheorie. *NTM-Schriftenreihe* 16:2, 22–39; 17:1, 32–48; 17:2, 38–58.

———. 1981. Über die Anstöße zu Kummers Schöpfung der "Idealen Complexen Zahlen." In *Mathematical Perspectives, Essays on mathematics and its historical development presented to Prof. Dr. Kurt-R. Biermann on the occasion of his 60th birthday*, ed. J. Dauben, pp. 179–199. New York etc.: Academic Press.

———. 2005. Carl Friedrich Gauss's *Disquisitiones Arithmeticae* (1801). In *Landmark Writings in Western Mathematics, 1640–1940*, ed. I. Grattan-Guinness, pp. 303–315. Amsterdam: Elsevier.

ORE, Oystein. 1957. *Niels Henrik Abel. Mathematician Extraordinary.* Minneapolis: University of Minnesota Press. Repr. New York: Chelsea 1974.

PEACOCK, George. 1834. Report on the Recent Progress and Present State of Certain Branches of Analysis. In *Report on the Third Meeting of the British Association for the Advancement of Science held at Cambridge in 1833*, pp. 185–352. London: Murray.

PETRI, Birgit, SCHAPPACHER, Norbert. 2004. From Abel to Kronecker. Episodes from 19th Century Algebra. In *The Legacy of Niels Henrik Abel*, ed. O.A. Laudal & R. Piene, pp. 227–266. Berlin, etc.: Springer.

POINSOT, Louis. 1808. [Review of] Traité de la résolution des équations numériques de tous les degrés … par J. L. Lagrange. *Magazin encyclopédique, ou Journal des sciences, des lettres et des arts* 4, 343–375. Repr. in [Lagrange 1770/1826], pp. v–xx.

———. 1819–1820. Mémoire sur l'application de l'algèbre à la théorie des nombres. *Mémoires de l'Académie royale des sciences. Années 1829 et 1820* (1824), 99–183.

REICH, Karin. 1996. Frankreich und Gauss, Gauss und Frankreich. Ein Beitrag zu den deutsch-französischen Wissenschaftsbeziehungen in den ersten Jahrzehnten des 19. Jahrhunderts. *Berichte zur Wissenschaftsgeschichte* 19, 19–34.

———. 2000. Die Entdeckung und frühe Rezeption der Konstruierbarkeit des regelmäßigen 17-Ecks und dessen geometrische Konstruktion durch Johannes Erchinger (1825). In *Mathesis. Festschrift zum siebzigsten Geburtstag von Matthias Schramm*, ed. R. Thiele, pp. 101–118. Berlin: Diepholz.

RIEGER, Georg Johann. 1957. Die Zahlentheorie bei C.F. Gauss. In *C.F. Gauss 1777–1855. Gedenkband anlässlich des 100. Todestages am 23. Februar 1955*, ed. H. Reichardt, pp. 37–77. Leipzig: Teubner.

RITTER, Joachim, GRÜNDER, Karlfried (eds.). 1998. *Historisches Wörterbuch der Philosophie*, vol. 10, St–T. Basel: Schwabe & Co.

SCHAPPACHER, Norbert. 1997. Some Milestones of Lemniscatomy. In *Algebraic Geometry. Proceedings Bilkent Summer School, Ankara 1995*, ed. S. Sertöz, pp. 257–290. Lecture Notes in Pure and Applied Mathematics Series 193. New York: Marcel Dekker.

———. 1998. On the History of Hilbert's Twelfth Problem. A comedy of errors. In *Matériaux pour l'histoire des mathématiques au XX^{e} siècle. Actes du colloque à la mémoire de Jean Dieudonné (Nice, 1996)*, pp. 243–273. Séminaires et Congrès 3. Paris: Société Mathématique de France.

SCHLESINGER, Ludwig. 1922. *Über Gauß' Arbeiten zur Funktionentheorie.* In [Gauss 1922–1933], Abhandlung 2.

SCHÖNEMANN, Theodor. 1845. Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist. *Journal für die reine und angewandte Mathematik* 31, 269–325.

———. 1846. Von denjenigen Moduln, welche Potenzen von Primzahlen sind. *Journal für die reine und angewandte Mathematik* 32, 93–105.

———. 1850. Notiz. *Journal für die reine und angewandte Mathematik* 40, 188.

SERRE, Jean-Pierre. 1967. Complex Multiplication. In *Algebraic Number Theory*, ed. J.W.S. Cassels, A. Fröhlich, pp. 292–296. London, New York: Academic Press.

SERRET, Joseph-Alfred. 1849. *Cours d'algèbre supérieure.* Paris: Bachelier. 2nd ed. Paris: Mallet-Bachelier, 1854. 3rd ed. 2 vols. Paris: Gauthier-Villars, 1866.

Shimura, Goro, Taniyama, Yutaka. 1961. *Complex Multiplication of Abelian Varieties ad its Applications to Number Theory.* Publications of the Mathematical Society of Japan 6. Tokyo: Mathematical Society of Japan.

Smith, Henry John Stephen. 1859–1865. Report on the Theory of Numbers. *Report of the British Association for the Advancement of Science* 1859, 228-267; 1860, 120–169; 1861, 292–340; 1862, 503–526; 1863, 768–786; 1865, 322–375. Repr. in *The Collected Mathematical Papers*, ed. J.W.L. Glaisher, vol. 1. Oxford: Clarendon Press, 1894.

Sommer, Julius. 1907. *Vorlesungen über Zahlentheorie. Einführung in die Theorie der algebraischen Zahlkörper.* Leipzig: Teubner.

Tate, John. 1971. Symbols in Arithmetic. In *Actes du Congrès international des Mathématiciens. 1–10 septembre 1970, Nice*, vol. 1, pp. 201–211. Paris: Gauthier-Villars.

Ullrich, Peter. 2001. Gotthold Eisensteins Exemplar der Gauß'schen *Disquisitiones Arithmeticae*, erneut betrachtet. In *Neue Welten. Wilhelm Olbers und die Naturwissenschaften um 1800*, ed. G. Biegel, G. Oestmann, K. Reich, pp. 202–221. Braunschweig: Braunschweigisches Landesmuseum.

Vierhaus, Rudolf. 1987. Wilhelm von Humboldt. In *Berlinische Lebensbilder. Wissenschaftspolitik in Berlin,* pp. 63–76 Einzelveröffentlichungen der Historischen Kommission zu Berlin 60. Berlin: Colloquium Verlag.

Vlăduţ, Sergeï G. 1991. *Kronecker's Jugendtraum and Modular Functions.* New York, Philadelphia, etc.: Gordon & Breach.

Waltershausen, Wolfgang Sartorius von. 1856. *Gauss zum Gedächtniss.* Leipzig: Hirzel.

Weil, André. 1976. *Elliptic Functions According to Eisenstein and Kronecker.* Ergebnisse der Mathematik und ihrer Grenzgebiete 88. Berlin, etc.: Springer.

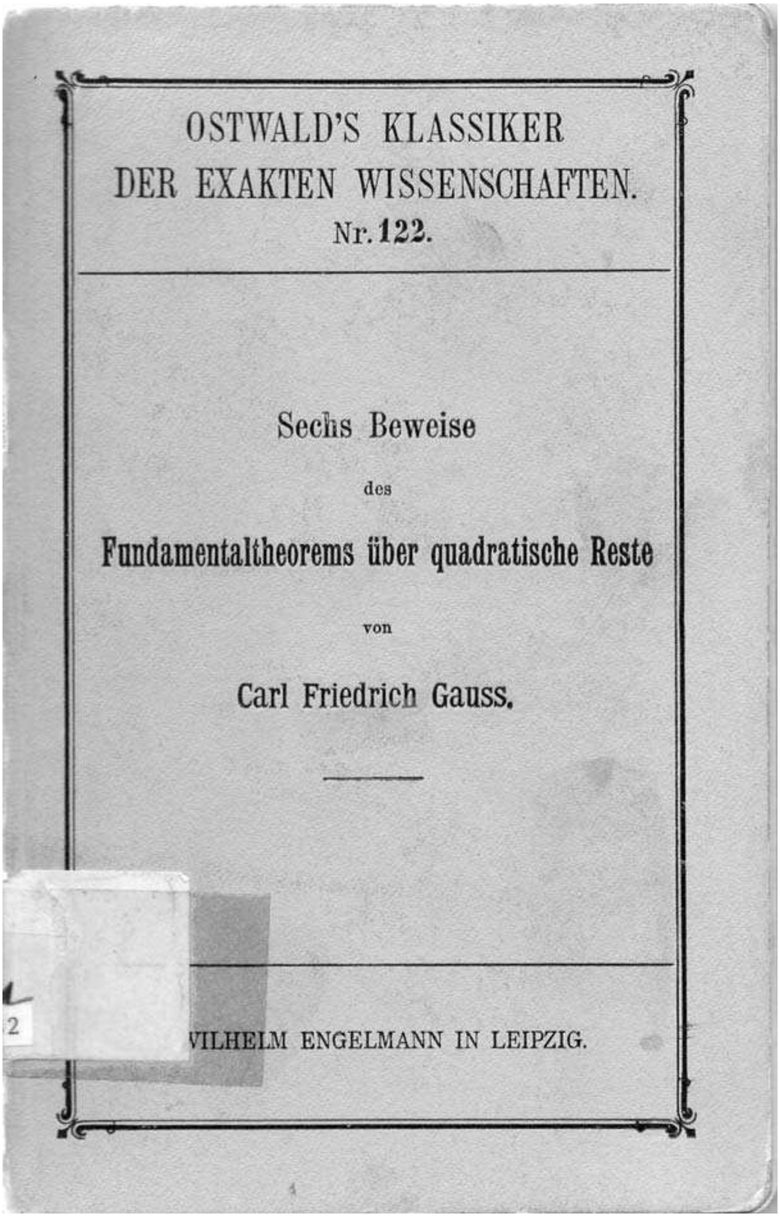
———. 1979. *Œuvres scientifiques. Collected Papers.* 3 vols. New York, Heidelberg, Berlin: Springer.

———. 1984. *Number Theory. An Approach Through History from Hammurapi to Legendre.* Boston, etc.: Birkhäuser.

———. 1986. Gauss et la composition des formes quadratiques binaires. In *Aspects of Mathematics and its Applications*, pp. 895–912. North-Holland Mathematical Library 34. Amsterdam: North-Holland.

Wussing, Hans. 1969. *Die Genesis des abtrakten Gruppenbegriffs. Ein Beitrag zur Entstehungsgeschichte der abtrakten Gruppentheorie.* Berlin: VEB Deutscher Verlag der Wissenschaften. English transl. A. Shenitzer. Cambridge: MIT Press, 1984.

———. 2001. Implicit Group Theory in the Domain of Number Theory, Especially Gauß and the Group Theory in his "Disquisitiones Arithmeticae" (1801). *Revista Brasileira de História da Matemática* 1-1, 57–65.



OSTWALD'S KLASSIKER
DER EXAKTEN WISSENSCHAFTEN.
Nr. 122.

Sechs Beweise
des
Fundamentaltheorems über quadratische Reste
von
Carl Friedrich Gauss.

WILHELM ENGELMANN IN LEIPZIG.

Fig. I.2A. Gauss's *theorema fundamentale* of the D.A. becomes a popular German classic: volume 122 of Ostwalds Klassiker der Exakten Wissenschaften
(Courtesy of the Bibliothèque de l'IRMA, Strasbourg)

I.2

Several Disciplines and a Book (1860–1901)

CATHERINE GOLDSTEIN and NORBERT SCHAPPACHER

Carl Friedrich Gauss died on February 2, 1855. Jacobi had died almost exactly four years earlier, and Eisenstein in 1852. Cauchy died in 1857. Dirichlet became Gauss's successor in Göttingen, and died in 1859.[1] Kummer, for his part, was then turning to geometry, publishing only an occasional number-theoretical paper. In France, Hermite's research was shifting to invariant theory and differential equations. Thus, the erstwhile proud and active leading group of European researchers in the domain opened up by the *Disquisitiones Arithmeticae* was decimated dramatically by the 1860s. Only Leopold Kronecker in Berlin represented a strong element of continuity across these years.

After Gauss's and Dirichlet's deaths, the Göttingen scene was dominated by non-arithmetical occupations with Gauss's legacy. Among the brains of deceased Göttingen colleagues that the physiologist Rudolf Wagner managed to collect and examine were Gauss's and Dirichlet's. In an attempt to go beyond weighing and superficial descriptions, he used in particular Gauss's brain and that of the professor of pathology Conrad Heinrich Fuchs to develop and calibrate new parameters. They provided him with rankings: Göttingen university professors arrived on top and orang-outangs at the bottom.[2]

1. Literary Activities

A more traditional approach to Gauss's remains was the grand publication of his collected works (*Werke*), including pieces from his *Nachlass*, his unpublished notes

[1] Dirichlet's successor was Bernhard Riemann who would die in 1866, the year that Göttingen became a Prussian town. The chair was then offered to Kronecker, but he preferred to stay in Berlin, with Kummer and Weierstrass. The position was finally given to Alfred Clebsch.

[2] [Hagner 2004], pp. 142–149.

and correspondence. This major undertaking of the *Königliche Gesellschaft der Wissenschaften zu Göttingen* was finally realized in two ventures, separated by some twenty years. The first phase was directed by the mathematician-astronomer Ernst Schering[3] who actually did most of the work himself, editing in particular single-handedly the first volume, a newly corrected printing of the *Disquisitiones Arithmeticae*, which appeared in 1861. For Gauss's other arithmetic publications and some related *Nachlass* material in vol. II (1863) – in particular, the early manuscript of what may have been the planned and never published sec. 8 of the D.A. – Schering enlisted the help of Richard Dedekind,[4] who was also editing Dirichlet's lectures on number theory. Schering brought out six volumes by 1874;[5] he died in 1897, at a time when a renewed interest in Gauss's *Nachlass* was growing, as Paul Stäckel's success in locating Gauss's mathematical diary in 1898 shows. The subsequent six volumes were published between 1900 and 1929, under Felix Klein's supervision[6] with the astronomer Martin Brendel as managing editor. Here the parts having to do with arithmetic, as well as with elliptic and modular functions, were commented by Paul Bachmann, Paul Stäckel, Ludwig Schlesinger, and Robert Fricke.[7] We shall see that this second phase of the Gauss edition coincided with a new boom in number theory in which Göttingen played a central role.

In the middle of these editorial achievements, concerns arose about making Gauss more readily accessible, in particular to students of mathematics.

> The handsome complete editions which have been realized of the works of almost all great mathematicians since *Lagrange* have a double significance. On the one hand, they are to be a dignified monument for those illustrious minds; on the other hand, they are to render their creations more accessible to a studious posterity than the originals, of which some are scattered in periodicals, and others have become rare. But there can be no doubt that this latter goal can only be imperfectly achieved. For the volume and the layout of the complete editions imply that – most literally – the means to ascend to these sources are rarely at the disposal of those who would like to quench their thirst there.[8]

[3] He became in a way Gauss's successor when he was appointed head of the newly created section of theoretical astronomy at the Göttingen observatory in 1867.

[4] A personal conflict between the two resulted from this collaboration, see [Lipschitz 1986], p. 90. Riemann died before delivering anything useful about Gauss's *Nachlass* on elliptic functions: see Schering's grudging remark about him in [Gauss 1866], p. 492.

[5] He also published (Gotha: F.A. Perthes, 1871) a new printing of Gauss's 1809 *Theoria motus corporum coelestium* in a format which looked like vol. 7, except that it was edited by himself, "member of the Göttingen Society," instead of "by the Society." Furthermore, Schering oversaw some "second printings" (*Zweiter Abdruck*) which for vol. 2, reedited in 1876, contains additional *Nachlass* material with Schering's comments.

[6] Klein had obtained a chair in Göttingen in 1886.

[7] Bachmann who had attended Dirichlet's lectures in Göttingen obtained his doctorate under Kummer in 1862, see § 3.1 below. The three others obtained theirs between 1885 and 1887, Stäckel and Schlesinger in Berlin, partly with Kronecker, Fricke with Klein.

[8] From Heinrich Simon's preface to his German edition of Gauss's "Disquisitiones generales circa seriem infinitam ..." (Berlin: Springer, 1888): *Die stattlichen Gesammt-Ausgaben,*

The problem with the D.A. for German students, besides its rarity or price, was the Latin. A selection of Gauss's texts in German (translated where applicable) was in fact published in these decades, including several issues of the popular low-budget series *Ostwald's Klassiker der exakten Naturwissenschaften*.[9] There was also a project to convince Schering[10] to translate the D.A. into German, as the following letter shows – incidentally reflecting the antagonism between Dedekind and Kronecker to which we shall return below:

> If you write once more to Professor Schering, would you please tell him roughly this: There can be no doubt about the importance of Gauss's *Disquisitiones Arithmeticae* for the development of mathematics. It is a work which holds in mathematics approximately the same position as Kant's *Critique of Pure Reason* holds in philosophy. ... In spite of this eminent importance, the work is hardly read. I am convinced that a statistical investigation would show that not even 3% of all mathematicians have read the work. Professor Schering is completely right: the majority of the students get by on surrogates. It is in particular the Dirichlet-Dedekind lectures which help satisfy the desire for arithmetical knowledge. But this is precisely the trouble. Professor Kronecker, probably one of Dirichlet's best students, thinks ... that it is not an advantage to see through the spectacles of commentators. The students have to study such a work themselves. ... However, ... not all mathematicians have the necessary linguistic faculties.[11]

die von den Werken fast aller grossen Mathematiker seit Lagrange *veranstaltet worden sind, haben eine zwiefache Bedeutung. Sie sollen einerseits ein würdiges Denkmal jener erlauchten Geister sein, andererseits aber die Schöpfungen derselben der lernenden Nachwelt zugänglicher machen, als dies bei den Originalen der Fall ist, die teils in periodischen Schriften zerstreut, teils selten geworden sind. Nun ist nicht zu verkennen, dass der letzere Zweck nur in beschränktem Massse erreicht werden kann. Denn Umfang und Ausstattung der Gesammt-Ausgaben bringen es mit sich, dass – im prosaischsten Sinne – die Mittel, durch die man zu diesen Quellen steigt, denen, die daselbst zu schöpfen begehren, nur selten zu Gebote stehen.*

[9] In this series, the following numbers reproduced works by Gauss : 2, 5, 14, 19, 53, 55, 122, 153, 167, 177, 225, 256. The last is Gauss's mathematical diary; the only strictly arithmetical little volume is no. 122, published by Eugen Netto in 1901, which contains Gauss's six proofs of the quadratic reciprocity law.

[10] Springer, who at that time was just starting to get into mathematics publishing, would indeed publish such a translation four years later; but it was Hermann Maser who translated, not just the D.A., but also related texts by Gauss from vol. 2 of Gauss's *Werke*, and included Dedekind's comments with the latter's permission, [Gauss 1889]. One may note that Maser dropped Gauss's dedication of the D.A. to the archduke. Maser had published a German translation of Adrien-Marie Legendre's *Théorie des nombres* in 1886.

[11] Letter of Carl Itzigsohn to Julius Springer, March 23, 1885 (Korrespondenzarchiv, Springer-Verlag Heidelberg, Abteilung A, Weierstraß 23; Weierstraß/Itzigsohn): *Wenn Sie nochmals an Herrn Professor Scheering* [sic] *schreiben, so bitte ich dem Herrn etwa Folgendes zu sagen: Welche Wichtigkeit Gauß:* Disquisitiones Arithmeticae *für die Entwicklung der Mathematik gehabt haben, darüber existirt wohl kein Zweifel. Es ist ein Werk, das ungefähr in der Mathematik dieselbe Stellung einnimmt, wie die* Kritik der reinen Vernunft *von Kant in der Philosophie. ... Trotz dieser eminenten Wichtigkeit wird*

The "surrogates" (in Itzigsohn's words) included of course Dedekind's edition of Dirichlet's *Vorlesungen über Zahlentheorie*, which, as explained in chap. I.1, simplified and popularized the D.A., but also the various syntheses or textbooks which integrated parts of the D.A. in the second half of the century; an example is Bachmann's textbook on cyclotomy, [Bachmann 1872], which would finally become the third of six volumes of his "attempt at a comprehensive presentation" of number theory.[12] They provided a uniform basic training in number theory,[13] and their mediating role is testified to from many quarters by the generation born in the 1860s. The young Hermann Minkowski, for example, would read Dirichlet's *Vorlesungen über Zahlentheorie* first and then the *Disquisitiones Arithmeticae*.[14] Edmond Maillet, an engineer trained at the *Ecole Polytechnique*, who obtained the *Grand Prix* of the French Academy of Sciences in 1896 for a memoir on finite groups and was one of the rare French mathematicians to use Kummer's ideal factors, characteristically answered, when asked about his formative readings:

> On M. Jordan's advice, I read on the one hand Serret's *Algèbre supérieure*, Dirichlet-Dedekind's *Zahlentheorie*, Bachmann's *Kreistheilung*, probably some Gauss…[15]

But one may wonder if Carl Itzigsohn's complaint about the very small readership of the D.A. does not correspond to a deeper and larger phenomenon: a low point, or at least a decline[16] of the ebullient research field opened at the middle of the century, as its most important contributors left it. This at any rate is the impression conveyed by the contemporary mathematicians themselves.

das Werk fast gar nicht gelesen. Ich bin fest überzeugt, daß eine statistische Untersuchung ergeben würde, daß nicht 3% aller Mathematiker das Werk gelesen haben. Herr Prof. Sch.[ering] hat vollkommen recht, ein großer Theil der Studirenden behilft sich mit Surrogaten. Namentlich sind es die Dirichlet-Dedekindschen Vorlesungen, welche das Bedürfnis nach arithmetischen Kenntnissen befriedigen helfen. Indeß hierin liegt eben gerade der Fehler. Herr Prof. Kronecker, wohl einer der besten Schüler Dirichlet's, ist der Ansicht …, daß es kein Vorteil ist, durch die Brille von Commentatoren zu sehen. Die Studenten müssen ein derartiges Orgina[le]s [sic] *Werk selbst studiren. … Indeß, … stehen nicht allen Mathematikern diejenigen philologischen Hilfsmittel zu Gebote.* We heartily thank Reinhard Siegmund-Schultze for having shared this letter and his transcription of it with us. About Itzigsohn, see [Bölling 1994], pp. 11–20.

[12] The whole series, mostly written after Bachmann's early retirement from his Münster chair in 1890, comprises 5 parts in 6 physical volumes. [Bachmann 1872] was reedited posthumously in 1921 by Robert Haussner, as vol. 3 of the series. Bachmann also published other number-theoretical books, for instance on Fermat's Last Theorem.

[13] Gaston Darboux, reviewing the third edition of Dirichlet's *Vorlesungen* in the *Bulletin des sciences mathématiques et astronomiques* 3 (1872), p. 168, stated that "the order followed in the book is that adopted by all the professors."

[14] See [Strobl 1985], p. 144, and J. Schwermer's chap. VIII.1 below.

[15] This appears in a survey organized by the journal *L'Enseignement mathématique* 8 (1906), p. 222: *Sur le conseil de M. Jordan, je lus* l'Algèbre supérieure *de Serret, la* Zahlentheorie *de Dirichlet-Dedekind, la* Kreistheilung *de Bachmann, du Gauss probablement…*

[16] Ralf Haubrich speaks of *Niedergang* as far as higher reciprocity laws were concerned, [Haubrich 1992], p. 35.

Dedekind published his own development of Kummer's work on algebraic numbers – in particular his theory of ideals, to which we shall return – within the supplements to his successive editions of Dirichlet's *Vorlesungen*, as "the safest means to win a larger circle of mathematicians to work in this field."[17] But his expectations were disappointed. On March 11, 1876, Rudolf Lipschitz proposed a French translation of the relevant supplement, regretting at the same time that the theory it contained was "not appreciated at its true value, even in Germany." In his grateful reply of April 29, Dedekind wrote that until now only one person, Heinrich Weber, had expressed an active interest in his work.[18]

On the more classical topic of quadratic forms, Hermite wrote to Henry Smith in 1882 about a prize posted by the Paris Academy on the representation of integers as sums of five squares:

> Until now, I do not know of any paper submitted. This is explained by the direction of the mathematical trend which does not go now toward arithmetic. You are the only one in England to follow the path opened by Eisenstein. M. Kronecker is the only one in Germany; among us, M. Poincaré, after putting forward some good ideas on what he calls arithmetical invariants, now seems to think only about Fuchsian functions and differential equations.[19]

Dedekind's and Hermite's declarations seem to agree. But the fact that the names mentioned in both are different points to another process: the dissociation of several components of what we have called arithmetic algebraic analysis in chap. I.1. The research work on the theory of forms, for instance, was more and more oriented toward algebra, in particular invariant theory, with no concern for the nature of the coefficients of the forms, as is witnessed by the works of Francesco Faà di Bruno, Arthur Cayley, Alfred Clebsch, and others.[20] Meanwhile, complex analytic functions were developing into an independent topic. And the track from them to congruences and reciprocity laws seemed progressively washed out.

2. Citation Networks

To go beyond such local testimonies and get a global view of the situation, historians have at their disposal a new tool in the 1870s, the *Jahrbuch über die Fortschritte*

[17] See [Dedekind 1930–1932], vol. 3, p. 464. Dedekind added his theory inside a new supplement (the tenth) on the composition of forms, in the second edition in 1871; he would later expand and rewrite it, rendering it autonomous as an eleventh supplement to the editions of 1879 and 1894.

[18] [Lipschitz 1986], pp. 47–49. Quote on p. 47: *dabei selbst in Deutschland nicht nach ihrer vollen Gebühr allgemein gewürdigt werden.*

[19] [Smith 1894], vol. 1, p. lxvii: *Jusqu'ici je n'ai pas eu connaissance qu'aucune pièce ait été envoyée, ce qui s'explique par la direction du courant mathématique qui ne se porte plus maintenant vers l'arithmétique. Vous êtes seul en Angleterre à marcher dans la voie ouverte par Eisenstein. M. Kronecker est seul en Allemagne, et chez nous, M. Poincaré, qui a jeté en avant quelques idées heureuses sur ce qu'il appelle les invariants arithmétiques semble maintenant ne plus songer qu'aux fonctions fuchsiennes et aux équations différentielles.* On the prize, see J. Schwermer's chap. VIII.1.

[20] At least the latter two also integrated projective geometry into their agenda.

der Mathematik. These yearly volumes edited in Berlin with the support of Borchardt, Kronecker and Weierstrass, provided reviews of all mathematical publications. Number theory occupied the 3rd section, after a section on pedagogical and historical questions, and one on algebra.[21] It included elementary arithmetic (*Niedere Zahlentheorie*, that is, here, school arithmetic); higher arithmetic, divided into generalities and the theory of forms; continued fractions.[22] A quantitative analysis of the *Jahrbuch* reveals that between 1870 and World War I, higher arithmetic filled up 3.5% to 4% of the pages of the *Jahrbuch*, which gives some weight and some perspective to Itzigsohn's evaluation above, but still represents some 3500 papers of all kinds, from short notes on a Diophantine question in the *Educational Times* to book-length memoirs in the *Journal für die reine und angewandte Mathematik*.[23]

A finer structuring of this corpus of publications is of course necessary. It can be obtained by pursuing the web of mutual references, implicit and explicit.[24] This allows us to verify that higher arithmetic was parcelled out and to distinguish several clusters of articles; inside each cluster, references to each other's articles and results are frequent, the papers are often close in terms of methods, points of view, or objectives; at least an awareness of the works of others is indicated, while the *mathematical* exchanges between two different clusters of articles are limited, in some cases even tainted by technical misunderstanding or disapproval.[25] For reasons of space, we only delineate briefly here the (numerically) most important clusters

[21] This place may seem natural to us. However, the *Répertoire bibliographique des sciences mathématiques*, a parallel enterprise begun in the 1880s, would classify number theory almost at the end of the analysis section (under the letter "I," i.e., in the ninth place, as an *application* of analysis). On the *Répertoire*, see [Rollet, Nabonnand 2002]. The history of the *Jahrbuch* is discussed in [Siegmund-Schultze 1993].

[22] During the first decade of the *Jahrbuch*, generalities, theory of forms, and continued fractions were the three subsections of number theory. The separate section on continued fractions reminds us of the numerical importance of the topic during the XIXth century, where it was linked in particular to approximation; see [Brezynski 1991].

[23] For more details, in particular on the distribution according to countries and on the evolution through time, see [Goldstein 1994] and [Goldstein 1999].

[24] Such an approach was advocated decades ago by several authors, in particular Eugène Garfield, Derek Price, and Thomas Kuhn. To identify research groups, Kuhn suggested "the recourse … above all to formal and informal communication networks including those discovered in correspondence and in the linkage among citations," [Kuhn 1970], p. 178. See also [MacKenzie 1986]. However, applying this idea to XIXth century mathematical texts like ours to study content-related issues is not straightforward, and automatic quotation indexation would not be adequate; see [Goldstein 1999].

[25] Examples involving Ernest de Jonquières and Rudolf Lipschitz, or James Sylvester and Dedekind, are given in [Goldstein 1994]. We would like to stress here that our groupings of texts *do not* usually coincide with the personal links between mathematicians, that is with the "communication networks," and thus of course have no bearing on their works in other domains. For instance, Hermite entertained a friendly correspondence with Sylvester and had many mathematical exchanges on invariant theory, but disagreed on his number-theoretical choices for his students at Johns Hopkins, see [Parshall 1998], p. 221 and chap. VI.1 below.

and their respective relations to the D.A.

The largest group by far in the last decades of the XIX$^{\text{th}}$ century – we shall designate it as "cluster L-G" (for Legendre and Gauss) – attests to the interest in number theory inside and outside the academic milieu, some contributors being engineers or highschool teachers, others university professors. However, it also counts among the authors of its papers renowned figures like James Sylvester, Angelo Genocchi, and Edouard Lucas.[26] As these names suggest, the group is quite international, though German authors are underrepresented in it. These articles witness the vitality of research themes dating back to the first decades of the XIX$^{\text{th}}$ century: primitive roots, Legendre symbol and quadratic reciprocity, prime numbers, as well as cyclotomic and Diophantine equations.[27] Accordingly, they will find their sources in both Legendre's *Théorie des nombres* and the D.A., sometimes quoted through a "surrogate," in particular the first chapters of Dirichlet's *Vorlesungen*. The most distinctive common feature is negative: these papers avoid recourse to complex functions, sometimes also to complex numbers, and some of the authors make their opposition to the use of analysis in number theory quite explicit. Edouard Lucas for instance presented his book project in these terms to Ernesto Cesàro:

> My treatise is based on a scheme totally different from anything that exists; there is no notion of continuity, exponential, logarithm, not even a $\sqrt{2}$.[28]

Several authors, like Genocchi or Lucas, were also involved in historical work, retrieving and editing texts of medieval and early-modern algebraists, from Fibonacci to Fermat, sometimes even promoting them as a source for mathematical inspiration. From the D.A., they borrowed of course research topics, but also a taste for thorough and precise explorations of their subject, with no external techniques. The lack of advanced tools did not prevent these articles from being innovative and fruitful, like Sylvester's on cubic ternary equations or Lucas's on primality.[29] Indeed, this approach was not only in favour among outsiders from the academic milieu, it was also a privileged entrance door to number theory in places where no advanced academic tradition existed in this domain and thus is important to take into account in an international perspective.[30] However, most of the authors of this group did not train students in number theory[31] and with time and the development of multi-country

[26] On Sylvester, see [Parshall 2006]; on Genocchi, see [Conte, Giacardi 1991] and A. Brigaglia's chap. VII.1 below; on Lucas, see [Décaillot 1999] and chap. VI.2.

[27] See [Dickson 1919–1923], vol. 1 and vol. 2.

[28] Letter of October 4, 1890, quoted in [Décaillot 1999], vol. 1, p. 64 and p. 154: *Mon ouvrage repose sur un plan absolument différent de tout ce qui existe; on n'y trouve aucune notion de continuité, d'exponentielle, de logarithme, pas même* $\sqrt{2}$. We avoid using the tempting word "elementary" to describe these papers, because this word had a different use in the 1870s.

[29] On Sylvester's algebraico-geometric perspective, cf. [Schappacher 1991] and [Lavrinenko 2002]. On Lucas and his relation to the D.A., see A.-M. Décaillot's chap. VI.2 below.

[30] See on this question the issues raised concerning Leonard Dickson's *History of the Theory of Numbers* in D. Fenster's chap. VII.3 below.

[31] One of the rare exceptions is Sylvester, who launched a small cohort of mathematicians

education,[32] most of these papers tended to drift away from the research journals.

A second group of articles, say the cluster D (for Dirichlet), shares not only interreferences but also citations to Dirichlet's analytic work. Well represented until the 1890s, it then first declined, but came back to the forefront in the first decade of the XX$^{\text{th}}$ century with a more sophisticated, complex-analytic approach, inherited from Riemann and centering around Dirichlet series, i.e., series of the type $\sum_n \frac{a_n}{n^s}$, for a complex variable s and (real or complex) coefficients a_n. In the 1870s and 1880s, a small industry also developed around arithmetical functions, i.e., functions defined only on integers, such as the function giving the sum of divisors of an integer or the function counting the number of prime factors. This topic is illustrated by names such as Pafnuti Čebyšev, Ernesto Cesàro, Nicolai Bugaiev, but also Joseph Liouville, James Glaisher, and Leopold Gegenbauer.[33] Linked on the one hand to the evaluation of mean properties and asymptotic values (and thus referring to Dirichlet's seminal articles on this topic), it connects on the other hand to the cluster L-G since certain constructions allow one to dispense with advanced complex analysis. Direct references to the relevant articles of the D.A. (arts. 302, 304, etc.) are rare, serving merely to indicate the historical origin of some of the questions.

The papers of the third group – which we shall call H-K (for Hermite and Kronecker) – became sporadic during the period considered, which is compatible with Hermite's remark to Smith quoted above; they were, however, often seminal papers of otherwise well-known mathematicians, with central academic positions: from Emile Picard via Leo Königsberger to Aleksandr Nikolaevič Korkin, and Luigi Bianchi. Thematically, they dealt with modular equations and above all with the arithmetic theory of forms[34] developing in particular the explicit theory of ternary, and then quaternary, quadratic forms, as well as the concepts needed to adapt Gauss's classification to general n-ary forms.[35] The main common references here are Hermite's articles on continuous reduction and the work of Hermite and Kronecker which is situated at the junction of the arithmetic of forms and elliptic functions. References to the D.A. again read more and more like historical notes rather than mathematical reference points, even though we have many testimonies that their authors read and pondered Gauss's book. This cluster of articles appears to continue the tradition of arithmetic algebraic analysis for a few decades,[36] but explicit connections to con-

working on partitions. Of course, again, we are taking into account here only Sylvester's articles which are reviewed under the label "number theory," not his articles on algebraic invariant theory for instance.

[32] One can compare in this respect the two cases, separated by 40 years, of Angelo Genocchi and Luigi Bianchi, in A. Brigaglia's chap. VII.1 below.

[33] For the work of Čebyšev and Bugaiev, see [Ozhigova, Yuškevič 1992], pp. 171–201.

[34] But the papers belonging to this group do *not* coincide with those reviewed in the section on forms of the *Jahrbuch*; for instance, some papers like those of Théophile Pépin reviewed in this section refer only to the D.A. and clearly belong to the cluster L-G.

[35] On these topics, see C. Houzel's chap. IV.2, C. Goldstein's chap. VI.1, A. Brigaglia's chap. VII.1, J. Schwermer's chap. VIII.1.

[36] Geometrical interpretations in them, in particular via lattices, follow Gauss's 1831 com-

gruences and reciprocity laws were generally abandoned.[37] During the summer of 1844, when Kummer began his investigations, Eisenstein wrote to Moritz Stern:

> The difficulty [of higher reciprocity laws] depends on the first elements of the complex numbers about which not much is known now. … Also Jacobi agrees completely with me that the theory of general complex numbers can only be accomplished by a complete theory of *higher forms*.[38]

The study of decomposable forms – forms of higher degree which factor over a given domain of algebraic (complex) numbers, and are expressible in terms of norms of those numbers – appeared to the cluster H-K, as it did in Hermite's programme, to be a viable alternative to Kummers's theory of ideal factors.[39]

3. Beyond Kummer and Back to Gauss

The reader familiar with the development of number theory during the XIX^th^ century as it is usually presented may be surprised by our survey and wonder what happened to ideal factors and Kummer's achievements after the 1860s. An early announcement by Kummer himself in 1859, promoting a generalization of his theory to all algebraic numbers about to be published by Kronecker, hinted again at decomposable forms:

> Regarding … the general propositions which are common to all theories of complex numbers, I may also refer to a work by *Herr Kronecker* which will appear soon, and in which the theory of the most general complex numbers, in its connection with the theory of decomposable forms of all degrees, is developed completely and in magnificent simplicity.[40]

But Kronecker did not publish anything along these lines until the 1880s, and when he did, his theory had to compete with Dedekind's theory of ideals already alluded to above. Together, these works are usually seen as paving the way from the D.A. to the domain of number theory called " algebraic number theory," which blossomed in the first decades of the XX$^{\text{th}}$ century. Algebraic number theory is often perceived as a natural extension of the D.A., via Kummer's work and that of Dedekind and Kronecker. The global description of number-theoretical publications presented above

ments on August Ludwig Seeber's thesis. On this development towards Minkowski's geometry of numbers and beyond, see J. Schwermer's chap. VIII.1 below.

[37] One of the exceptions is the work of Kronecker discussed in chap. I.1, § 4.3. See also [Dickson 1919–1923], vol. 3, chap. XIX.

[38] [Eisenstein 1975], vol. 2, p. 793: *aber die Schwierigkeit hängt hier von den ersten Elementen der complexen Zahlen ab, über welche man noch gar nichts weiß. … Auch Jacobi ist ganz meiner Ansicht, dass die Theorie der allgemeinen complexen Zahlen erst durch eine vollständige Theorie der* höheren Formen *ihre Vollendung erhalten kann.*

[39] See [Haubrich 1992], p. 36–37, and the literature cited there which proves the continuing activity in the field of decomposable forms all through the XIX$^{\text{th}}$ century.

[40] [Kummer 1975], vol. 1, p. 737: *Ich kann in Betreff … der allgemeinen Sätze, welche allen Theorien complexer Zahlen gemein sind auch auf eine Arbeit von Hrn.* Kronecker *verweisen, welche nächstens erscheinen wird, in welcher die Theorie der allgemeinsten complexen Zahlen, in ihrer Verbindung mit der Theorie der zerlegbaren Formen aller Grade, vollständig und in großartiger Einfachheit entwickelt wird.*

shows that there were alternative paths of development. We shall now reevaluate the relation to the D.A. of these articles taking up and generalizing Kummer's theory, and more generally of algebraic number theory.

In the 1870s, a mere handful of papers[41] – the small number confirms Dedekind's disillusion and the decline of interest in these questions at the time – were devoted to generalizing Kummer's theory of ideal numbers from the domain of complex numbers generated by the λ^{th} roots of unity, to domains generated by the roots of other equations.[42] The difficulties of such a generalization included the right choice of domain; e.g., if a and b vary over all integers, the domain of numbers of the form $a+b\sqrt{-3}$ does not admit unique prime factorization, while the slightly larger domain of numbers $a + b\left(\frac{-1+\sqrt{-3}}{2}\right)$, which is generated by a 3^{rd} root of 1, does. Another, related, problem was to find a correct invariant to play the role of the discriminant of the cyclotomic equation in Kummer's setting, and to characterize the primes which divide it.[43]

3.1. Early Attempts

Three mathematicians took up this task in the 1860s: Richard Dedekind (1831–1916), Eduard Selling (1834–1920), and Paul Bachmann (1837–1920). They had all attended Dirichlet's lectures in Göttingen at the end of the 1850s, and had read the D.A. early on. Kronecker played for them a role which bears some analogy to Gauss's mighty shadow hanging over Abel, Jacobi, and others some thirty years before. Selling, for instance, admitted in his paper:

> Both my timidity to touch the big questions connected with the theory of these numbers, and my knowing that *Herr Kronecker* has been pursuing these investigations for a long time and has already overcome all the difficulties which had stopped me at first, and the hope that the mathematical public would soon be gratified by an extensive publication of his results, has so far kept me from publishing this study

[41] Besides those named below, one might add Arnold Meyer's dissertation. Born in 1844, Meyer studied with Karl Weierstrass and Kummer in Berlin, then with Hermite in Paris, before joining Ludwig Schäfli in Zürich. His dissertation written in 1870–1871 used ideal factorization in domains generated by roots of a cubic equation as a means to study certain decomposable ternary forms; however, his subsequent work on ternary forms belongs strictly to our cluster H-K of papers and the dissertation itself was published only in 1897.

[42] While establishing his higher reciprocity laws, Kummer himself began the task for domains generated by all λ^{th} roots of unity and a root of $X^{\lambda} - a$, where a itself is a λ-cyclotomic number.

[43] The two problems we are alluding to here are that of hitting on the notion of algebraic integer, and that of correctly defining the discriminant of a number field (which in general is a proper divisor of the greatest common divisor of the discriminants of all algebraic integers of the field) and to relate it to ramification; see [Edwards 1980], pp. 330–337, and [Haubrich 1992], pp. 57–59. Dedekind gave $\mathbf{Q}(\alpha)$, where $\alpha^3 - \alpha^2 - 2\alpha - 8 = 0$, as an example of an extension where taking the g.c.d. of the discriminants of the minimal polynomials of the elements leads to a parasitic factor, namely 2.

which I had elaborated in less generality already in the autumn of 1859.[44]

Selling's goal was to handle the domain generated by all the roots of an arbitrary irreducible polynomial f with integer coefficients. His work is most interesting as an early courageous attempt[45] to generalize Kummer directly, determining the ideal prime decomposition of a rational prime p in this domain by reading f modulo (powers of) p. Mathematically, his convoluted style makes difficult reading.[46] Kurt Hensel would later toil to understand it and, even though he did not like the experience, it is very likely that he received key insights from it for his introduction of p-adic numbers.[47]

But after this attempt, Selling turned to the more convivial topic of ternary forms in the Hermitian tradition and his few number-theoretical papers then belong to the cluster H-K mentioned above.

As for Paul Bachmann, he returned from Göttingen to Berlin where he obtained his dissertation on group theory under Kummer's supervision in 1862 and prepared for his *Habilitation* on complex units which he obtained at Breslau University in 1864. In 1867, he published in the *Journal für die reine und angewandte Mathematik* a short article on the arithmetic of complex numbers generated by two independent square roots: he studied the prime ideal factors, the units, the class number. But then, like Selling, he devoted his subsequent number-theoretical papers to ternary forms, reproving and completing some of Hermite's results.[48]

[44] [Selling 1865], p. 17: *Sowohl die Scheu, die grossen mit der Theorie dieser Zahlen zusammenhängenden Fragen zu berühren, als die Kenntniss davon, dass Herr* Kronecker *dieselben Untersuchungen seit lange* [sic] *pflege und bereits alle Schwierigkeiten, die mir zunächst ein Ziel gesetzt hatten, überwunden habe und die Hoffnung, dass das mathematische Publikum sich bald einer ausgedehnten Veröffentlichung seiner Resultate zu erfreuen habe, hatte mich bisher abgehalten, diese in geringerer Allgemeinheit schon im Herbste 1859 ... ausgearbeitete Untersuchung zu veröffentlichen.* Dedekind would also cautiously refer to Kronecker's announced, und still unpublished, theory in the prefaces to his second and third editions of Dirichlet's *Vorlesungen*, in 1871 and 1879, where he explained his own theory. To be fair, one has to add that the Bavarian Ministry appointed Selling *Extraordinarius* at Würzburg in 1860, against the vote of the faculty, on the strength of a letter from Kronecker.

[45] Partly anticipated by unpublished work of Dedekind; see [Haubrich 1992], p. 164–165.

[46] Indeed, it seems to have fooled most commentators, even Bourbaki (Weil) who wrote that Selling's boldness could only lead to nonsense; see the historical note on commutative algebra and algebraic number theory in their *Eléments d'histoire des mathématiques*. One crucial problem for a modern reader is Selling's misleading notation – for instance [Selling 1865], p. 23: "$f(j) \equiv 0 \pmod{p}$" – which suggests that he worked over a finite field $\mathbf{F}_{p^r}$, while he meant a higher congruence modulo p which he could later refine modulo powers of p.

[47] We are indebted to Hans-Joachim Vollrath and Birgit Petri for all our information about Selling; see B. Petri's forthcoming thesis on Kurt Hensel for more details.

[48] A good testimony of the links expected inside our cluster H-K in the 1870s (here centred around ternary quadratic forms) is provided by a letter of Georg Cantor to Richard Dedekind of November 1873, see [Dugac 1976], p. 226. Having received a copy of

3.2. Dedekind's Ideals

Richard Dedekind had been a kind of mentor for Selling and Bachmann – they attended his Göttingen lectures – and he was to be the most influential of the three.[49]

According to his friend, Hans Zincke, Dedekind had studied the D.A. already when he was a pupil at the Braunschweig *Collegium Carolinum* in 1849–1850.[50] In Göttingen, however, Dedekind was above all influenced by Dirichlet and Riemann with whom he shared a predilection for conceptual definitions. He would explain to Rudolf Lipschitz in 1876 how, in his number-theoretical work, he had tried to "build research not on accidental forms of presentation but on simple basic concepts."[51] Twenty years later, he would still put forward the same point, this time in his memories of the D.A.:

> I first recall a beautiful passage from the *Disquisitiones Arithmeticae* which had made the deepest impression on me already in my youth: "But in our judgment, such truths ought to be extracted from notions rather than notations." These last words, when taken in the most general sense, express a great scientific idea, a preference for the intrinsic against the extrinsic. This antithesis repeats itself in mathematics in almost all fields; for instance Riemann's definition of functions via intrinsic characteristic properties from which the extrinsic forms of representations necessarily flow.[52]

Dedekind started his own investigations with an algebraic project, linked to the

Bachmann's work on ternary forms and learning that Selling would publish on this theme, Cantor reminded Dedekind of his own habilitation of 1869 on the same subject, and wondered if they would quote Smith's work of 1867.

[49] Dedekind's work has been extensively studied. We shall be very brief here, stressing above all his relation to the D.A. See [Dugac 1976], [Edwards 1980], [Edwards 1983], [Edwards 1992b], [Edwards, Neumann, Purkert 1981], [Neumann 1979–1980], and the very thorough thesis [Haubrich 1992] which regrettably remains unpublished.

[50] [Dugac 1976], p. 14, citing Zincke's 1916 "Reminiscences of Richard Dedekind." Hans (Zincke) Sommer was to become both a musicologist and a specialist of optics at Braunschweig. Dedekind had also studied, before 1855, H. Seeger's notes of Dirichlet's lectures on the applications of calculus to number theory and on number theory.

[51] Letter of June 10, 1876, in [Lipschitz 1986], p. 60, quoted in [Haubrich 1992, p. 12]: *die Forschung nicht auf zufällige Darstellungsformen der Ausdrücke sondern auf einfache Grundbegriffe zu stützen.* In [Dugac 1976], p. 71, it is recalled that substituting concepts for computations was for Dirichlet a hallmark of modern analysis, as he wrote in his obituary of Jacobi.

[52] [Dedekind 1930–1932], vol. 2, pp. 54–55, with a reference to D.A., art. 76: *Ich erinnere zunächst an eine schöne Stelle der Disquisitiones Arithmeticae, die schon in meiner Jugend den tiefsten Eindruck auf mich gemacht hat:* At nostro quidem judicio huiusmodi veritates ex notionibus potius quam ex notationibus hauriri debebant. *In diesen letzten Worten liegt, wenn sie im allgemeinsten Sinne genommen werden, der Ausspruch eines großen wissenschaftlichen Gedankens, die Entscheidung für das Innerliche im Gegensatz zu dem Äußerlichen. Dieser Gegensatz wiederholt sich auch in der Mathematik auf fast allen Gebieten; man denke nur an die Funktionentheorie, an Riemanns Definition der Funktionen durch innerliche charakteristiche Eigenschaften, aus welchen die äußerlichen Darstellungsformen mit Notwendigkeit entspringen.*

elaboration of a theory of higher congruences.[53] He studied Gauss's cyclotomy in depth, read Abel and Galois, and taught this topic at Göttingen. This led him first to reshape Gauss's presentation which failed to meet his main criterion:

> In Gauss's synthetic presentation the aim to be brief won out over the principle of deducing everything from a unified algebraic idea. When I first thoroughly studied cyclotomy over the Whitsun holidays in 1855, I had to fight for a long time, even though I understood all the details, to recognize irreducibility as the principle which would drive me with necessity to all the details once I asked simple, natural questions about it.[54]

In this perspective, the auxiliary (irreducible) equation, whose roots are the e so-called periods of f terms ($ef = \lambda - 1$, λ a prime number) associated to the cyclotomic equation in Gauss's sec. 7, corresponds to the subgroup of order f of the Galois group $(\mathbf{Z}/\lambda\mathbf{Z})^*$. From there Dedekind turned to Kummer's theory in December 1855 trying to find an algebraic core in Kummer's computational arguments.[55] This first stage of Dedekind's theory, which he never published, suffered according to his own account from an unsatisfactory concept of the discriminant and from a number of exceptions requiring specific treatments.

The second stage, delayed by his editorial activities for the collected works of Gauss, Dirichlet, and later Riemann, was finally written up, as mentioned above, in Supplement X of the 2$^{\text{nd}}$ edition of Dirichlet's *Vorlesungen* in 1871, and completed and reformulated in Supplement XI of the subsequent editions (1879 and 1894).[56] Although the supplement as a whole is devoted to Gauss's theory of composition of binary quadratic forms, Dedekind passed quickly from Gauss and Dirichlet to Kummer's theory of ideal numbers, and then to his own "higher standpoint," introducing a concept

[53] See [Scharlau 1982]. Dedekind's paper was surely written before he saw Gauss's manuscript of the *Caput octavum* which he would edit in vol. 2 of Gauss's *Werke*; see [Haubrich 1992], pp. 139–145, and G. Frei's chap. II.4, § 3.2.1 below.

[54] [Dedekind 1930–1932], vol. 3, pp. 414–415, quoted in [Haubrich 1992], p. 94: ... *daß in der synthetischen Darstellung von Gauß das Streben nach Kürze den Sieg über die Forderung davongetragen hat, alles aus einem einheitlichen algebraischen Gedanken abzuleiten. Bei meinem ersten gründlichen Studium der Kreisteilung in den Pfingstferien 1855 hatte ich, obgleich ich das Einzelne wohl verstand, doch lange zu kämpfen, bis ich in der Irreduktibilität das Prinzip erkannte, an welches ich nur einfache, naturgemäße Fragen zu richten brauchte, um zu allen Einzelheiten mit Notwendigkeit getrieben zu werden.* Cf. O. Neumann's chap. II.1 below.

[55] He actually found an error in it in 1857, as did Cauchy and other French mathematicians who were scrutinizing Kummer's articles in the context of Fermat's Last Theorem, the topic of the 1857 prize of the Paris Academy; see [Edwards 1975]. Dedekind's notes on the gap were communicated by Dirichlet to Liouville; they are reproduced in [Haubrich 1992], appendix 2, pp. 192–194.

[56] Our topic being the history of the D.A., we do not go into the differences between the successive versions of Dedekind's theory. We refer instead to [Dedekind 1930–1932], vol. 1, pp. 202–203, and to the two studies [Edwards 1980] and [Haubrich 1992], chap. IX, which look at this evolution from opposite angles.

> that seems well adapted to serve as a foundation for higher algebra and the parts of number theory linked with it,[57]

that of a field (*Körper*), i.e., for him, a system of real or complex numbers stable under the four usual operations. He mostly concentrated on those generated over the rationals by a finite number of algebraic numbers. An algebraic integer in a given field is *defined* as a number of the field satisfying a polynomial equation with leading coefficient 1 and (ordinary) integer coefficients. Dedekind also introduced "ideals," i.e., systems of numbers stable under addition, subtraction and multiplication by the integers of the field; the name alludes of course to Kummer's ideal numbers. As is well known, he defined a concept of primality for these ideals and obtained a complete theory of unique prime factorization, at the level of ideals.[58] A few years later, in collaboration with Heinrich Weber, he successfully transposed the same ideas to the theory of algebraic functions. The fully fledged theory of ideals would in turn serve as a model for so-called *modern algebra* after World War I, in particular in the works of Emmy Noether.

While most authors before the 1860s had been happy to explore families of explicitly given complex numbers, in order to prove new cases of the reciprocity laws, Dedekind on the contrary, wanted to

> deflect attention from the integers and thus to let the concept of a finite field [i.e. here, a field of finite degree over the rationals] Ω come to the fore more clearly.[59]

This emphasis should be appreciated with respect to Dedekind's global view of the structure of mathematics. His brand of logicism, developed in parallel with his theory of ideals and fields, would base pure mathematics on numbers, and thus ultimately on set-theoretical concepts inherited from them, such as the notion of field. According to Dedekind's view, they alone provided the theory with both unity and rigour.[60] For Dedekind, pure mathematics *was arithmetic*, but an arithmetic which amalgamated number theory and algebra. He would thus describe the theory of equations itself as the "science of the relationship between fields" (*die Wissenschaft von der Verwandtschaft der Körper*); in turn, he would perceive the concept of field arithmetically, describing the inclusion of fields, for instance, as a division.[61] The

[57] [Dedekind 1930–1932], vol. 3, p. 224: ... *welcher wohl geeignet scheint, als Grundlage für die höhere Algebra und die mit ihr zusammenhängenden Teile der Zahlentheorie zu dienen.*

[58] He also saw in 1873 how Gauss's theory of cyclotomy could be presented in terms of fields and "substitutions," i.e., field homomorphisms; see [Dedekind 1930–1932], vol. 3, pp. 414–416.

[59] Letter to Lipschitz on June 10, 1876, [Lipschitz 1986], p. 61: ... *um zunächst die Aufmerksamkeit von den ganzen Zahlen abzulenken und dadurch den Begriff eines endlichen Körpers Ω deutlicher hervortreten zu lassen.*

[60] See Dedekind's *Was sind und was sollen die Zahlen?*, [Dedekind 1930–1932], vol. III, pp. 335–391. On Dedekind and arithmetization, see [Dugac 1976], [Ferreirós 1999], as well as B. Petri's and N. Schappacher's chap. V.2 below.

[61] [Dedekind 1930–1932], vol. 3, p. 409. Cf. [Haubrich 1992], pp. 106–107, and [Corry 1996/2004], Part One, chap. 2.

theory of number fields and their ideals incarnates Dedekind's whole programme.

3.3. Zolotarev's Theory of Algebraic Numbers

Another successful generalization of Kummer's theory was proposed in the same decade by Egor Ivanovič Zolotarev. A student of Čebyšev's at Saint-Petersburg, Zolotarev was led to this question as an auxiliary problem for treating certain integrals; see for instance [Zolotarev 1880], p. 51. Using a mixture of elementary arithmetic and Jacobi's theory of transformations, he had proved in [Zolotarev 1872] the validity of an algorithm proposed by Čebyšev to determine the reducibility of integrals of the form $\int \frac{(x+A)dx}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}$ for rational coefficients $\alpha, \beta, \gamma, \delta$; he now wanted to generalize these results to arbitrary algebraic coefficients.

Just as Selling and Dedekind had initially set out, Zolotarev followed Kummer and tried to describe the (ideal) factorization of the prime number p in a domain generated by a root α of the algebraic equation $F(x) = 0$ by factoring F modulo p and then defining the divisibility of an element of the domain by a corresponding "ideal factor" of p via higher congruences, modulo powers of p and $F(x)$. Treating one p at a time and looking at what we would describe now as the semi-local situation above p, he finally arrived at a complete theory which was, however, only published after his untimely death in 1878.[62]

Zolotarev also collaborated with Korkin on the theory of quadratic forms, in Hermite's lineage. For $n = 2, 3, 4, 5$, they gave precise bounds for the minima of n-ary quadratic forms evaluated on integers.[63] Connecting approximations, elliptic integrals, quadratic forms, higher congruences and algebraic numbers, Zolotarev's is one of the very rare works to incarnate the survival of arithmetic algebraic analysis. However, while Kronecker and Eisenstein used Kummer's theory of ideal numbers to give arithmetic interpretations of results in the theory of elliptic functions, Zolotarev emphasized *the other direction*; he developed ideal factorization in order to get new results in integral calculus. This order of things was probably better received around Čebyšev, and it also found a positive echo in Smith's Presidential Address to the London Mathematical Society in 1876, where Smith relied on such applications of number theory to advocate its development in Great-Britain; see [Smith 1894], vol. 2, pp. 175–176.

3.4. General Arithmetic According to Kronecker

Leopold Kronecker considered himself a faithful follower of Gauss in general, and of the *Disquisitiones Arithmeticae* in particular. He liked to present findings of his as observations that brought out the true, general essence of an idea which occured in

[62] Zolotarev's theory is described in P. Piazza's chap. VII.2 below. Further references and developments are indicated in [Haubrich 1992], pp. 163–164. This case shows the problems of communities, in particular linguistic ones, as late as 1880: Dedekind and his followers would criticize Zolotarev's work on the basis of an incomplete version of his theories, the only part available to them.

[63] These papers, as opposed to those on algebraic numbers, fully belong to our cluster H-K. See also J. Schwermer's chap. VIII.1 below.

the D.A. in a specific context. For instance, before the Berlin Academy in December 1870, he took the final articles 305, 306 of D.A., sec. 5 – where Gauss discussed the cyclicity of the classes of quadratic forms in the principal genus – as the starting point for a showcase application of his approach:

> The exceedingly simple principles on which the Gaussian method rests can be applied not only at the indicated place, but also in the most elementary parts of number theory. This indicates, as it is easy to convince oneself, that those principles belong to a more general and abstract sphere of ideas. It therefore seems adequate to rid their presentation of all inessential restrictions, so that one no longer has to repeat the same deductions in the various cases where they are used.[64]

The abstract result that Kronecker thus developed amounts to what is called today the structure theorem of finitely generated abelian groups.[65]

We saw above that Kummer announced Kronecker's theory of algebraic numbers as forthcoming already in 1859. It seems impossible to say what this original theory would have looked like had it been published in a timely manner and how it would have then been tied to the D.A.[66]

Kronecker offered the most important publication on his theory, the *Grundzüge einer arithmetischen Theorie der algebraischen Grössen* (Foundations of an arithmetical theory of algebraic magnitudes), to his teacher and friend Kummer in 1881, for the 50th anniversary of Kummer's doctorate.[67] Over the domain of rational numbers, a genus domain (*Gattungsbereich*) is obtained by adjoining a root λ of an

[64] [Kronecker 1895–1931], vol. 1, pp. 274–275: *Die überaus einfachen Principien, auf denen die* Gauss*'sche Methode beruht, finden nicht blos an der bezeichneten Stelle, sondern auch sonst vielfach und zwar schon in den elementarsten Theilen der Zahlentheorie Anwendung. Dieser Umstand deutet darauf hin, und es ist leicht sich davon zu überzeugen, dass die erwähnten Principien einer allgemeineren, abstrakteren Ideensphäre angehören. Deshalb erscheint es angemessen die Entwickelung derselben von allen unwesentlichen Beschränkungen zu befreien, sodass man alsdann einer Wiederholung derselben Schlussweise in den verschiedenen Fällen des Gebrauchs überhoben wird.*

[65] Cf. [Wussing 1969], pp. 44–48. In art. 306, Gauss himself had stressed the analogy between various structures encountered in different parts of the D.A.; see chap. I.1, § 1.4 above. Kronecker first applied his observations to a system of ideal numbers.

[66] In his publications of the 1880s, Kronecker would take pains to convince his readers of the early conception of his work, emphasizing its connection with Dirichlet's and Eisenstein's work, and even with his own 1845 dissertation. But he also mentioned Weierstrass's influence which made him extend his programme to include algebraic functions with complex coefficients along with algebraic numbers. See [Kronecker 1895–1931], vol. 2, pp. 324–326; also pp. 195–200. In the preface of this latter article, which was published in 1881, but presented as an 1862 communication to the Berlin Academy, Kronecker, apparently to fix priorities, mentioned his Berlin courses on related topics from the 1850s and 1860s, listing colleagues who had attended them, as well as his exchanges with Weierstrass, Dedekind, and Weber. But we are not aware of any reliable source for Kronecker's theory of algebraic numbers from before the 1870s.

[67] [Kronecker 1895–1931], vol. 2, pp. 239–387. For a very readable first introduction to this theory in the case of algebraic numbers, see [Edwards 1980], pp. 353–368.

irreducible polynomial f.[68] A crucial difference with Selling and Zolotarev is that Kronecker, instead of reading the (minimal) equation f itself modulo primes p, passed to the "fundamental form" of the domain, $\omega = \omega_1 u_1 + \ldots + \omega_n u_n$, where u_i are indeterminates and ω_i a system of elements of the domain such that any algebraic integer of the domain is a linear combination of the ω_i with *integral* coefficients. This ω satisfies an algebraic equation $F(\omega) = 0$ whose coefficients are functions of the indeterminates u_i (with integral coefficients). Taking this "fundamental equation" F modulo a prime p yields the ideal decomposition of p in the domain.[69]

Forms are a pillar of Kronecker's late theory; in the *Grundzüge*, they are in general just polynomials in arbitrarily many variables, with no homogeneity required. Another pillar is the concept of "module systems" (*Modulsysteme*): an element m of the genus domain is said to be divisible by a system of elements $m_1, \ldots, m_k$ of the domain if one has $m = a_1 m_1 + a_2 m_2 + \ldots a_k m_k$, where the a_i belong to the domain. This is also expressed as a (generalized) congruence $m \equiv 0\,(\text{modd.}\, m_1, \ldots, m_k)$. The system $m_1, \ldots, m_k$ is called a module system; studying it comes down to studying the form $u_1 m_1 + u_2 m_2 + \ldots u_k m_k$, with indeterminates u_i. Module systems can be composed, and thus decomposed into products of other, eventually indecomposable, module systems. They are used by Kronecker to give a concrete definition of the greatest common divisor of several algebraic integers, and more generally to provide a theory of divisibility in genus domains.[70]

There are frequent allusions and references to Gauss in Kronecker's late expositions of his theory. The algebraic basis Kronecker relied upon owed much to Gauss's work on the fundamental theorem of algebra. When introducing the term "rationality domain" (*Rationalitätsbereich*), Kronecker recalls "Gauss's classical model of borrowing terminology from the classification of the descriptive natural sciences."[71] The introduction of indeterminates into the theory of numbers is attributed to Gauss

[68] That is, for us, a number field. We translate "Gattung" by "genus" since Kronecker himself indicated *genus* as the Latin equivalent of his term; see [Kronecker 1895–1931], vol. 2, p. 251. Kronecker developed his theory not only over the "absolute rationality domain," i.e., **Q**, but also over any rationality domain (*Rationalitätsbereich*) obtained from **Q** by the adjunction of finitely many indeterminates. Thus algebraic functions and algebraico-geometric applications are included; see [Edwards 1992b] for more details and a comparison with the theory of Dedekind and Weber.

[69] Using such ω_i to represent all algebraic integers of the domain solves the first problem mentioned before in § 3.1 above. As for the second, the discriminant of F is equal to $dU^2(u_1, \ldots, u_n)$, where U is a form in the indeterminates with coprime coefficients and the integer d is the correct discriminant of the domain. It may happen that for all integral values of the u_i, the values of U have a common divisor. This accounts for the parasitic factors of the discriminant occurring in theories which deal directly with the discriminants of the (minimal) equations of algebraic integers of the domain.

[70] Module systems correspond more or less to Dedekind's ideals, but Kronecker's main notions are independent of the ambient domain. Moreover, the operations available on their respective objects are not completely equivalent. See in particular [Edwards 1980], pp. 355–364, [Edwards 1992a], pp. 9–17, and his chap. II.2 below, and [Neumann 2002].

[71] [Kronecker 1895–1931], vol. 2, p. 249: *durchweg nach* Gauss' *klassischem Muster der Systematik der beschreibenden Naturwissenschaften entlehnten Bezeichnungen.* Other

and module systems are presented as a simultaneous generalization of Gauss's congruences and of the equivalence of quadratic forms.[72] Like their Gaussian analogues, module systems allow one to avoid any recourse to infinite sets and they are adapted to explicit computations; the principles of their composition, as well as that of forms, find their obvious sources in the D.A.[73] This selection from the resources offered by the D.A. fits well Kronecker's wish to take "refuge in the safe haven of actual mathematics":

> I recognize a true scientific value – in the field of *mathematics* – only in concrete mathematical truths, or, to put it more pointedly, only in mathematical formulas.[74]

Kronecker also mentioned a particular reason for not publishing his theory in the 1860s, which indicates a difference of scope between him and Dedekind; Kronecker had failed to obtain a general theory for what he called the "association of genera" (*Assoziation der Gattungen*).[75] This alludes to his work on complex multiplication where he had seen how to use modular functions to realize with actual algebraic numbers (in a bigger genus domain) the properties of the module systems belonging to a given imaginary quadratic domain:

> In fact, all deeper properties of the genus $\sqrt{-n}$ pertaining to composition and partition into classes [of the module systems in this genus] have, so to say, their image in the elementary properties of the associated genus Γ.[76]

This is a strong reminder of the Kronecker we encountered in chap. I.1 above, through his work on complex multiplication, as a champion of the integrated field which we called arithmetic algebraic analysis. That aspect did continue to be very much present in the minds of some of his contemporaries and in his own work.[77] In his obituary of

parts of his terminology are closer to Dirichlet, but Gauss is still mentioned; see [Kronecker 1895–1931], p. 262–263. On mathematics as a science in Kronecker's writings, see J. Boniface's chap. V.1 below.

[72] [Kronecker 1895–1931], vol. 3.1, pp. 147–154, 211–213, 249–275.

[73] [Kronecker 1895–1931], vol. 2, pp. 237–388, § 21, V, and § 22, V. Also seen in the Gaussian vein was Kronecker's theory of composition of abelian equations; see [Kronecker 1895–1931], vol. 4, pp. 115–121, which refers to D.A., art. 358, at the beginning.

[74] Letter to Cantor from 1884, quoted (with English translation) from [Edwards 1995], pp. 45–46: *Ich [habe] mich in den sicheren Hafen der wirklichen Mathematik geflüchtet.... Einen wahren wissenschaftlichen Werth erkenne ich – auf dem Felde der* Mathematik *– nur in concreten mathematischen Wahrheiten, oder schärfer ausgedrückt, 'nur in mathematischen Formeln.'* For a comparison with Gauss's foundational views, see H. Edwards's chap. II.2 and J. Boniface's chap. V.1 below.

[75] [Kronecker 1895–1931], vol. 2, p. 321–324.

[76] [Kronecker 1895–1931], vol. 2, p. 323: *Es haben überhaupt alle tieferen, auf die Composition und Classenteintheilung bezüglichen Eigenschaften der Gattung* $\sqrt{-n}$ *in den elementaren Eigenschaften der associirten Gattung* Γ, *so zu sagen, ihr Abbild.* In modern terms, this means that Kronecker hesitated to publish because he lacked an explicit construction of what we call the Hilbert class field of an algebraic number field. See [Edwards 1980], pp. 328–330.

[77] Kronecker enthusiastically endorsed Dirichlet's analytical methods in number theory,

Kronecker, in 1892, Hermite did not even mention the *Grundzüge*, but commented:

> M. Kronecker completely showed that the theory of quadratic forms of negative determinant was an anticipation of the theory of elliptic functions, in such a way that the concepts of classes and genus … could have been obtained by the analytical study and the examination of the properties of the transcendental function.[78]

In Jules Tannery's 1895 lectures on number theory, on the other hand, Kronecker's is the only theory of algebraic numbers mentioned, and it is presented as belonging to the algebraic, not to the arithmetic part of the book, which allows the display of links from arithmetic to algebra to analysis and back:

> I have hardly taken up the question of the nature of *algebraic numbers* in these lectures, … and I have scarcely indicated how Kronecker was able, using congruences and module systems, to build his exposition of algebra on a purely arithmetical basis, and how, from a completely different viewpoint, one could consider algebra not as an extension of arithmetic but as part of analysis, an algebraic number being just a special, well defined case of a general irrational number. … This study leads to some of the results owed to Kronecker.[79]

However, during the last decade of his life, Kronecker's arithmetization programme increasingly determined his outlook on the theory of algebraic numbers and functions. The ultimate goal then was to unify number theory, algebra, and analysis on a new basis, with the rational integers as the only fundamental objects, and such that the encompassing status of the theory was obtained by freely adjoining indeterminates and working modulo congruences according to module systems:[80]

practiced elliptic and modular functions himself, and devoted numerous papers to the analysis of the existing proofs of reciprocity laws. He likened the difference between purely arithmetical and analytical methods to that between manual and machine work; see A. Hurwitz, notes for a scientific biography of L. Kronecker, Archives of ETH Zürich, Hs 582 : 142, sheet 3v: *Der rein arithmetische Weg zur Lösung einer arithmetischen Aufgabe, sagt Kronecker, verhält sich zu dem Wege, der die Analysis zu Hilfe nimmt, wie Handarbeit zur Maschinenarbeit. Während jeder einzelne Schritt bei der Handarbeit auch dem Nichtkenner plausibel ist, geschieht bei der Maschinenarbeit Vieles innerhalb der Maschine, was dem Auge verborgen bleibt.* See also C. Houzel's chap. IV.2 below.

[78] [Hermite 1905–1917], vol. 4, p. 341: *M. Kronecker a mis en complète evidence que la théorie des formes quadratiques, de déterminant négatif, a été une anticipation de la théorie des fonctions elliptiques, de telle sorte que les notions de classes et de genres … auraient pu s'obtenir par l'étude analytique et l'examen des propriétés de la transcendante.* See C. Goldstein's chap. VI.1 below.

[79] [Tannery 1895], pp. iii–iv: *C'est à peine si dans les conférences, j'avais soulevé la question de la nature des* nombres algébriques*, … c'est à peine si j'avais indiqué comment, par l'emploi des congruences et des systèmes de modules, Kronecker avait pu fonder l'exposition de l'Algèbre sur une base purement arithmétique, et comment à un point de vue tout autre, on pouvait regarder l'Algèbre, non comme un prolongement de l'Arithmétique, mais comme une partie de l'analyse, le nombre algébrique n'étant qu'un cas particulier, nettement défini d'ailleurs, de l'irrationnelle générale. … Cette étude conduit à quelques-uns des résultats que l'on doit à Kronecker.*

[80] See J. Boniface's chap. V.1, and § 2 of B. Petri's and N. Schappacher's chap. V.2 below.

> With the *systematic* introduction of "indeterminates" which goes back to *Gauss*, the special theory of integers has expanded into the general arithmetic theory of polynomials in the indeterminates with integer coefficients. This general theory allows one to avoid all concepts foreign to arithmetic proper, that of negative, of fractional, of real and imaginary algebraic numbers. The concept of negative number can be avoided when one replaces in the formulas the factor -1 by the indeterminate x and the sign of equality by the Gaussian sign of congruence. Thus the equation $7-9=3-5$ will be transformed into the congruence $7+9x \equiv 3+5x \pmod{x+1}$.[81]

This programme to restructure pure mathematics thus also took its cue from the D.A. It has its historical counterpart in a specific reinterpretation of the lines of development opened by Gauss in the D.A. Kronecker's student Kurt Hensel wrote in the introduction of his edition of Kronecker's number-theoretical lectures:

> In the introduction of his "Disquisitiones arithmeticae" Gauss fixes the domain of the natural integers as the field of arithmetic, but he himself was forced to extend this domain, as he added in the fifth section of this same work the realm of quadratic forms with two variables, in the seventh the functions of x which, once set equal to zero, produce the cyclotomic equation. Kronecker characterizes then the investigation of rational numbers and rational functions of one and several variables to be the task of general arithmetic a priori.[82]

3.5. Newcomers

Early in 1857, Dedekind had written to his sister that Kronecker and he were the only readers of each other's work, because of its great abstraction. However, they were

Kronecker's presentations grew increasingly explicit in this respect; compare for instance the *Grundzüge*, [Kronecker 1895–1931], vol. 2, pp. 237–388, § 13, where the existence of a real zero of polynomials of odd degree is assumed, to the 1897 article on the concept of number [Kronecker 1895–1931], vol. 3.1, pp. 271–272.

[81] [Kronecker 1895–1931], vol. 3.1, p. 260: *mit der* principiellen *Einführung von "Unbestimmten"* (indeterminatae)*, welche von* Gauss *herrührt, hat sich die specielle Theorie der ganzen Zahlen zu der allgemeinen arithmetischen Theorie der ganzen ganzzahligen Functionen von Unbestimmten eweitert. Diese allgemeine Theorie gestattet alle der eigentlichen Arithmetik fremden Begriffe, den der negativen, der gebrochenen, der reellen und der imaginären algebraischen Zahlen, auszuscheiden. Der Begriff der* negativen *Zahlen kann vermieden werden, indem in den Formeln der Factor* -1 *durch eine Unbestimmte x und das Gleichheitszeichen durch das* Gauss'*sche Congruenzzeichen* modulo $x+1$ *ersetzt wird. So wird die Gleichung* $7-9=3-5$ *in die Congruenz* $7+9x \equiv 3+5x \pmod{x+1}$ *transformirt.* Cf. also [Kronecker 1895–1931], vol. 2, p. 355.

[82] [Kronecker 1901], p. VI: *Gauss bestimmt in der Einleitung zu seinen "Disquisitiones arithmeticae" das Gebiet der natürlichen ganzen Zahlen als das Feld der Arithmetik, aber er selbst war gezwungen, dieses Gebiet dadurch zu erweitern, daß er in der fünften Sektion desselben Werkes das Reich der quadratischen Formen von zwei Variablen, in der siebenten die Funktionen von x hinzunahm, welche gleich null gesetzt die Kreisteilungsgleichungen ergeben. Kronecker bezeichnet nun von vorn herein die Untersuchung der rationalen Zahlen und der rationalen Funktionen von einer und von mehreren Variablen als die Aufgabe der allgemeinen Arithmetik.*

not satisfied with each other's final approach. Kronecker would criticize Dedekind's theory of ideals for its use of completed infinites, and its invention of unnecessary new concepts, and Dedekind would find holes in the *Grundzüge* and consider polynomials a device foreign to the matter in question.[83]

In the last decades of the century, several younger people – born between 1859 and 1864 – entered this field, announcing the blossoming of the early XX$^{\text{th}}$ century; Kronecker's student Kurt Hensel in Berlin whose 1884 dissertation concerned the delicate issue of the divisors of the discriminant,[84] Adolf Hurwitz in Leipzig who had just written a dissertation on elliptic modular functions under Felix Klein's supervision, as well as Hermann Minkowski and David Hilbert in Königsberg. Whereas Hensel was closely associated with Kronecker's programme, the latter three, who became acquainted when Hurwitz obtained a position in Königsberg,[85] cared little about the preferences of either Dedekind or Kronecker. An anecdote describes how Hilbert and Hurwitz went for a walk during which one of them presented Dedekind's proof for the unique decomposition into prime ideals, the other Kronecker's analogue, and they found both awful.[86] More positively, Minkowski – whose prize-winning 1882 memoir on quadratic forms referred only to Gauss, Dirichlet, Eisenstein, and (for a small technical point) Weber, who had discovered his talent[87] – would devote his Bonn *Habilitationschrift* to a question raised by Kronecker's *Grundzüge*, about the concept of equivalence of forms, but would later express some of his results in terms of Dedekind's number fields. In several papers of the mid 1890s, while also using Dedekind's notions of (number) field and ideal, Hurwitz defined ideals via finite sets

[83] See [Kronecker 1895–1931], vol. 3.1, p. 156, footnote; [Dedekind 1930–1932], vol. 2, p. 53; [Edwards 1980], [Edwards, Neumann, Purkert 1982], [Haubrich 1992], pp. 128–130. On February 17, 1882, Dedekind wrote to Cantor that Kronecker's "way would, I believe, please me more if he had completely separated the theory of numbers from that of functions;" see [Dugac 1976], p. 254. Of course, function fields and number fields would both be subsumed later into the concept of global field, but for Kronecker and Dedekind, and for their own historians, two different projects for algebraic numbers (and functions), and eventually for pure mathematics, were available to students in Germany in the 1880s.

[84] His reflections about the analogy between algebraic numbers and functions eventually led him to the creation of a new arithmetic-algebraic-analytic object, the p-adic numbers, which in turn would drive the abstract algebraic study of general fields; see [Purkert 1971–1973], [Ullrich 1998] and the forthcoming thesis by B. Petri. Doctoral students of Kronecker in the 1880s include Adolf Kneser, who turned to other topics, Mathias Lerch, whose number-theoretical articles pursued Dirichlet's analytical tradition, and Paul Stäckel, the discoverer of Gauss's mathematical diary and collaborator in the edition of the Gauss's *Werke*.

[85] D. Fenster's and J. Schwermer's chap. II.3 below throws light on Hurwitz's further work on quadratic forms which we do not touch upon here.

[86] [Blumenthal 1935], p. 397. Cf. Hilbert's letter to Hurwitz criticizing the fourth edition of Dirichlet-Dedekind, [Dugac 1976], p. 270.

[87] This memoir, the laudatory letter sent by Weber to Dedekind about Minkowski, and Minkowski's relation to Gauss's D.A. are discussed in J. Schwermer's chap. VIII.1.

of generators, and used a basically Kroneckerian approach based on polynomials in several unknowns to derive the unique decomposition of ideals into prime ideals.[88]

3.6. Hilbert's Zahlbericht

In 1897, Hilbert published for the recently created *Deutsche Mathematiker-Vereinigung* a report on algebraic numbers, *Die Theorie der algebraischen Zahlkörper*, which would become known as the *Zahlbericht*.[89] Hilbert thoroughly read the literature in the preparation of it, and although he complained about Kummer's computations (*Rechnereien*), he quoted his papers abundantly. The *Zahlbericht* presents the arithmetic theory of a general (number) field K: integers, discriminant, units, ideals, ideal classes; it studies in detail the decomposition of the prime ideals of K in a Galois extension of K,[90] as well as particular cases, such as quadratic or cyclotomic fields. Moreover, Hilbert again gave a central position to higher reciprocity laws, dear to Gauss and Kummer, albeit in a new framework of number fields.[91]

Throughout the report, Hilbert placed number fields at the centre of attention and also defined ideals in Dedekind's style as sets of algebraic integers which are closed under linear combinations with algebraic integer coefficients. But for several proofs, in particular for the uniqueness of decomposition into prime ideals in arbitrary number fields and for the divisors of the discriminant, he adopted essentially the Kronecker-Hurwitz method. However, this methodological syncretism progressively fell into oblivion as Dedekind's conceptual heritage increasingly won the day; in Hilbert's own summary of his report for the *Enyclopädie der mathematischen Wissenschaften mit Einschluß ihrer Anwendungen*, published in 1900, proofs are mostly omitted so that Dedekind's concepts come out prominently, a tendency which would be amplified in the following century with the success of modern algebra.

Gauss and the D.A. have almost vanished from the main text of Hilbert's *Zahlbericht*,[92] but they do figure prominently in Hilbert's imposing preface. This preface is a manifesto for the incipient discipline that Hilbert presented in the main text, and whose position within pure mathematics is defined here. First, Hilbert appealed to "our master Gauss" to celebrate through well-chosen (and oft-repeated since) quotes "the charms of the investigations" in this "divine science" of number theory. Like Dedekind and Kronecker, Hilbert reserved for arithmetic, "the Queen

[88] Much to Dedekind's chagrin, who criticized this approach as lacking methodological purity and conceptual unity; see [Dedekind 1930–1932], vol. 2, pp. 50–58, and [Hurwitz 1895], p. 198: *... in der Meinung, dass meine Arbeit keine Verteidigung verdient, wenn sie nicht für sich selbst spricht.* See also [Dugac 1976], p. 266.

[89] See [Schappacher 2005] for an introduction to the writing and content of this report.

[90] That is an extension of K generated by all the roots of an irreducible polynomial. Thus, Hilbert considered relative situations where the base field was no longer the field of rationals but an arbitrary number field K.

[91] He shifted the emphasis from ℓ^{th} powers to norms of elements in an extension generated by the root of a polynomial of degree ℓ.

[92] There are 7 references to Gauss among which 5 are to the D.A., against 52 references to Kummer. Hilbert made it clear that he offered a new synthesis, not a historical report; all references are technical.

of mathematics" (another allusion to Gauss), a key position inside pure mathematics. But with Hilbert this "royalty claim"[93] is no longer restricted to the unification of number theory and algebra, or even analysis:

> Thus we see how arithmetic, the "Queen" of the mathematical sciences, conquers large areas in algebra and function theory, and takes the leading role in them ... Finally, there is the additional fact that, if I am not mistaken, the modern development of pure mathematics takes place chiefly *under the sign of number*: Dedekind's and Weierstrass's definitions of fundamental concepts of arithmetic and Cantor's general construction of the concept of number lead to an *arithmetization of function theory*. ... The *arithmetization of geometry* is accomplished by the modern investigations of non-Euclidean geometry.[94]

Thus Hilbert endowed number theory with two different roles. On the one hand, the *Zahlbericht* itself presents a model for what should be a fully developed discipline, here number theory:[95] it defines its proper subject matter,[96] algebraic number fields; it has its key problems, that will be made explicit in Hilbert's subsequent papers, like prime decomposition in a field extension, relative reciprocity laws and the construction of class fields; it has a rigorous system of proofs. Moreover, as a closed, mature system, number theory, as described by Hilbert, integrates its own development:

> Instead of that erratic progress characteristic of the youngest age of a science, a sure and continuous development occurs now thanks to the systematic construction of the theory of number fields.[97]

[93] Erhard Scholz coined this expression at our 1999 Oberwolfach workshop.

[94] [Hilbert 1932–1935], vol. 1, pp. 65–66: *So sehen wir, wie die Arithmetik, die "Königin" der mathematischen Wissenschaft, weite algebraische und funktionentheoretische Gebiete erobert und in ihnen die Führerrolle übernimmt ... Es kommt endlich hinzu, daß, wenn ich nicht irre, überhaupt die moderne Entwicklung der reinen Mathematik vornehmlich* unter dem Zeichen der Zahl *geschieht: Dedekinds und Weierstrass' Definitionen der arithmetischen Grundbegriffe und Cantors allgemeine Zahlgebilde führen zu einer* Arithmetisierung der Funktionentheorie ... *Die* Arithmetisierung der Geometrie *vollzieht sich durch die modernen Untersuchungen über Nicht-Euklidische Geometrie.* On arithmetization at the beginning and at the end of the XIXth century, cf. J. Ferreiròs's chap. III.2, and B. Petri's and N. Schappacher's chap. V.2 below.

[95] See chap. I.1, § 5, in particular footnote 184.

[96] Ralf Haubrich pointed out to us that the very concept of "the subject matter of a discipline" changed during the century: while it was a thing "already there" at the beginning and had the status of a natural object, like a star, the subject matter of a discipline at the end of the century was *defined* within the discipline. On the related simultaneous change in the ontology of mathematical objects, see [Gray 1992].

[97] [Hilbert 1932–1935], vol. 1, pp. 65–66: *An Stelle eines solchen für das früheste Alter einer Wissenschaft charakteristischen, sprunghaften Fortschrittes ist heute durch den systematischen Aufbau der Theorie der Zahlkörper eine sichere und stetige Entwicklung getreten.*The allusion is to Gauss's difficult determination of the sign of Gauss sums. The allusion is all the more fitting in that Gauss's presentation of this episode, on the contrary, reveals the Romantic values of the early XIXth century, see S. Patterson's chap. VIII.2. Similarly, one can contrast the idea of system present in Hilbert's preface to that in the

This development includes a representation of the past as well as one of the future, and the D.A. again is used here both as a prestigious origin and as a foil:

> As to the *position of number theory* inside the whole of mathematical science, Gauss presents number theory in the preface of the *Disquisitiones Arithmeticae* still only as a theory of the natural integers with the explicit exclusion of all imaginary numbers. … [Now] the theory of number fields … has become the most essential part of modern number theory.[98] The service, of laying down the first germ of the theory of number fields is again due to Gauss. Gauss recognized the natural source for the laws of biquadratic residues in an "extension of the domain of arithmetic." [99]

On the other hand, this internal reorganization is completed by an external one, positing number theory in the foundational enterprise of the turn of the century to which Hilbert would soon contribute his new *Grundlagen der Geometrie* (1899). Comforted by the fact that both in Dedekind's (algebraico-set-theoretical) and in Kronecker's (arithmetized) programmes, reflections on numbers in general and number-theoretical results are elaborated side by side, what may almost appear as a play on the expression "theory of numbers"[100] allows Hilbert to link number theory to the recent movement of arithmetization of mathematics – in its Göttingen form, that is, including geometry. Thus the idea of number theory as a royal discipline that was taking the lead in all fields of mathematics, and the purposeful reference to the D.A. and its author – the edition of whose *Werke* was just starting then afresh in Göttingen under Felix Klein's supervision – fit well with Hilbert's – and Göttingen's – most far-reaching projects at the time.[101]

4. Long Shadows

At the turn of the century, both Gauss's D.A. and number theory in general had thus found quite a stable and prestigious place inside mathematics. Or, more precisely,

D.A., see chap. I.1, § 2.4.

[98] In view of the papers really published in number theory at that moment, such a statement is a *coup de force*. It serves in fact as a normative *definition* of what ought to be "modern" number theory.

[99] [Hilbert 1932–1935], vol. 1, p. 64: *Was die* Stellung der Zahlentheorie *innerhalb der gesamten mathematischen Wissenschaft betrifft, so faßt Gauss in der Vorrede zu den Disquisitiones Arithmeticae die Zahlentheorie noch lediglich als eine Theorie der ganzen natürlichen Zahlen auf mit ausdrücklicher Ausschließung aller imaginären Zahlen. … Die Theorie der Zahlkörper insbesondere ist … der wesentlichste Bestandteil der modernen Zahlentheorie geworden. Das Verdienst, den ersten Keim für die Theorie der Zahlkörper gelegt zu haben, gebührt wiederum Gauss. Gauss erkannte die natürliche Quelle für die Gesetze der biquadratischen Reste in einer "Erweiterung des Feldes der Arithmetik."* Here, Hilbert follows Dedekind's point of view on the extension of arithmetic, see the end of § 3.4.

[100] This expression was used for number theory, but also for various theories of *real* numbers, such as those of Dedekind and Cantor, mentioned in Hilbert's preface.

[101] See in particular [Rowe 1989].

places, as neither the position of number theory, nor the uses of the D.A. were uniform from country to country, or even within each country.[102]

In Germany, the Neo-Gaussian movement created by the commentaries on Gauss's *Werke* and the reedition of Gauss's articles[103] expanded after the *Zahlbericht*. Around 1910, Bachmann was happy to announce that number theory was being taught in twelve German universities, see [Bachmann 1921], p. viii. Theses and articles on number-theoretical and related topics multiplied. The discipline initiated by the *Zahlbericht*, which would soon be called "algebraic number theory,"[104] blossomed especially, although not exclusively,[105] within the international area of Göttingen's influence:[106] Rudolf Fueter, Philipp Furtwängler, Alexander Ostrowski,[107] Legh Wilber Reid, Luigi Bianchi, Andreas Speiser, Teiji Takagi figured among its young authors. A harvest of textbooks in several languages framed and reinforced this development, all the way from Julius Sommer's 1907 *Vorlesungen über Zahlentheorie. Einführung in die Theorie der algebraischen Zahlkörper*, or Reid's 1910 *The Elements of the Theory of Algebraic Numbers* which were both supported by Hilbert and focused on quadratic number fields, to the *Lezioni sulla teoria dei numeri algebrici* by Bianchi in 1924.[108]

But the situation was not uniform. We have seen above that Smith in 1876 had

[102] Detailed examples illustrating this variety of research groups, inside a country or on the contrary beyond frontiers, are given in parts VI and VII below, centered on France, Italy, Russia, and the United States. For global comparative data between the number-theoretical production of members of the Deutsche Mathematiker-Vereinigung and of the Société mathématique de France between 1897 and WW1, see [Gispert, Tobies 1996], in particular p. 430.

[103] To those should be added the various celebrations organized in Germany around Gauss's hundredth anniversary in 1877: for instance, Dedekind's contribution to the Gauss Festschrift organized in Braunschweig is a display of his familiarity with the D.A., see [Dedekind 1930–1932], vol. 1, pp. 105–158.

[104] Edmund Landau used *Algebraische Zahlentheorie* as the heading of the corresponding part of his *Vorlesungen* in 1927.

[105] Heinrich Weber also continued to play a key role in this development, as did some young Berliners like Robert Remak and Edmund Landau (who then joined the Göttingen staff), also Hensel's students, most notably Adolf Fraenkel and Helmut Hasse. Gauss's editors included the older generation (Bachmann), and people who had defended their theses in the middle of the 1880s, either with Klein (Fricke), or with Kronecker (Stäckel, Schlesinger).

[106] Although the name of Klein is rarely associated with number theory, he not only took charge of the Gauss edition and related projects (editing in particular Gauss's diary in 1901), fostering what we call the Neo-Gaussian movement, but himself taught number theory at Göttingen. Geometrical insights, like those provided by Minkowski's geometry of numbers, particularly appealed to him, both because they connected number theory to other fields and because they were supposed to mitigate its overly abstruse aspects; see [Klein 1894] and [Klein 1926/1967], pp. 26–27, in perfect harmony with the preface of the *Zahlbericht*, and presumably comforting his opposition to Berlin trends.

[107] Ostrowski worked first with Hensel in Marburg before joining Göttingen during WW I.

[108] See A. Brigaglia's chap. VII.1.

tried to promote the study of number theory in Great Britain on the strength of its applications to more indigenous topics:

> It is worthy of remembrance that some of the most fruitful conceptions of modern algebra had their origin in arithmetic, and not in geometry or even in the theory of equations. The characteristic properties of an invariant, and of a contravariant, appear with distinctness for the first time in the *Disquisitiones Arithmeticae*.[109]

Besides Zolotarev's applications of his theory of algebraic numbers to integral calculus, Smith also emphasized asymptotic results[110] and the possible bridges to analysis provided by the approximation processes used by Jacobi and Hermite.

Analysis, indeed, and not algebraic structures nor the general arithmetic of polynomials, appeared to many as the greatest unifying force. In his well-known 1951 "The Queen of Mathematics," Eric Temple Bell – after first declaring that "[Gauss's] work is as vital as it was in 1801, when he published his *Disquisitiones Arithmeticae*," stated:

> There was remarkable progress since the time of Gauss, and especially since 1914, when modern analysis was applied to problems in the theory of numbers that had withstood the strongest efforts of Gauss's successors for over a century.[111]

"Modern analysis" referred in particular to the achievements of Godfrey H. Hardy, John E. Littlewood, and Edmund Landau (all belonging to our cluster D above). The royalty claim for arithmetic was challenged by no less a figure than Henri Poincaré in his lecture at the First International Congress of Mathematicians in 1897:

> Analysis unfolds for us infinite perspectives that arithmetic has not dreamed of; it shows us at a glance a grandiose composition, whose arrangement is simple and symmetric. Against this, in number theory, where the unforeseen reigns, the view is so to speak blocked at every step.[112]

Poincaré's own number-theoretical contributions mostly belong to our group H-K and this commentary, when compared to Hilbert's preface, underlines the nature

[109] [Smith 1894], vol. 2, pp. 166–190. Smith mentions specifically arts. 157, 267, 268.

[110] Again referring to the D.A. as their origin: "the first asymptotic results that were obtained are due to Gauss and are given without demonstration in the Disquisitiones arithmeticae," (arts. 302, 304, *additamenta* to 306.X).

[111] [Bell 1951/1956], pp. 498–499 for the quotes, and p. 508 for details along the same lines as Smith.

[112] [Poincaré 1897/1991], p. 26: *L'analyse nous déroule des perspectives infinies que l'arithmétique ne soupçonne pas: elle nous montre d'un coup d'œil un ensemble grandiose dont l'ordonnance est simple et symétrique; au contraire, dans la théorie des nombres où règne l'imprévu, la vue est pour ainsi dire arrêtée à chaque pas.* The quote and its context are discussed in C. Goldstein's chap. VI.1 below. The increasing international tension of the time could render statements more political: in the *Revue du Mois*, a cultural journal created by Emile Borel, a comment on a result of Hilbert and Landau concerning the expression of a definite polynomial as a sum of squares ends with the remark that there is no need to regret that "the young French mathematical school has forsaken these arithmetical studies, favoured in Germany, to attach themselves to the immense field of investigations linked with differential and integral calculus," see the motto, part VI below.

of the dissociation already mentioned of the research field built on the D.A. in the 1850s. Although both Hilbert and Poincaré shared the same diagnosis on past number theory, the domain of the "erratic," "where the unforeseen reigns," and although both extolled a majestic layout, they put forward opposed remedies.

It would be misleading to summarize this dissociation by opposing algebraic trends to analytic ones, or France to Germany, for instance. The promotors of an "algebraic theory of numbers" at the end of the XIX$^{\text{th}}$ century included projects as different as those of Lucas and Hilbert, mathematicians for whom algebra meant a classical theory of equations or, on the contrary, group theory, those for whom analysis should be avoided at all costs, or assimilated, or even used *faute de mieux.*

As our global picture of number theory has stressed, contrasted views coexisted inside a single country. We have seen that, when Hilbert and Hensel affirmed the necessity of extending number theory beyond ordinary integers, they meant different extensions, they referred to different parts of Gauss's corpus to sustain their views, and they even interpreted differently that part of the *Disquisitiones Arithmeticae* (sec. 7 on cyclotomy) which they both claimed. On a larger scale, Genocchi, Cesàro, and Bianchi in Italy, Lucas, Hadamard, and Picard in France, provide representatives of our three main groups in each country. *Contra* Reid, Leonard Dickson, a prominent proponent of number theory in the United States, devoted his textbooks on this topic to forms, not to algebraic numbers.[113] A few years after Poincaré's statement, Albert Châtelet proposed his own syncretism, in his *Leçons sur la théorie des nombres*, based on Hermite's approach, but integrating Minkowski's work on the geometry of numbers, as well as "the first elements of the theory of the complex integers of a field and of their arithmetic."[114] Distinct networks of mathematical solidarities cut across national boundaries.[115]

While the chapter entitled "Forms" of the *Jahrbuch über die Fortschritte der Mathematik* regularly displayed a few articles at the beginning of the XX$^{\text{th}}$ century, its chapter "Generalities," hosting papers on the distribution of primes or laws of reciprocity in number fields, besides those on congruences or Diophantine problems, tended to explose. It was a reclassification that was used to register the new views on number theory at the beginning of the XX$^{\text{th}}$ century. The *Jahrbuch* first gathered number theory and algebra under the same section, then identified algebraic numbers and analytic methods as incipient topics, gathering them together in a separate subsection, and finally, in the 1930s, recognized both as autonomous branches in this section, under specific headings, *Idealtheorie* and *Analytische Zahlentheorie*.

[113] See resp. chap. VII.1, part VI, and chap. VII.3.

[114] [Châtelet 1913], p. viii: *Les Chapitres IV, V et VII, plus spécialement consacrés aux nombres algébriques, constituent les premiers éléments de la théorie des entiers complexes d'un corps et de son arithmétique*. Châtelet mentioned that he did not want to tie himself to a specific school and he borrowed procedures indifferently from Dedekind and Kronecker, as well as from Minkowski and Hurwitz.

[115] We have underlined several times the role of lectures and students to provide mathematical continuities. It has been a crucial element in German countries, see *a contrario* the case of Italy in chap. VII.1.

This *Jahrbuch* classification was compatible with that adopted by Bachmann for his presentation of number theory in different branches (each discussed in a specific volume), and also with the one used in the *Encyclopädie der mathematischen Wissenschaften.* This new order of topics defined a different place for the main content of the D.A.: congruences, quadratic reciprocity, and also binary quadratic forms – equivalence, classes, reduction, but usually not genus theory nor the composition of forms – were now seen as *elementary* number theory.[116] The other parts[117] of number theory at that time – namely the theory of forms, algebraic number fields, and analytic number theory – entertained varied relations with the D.A.: all of them could be seen in some respects as stemming from Gauss's book, while none of them could claim Gauss's disciplinary heritage for itself alone.[118]

However, the structure of the *Disquisitiones Arithmeticae* and its history did inform other classifications of number theory.[119] The Subject Index of the *Catalogue of Scientific Papers 1800–1900* classifies number theory following an order which, after some introductory sections on divisibility and Diophantine equations, reminds one of Smith's *Report on the Theory of Numbers*, see chap. I.1, § 5.2: congruences and forms are handled consecutively and the list concludes with a number of miscellanea on cyclotomy, presented as the application of circular functions to number theory, and on other analytical aspects. Of particular interest is the fact that the *Catalogue* distinguishes between "forms of higher degree which cannot be considered as products of linear factors," and "forms of higher degree which can be considered as products of linear factors." The last are classified with "algebraic numbers" and "ideals" – thus joining together the various programmes proposed for the arithmetical study of algebraic numbers, an amusing testimony of the historical crossroads we have already met.

The shadow of the table of contents of the D.A. does not haunt only such retrospective catalogues surveying the mathematical literature of the past. In his famous Paris lecture, in 1900, Hilbert dedicated to number theory 6 out of 23 problems (nos. 7–12).[120]

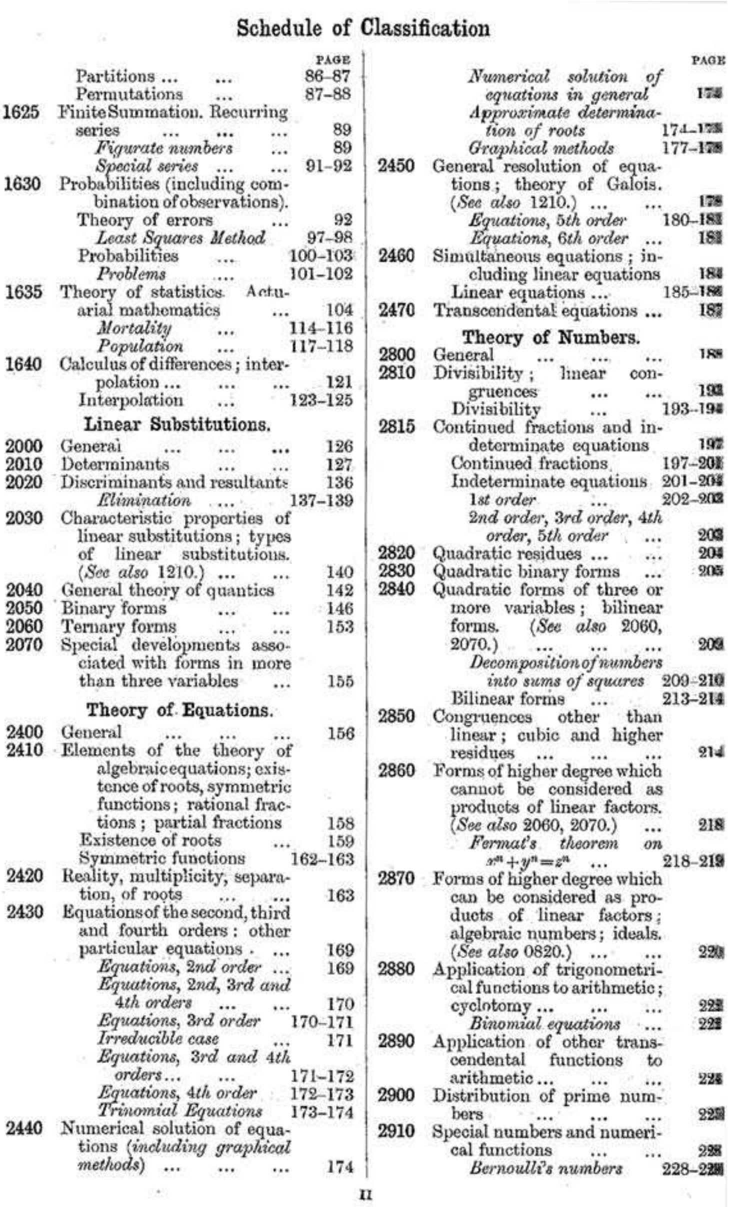
[116] What Gauss called "elementary" in the preface of the D.A. was the part of arithmetic dealing with the writing of integers and the usual operations. On the other hand, books on the *elements* of the theory of number fields, like Reid's, would soon restructure the arithmetic study of **Z** on the model of the *Zahlbericht* or propose a detailed presentation of the simplest case, that of quadratic fields.

[117] Probably because of the expansion of advanced teaching, the links between the academic disciplines and the research fields seem at this time closer than what we described in chap. I.1 for the 1850s.

[118] At the 2001 Oberwolfach meeting, Ralf Haubrich proposed seven criteria to characterize a mathematical discipline (subject matter, key concepts and results, systematization, proofs,...) and showed that algebraic number theory and Gaussian number theory (see chap. I.1, § 5.2) differ on all accounts. Alain Herreman has semiotically opposed Gauss's sec. 5 with set-theoretical formulations in "Vers une analyse sémiotique de la théorie des ensembles: hiérarchies et réflexivité," http://perso.univ-rennes1.fr/alain.herreman/.

[119] See also Dickson's *History* discussed in D. Fenster's chap. VII.3 below.

[120] We can compare this to the mere 4% of publications that this field represented at the time.



Schedule of Classification

		PAGE
	Partitions	86–87
	Permutations ...	87–88
1625	Finite Summation. Recurring series	89
	Figurate numbers ...	89
	Special series	91–92
1630	Probabilities (including combination of observations).	
	Theory of errors ...	92
	Least Squares Method	97–98
	Probabilities ...	100–103
	Problems ...	101–102
1635	Theory of statistics Actuarial mathematics ...	104
	Mortality ...	114–116
	Population ...	117–118
1640	Calculus of differences; interpolation	121
	Interpolation ...	123–125
	Linear Substitutions.	
2000	General	126
2010	Determinants	127
2020	Discriminants and resultants	136
	Elimination ...	137–139
2030	Characteristic properties of linear substitutions; types of linear substitutions. (*See also* 1210.)	140
2040	General theory of quantics	142
2050	Binary forms	146
2060	Ternary forms	153
2070	Special developments associated with forms in more than three variables ...	155
	Theory of Equations.	
2400	General	156
2410	Elements of the theory of algebraic equations; existence of roots, symmetric functions; rational fractions; partial fractions	158
	Existence of roots ...	159
	Symmetric functions	162–163
2420	Reality, multiplicity, separation, of roots	163
2430	Equations of the second, third and fourth orders: other particular equations	169
	Equations, 2nd order ...	169
	Equations, 2nd, 3rd and 4th orders	170
	Equations, 3rd order	170–171
	Irreducible case ...	171
	Equations, 3rd and 4th orders	171–172
	Equations, 4th order	172–173
	Trinomial Equations	173–174
2440	Numerical solution of equations (*including graphical methods*)	174
	Numerical solution of equations in general	174
	Approximate determination of roots	174–175
	Graphical methods	177–178
2450	General resolution of equations; theory of Galois. (*See also* 1210.)	178
	Equations, 5th order	180–181
	Equations, 6th order ...	181
2460	Simultaneous equations; including linear equations	184
	Linear equations ...	185–186
2470	Transcendental equations ...	187
	Theory of Numbers.	
2800	General	188
2810	Divisibility; linear congruences	192
	Divisibility ...	193–194
2815	Continued fractions and indeterminate equations	197
	Continued fractions	197–201
	Indeterminate equations	201–204
	1st order ...	202–203
	2nd order, 3rd order, 4th order, 5th order ...	203
2820	Quadratic residues	204
2830	Quadratic binary forms ...	205
2840	Quadratic forms of three or more variables; bilinear forms. (*See also* 2060, 2070.)	209
	Decomposition of numbers into sums of squares	209–210
	Bilinear forms ...	213–214
2850	Congruences other than linear; cubic and higher residues	214
2860	Forms of higher degree which cannot be considered as products of linear factors. (*See also* 2060, 2070.) ...	218
	Fermat's theorem on $x^n+y^n=z^n$ ...	218–219
2870	Forms of higher degree which can be considered as products of linear factors; algebraic numbers; ideals. (*See also* 0820.)	220
2880	Application of trigonometrical functions to arithmetic; cyclotomy	222
	Binomial equations ...	222
2890	Application of other transcendental functions to arithmetic	224
2900	Distribution of prime numbers	225
2910	Special numbers and numerical functions	228
	Bernoulli's numbers	228–229

II

Fig. I.2B. The Theory of Numbers in the *Catalogue of Scientific Papers* (Courtesy of the Bibliothèque Mathématiques-Recherche Jussieu, Paris)

Of these, the first two lie outside the scope of the D.A.: nos. 7, 8, which concern irrationality and the distribution of primes. But the three[121] problems 9, 11, 12 correspond neatly, and in the order of Hilbert's list, to the *Disquisitiones*, although presented from Hilbert's point of view, i.e., centered around the notion of number field: no. 9 asks for the generalization to number fields of the general reciprocity law; no. 11 for a theory of forms over such fields; and no. 12 concerns complex multiplication and is thus at the junction of number theory, algebra, and function theory, just like Gauss's famous sec. 7. In problem 11, for instance, Hilbert wrote:

> Our present knowledge of the theory of quadratic number fields puts us in a position *to successfully attack the theory of quadratic forms with any number of variables and with any algebraic numerical coefficients.* This leads in particular to the interesting problem: to solve a given quadratic equation with algebraic numerical coefficients in any number of variables by integral or fractional numbers belonging to the algebraic realm of rationality determined by the coefficients.[122]

The *Disquisitiones Arithmeticae* survived at the beginning of the XX$^{\text{th}}$ century as a cultural icon, as a historical source, as a frame for number theory. But this did not mean that its role as a mathematical resource had come to an end. On various occasions in this book, the authors allude to the way in which relatively recent results by André Weil, Kurt Heegner, John Tate, and – even more recently – Manjul Bhargava, and others, connect to specific articles or techniques of the D.A.[123]

We find it fitting to mention as a final example an article which puts us precisely one century after the publication of the *Disquisitiones Arithmeticae*, and links it, unexpectedly, to perhaps the single important branch of number theory which has only fully blossomed in the XX$^{\text{th}}$ century, Diophantine geometry,[124] and which, moreover, is related to precisely that part of number theory which Gauss essentially excluded from the D.A.: Diophantine analysis. In his 1901 article on the arithmetic of algebraic curves, Henri Poincaré proposed to interpret Diophantine questions geometrically[125] and to classify them up to birational equivalence: he not only

[121] The remaining problem, the tenth, is about Diophantine equations, and, here as in Dickson's *History of the Theory of Numbers*, is squeezed between divisibility and the theory of forms.

[122] [Hilbert 1932–1935], vol. 3, pp. 310–311: *Unsere jetzige Kenntnis der Theorie der quadratischen Zahlkörper setzt uns in den Stand,* die Theorie der quadratischen Formen mit beliebig vielen Variablen und beliebigen algebraischen Zahlkoeffizienten erfolgreich in Angriff zu nehmen. *Damit gelangen wir insbesondere zu der interessanten Aufgabe, eine vorgelegte quadratische Gleichung beliebig vieler Variablen mit algebraischen Zahlkoeffizienten in solchen ganzen oder gebrochenen Zahlen zu lösen, die in dem durch die Koeffizienten bestimmten algebraischen Rationalitätsbereiche gelegen sind.*

[123] See chap. I.1, footnotes 21, 37, 79; part II and part VIII below.

[124] Cf. the volumes on number theory in the *Encyclopaedia of Mathematical Sciences*, published in the 1990s.

[125] Interesting new links between geometry and number theory have been created during the last decades of the XX$^{\text{th}}$ century. Only a few hints have been given here, see J. Schwermer's chap. VIII.1 on Minkowski and [Schappacher 1991].

alluded to Gauss's equivalence of quadratic forms in the introduction, as a model for this birational equivalence of curves, but he also proposed as a point of departure of his work a fresh look at a specific article of the D.A.:

> To recognize when a conic has a rational point is a problem that Gauss has taught us how to solve in the chapter of his *Disquisitiones Arithmeticae* entitled *Repraesentatio ciffrae*. The conics without a rational point are arranged in several classes and the conditions of this arrangement follow immediately from the principles of the same chapter in Gauss.[126]

5. Paradises Lost

That the *Disquisitiones Arithmeticae* is both a mathematical work and a historical event does not mean that it is an obvious object for the history of mathematics. Immediately after its publication, concepts, results, themes, were detached, reintegrated in other points of views, and grew to have each their own story to tell.[127] The way they could be isolated or amalgamated depends, as we have seen, on many factors, some of which stem from the D.A., some from other publications; some are the result of generational shifts among the readers or of the ambient scientific priorities. Different parts of the D.A. have been activated at different times, then left aside for a while and reactivated again, with completely different research horizons in mind.

Even if we could follow each of these fragments, we would still miss our target. The *Disquisitiones Arithmeticae* had several functions: a mythical model for number-theoretical activities, a technical reference, a familiar companion of everyday mathematical experience. The content of the book has at times defined number theory, and at others has been cut and reshaped to fit new disciplinary views. All these different scales matter for the history of the book. They require the reconstitution of relevant strata of textual organization and of the contexts which have allowed these strata to be interpreted and used efficiently for doing mathematics. Our choice here to stick to explicit mentions of the D.A. has already led us to historical evidence of all kinds, from personal correspondence to lectures, from treatises of cultural history to political gazettes, from catalogues to research papers. And these mentions have been of all sorts: one article of the D.A., a notation, a whole section, a way of thinking.

Our main goal in this part has been to reshape the global representation of the history of the D.A. – this will help, we hope, to situate more accurately the results of the following chapters. We were not satisfied with the usual summary – a period of latency and awe, then a succession of a small number of brilliant contributors, one or two per generation,who were deeply involved with the book, and finally the blossoming of algebraic number theory at the turn of the twentieth century. What we

[126] [Poincaré 1901], p. 485: *Reconnaître si une conique admet un point rationnel, c'est un problème que Gauss nous a enseigné à résoudre, dans son chapitre des* Disquisitiones*, intitulé* Repraesentatio ciffrae*. Les coniques qui n'ont pas de point rationnel se répartissent en plusieurs classes et les conditions de cette répartition se déduisent immédiatement des principes de ce même chapitre de Gauss.* The reference is to D.A., art. 299, on ternary forms; a plane conic is the zero set of a ternary quadratic form.

[127] Specific examples are traced in part II, part IV, and part VIII below.

wanted was to pay more attention to the relations among mathematicians (and among their results), and to the actual mechanisms of knowledge transfer, in particular from one generation to another,[128] that is, to understand some part of the dynamics in the changing role of the D.A. and of number theory.

What we have seen here is, first, that a serious study of a limited part of the book (all that touching the theory of equations) took place quite quickly, and that it nourished a vast expansion of algebra.[129] For a while, it tended to relegate congruences to a supporting role – the topic which, in what survives of Gauss's original plans, secured the coherence of the whole – and it pointed toward an assimilation of arithmetic and algebra.

Then, from the mid 1820s on, new types of readers of the D.A. appeared: they immersed themselves in the D.A., often on their own, early in their mathematical life; and they made it the arithmetical seed of a large international area of research, this time mixing number theory, algebra, and analysis. The mixture operated in many ways: using analytical techniques to prove statements left open in the D.A.; encapsulating links between properties of integers and continuous functions in an algebraic formula; and creating algebraic analytic concepts by means of those introduced in the D.A. Here we find the well-known names of Jacobi, Dirichlet, Kummer, Eisenstein, Hermite, Kronecker, and others. But we want to stress that they intervened in an essentially unique network, precipitated out by intense exchanges among these mathematicians, accompanied by a characteristic discourse concerning the value of unity, even when their work displayed different mathematical agendas.

The mechanisms at work in the 1860s are still unclear for us.[130] During the following decades, textbooks in various languages gave ready access to large parts of the D.A. The edition of Gauss's *Werke* and related publications also set up, specially in Germany, a "usable" Gauss,[131] a classic, of whom set pieces were made accessible to a larger audience. But in the last quarter century, components of research that were closely linked in the preceding period seem to drift apart: number theory now encompasses several rather well-established disciplines, each with its own privileged problems and relations to the D.A.

Because of its status in the standard history, we have revisited the development of one component, that of Kummer's ideal numbers. It presents several intriguing features: first of all, unlike other components, such as forms or modular equations,

[128] We think that this issue, which ought to take into account teaching, available techniques and problems, and cultural agendas, is important for the understanding of scientific development and has not yet been sufficiently studied in the history of mathematics.

[129] This stage has already been identified in [Neumann 1979–1980].

[130] This puzzlement is due partly to the increased size of the mathematical scene, but especially to the discontinuity in our sources, due in turn to the almost simultaneous disappearance, for various reasons, of the main contributors of the preceding period. The *Jahrbuch*, on the other hand, only appeared at the end of the 1860s.

[131] We mean by this something of public utility, contributing to the self-understanding and to the action of a community, here mathematical; see William J. Bouwsma, *A Usable Past. Essays in European Cultural History*. Berkeley: University of California Press, 1990.

it concerns a mere handful of articles and appears to be mainly a German affair.[132] Then, it makes evident the paradoxical nature of Dedekind's activities. The most important influences on him were those of Dirichlet and Riemann; unlike most of his German colleagues, he had virtually no research students.[133] But he mediated in three different and important ways the number-theoretical work of the first half century for the generation coming to (mathematical) age in the 1880s. He edited Dirichlet's *Vorlesungen über Zahlentheorie*, one of the most influential "surrogates" for the D.A.; he annotated and wrote commentaries on Gauss's writings for the *Werke*, thus imprinting his mark on the interpretation of Gauss for decades to come; and finally, in his own mathematical work, he synthetized various threads coming from the D.A.; in particular Galois (group) theory, higher congruences, and Kummer's ideal numbers. However the continuity running from his work to the new generation is really a product of the latter.

Indeed a decisive event at the end of the century was the meeting of Hilbert, Minkowski, and Hurwitz,[134] soon connected to Klein's Göttingen. Besides their syncretic approach – which nonetheless privileged Dedekind's ideals and number fields as key objects – their skill in evocative presentation and their numerous students around the world were instrumental in establishing within a few years a new *subdiscipline* within number theory, algebraic number theory – one which put reciprocity laws back at center stage.[135]

This group produced not only influential mathematics but equally influential views of the development of mathematics, such as Klein's *Vorlesungen über die Entwicklung der Mathematik in XIX*$^{\text{ten}}$ *Jahrhundert* and the preface to Hilbert's *Zahlbericht*. Indeed historical representations are often created by mathematicians themselves; they seem all the more natural because they stem from mathematical practice and are coherent with it.[136] However, as seen above, a multitude of practices stem from the D.A. (with, perhaps, still more to come). As opposed to a person, a book like the D.A. has several identities.

Some of these identities, some of the works and memories linked to them, have been transmitted to the present. But only some. Those which have been lost for a while may well serve to give a more concrete meaning to the present:

[132] It is still difficult to properly evaluate the impact of Zolotarev's theory.

[133] An evocative, if incomplete, information is contained in the Mathematics Genealogy Project, which lists no descendent at all for Dedekind, but, for instance, 3867 for his Berlin contemporary Lazarus Fuchs.

[134] It is remarkable that Minkowski began with the theory of forms, Hilbert with invariant algebra, and Hurwitz with modular elliptic functions, each incarnating key components of arithmetic algebraic analysis originating from the D.A.

[135] See the interesting list of books given in [Lemmermeyer 2000], p. xii, note 6, which are all linked to this milieu.

[136] In this respect, it is interesting to contrast the various types of historical activities in some of the number theorists we have looked at: Lucas's involvement with Fermat's manuscripts, Hilbert's rational reconstruction of the evolution of number theory, Dickson's topical *History of the Theory of Numbers*.

> Yes, if a memory, thanks to forgetfulness, has been unable to contract any tie, to forge any link between itself and the present, if it has remained in its own place, of its own date, if it has kept its distance, its isolation in the hollow of a valley or on the peak of a mountain, it makes us suddenly breathe an air new to us just because it is an air we have formerly breathed, an air purer than that the poets have vainly called Paradisiacal, which offers that deep sense of renewal only because it has been breathed before, inasmuch as the true paradises are paradises we have lost.[137]

References

BACHMANN, Paul. 1872. *Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie*. Leipzig: Teubner.

———. 1892. *Zahlentheorie. Versuch einer Gesamtdarstellung dieser Wissenschaft in ihren Hauptteilen.* Part 1: *Die Elemente der Zahlentheorie*. Leipzig: Teubner.

———. 1921. *Grundlehre der neueren Zahlentheorie*. 2nd ed. Göschens Lehrbücherei I.3. Berlin, Leipzig: de Gruyter.

BELL, Eric Temple. 1951. *Mathematics—Queen and Servant of Science*. New York: McGraw-Hill. Part. repr. The Queen of Mathematics. In *The World of Mathematics*, ed. J. Newman, vol. 1, pp. 498–518. New York: Simon and Schuster, 1956.

BLUMENTHAL, Otto. 1935. Lebensgeschichte. In [Hilbert 1932–1935], vol. 3, pp. 388–429.

BÖLLING, Reinhard. 1994. *Das Fotoalbum für Weierstraß – A Photo Album for Weierstrass*. Braunschweig, Wiesbaden: Vieweg.

BREZYNSKI, Claude. 1991. *History of Continued Fractions and Padé Approximants*. Berlin: Springer.

CHÂTELET, Albert. 1913. *Leçons sur la théorie des nombres*. Paris: Gauthier-Villars.

CONTE, Alberto, GIACARDI, Livia (eds.). 1991. *Angelo Genocchi e i suoi interlocutori scientifici. Contributi dall'epistolario.* Studi e Fonti per la Storia della Università di Torino 4. Torino: Deputazione subalpina di storia patria.

CORRY, Leo. 1996. *Modern Algebra and the Rise of Mathematical Structures*. Science Networks 17. Basel, Boston, Berlin: Birkhäuser. 2nd ed., 2004.

DÉCAILLOT, Anne-Marie. 1999. *Edouard Lucas (1842–1891): le parcours original d'un scientifique français dans la deuxième moitié du XIXe siècle*. Thèse de l'université René Descartes. Paris.

DEDEKIND, Richard. 1930–1932. *Gesammelte mathematische Werke*, ed. R. Fricke, E. Noether, O. Ore. 3 vols. Braunschweig: Vieweg.

DICKSON, Leonard Eugene. 1919–1923. *History of the Theory of Numbers.* 3 vols. Washington: The Carnegie Institute. Repr. New York: Chelsea, 1956.

[137] Stephen Hudson's transl. from Marcel Proust, *Le temps retrouvé*: *Oui, si le souvenir, grâce à l'oubli, n'a pu contracter aucun lien, jeter aucun chaînon entre lui et la minute présente, s'il est resté à sa place, à sa date, s'il a gardé ses distances, son isolement dans le creux d'une vallée ou à la pointe d'un sommet; il nous fait tout à coup respirer un air nouveau, précisément parce que c'est un air qu'on a respiré autrefois, cet air plus pur que les poètes ont vainement essayé de faire régner dans le Paradis et qui ne pourrait donner cette sensation profonde de renouvellement que s'il avait été respiré déjà, car les vrais paradis sont les paradis qu'on a perdus.*

DUGAC, Pierre. 1976. *Richard Dedekind et les fondements des mathématiques*. Paris: Vrin.

EDWARDS, Harold M. 1975. The Background of Kummer's Proof of Fermat's Last Theorem for Regular Primes. *Archive for History of Exact Sciences* 14, 219–236.

———. 1980. The Genesis of Ideal Theory. *Archive for History of Exact Sciences* 23, 321–378.

———. 1983. Dedekind's Invention of Ideals. *Bulletin of the London Mathematical Society* 15, 8–17.

———. 1992a. Kronecker's Arithmetical Theory of Algebraic Quantities. *Jahresberichte der Deutschen Mathematiker-Vereinigung* 94, 130–139.

———. 1992b. Mathematical Ideas, Ideals, and Ideology. *The Mathematical Intelligencer* 14, 6–19.

———. 1995. Kronecker on the Foundations of Mathematics. In *From Dedekind to Gödel. Essays on the Development of the Foundations of Mathematics*, ed. J. Hintikka, pp. 45–52. Synthese Library, Studies in Epistemology, Logic, Methodology, and Philosophy of Science 251. Dordrecht, Kluwer.

EDWARDS, Harold M., NEUMANN, Olaf, PURKERT, Walter. 1982. Dedekinds "Bunte Bemerkungen" zu Kroneckers "Grundzüge." *Archive for History of Exact Sciences* 27, 49–85.

EISENSTEIN, Gotthold. 1975. *Mathematische Werke*. 2 vols. New York: Chelsea.

FERREIRÓS, Jose. 1999. *Labyrinth of Thought. A History of Set Theory and its Role in Modern Mathematics*. Basel, Boston: Birkhäuser.

GAUSS, Carl Friedrich. 1866. *Werke*, vol. III, *Analysis*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universitäts-Druckerei.

———. 1889. *Untersuchungen über höhere Arithmetik*, ed. and German transl. H. Maser. Berlin: Springer. Repr. New York: Chelsea, 1965; 2nd ed., 1981.

GISPERT, Hélène, TOBIES, Renate. 1996. A Comparative Study of the French and German Mathematical Societies before 1914. In *L'Europe mathématique. Mathematical Europe*, ed. C. Goldstein, J. Gray, J. Ritter, pp. 407–430. Paris: Maison des sciences de l'homme.

GOLDSTEIN, Catherine. 1994. La théorie des nombres dans les *Comptes rendus de l'Académie des sciences* (1870–1914) : un premier examen. *Rivista di Storia della Scienza* 2nd ser. 2, 137–160.

———. 1999. Sur la question des méthodes quantitatives en histoire des mathématiques : le cas de la théorie des nombres en France (1870–1914). *Acta historiæ rerum naturalium necnon technicarum* New ser. 3, 187–214.

———. 2005. Johann Peter Gustav Lejeune-Dirichlet, *Vorlesungen über Zahlentheorie*, first edition (1863). In *Landmark Writings in Western Mathematics*, ed. I. Grattan-Guinness, pp. 480–490. Amsterdam, Boston, etc.: Elsevier.

GRAY, Jeremy. 1996. The Nineteenth-Century Revolution in Mathematical Ontology. In *Revolutions in Mathematics*, ed. D. Gillies, pp. 226-248. Oxford: Oxford University Press.

HAGNER, Michael. 2004. *Geniale Gehirne. Zur Geschichte der Elitegehirnforschung*. Göttingen: Wallstein.

HAUBRICH, Ralf. 1992. *Zur Entstehung der algebraischen Zahlentheorie Richard Dedekinds*. Dissertation, Georg-August-Universität Göttingen. Göttingen.

Hermite, Charles. 1905–1917. *Œuvres*, ed. E. Picard. 4 vols. Paris: Gauthier-Villars.

Hilbert, David. 1932–1935. *Gesammelte Abhandlungen.* 3 vols. Berlin: Julius Springer.

Hurwitz, Adolf. 1985. Über einen Fundamentalsatz der arithmetischen Theorie der algebraischen Grössen. *Nachrichten von der königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-physikalische Klasse* 1985, 230–240. Repr. in *Mathematische Werke*, vol. 2, pp. 198–207. Basel: Birkhäuser, 1963.

Klein, Felix. 1894. *Lectures on Mathematics. The Evanston Colloquium.* New York: Macmillan. Repr. Providence (R.I): AMS, 1911; 2000.

———. 1926. *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert*, ed. R. Courant, O. Neugebauer, vol. 1. Berlin: Springer; repr. (with vol. 2) New York: Chelsea, 1967; repr. Berlin, Heidelberg, New York: Springer, 1979.

Kronecker, Leopold. 1895–1931. *Werke*, ed. K. Hensel. 5 vols. Leipzig: Teubner. Rep. New York: Chelsea, 1968.

———. 1901. *Vorlesungen über Zahlentheorie*, vol. 1, ed. K. Hensel. Leipzig: Teubner. Repr. Berlin, Heidelberg, New York: Springer, 1978.

Kuhn, Thomas S. 1970. *The Structure of Scientific Revolutions.* International Encyclopedia of Unified Science 2, II. 2nd enlarged ed. Chicago: Chicago University Press.

Kummer, Ernst Eduard. 1975. *Collected Papers*, ed. A. Weil. 2 vols. Berlin, Heidelberg, etc.: Springer.

Lavrinenko, Tatiana. 2002. Solving an indeterminate third degree equation in rational numbers. Sylvester and Lucas. *Revue d'histoire des mathématiques* 8-1, 67–111.

Lemmermeyer, Franz. 2000. *Reciprocity Laws from Euler to Eisenstein.* Berlin, etc.: Springer.

Lipschitz, Rudolf. 1986. *Briefwechsel mit Cantor, Dedekind, Helmholtz, Kronecker, Weierstrass*, ed. W. Scharlau. Dokumente zur Geschichte der Mathematik 2. Braunschweig, Wiesbaden: Vieweg.

McKenzie, Donald F. 1986. *Bibliography and the Sociology of Texts.* London: British Library. 2e ed. Cambridge: Cambridge University Press, 1999.

Neumann, Olaf. 1979–1980. Bemerkungen aus heutiger Sicht über Gauss' Beiträge zu Zahlentheorie, Algebra und Funktionentheorie. *NTM-Schriftenreihe* 16:2, 22–39; 17:1, 32–48; 17:2, 38–58.

———. 2002. Was sollen und was sind Divisoren?, *Mathematische Semesterberichte* 48, 139–192.

Ozhigova, Elena Petrovna, Yuškevič, Adolph Andrei Pavlovič. 1992. Problems of Number Theory. In *Mathematics of the 19th Century. Mathematical Logic. Algebra. Number Theory. Probability Theory*, ed. A. N. Kolmogorov and A. P. Yuškevič, chap. 3. Basel, Boston, Berlin: Birkhäuser.

Parshall, Karen. 1998. *James Joseph Sylvester. Life and Work in Letters.* Oxford: Clarendon Press.

———. 2006. *James Joseph Sylvester: Jewish Mathematician in a Victorian World.* Baltimore: The Johns Hopkins University Press.

Poincaré, Henri. 1897. Les rapports de l'analyse et de la physique mathématique. *Acta Mathematica* 21, 331–341. Repr. *Revue générale des sciences pures et appliquées* 8, 857–861. Repr. in *L'analyse et la recherche*, ed. G. Ramunni. Paris: Hermann, 1991.

———. 1901. Sur les propriétés arithmétiques des courbes algébriques. *Journal de mathématiques pures et appliquées* 5^{e} ser., 7-3, 161–233. Repr. in *Œuvres*, vol. 5, ed. A. Châtelet, pp. 483–550. Paris, Gauthier-Villars, 1950.

PURKERT, Walter. 1971–1973. Zur Genesis des abstrakten Körperbegriffs. *NTM-Schriftenreihe* 8:1, 23–37; 10:2, 8–20.

———. 1981. Richard Dedekind – zum 150. Geburtstag. *Mitteilungen der Mathematischen Gesellschaft der Deutschen Demokratischen Republik* 2/4, 84–110.

ROLLET, Laurent, NABONNAND, Philippe. 2002. Une bibliographie mathématique idéale ? Le *Répertoire bibliographique des sciences mathématiques*. *Gazette des mathématiciens* 92, 11–26.

ROWE, David. 1989. Klein, Hilbert, and the Göttingen Mathematical Tradition. *Osiris* 5-2, 186–213.

SCHAPPACHER, Norbert. 1991. Développement de la loi de groupe sur une cubique. In *Séminaire de Théorie des Nombres de Paris 1988–1989*, ed. C. Goldstein, pp. 159–184. Progress in Mathematics 91. Boston, Basel, etc.: Birkhäuser.

———. 2005. David Hilbert, Report on Algebraic Number Fields (*Zahlbericht*) (1897). In *Landmark Writings in Western Mathematics*, ed. I. Grattan-Guinness, pp. 700–709. Amsterdam, Boston, etc.: Elsevier.

SCHARLAU, Winfried. 1982. Unveröffentliche algebraische Arbeiten Richard Dedekinds aus seiner Göttinger Zeit 1855–1858. *Archive for History of Exact Sciences* 36, 63–74.

SELLING, Eduard. 1865. Über die idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln einer beliebigen irreductiblen Gleichung rational gebildet sind. *Zeitschrift für Mathematik und Physik* 10, 17–47.

SIEGMUND-SCHULTZE, Reinhard. 1993. *Mathematische Berichterstattung in Hitlerdeutschland. Der Niedergang des "Jahrbuchs über die Fortschritte der Mathematik."* Göttingen: Vandenhoeck & Ruprecht.

SMITH, Henry John Stephen. 1894. *The Collected Mathematical Papers*, ed. J.W.L. Glaisher. 2vols. Oxford: Clarendon Press.

STROBL, Walter. 1985. Aus den wissenschaftlichen Anfängen Hermann Minkowskis. *Historia Mathematica* 12, 142–156.

TANNERY, Jules. 1895. *Introduction à l'étude de la théorie des nombres et de l'algèbre supérieure*. Paris: Nony.

ULLRICH, Peter. 1998. The Genesis of Hensel's p-adic Numbers. In *Karl der Grossen und sein Nachwirken. 1200 Jahre Kultur und Wissenschaft in Europa*, ed. P.L Butzer, H. Th. Jongen, and W. Oberschelp, vol. 2, pp. 163-178. Turnhout: Brepols.

WUSSING, Hans. 1969. *Die Genesis des abtrakten Gruppenbegriffs. Ein Beitrag zur Entstehungsgeschichte der abtrakten Gruppentheorie.* Berlin: VEB Deutscher Verlag der Wissenschaften. English transl. A. Shenitzer. Cambridge: MIT Press, 1984.

ZOLOTAREV, Egor Ivanovich. 1872. Sur la méthode d'intégration de M. Tchebychef. *Mathematische Annalen* 5, 560–580. Repr. *Journal de mathématiques pures et appliquées* 2nd ser. 19 (1874), 161–188.

———. 1880. Sur la théorie des nombres complexes. *Journal de mathématiques pures et appliquées* 3^{e} ser. 6, 51–94, 129–166. Repr. in *Polnoe Sobranie Sochineny Egora Ivanovicha Zolotareva* (Collected Papers of Egor lvanovich Zolotarev), vol. 1, pp. 72–179. Leningrad: V.A. Steklov Institute of Physics and Mathematics.

Part II

Algebraic Equations, Quadratic Forms, Higher Congruences: Key Mathematical Techniques of the *Disquisitiones Arithmeticae*

Mr. Gauss a traité d'une manière entièrement nouvelle toute cette théorie, dans un ouvrage singulièrement remarquable, dont il nous est impossible de donner une idée, parce que tout y est nouveau, jusqu'au langage et à la notation.

Jean-Baptiste Delambre to the Emperor Napoléon
February 8, 1808

II.1

The *Disquisitiones Arithmeticae* and the Theory of Equations

Olaf Neumann

Carl Friedrich Gauss enriched the theory of algebraic equations with his four proofs of the Fundamental Theorem of Algebra – see [Netto 1913] –, but also with the *Disquisitiones Arithmeticae* (abbreviated in what follows by D.A.). Our goal is to discuss sec. 7 of the D.A., "On the equations on which the division of the circle depends." This section, which comprises 32 articles, is entirely devoted to the equations $x^n - 1 = 0$ (that is, what we call cyclotomy theory)[1] and to some striking number-theoretic implications.[2] It uses the basic concepts of the theory of equations at that time: roots and their relations, resolvents. However, our main thesis is that Gauss's cyclotomy theory marks a turning point in the theory of equations since it brought to the fore the concept of irreducibility. More precisely, Gauss insisted on the systematic search for "equations of as low an order as possible" satisfied by a given quantity. Such equations cannot be factorized into equations of lower degree with respect to a given domain of rationality; moreover, Euclidean algorithm shows that, for a given quantity, they are uniquely determined up to constant factors. Such equations, for which Gauss apparently did not introduce a specific name, were called irreducible in the writings of Niels Henrik Abel and Evariste Galois, see [Abel 1829], § 1, and [Galois 1831/1846].

1. Equations Before 1801: A Combinatorial Approach

The major breakthrough of the modern theory of equations was the solution of cubic and quartic numerical equations by radicals. These great achievements can be traced

[1] The word "cyclotomy" is of Greek origin and means "division of the circle." It seems that James Joseph Sylvester was the first mathematician who used this term.

[2] Gauss proved in particular that every square root of a rational integer is a linear combination of roots of unity with rational-integer coefficients (art. 356). This result links the theory of cyclotomy and the theory of quadratic residues.

back to Scipione del Ferro, Niccolò Fontana (nicknamed "Tartaglia," that is, the stammerer), Girolamo Cardano and Ludovico Ferrari, a pupil of Cardano. A crucial next step was the development of symbolic algebra through the work of François Viète, Thomas Harriot and René Descartes. During the following century and a half, the guiding principles of argumentation were based on the transformations of an equation and the relations between roots and coefficients, see, e.g., [Scholz 1990]. Moreover, it was observed that the formulae were really formal, in the sense that they remained valid if one inserted indeterminate quantities instead of numbers as coefficients. The discussion of Cardano's formula had a very important side effect: it prompted the (unavoidable) use of complex numbers.

Eventually, the writings of Jean-Baptiste le Rond d'Alembert, Leonhard Euler, François Daviet de Foncenex and Joseph-Louis Lagrange convinced mathematicians that every equation of degree n with real (or complex) coefficients has n real or complex roots.[3] They felt free to operate formally with all the roots of an equation and became able to gather information on the roots from the coefficients without solving the equation. A basic insight and indispensable tool was the result that every symmetric polynomial can be written as a polynomial in the elementary symmetric functions in a unique way. This result cannot be attributed with certainty to any specific author; in 1770 Lagrange called it "self-evident" (*évident par soi-même*, [Lagrange 1770–1771], art. 98). Gauss proved it in his second treatise on the Fundamental Theorem of Algebra, while he had mentioned it already in his dissertation.[4] At a decisive place in his *Disquisitiones Arithmeticae* (art. 338), Gauss also used Isaac Newton's expression of the sums of the k^{th} powers in terms of the elementary symmetric functions, i.e. a special instance of this fundamental theorem on symmetric polynomials – see [Edwards 1984], §§ 8–12.

Around 1770, three outstanding mathematicians, namely Lagrange, Alexandre-Théophile Vandermonde and Edward Waring, tackled a wide-ranging program to form auxiliary equations (*resolvents*) according to the following recipe. For any equation with roots $x_1, \dots, x_n$, say

$$f(x) = (x - x_1) \dots (x - x_n) = 0, \tag{1}$$

choose a rational function $r(x_1, \dots, x_n)$, and subject it to *all* permutations of the $x_1, \dots, x_n$; one gets a certain number N of formally different functions $r = r_1, \dots, r_N$. Let us then form the equation (*resolvent*)

$$g(x) = (x - r_1) \dots (x - r_N) = 0. \tag{2}$$

The coefficients of $g(x)$ are symmetric in $x_1, \dots, x_n$ and can be calculated in terms of the elementary symmetric functions, i.e. the coefficients of $f(x) = 0$ – cf. [Lagrange 1770–1771], [Vandermonde 1770–1771], [Waring 1770]. One expects to get accessible equations $g(x) = 0$ if one starts with suitable functions r. Lagrange

[3] This is the "Fundamental Theorem of Algebra." On this development, see [Dieudonné 1978], chap. 2.2; [Tignol 1988], chap. 9; [Yuškevič 1972], chap. 2; [Gilain 1992].

[4] Respectively: [Gauss 1816], art. 4 and [Gauss 1799], art. 8.

himself spoke of a "certain kind of calculus of combinations,"[5] hence the choice of our title for this section.

Today's reader should keep in mind that, in general, a permutation of the $x_1, \dots, x_n$ does *not* induce an automorphism of the splitting field of $f(x)$, since the expression $r(x_1, \dots, x_n)$ as a function need not be unique. However, uniqueness is true for the general equation $f(x) = 0$, that is, the equation whose coefficients are (algebraically) independent indeterminates. That is why Lagrange's treatment of the general equation fits Évariste Galois's approach, basically without alterations. Galois's fundamental insight was to understand how to restrict the permutations of the roots in order to obtain an appropriate group for every equation.

2. Solvable Equations

Experience had shown that equations of degree $n \le 4$ could be solved by chains of so-called *pure equations* $x^m - a = 0$, of degree $m \le n$, and by adjunction of roots of unity. The task of solving equations algebraically had been then modelled on the equations of degree up to 4: it meant solving an equation in a similar fashion by a chain of pure equations $x^m - a = 0$, in other words, iterating the operations of addition, subtraction, multiplication, division, and extraction of roots. Apparently, quite often, it is tacitly assumed that the indices of the radicals do not exceed the degree of the given equation.[6] To take a root with a composite index $m = k \cdot l$, one can first extract a root with index k and then a root with index l: $\sqrt[m]{a} = \sqrt[l]{\sqrt[k]{a}}$. Thus we may confine ourselves to extractions of roots with prime-number indices. But $\sqrt[m]{a}$ is determined only up to an arbitrary m^{th} root of unity and, in general, to get all solutions of an equation, this ambiguity cannot be avoided, as is already demonstrated by the formulae for the roots of quadratic and cubic equations. The roots of unity must thus be taken into account.

Before Vandermonde's paper [Vandermonde 1770–1771], it was known that the special equations $x^n - 1 = 0$ with $n \le 10$ can be solved by radicals of indices $< n$. Vandermonde's greatest achievement was the discovery that similar methods worked for $x^{11} - 1 = 0$ as well. In order to solve this equation, he gave explicit formulae containing $\sqrt{5}$, other square roots, 5th roots, and, in particular, in hidden form, the 5th roots of unity. Vandermonde claimed he could solve *every* equation $x^n - 1 = 0$ with a *prime number n* by means of suitable radicals of indices $< n$. Unfortunately,

[5] [Lagrange 1770–1771], art. 109: *Voilà, si je ne me trompe, les vrais principes de la résolution des équations et l'analyse la plus propre à y conduire ; tout se réduit, comme on voit, à une espèce de calcul des combinaisons, par lequel on trouve* à priori *les résultats auquels on doit s'attendre. Il serait à propos d'en faire l'application aux équations du cinquième degré et des degrés supérieurs, dont la résolution est jusqu'à présent inconnue.... Nous nous contenterons ici d'avoir posé les fondements d'une théorie qui nous paraît nouvelle et générale.*

[6] Otherwise, for instance, one could consider any solution of $x^{n-1} + \cdots + x + 1 = (x^n - 1)/(x - 1) = 0$ as a radical $\sqrt[n]{1}$ by definition, and the equation being solved by radicals this way. It is to be regretted that questions of this kind are usually not discussed carefully in the historiography nor in textbooks on algebra.

he did not offer any sound argument how to do that.[7] Yet no less a mathematician than Leopold Kronecker praised Vandermonde's memoir:

> With Vandermonde's memoir on the resolution of equations, presented in 1770 to the Parisian Academy, began a new blossoming of algebra; the profundity of the view which is expressed in such clear words in this work arouses nothing less than our astonishment.[8]

Extremely important examples of auxiliary quantities which satisfy pure equations are the so-called "Lagrange resolvents" introduced by Vandermonde as well as Lagrange – see [Vandermonde 1770–1771] and [Lagrange 1770–1771]; they deserve a detailed discussion. As above, let us take some equation with simple roots $x_1, \dots, x_n$, the equation (1) for example. If α denotes a primitive n^{th} root of unity, let us form the n expressions

$$V_i = x_1 + \alpha^i \cdot x_2 + \alpha^{2i} \cdot x_3 + \cdots + \alpha^{(n-1)i} \cdot x_n \qquad (1 \le i \le n). \tag{3}$$

These are the Lagrange resolvents. We get thus a system of n linear equations for $x_1, \dots, x_n$. Since $\sum_{i=1}^{n} \alpha^{-(j-1)i} = 0$ for $j \neq 1$ and n for $j = 1$, we have

$$x_j = \frac{1}{n} \cdot \left(\sum_{i=1}^{n-1} \alpha^{-(j-1)i} \cdot V_i + V_n \right) \qquad (1 \le j \le n). \tag{4}$$

The quantity $V_n = x_1 + \cdots + x_n$ equals (-1) times the coefficient of x^{n-1} in the equation (1) and is therefore known. On the other hand, it is easy to check that the n^{th} powers $V_i^n =: R_i^{(1)}$ remain unchanged under all cyclic permutations of $(x_1, \dots, x_n)$. Therefore, every quantity $R_i^{(1)}$ takes $(n-1)!$ formally different values under *all* permutations of the $x_1, \dots, x_n$. Thus the coefficients of the polynomial

$$F_i(x) := (x - R_i^{(1)}) \dots (x - R_i^{((n-1)!)}) \qquad (1 \le i \le n)$$

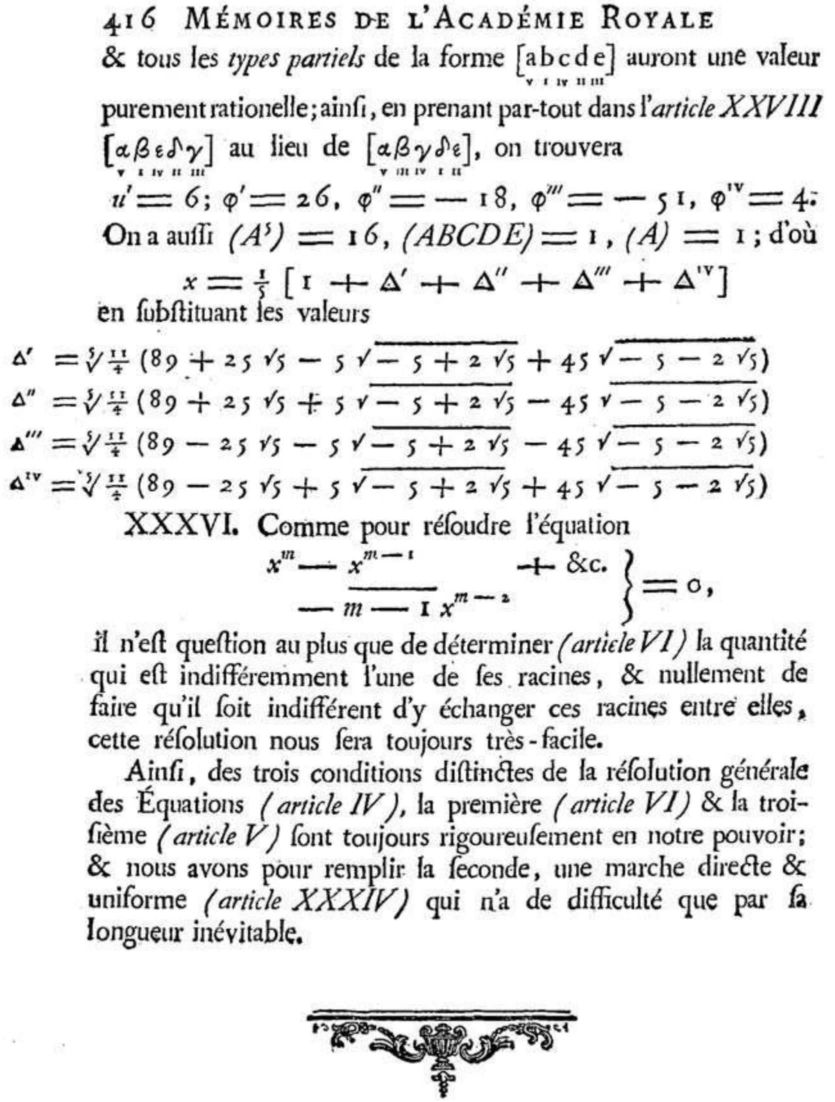
are symmetric in $x_1, \dots, x_n$, and by the fundamental theorem on symmetric functions they are rational functions of the coefficients of $f(x)$ and of the n^{th} roots of unity. For $n = 3$, one gets Cardano's formula again.

From the equation (4), one derives formally

$$x_j = \frac{1}{n} \cdot \left(\sum_{i=1}^{n-1} \alpha^{-(j-1)i} \cdot \sqrt[n]{R_i^{(1)}} + V_n \right) \qquad (1 \le j \le n). \tag{5}$$

[7] Vandermonde's work is considered in some detail in [Nový 1973], pp. 36–41, and [van der Waerden 1985]. The relationship between Vandermonde and Gauss is discussed at length in [Loewy 1918], [Lebesgue 1955] (with certain doubtful conclusions) and [Neumann 2007] (see also [van der Waerden 1985], p. 79, [Neumann 2006]).

[8] Preface to the German translation of [Vandermonde 1770–1771]: *Mit Vandermonde's im Jahre 1770 der Pariser Akademie vorgelegten Abhandlung über die Auflösung der Gleichungen beginnt der neue Aufschwung der Algebra; die Tiefe der Auffassung, welche sich in dieser Arbeit in so klaren Worten ausspricht, erregt geradezu unser Erstaunen.*



& tous les *types partiels* de la forme $[\underset{\text{v i iv ii iii}}{abcde}]$ auront une valeur purement rationelle; ainſi, en prenant par-tout dans l'*article XXVIII* $[\underset{\text{v i iv ii iii}}{\alpha\beta\varepsilon\delta\gamma}]$ au lieu de $[\underset{\text{v iii iv i ii}}{\alpha\beta\gamma\delta\varepsilon}]$, on trouvera

$u' = 6;\ \varphi' = 26,\ \varphi'' = -18,\ \varphi''' = -51,\ \varphi^{\text{iv}} = 4.$

On a auſſi $(A^5) = 16$, $(ABCDE) = 1$, $(A) = 1$; d'où

$$x = \tfrac{1}{5}\,[1 + \Delta' + \Delta'' + \Delta''' + \Delta^{\text{iv}}]$$

en ſubſtituant les valeurs

$$\Delta' = \sqrt[5]{\tfrac{11}{4}}\,(89 + 25\sqrt{5} - 5\sqrt{-5 + 2\sqrt{5}} + 45\sqrt{-5 - 2\sqrt{5}})$$
$$\Delta'' = \sqrt[5]{\tfrac{11}{4}}\,(89 + 25\sqrt{5} + 5\sqrt{-5 + 2\sqrt{5}} - 45\sqrt{-5 - 2\sqrt{5}})$$
$$\Delta''' = \sqrt[5]{\tfrac{11}{4}}\,(89 - 25\sqrt{5} - 5\sqrt{-5 + 2\sqrt{5}} - 45\sqrt{-5 - 2\sqrt{5}})$$
$$\Delta^{\text{iv}} = \sqrt[5]{\tfrac{11}{4}}\,(89 - 25\sqrt{5} + 5\sqrt{-5 + 2\sqrt{5}} + 45\sqrt{-5 - 2\sqrt{5}})$$

XXXVI. Comme pour réſoudre l'équation

$$\left.\begin{matrix} x^m - x^{m-1} & + \text{ \&c.} \\ -\overline{m-1}\,x^{m-2} & \end{matrix}\right\} = 0,$$

il n'eſt queſtion au plus que de déterminer (*article VI*) la quantité qui eſt indifféremment l'une de ſes racines, & nullement de faire qu'il ſoit indifférent d'y échanger ces racines entre elles, cette réſolution nous ſera toujours très-facile.

Ainſi, des trois conditions diſtinctes de la réſolution générale des Équations (*article IV*), la première (*article VI*) & la troiſième (*article V*) ſont toujours rigoureuſement en notre pouvoir; & nous avons pour remplir la ſeconde, une marche directe & uniforme (*article XXXIV*) qui n'a de difficulté que par ſa longueur inévitable.

Fig. II.1A. Vandermonde's treatment of $r^{11} - 1 = 0$
by means of $x^5 - x^4 - 4x^3 + 3x^2 + 3x - 1$
From *Histoire de l'Académie des sciences pour l'année 1771*
(Académie des sciences de l'Institut de France)

Here a delicate point arises. Of course, one wants first to calculate the $R_i^{(1)}$'s in terms of known quantities. When one knows each of the $R_i^{(1)}$'s, then, in general, the ambiguity of the n^{th} roots $\sqrt[n]{R_i^{(1)}}$ yields n^{n-1} different values of the right-hand side in the equation (5) whereas we have only n roots $x_1, \ldots, x_n$.[9] A way out of this difficulty was indicated by Gauss, as far as cyclotomy is concerned, and by Abel, referring to the general case – see [Abel 1829], after the equation (35). In art. 360 of the D.A., Gauss made a cryptic remark alluding to certain radicals T, T', T'', ... and a root of unity R:

> There are special tricks which allow to turn the fractions $\frac{T'}{T}$, $\frac{T''}{T}$,... into rational entire functions [i.e., polynomials] of R.[10]

Those "special tricks" were later displayed in the posthumously published manuscript [Gauss 1863], which continues the seventh section of the D.A. Gauss's calculations were rediscovered by several authors and reproduced in Heinrich Weber's textbooks, [Weber 1898], § 177, and [Weber 1912], § 76. The arguments used by both Gauss and Abel come down to the observation made explicit by Abel in [Abel 1829] (after his equation (38)) that each of the products $V_i \cdot V_1^{n-i}$ $(1 \leq i \leq n-1)$ is likewise invariant under all cyclic permutations of $(x_1, \ldots, x_n)$. The same products occur with Gauss in D.A., art. 360 III. If $V_1 \neq 0$, then each V_i $(i < n)$ is a product of V_1^{i-n} times a quantity depending on i, which is to be regarded as known. In other words, one makes do with the *single* radical $\sqrt[n]{R_1^{(1)}}$ which exactly takes n values!

The exceptional case $V_1 = 0$ is not mentioned by Abel. Gauss affirms to the reader that this case cannot happen at all in cyclotomy and claims to have a proof of this fact which is too long to be inserted there. But indeed, in his manuscript [Gauss 1863], he deduced from his calculations that $V_1 \neq 0$ in case of cyclotomy (see formula (15) in the next section). Note that, from the equation (4) above, it follows that there is at least one index $i < n$ with $V_i \neq 0$. If n is a prime, then each of the powers α, α^2, ..., α^{n-1} is a primitive n^{th} root of unity, and instead of $V_1 = 0$ we can take any V_i with $V_i \neq 0$ and $i < n$. The remaining case $V_1 = 0$, for a composite number n, calls for some more sophisticated arguments and is treated in the above-mentioned textbooks, [Weber 1898], § 172, and [Weber 1912], § 65.

The problem of solving algebraic equations, as described above, dominated algebraic thinking until around 1850 (see [Serret 1849], Introduction). The entry 37 in Gauss's diary, [Gauss 1796-1814], shows that in 1796 he had rediscovered the Lagrange resolvents and hoped to solve general equations by radicals in terms of those resolvents (*resolutio aequationum universalis*). But very soon, in 1797, he

[9] This difficulty is often overlooked, e.g., in [Tignol 1988], chap. 12, § 5, p. 257, which makes the discussion of Gauss's results incomplete. The same objection was already raised by Gauss himself against [Lagrange 1808], p. 311 (note XIV, art. 41, p. 367, in *Œuvres*, vol. VIII), see [Gauss 1863], art. 8, announced by Gauss in a letter to Olbers, on July 3, 1808, [Gauss & Olbers 1900–1909], pp. 419–420.

[10] Art. 360.III: *Dantur etiam artificia peculiaria per quae fractiones* $\frac{T'}{T}$, $\frac{T''}{T}$ *etc. in functiones* integras *ipsius R convertere licet.*

gave up this hope,[11] and in § 9 of his dissertation [Gauss 1799], he spoke openly of his conviction that the general equations of degree greater than 4 would not be solvable by radicals. In that same year 1799, Paolo Ruffini published the first of a series of writings in which he attempted to prove that the general quintic is not algebraically solvable – see [Nový 1973] and [van der Waerden 1985]. Let us now resume the discussion of Gauss's D.A.

3. Gauss's Turn towards Irreducibility

As already said in the introduction, sec. 7 of the D.A. is entirely devoted to the equation $x^n - 1 = 0$. Since at that time the roots of $x^n - 1 = 0$ were well known to be trigonometric expressions

$$\zeta^k = \cos(2\pi k/n) + \sqrt{-1} \cdot \sin(2\pi k/n) \qquad (0 \leq k \leq n-1), \tag{6}$$

Gauss did not hesitate to consider them as the vertices of a regular n-gon inscribed in the unit circle in the plane. Those vertices divide the perimeter into n equal parts, whence the name *cyclotomy* for the theory of these equations. The regular n-gon is nothing else than the geometric picture of the fact that the n^{th} roots of unity are the powers of one of them, say, ζ:

$$1 = \zeta^0, \zeta, \zeta^2, \ldots, \zeta^{n-1} \qquad (\zeta^n = 1). \tag{7}$$

Where did Gauss find the principles for his investigation of the roots of unity? In his excellent essay [Bachmann 1922], pp. 33–34, Paul Bachmann convincingly argued that Gauss's cyclotomy theory originated mainly in purely *arithmetical* questions concerning congruences $x^{p-1} \equiv 1 \bmod p$, for prime numbers p.[12]

Cyclotomy theory gave a splendid example of how to use the relations between the roots of as peculiar an equation as $x^n - 1 = 0$ and provided the model to deal with important wider classes of equations. This aspect is certainly explicit in the great work of Abel and Galois – see [Abel 1829] and [Galois 1831].

In order to appreciate Gauss's achievements, I shall paraphrase Richard Dedekind's masterful and at the same time very personal review [Dedekind 1873] of Bachmann's book on cyclotomy, [Bachmann 1872]. Dedekind was a reliable expert on Gauss's writings and co-editor of his *Werke*.

As usual we shall call an n^{th} root of unity *primitive* if and only if its powers exhaust all n^{th} roots of unity.[13] If ζ is a primitive n^{th} root of unity, then all primitive roots of unity are given by the powers ζ^i with $(i, n) = 1$. Therefore, their total

[11] Alfred Loewy, in his comment on the entry 37, [Gauss 1796–1814/1917], pp. 504–505, points out a passage from the still today unpublished portion of the *Analysis residuorum*: Gauss stated here that *nulla spes superesse videtur Aequationum solutionem generalem possibilem esse*, but appended in a footnote: *tantum non de impossibilitate sumus certi.*

[12] See also G. Frei's chapter II.4 in the present volume.

[13] Gauss himself spoke of *radices primitivae*, e.g., in entry 136 of his diary [Gauss 1796–1814], as well as of *radices propriae* (in [Gauss 1863]).

number is $\phi(n)$, the number of prime residue classes modulo n. The polynomial

$$\Phi_n(x) = \prod_{(i,n)=1} (x - \zeta^i) \tag{8}$$

is now called the n^{th} *cyclotomic polynomial*. Gauss gave an explicit expression for $\Phi_n(x)$ and knew that its coefficients are rational integers.[14] Obviously, one has the decomposition

$$x^n - 1 = \prod_{d|n} \Phi_d(x), \tag{9}$$

where d runs through all divisors of n.

In the D.A., Gauss treated only the case of an odd prime number n completely. In that case one has

$$X = \Phi_n(x) = \frac{x^n - 1}{x - 1} = x^{n-1} + \cdots + x + 1. \tag{10}$$

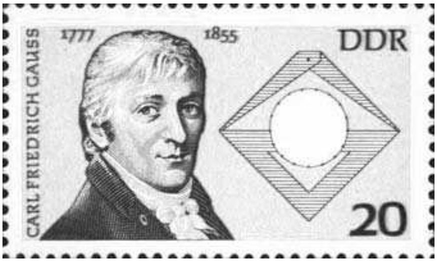


Fig. II.1B. A representation of the 17-division of the circle next to Gauss's portrait (Deutsche Post)

As Dedekind stressed in [Dedekind 1873], p. 414, Gauss's theory of $X = \Phi_n(x) = 0$ naturally splits up into two parts, art. 342–358, and art. 359–366. About the first part Gauss said:

> We intend to resolve X gradually into more and more factors, and in such a way that their coefficients are determined by equations of as low an order as possible. In doing so, we will finally come to simple factors or to the roots Ω [the set of roots of X]. We will show that if the number $n-1$ is resolved in any way into integral factors α, β, γ etc. (we can assume each of them is prime), X can be resolved into factors of $(n-1)/\alpha$ dimensions with coefficients determined by an equation of degree α;

[14] This result was posthumously published in [Gauss 1917] p. 116. For further references, see [Neumann 1980], footnote 117.

> each of these will be resolved into β others of $(n-1)/\alpha\beta$ dimensions with the aid of an equation of degree β etc.[15]

As already said in the introduction, the search for "equations of as low an order as possible" amounts to the construction of equations which are *irreducible* with regard to a certain realm of rationally known quantities (in modern terms, to a certain field).

But Gauss first started his exposition by rigorously proving that X is irreducible over the rationals (art. 341), in other words, that $X = 0$ is the equation of lowest degree which is satisfied by a primitive n^{th} root of unity. To do so, he relied on his important art. 42 where the factorization over the rationals is reduced to the factorization over the integers ("Gauss's lemma"). As far as we know, this was the first instance of a proof of irreducibility for an infinite series of polynomials of degree greater than 2. Dedekind commented:

> Here enters for the first time the concept of irreducibility (art. 341) which has become crucial for the whole orientation of later algebra; although Gauss makes only a limited use of it (art. 346), I have no doubt that this fundamental principle has also led him to the discovery of particular points and that he has preferred the synthetic presentation only for the sake of brevity; certainly this is what the important words (art. 365) let us conclude: "and we can prove with complete rigour that these higher equations cannot by any means be avoided or reduced to lower ones [etc.]." The truth of the assertion contained in them is easy to prove at the present stage of algebra, namely since the development of Gauss's thoughts by Abel and Galois. In fact, from the seed laid by Gauss, a science is born, which one … could perhaps describe as the science of the algebraic affinities between numbers, or, if one wants to use an expression chosen by me, as the science of the affinities between fields.[16]

[15] D.A., art. 342: *Propositum disquisitionum sequentium … eo tendit, ut X in factores continuo plures* GRADATIM *resolvatur, et quidem ita, ut horum coëfficientes per aequationes ordinis quam infimi determinentur, usque dum hoc modo ad factores simplices sive ad radices Ω ipsas perveniatur. Scilicet ostendemus, si numerus* $n-1$ *quomodocunque in factores integros* $\alpha\beta$, γ *etc. resolvatur (pro quibus singulis numeros primos accipere licet),* X *in* α *factores* $\frac{n-1}{\alpha}$ *dimensionum resolvi posse, quorum coëfficientes per aequationem* α^{ti} *gradus determinentur; singulos hos factores iterum in* β *alios* $\frac{n-1}{\alpha\beta}$ *dimensionum adiumento aequationis* β^{ti} *gradus etc.*

[16] [Dedekind 1873], pp. 408–409: *Hierbei tritt zum ersten Male der Begriff der Irreduktibilität auf (art. 341), welcher entscheidend für die ganze Richtung der späteren Algebra geworden ist; obgleich Gauß nur einen geringen Gebrauch von demselben macht (art. 346), so zweifle ich doch nicht daran, dass dieses Grundprinzip ihn auch bei der Entdeckung des Einzelnen geleitet und dass er nur der Kürze halber die synthetische Darstellung vorgezogen hat; namentlich lassen hierauf die gewichtigen Worte schließen (art. 365):* omnique rigore demonstrare possumus, has equationes elevatas nullo modo nec evitari nec ad inferiores reduci posse [etc.]. *Die Wahrheit der in denselben enthaltenen Behauptung ist nach dem gegenwärtigen Stande der Algebra, namentlich seit der Fortbildung der Gaußschen Gedanken durch Abel und Galois, leicht zu beweisen. In der Tat ist aus dem von Gauß gelegten Keime eine Wissenschaft entstanden, welche man … vielleicht als die Wissenschaft von der algebraischen Verwandtschaft der Zahlen oder, wenn man sich eines von mir gewählten Ausdruckes bedienen will, als die Wissenschaft*

As to the role of irreducibility after Gauss, Otto Hölder pointed out that Galois's theory is linked to this concept, [Hölder 1899], p. 481, and Ludwig Sylow independently emphasized irreducibility arguments in Abel's and Galois's writings, [Sylow 1902], pp. 24–25.[17] However, I cannot agree with Sylow's claim that Gauss "did not use irreducibility as a means of argumentation,"[18] in view of arts. 346 and following of the D.A.

As for the cyclotomic polynomials $\Phi_n(x)$ for arbitrary indices n (see equation (8)), Gauss claimed in entry 136 of his diary, in 1808, that he could prove their irreducibility over the rationals for composite indices too. But up to the present time no one seems to have been able to reconstruct a proof "in Gaussian style."[19] Alfred Loewy, in his long comment on entry 116 (dated 1801) of Gauss's diary, pointed out that in all probability Gauss had a rigorous demonstration that $\Phi_n(x)$ is irreducible for prime powers n, when the D.A.were published. Indeed such a proof would require only a slight extension of the arguments in art. 341. Yet the arguments for arbitrary composite n are more sophisticated, let alone the generalization, due to Kronecker and Dedekind, that $\Phi_n(x)$ is irreducible over any number field with (number-theoretical) discriminant prime to n – see [Dedekind 1873], pp. 412–414. For the purpose of constructing regular n-gons geometrically, it suffices to know the irreducibility of $\Phi_n(x)$ in case of prime powers n. In particular, Gauss's enumeration of regular n-gons which are constructible by ruler and compass, in art. 365, is actually complete although he omitted one half of the proof.[20]

Gauss went on "to resolve X gradually into more and more factors" using a fact he had proven in art. 55: there are always numbers g such that the powers $1 = g^0$, $g, \dots, g^{n-3}, g^{n-2}$ taken modulo n exhaust all prime residue classes modulo n. Here the assumption that n is prime comes in. The numbers g are called primitive roots modulo n. For any decomposition $n - 1 = e \cdot f$, Gauss formed the so-called *periods* of f terms

$$\eta_i := \zeta^i + \zeta^{i \cdot h} + \cdots + \zeta^{i \cdot h^{f-1}} = \sum_{j=0}^{f-1} \zeta^{i \cdot h^j} \qquad (0 \le i \le e-1) \qquad (11)$$

with $h = g^e$. These sums are independent of the choice of g and satisfy an equation of degree e over the rationals which is irreducible. Moreover, the periods $\eta_0, \dots, \eta_{e-1}$ are rational functions of each other with rational coefficients (they are actually polynomials of each other), and every primitive n^{th} root of unity satisfies an equation of

von der Verwandtschaft der Körper bezeichnen könnte.

[17] I owe this reference to Christian Skau (Trondheim).

[18] [Sylow 1902], p. 25: *Mais il [Gauss] ne s'est pas servi de cette irréductibilité comme d'un moyen de raisonnement.*

[19] However, a proof such as given, for instance, in [Artin 1948], theorem 27, could have been carried out by Gauss as well.

[20] Again see Loewy's comment on entry 116 of the diary, [Gauss 1796–1814/1917], pp. 556–560.

degree f, whose coefficients are rational functions of any of the periods of f terms. Repeating this procedure by decomposing further the number f, one eventually obtains a chain of auxiliary equations as described in Gauss's words quoted above.[21] In art. 365, he applied this method to the geometric constructions of regular n-sided polygons and claimed, on this occasion without proof, that the degrees of all equations occuring in his theory cannot be chosen lower. Gauss's words were emphasized by Dedekind in the quotation inserted above. The same fact is expressed in entry 116 of the diary. The truth of this assertion can be deduced rather transparently from the irreducibility of X and some arguments which use only tools available to Gauss.[22]

A closer examination shows that the method in the first part of sec. 7 does not depend on the existence of the primitive roots modulo n. But this became completely clear only after Abel's fundamental paper [Abel 1829]. All that is needed is the irreducibility of X and the fact that all of its roots are powers of each other. We shall resume this topic in more detail below.

The second part of sec. 7 of the D.A., art. 359–364, is devoted to the solvability of $X = 0$ by radicals.

> The preceding discussion had to do with the discovery of auxiliary equations. Now we will explain a very remarkable property concerning their solution. Everyone knows that the most eminent geometers have been unsuccessful in the search for a general solution of equations of higher than fourth degree, or (to define the search more accurately) for the reduction of complete equations to pure equations. And there is little doubt that this problem does not so much defy modern methods of analysis as that it proposes the impossible. ... Nevertheless it is certain that there are innumerable complete equations of every degree which admit a reduction to pure equations, and we trust that the geometers will find it gratifying if we show that our auxiliary equations are always of this kind.[23]

Here the assumption that the exponent n be a prime number plays a crucial role. Gauss claims the solvability by radicals in as strong a version as possible. Let be $n - 1 = \alpha\beta\gamma$ a decomposition into three factors. Then, according to Gauss, in art. 360, the equations of degree β for the periods of γ terms can be solved by a single irreducible radical of index β if the periods of $\beta\gamma$ terms and the β^{th} roots of unity are considered to be known. In particular, putting $\alpha = \gamma = 1$ and $\beta = n - 1$, one

[21] For a coherent exposition, see [Tignol 1988], chap. 12, § 4.

[22] See for an elimination argument [Abel 1829], § 4, footnote *, and, more generally, [Loewy 1921].

[23] D.A., art. 359: *Disquisitiones praecc. circa* inventionem *aequationum auxiliarum versabantur: iam de earum* solutione *proprietatem magnopere insignem explicabimus. Constat, omnes summorum geometrarum labores, aequationum ordinem quartum superantium resolutionem generalem, sive (ut accuratius quid desideretur definitam)* AFFECTARUM REDUCTIONEM AD PURAS, *inveniendi semper hactenus irritos fuisse, et vix dubium manet, quin hocce problema non tam analyseos hodiernae vires superet, quam potius aliquid impossibilie proponat. ... Nihilominus certum est, innumeras aequationes affectas cuiusque gradus dari, quae talem reductionem ad puras admittant, geometrisque gratum fore speramus, si nostras aequationes auxiliares semper huc referendas esse ostenderimus.*

obtains expressions by radicals of prime indices less than n for the n^{th} roots of unity by an obvious recursion process.

Gauss gave only an outline of his proof,[24] but entries 55, 65, 66, 71, 73, 74 (dated 1797) and, last but not least, 116 of the diary [Gauss 1796–1814] show that he probably had full proofs of his claims. His main tools were the Lagrange resolvents defined in equation (3). Let g be a primitive root modulo n, ζ a primitive n^{th} root of unity, $n-1=e\cdot f$ a factorization, α a primitive e^{th} root of unity. For each i, $1\leq i\leq e-1$, Gauss introduced the Lagrange resolvents

$$(\zeta,\alpha^i):=\zeta+\alpha^i\cdot\zeta^g+\alpha^{2i}\cdot\zeta^{g^2}+\cdots+\alpha^{(n-2)i}\cdot\zeta^{g^{n-2}} \tag{12}$$

which now are called "Gaussian sums."[25] One has

$$(\zeta,\alpha^i)=\eta_0+\alpha^i\cdot\eta_1+\cdots+\alpha^{(e-1)i}\cdot\eta_{e-1}\qquad(1\leq i\leq e-1) \tag{13}$$

where $\eta_0,\ldots,\eta_{e-1}$ denote the periods of f terms. Gauss showed that the e^{th} power $T_i:=(\zeta,\alpha^i)^e$ is a linear combination of the powers of α with integer coefficients. The sequel of the arguments goes along the lines sketched in our § 2. Gauss omitted the proof that $T_i\neq 0$ for every i and that each of the e^{th} roots $\sqrt[e]{T_i}$ can be expressed by means of the single radical $\sqrt[e]{T_1}$ (see our quotation in § 2). In his manuscript [Gauss 1863], he made up for the missing proofs by including impressive calculations with his sums. In particular, he found explicit formulae for the quotients

$$\frac{(\zeta,\alpha^i)\cdot(\zeta,\alpha^k)}{(\zeta,\alpha^{i+k})} \tag{14}$$

which turned out to be linear combinations of the powers of α with integer coefficients as well; from this he could deduce the relation

$$(\zeta,\alpha^i)\cdot(\zeta,\alpha^{-i})=(-1)^i\cdot n. \tag{15}$$

This relation makes evident that every T_i is different from 0. In 1827, Jacob Jacobi wrote to Gauss that he had also studied the quotients (14) independently. Those results were published as late as in 1837 and rediscovered by several authors independently of each other.[26] It became common usage to call "Jacobi sums" the quotients (14).

The calculus of Gauss-Jacobi sums and Abel's results published in [Abel 1829] suggest that we reexamine the claim of Harold M. Edwards that "the equation $(x^p-1)/(x-1)=0$ for p^{th} roots of unity had not been shown to be solvable by radicals prior to Galois's work" (p denotes a prime number), [Edwards 1984], p. 27,

[24] See also [Edwards 1984], § 24, and [Tignol 1988], chap. 12, §§ 5–6.

[25] See also [Bachmann 1922], § 15, [Weber 1898], [Weber 1912], [Hasse 1950], [Ireland & Rosen 1990], [Lemmermeyer 2000], [Neumann 1980]. See also F. Lemmermeyer's chap. VIII.3 and S. Patterson's chap. VIII.2 in the present volume [Editors' note].

[26] See more detailed references in [Lemmermeyer 2000] and [Neumann 1980].

footnote †. If one merely demands solvability of $X = 0$ by a chain of irreducible radicals of prime index (as Edwards does) and not necessarily by a single radical of index $n - 1$ after adjoining the $(n - 1)^{\text{th}}$ roots of unity, then all claims with one exception made by Gauss follow from the irreducibility of X and Abel's theory expounded in [Abel 1829]. Moreover, the latter theory does not require the existence of primitive roots modulo n. The exception mentioned is Gauss's assertion that after adjoining the $(n - 1)^{\text{th}}$ roots of unity, the equation $X = 0$ could be solved by a single irreducible radical of index $n - 1$. It would suffice to prove that X remains irreducible after the adjunction of the $(n - 1)^{\text{th}}$ roots of unity. Whether and how Gauss succeeded in proving that around 1801 must be left open.

4. After Gauss

Gauss's solution of $X = 0$ was greeted with enthusiasm and admiration, and it was popularized very soon in textbooks on algebra and number theory, first of all in France.[27] The problem of algebraic solutions of equations, in the sense explained above, still dominated minds, and the description of other solvable equations was an intriguing question. Eventually, after more than two decades, several authors went beyond Gauss's published results. As already mentioned, the calculus of Gaussian sums was refined by Jacobi, as well as by Augustin-Louis Cauchy who presented a memoir, [Cauchy 1829], on this subject at the Académie des sciences on September 21, 1829. The Gauss-Jacobi sums were in particular very important in the search for the higher reciprocity laws of power residues.[28] Eduard Kummer founded his theory of ideal numbers on Gauss's theory of cyclotomic periods.[29]

However, before 1830, Abel's papers, [Abel 1826] and [Abel 1829], marked a breakthrough in the general theory of equations. The first one settled in the negative the question of whether the general quintic is solvable by radicals.[30] But the main issue was to characterize the solvable equations. Abel, in a manuscript dated 1828 and posthumously published, [Abel 1881], sketched an algorithm to decide whether a given equation be solvable by radicals or not. But in this regard Abel's result was rather soon superseded by the consequences of Galois's theory of equations, [Galois 1831].

Abel was above all the first who succeeded in generalizing and thereby in clarifying Gauss's method for solving $X = 0$. In his paper [Abel 1829], he described a new vast class of solvable equations. His aim, in his own words, was the following:

> It is true that algebraic equations are not generally solvable; but there is a particular class of them of all degrees, whose algebraic resolution is possible. Such are, for example, the equations of the form $x^n - 1 = 0$. The resolution of these equations is

[27] See [Gauss & Olbers 1900–1909], for instance pp. 103, 177, 419–420, 431, [Neumann 1980], [Neumann 2002], [Nový 1973], chap. 3, [Reich 1996] and [Reich 2000].

[28] See [Neumann 1980], [Ireland 1990] and [Lemmermeyer 2000].

[29] See [Bachmann 1872], [Dedekind 1873], [Dieudonné 1978], [Lemmermeyer 2000], [Neumann 1980].

[30] A careful discussion with references to the work of Ruffini and Pierre Laurent Wantzel will be found in [Tignol 1988], chap. 13.

> based on certain relations which exist among the roots. I have tried to generalize this remark while assuming that two roots of a given equation are linked together in such a way that one can express rationally one by the other and I have found that such an equation can always be solved through a certain number of lower equations.[31]

Thus, Abel was focusing on equations with the special property that their roots are rational functions of each other. To simplify, we shall use modern terminology and call them "normal equations." This class includes the cyclotomic equations $\Phi_n(x) = 0$ for all n (see equation (8)) since their roots are powers of each other. Abel followed up a program which was very similar to Gauss's ideas in the seventh section of the D.A.

New in comparison with the D.A. are Abel's results first on arbitrary irreducible normal equations (§§ 1–2) and then on the solvability of normal equations by radicals (§§ 3–4). In § 4 he used his famous commutativity condition: if x denotes a root such that all other roots are rational functions of it and θx, $\theta_1 x$ are two arbitrary roots, then $\theta\theta_1 x = \theta_1\theta x$. This condition was apparently suggested by elliptic functions, and it suffices for solvability by radicals.

Several times, Abel compared his methods and results with those of Gauss. For instance, after his *théorème VI*, he said:

> The preceding method is in fact the same as that which M. Gauss gives for the reduction of the equation with two terms $x^\mu - 1 = 0$.[32]

Abel also complemented the D.A., in § 3, *théorème V*, and § 5, with some proofs that were omitted by Gauss.

It is accepted that Galois set the theory of equations on a completely new track in his paper [Galois 1831]. The involved and exciting story of the initial assessment, arduous reception and eventual publication in 1846 of this brilliant work is recorded in [Edwards 1984], [Lützen 1990], [Tignol 1988], [Toti Rigatelli 1989] and [van der Waerden 1985]. Galois went beyond Abel insofar as he reduced arbitrary equations to irreducible normal resolvents and attached appropriate groups of permutations ("Galois groups") to irreducible normal equations. As an example, he mentioned that the Gaussian equation $X = \frac{x^n-1}{x-1} = 0$, for n a prime number, has the cyclic group of order $n - 1$ as its Galois group over the rationals.

In summary, while the guiding concepts for Abel were those of normal equation and of irreducibility, the group of an equation definitely became the dominating

[31] [Abel 1829], p. 131: *Il est vrai que les équations algébriques ne sont pas résolubles généralement ; mais il y en a une classe particulière de tous les degrés dont la résolution algébrique est possible. Telles sont p. ex. les équations de la forme $x^n - 1 = 0$. La résolution de ces équations est fondée sur certaines relations qui existent entre les racines. J'ai essayé à généraliser cette remarque en supposant que deux racines d'une équation donnée soient tellement liées entre elles, qu'on puisse exprimer rationnellement l'une par l'autre, et j'ai trouvé, qu'une telle équation peut toujours être résolue à l'aide d'un certain nombre d'équations moins élevées.*

[32] *La méthode précédente est au fond la même que celle que Mr. Gauss donne pour la réduction de l'équation à deux termes $x^\mu - 1 = 0$.*

concept following Galois. To solve an equation then would mean to reduce the Galois group step by step after adjoining suitable quantities.

It is very interesting how Galois distinguished himself from Gauss. He touched on that point in his announcement of his 1831 paper in the *Bulletin de Férussac* of April 1830, as well as in his letter to Auguste Chevalier.[33] Galois generalized Gauss's method of auxiliary equations, used in sec. 7 of the D.A., in a far-reaching manner by calling *équations de M. Gauss* those equations of some composite degree $m \cdot n$ which can be factorized into m factors of degree n by means of a single equation of degree m. Another name used by Galois is *équations imprimitives*. To Chevalier, he wrote:

> The simplest decompositions [of a group] are those which occur by M. Gauss's method. As these decompositions are obvious, even in the actual form of the group of the equation, it is not useful to rest long on this topic. Which decompositions are practicable for an equation that cannot be simplified by M. Gauss's method? I have called *primitives* the equations that cannot be simplified by M. Gauss's method; not that these equations are really indecomposable, as they can even be solved by radicals.[34]

In group-theoretical terms, roots of irreducible primitive equations are invariant under a maximal proper subgroup of the Galois group.[35]

In the theory of groups, Galois's basic innovation was the concept of a *décomposition propre* of a group, in other words, the decomposition of a group into cosets of a normal subgroup. He considered those chains of subgroups which we today call "normal series" and "composition series", respectively. This enabled him to formulate a very concise criterion for solvability by radicals:

> If these groups [i.e., the factors of a composition series] have each a prime number of permutations, the equation will be solvable by radicals; if not, no.[36]

Galois introduced the groups named after him by using arguments and tools which were already well-known to mathematicians like Lagrange, Gauss, Cauchy and Abel, namely the fundamental theorem on symmetric functions, the Euclidean algorithm for polynomials, the properties of irreducible polynomials and the like. One may speculate whether Lagrange would have discovered Galois's theory if he

[33] Respectively [Galois 1831], [Galois 1830], [Galois 1832].

[34] [Galois 1832]: *Les décompositions [d'un groupe] les plus simples sont celles qui ont lieu par la méthode de M. Gauss. Comme ces décompositions sont évidentes, même dans la forme actuelle du groupe de l'équation, il est inutile de s'arrêter longtemps sur cet objet. Quelles décompositions sont praticables sur une équation qui ne se simplifie pas par la méthode de M. Gauss? J'ai appelé* primitives *les équations qui ne peuvent se simplifier par la méthode de M. Gauss; non que ces équations soient réellement indécomposables, puisqu'elles peuvent même se résoudre par radicaux.* The emphasis is mine.

[35] Cf. the exposition in [Haupt 1954], no. 17,7.

[36] [Galois 1832]: *Si ces groupes ont chacun un nombre premier des permutations, l'équation sera soluble par radicaux; sinon non.*

had paid more attention to irreducibility or, even more to the point, to the construction of irreducible resolvents.

After its publication in 1846, Galois's theory was rapidly taken up by algebraists. It seems that its reception was considerably speeded up by one of his results which, from our perspective, looks rather special at first glance: an irreducible equation of prime degree is solvable by radicals if and only if each of its roots is a rational function of two of them. Yet this result could be understood without knowing anything about group theory.[37]

Galois's theory was still a theory of equations. The old writers like Lagrange, Gauss, Abel, and Galois were well aware of the fact that, for example, talking about irreducible equations one assumes that a certain realm of rationally known quantities is supposed to be given. In that sense one might be tempted to say that they knew what a field and a field extension are. But the study of fields was not yet an end in itself. It is typical for the whole situation that the concept of the degree of a field extension did *not* appear before Dedekind and Kronecker. Instead mathematicians worked only with the degrees of polynomials. Dedekind's first paper on the mutual reduction of two irreducible polynomials (dated between 1855 and 1858) remained unpublished until 1982 and was still devoted to arduous considerations of that type – see [Scharlau 1982] and the references given there. It was Dedekind who introduced the concept of degree and proved the multiplicativity of degrees for successive field extensions, see [Dedekind 1873].[38] The specific properties of the degrees allowed Dedekind considerably to simplify and to shorten earlier arguments by Gauss, Abel and Galois, and to extend them. The question to what extent Kronecker was influenced by Dedekind must be left open.

After Galois, therefore, the initial problem of algebraic solvability was superseded then by the more general question on "normal forms" of equations and the so-called inverse problem of Galois theory, i.e. the search for equations with given properties of the Galois group – see for instance [Hölder 1899] and [Wiman 1900]. As for further lines of development after Galois, the reader is referred to [Neumann 1997], [Nový 1973], [Tignol 1988], [Toti Rigatelli 1989], [Umemura 1984] and [van der Waerden 1985].[39] However, I would like to leave the concluding words to Dedekind, who illustrated beautifully the role played by the concept of irreducibility for the later readers of sec. 7 of the D.A.:

[37] What strong an impression this result had made on Joseph Liouville and other mathematicians can be seen from Liouville's "Avertissement" to Galois's writings in the volume XI of the *Journal de mathématiques pures et appliquées*. Abel had discovered one half of this theorem too, as he wrote in a letter to August Leopold Crelle on October 18, 1828, see [Abel 1828/1881], proposition B.

[38] In an important special case, Abel proved the multiplicativity of the degrees of irreducible polynomials by an elimination argument in [Abel 1829], § 4, footnote *.

[39] At least one of Tignol's judgements cannot be left without any objection. On pp. 396–397 in [Tignol 1988], he writes: "Galois always worked with the roots of the proposed equation, never with its coefficients." But with Galois the very definition of the group of an equation requires first to calculate an auxiliary equation out of the given equation and then to take an irreducible factor of that new equation over the basic realm of coefficients.

> As for the method of development, one cannot deny that in Gauss's synthetic presentation the effort towards brevity has won out over the requirement to derive everything from a unified algebraic idea. During my first thorough study of the division of the circle, during the Whitsun holidays of 1855, although I well understood the details [of that presentation], I had nonetheless to struggle a long time before I recognized in irreducibility the principle which I needed only to question, simply and naturally, in order to be necessarily led to all aspects. These ideas were completed through a deep study of the algebraic research of Abel and espacially Galois and led me to a sure conclusion through the discovery, at the beginning of December this same year, of the most general relations between two arbitrary irreducible equations;[40] later in my two Winter term courses of lectures on the division of the circle and higher algebra in 1856-1858, I followed the method obtained previously and I still believe today that it is equally suitable for students.[41]

Acknowledgments

I am very grateful to G. R. Robinson (Birmingham) and the editors for linguistic help and constructive criticism.

References

Abel, Niels Henrik. 1826. Beweis der Unmöglichkeit algebraische Gleichungen von höheren Graden als dem vierten allgemein aufzulösen. *Journal für die reine und angewandte Mathematik* 1, 65–84. French version: Démonstration de l'impossibilité de la résolution algébrique des équations générales qui passent le quatrième degré. In [Abel 1881b], vol. I, pp. 66–87. German new transl. in [Maser 1889a], pp. 8–28.

———. 1829. Mémoire sur une classe particulière d'équations résolubles algébriquement. *Journal für die reine und angewandte Mathematik* 4, 131–156. Amended version in [Abel 1881b], vol. I, pp. 478–507. German transl. in [Maser 1889a], pp. 29–56, and [Loewy 1900], pp. 3–36, with annotations and corrections.

———. 1828/1881. Extract of a letter to Crelle. In [Abel 1881b], vol. II, pp. 269–270.

[40] See [Scharlau 1982].

[41] [Dedekind 1873], pp. 414–415: *Was ferner die Methode der Entwicklung anbetrifft, so ist nicht zu leugnen, dass in der synthetischen Darstellung von Gauß das Streben nach Kürze den Sieg über die Forderung davongetragen hat, alles aus einem einheitlichen algebraischen Gedanken abzuleiten. Bei meinem ersten gründlichen Studium der Kreisteilung in den Pfingstferien 1855 hatte ich, obgleich ich das Einzelne wohl verstand, doch lange zu kämpfen, bis ich in der Irreduktibilität das Prinzip erkannte, an welches ich nur einfache, naturgemäße Fragen zu richten brauchte, um zu allen Einzelnheiten mit Notwendigkeit getrieben zu werden. Nachdem diese Gedanken durch eine eingehende Beschäftigung mit den algebraischen Untersuchungen von Abel und namentlich von Galois vervollständigt und durch die im Anfang Dezember desselben Jahres gelungene Auffindung der allgemeinsten Beziehungen zwischen irgend zwei irreduktiblen Gleichungen zu einem gewissen Abschluss gekommen waren, habe ich später in meinen beiden Wintervorlesungen über Kreisteilung und höhere Algebra 1856–1858 die damals gewonnene Methode befolgt, und ich glaube noch heute, dass sie auch für den Lernenden zweckmäßig ist.*

———. 1881a. Sur la résolution algébrique des équations. In [Abel 1881b], vol. II, pp. 217–243.

———. 1881b. *Œuvres complètes*, ed. L. Sylow, S. Lie. 2 vols. Christiania: Grøndahl & Søn. Repr. New York, London: Johnson, 1965.

Artin, Emil. 1948. *Galois Theory*. 2nd ed. Indiana: Notre Dame University.

Bachmann, Paul. 1872. *Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie*. Leipzig: Teubner. Repr. Vaduz: Sändig Reprint Verlag, 1968, 1988.

———. 1922. Über Gauss' zahlentheoretische Arbeiten. In C. F. Gauss, *Werke*, vol. X.2, Abh. 1, pp. 1–69. Berlin: Julius Springer, 1922–1931. First version: *Nachrichten von der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse* (1911), 455-508.

Cauchy, Augustin-Louis. 1829. Mémoire sur la théorie des nombres. *Bulletin des sciences mathématiques, astronomiques, physiques et chimiques* [*Bulletin de Férussac*] 12, 205–221. Repr. in *Œuvres complètes*, IIe ser., vol. II, pp. 88–107. Paris: Gauthier-Villars, 1958.

Dedekind, Richard. 1873. Anzeige von "P. Bachmann, *Die Lehre von der Kreistheilung und ihre Beziehungen zur Zahlentheorie*". *Literaturzeitung der Zeitschrift für Mathematik und Physik* 18, 14–24. Repr. in *Gesammelte mathematische Werke*, ed. R. Fricke, E. Noether, O. Ore, vol. 3, pp. 408–420. Braunschweig: Vieweg, 1932; repr. New York: Chelsea, 1969.

Dieudonné, Jean (ed.). 1978. *Abrégé d'histoire des mathématiques 1700–1900*. 2 vols. Paris: Hermann.

Dunnington, G. Waldo. 2004. *Carl Friedrich Gauss. Titan of Science*. 2nd ed. with additional material by J. Gray and F.-E. Dohse. The Mathematical Association of America.

Edwards, Harold M. 1984. *Galois Theory*. New York, etc.: Springer-Verlag.

Galois, Évariste. 1831/1846. Mémoire sur les conditions de résolubilité des équations par radicaux. *Journal de mathématiques pures et appliquées* 11, 417–433. Repr. in [Galois 1897], pp. 33–50, and in [Galois 1962], pp. 42–71. German transl. in [Maser 1889a], pp. 116–130. English transl. in [Edwards 1984], pp. 101–114, corrected in [Lützen 1990], p. 571.

———. 1832. Lettre du 29 mai 1832 à Auguste Chevalier. *Revue encyclopédique*, septembre, 568–576. Repr. in [Galois 1897], pp. 25–32, and in [Galois 1962], pp. 172–185. German transl. in [Maser 1889a], pp. 108–115.

———. 1897. *Œuvres mathématiques*. Paris: Gauthier-Villars.

———. 1962. *Ecrits et mémoires mathématiques*, ed. R. Bourgne, J.-P. Azra. Paris: Gauthier-Villars.

Gauss, Carl Friedrich. 1796–1814. Mathematical Diary. Original manuscript in Latin: Handschriftenabteilung Niedersächsische Staats- und Universitätsbibliothek Göttingen, Cod. Ms. Gauss Math. 48 Cim. Ed. (Latin with German annotations): Abdruck des Tagebuchs (Notizenjournals) in [Gauss 1917], pp. 483–575. French annotated transl. P. Eymard and J.-P. Lafon: Le journal mathématique de Gauss. *Revue d'histoire des sciences et de leurs applications* 9 (1956), 21–51. English commented transl. J. Gray: A commentary on Gauss's mathematical diary, 1796-1814, with an English translation. *Expositiones Mathematicae* 2 (1984), 97–130. Rep. in [Dunnington 2004], pp. 409-505. German transl. E. Schuhmann, with a historical introduction by K.-R. Biermann, and annotations by H. Wußing and O. Neumann: *Mathematisches Tagebuch 1796–1814*. 5th ed. Ostwalds Klassiker der exakten Wissenschaften 256. Leipzig: Akademische Verlagsgesellschaft Geest & Portig; Frankfurt am Main, Thun: Harri Deutsch, 2005.

———. 1799. Demonstratio nova theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse. Helmstedt: C. G. Fleckeisen. Repr. in *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. III, pp. 1–30. Göttingen: Universitäts-Druckerei, 1866. German transl. in [Netto 1913], pp. 3–36.

———. 1816. Demonstratio nova altera theorematis omnem functionem algebraicam rationalem integram unius variabilis in factores reales primi vel secundi gradus resolvi posse. *Commentationes societatis regiae scientiarum Gottingensis recentiores* 3, 107–134. Repr. in *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. III, pp. 31–56. Göttingen: Universitäts-Druckerei, 1866. German transl. in [Netto 1913], pp. 37–60.

———. 1863. Disquisitionum circa aequationes puras ulterior evolutio. Pub. in *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. II, pp. 243–265. Göttingen: Universitäts-Druckerei. German transl. in [Maser 1889b], pp. 630–652.

———. 1917. *Werke*, vol. X.1, *Nachtraege zur reinen Mathematik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Leipzig: Teubner.

GAUSS & OLBERS. 1900–1909. *Briefwechsel zwischen Olbers und Gauß*, ed. C. Schilling and I. Kramer. Wilhelm Olbers, sein Leben und seine Werke, ed. C. Schilling, vol. 2. Berlin: J. Springer. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 4. 2 vols. Hildesheim: G. Olms, 1976.

GILAIN, Christian. 1992. Sur l'histoire du théorème fondamental de l'algèbre : théorie des équations et calcul intégral. *Archive for History of Exact Sciences* 42, 91–136.

HASSE, Helmut. 1950. *Vorlesungen über Zahlentheorie*. Berlin, etc: Springer-Verlag.

HAUPT, Otto. 1954. *Einführung in die Algebra*, vol. II. 2nd ed. Leipzig: Akademie Verlag.

HÖLDER, Otto Ludwig. 1899. Galois'sche Theorie mit Anwendungen. In *Encyklopädie der mathematischen Wissenschaften*, vol. I, part I, art. IB3c, d, pp. 480–520. Leipzig: Teubner.

IRELAND, Kenneth, and ROSEN, Michael. 1990. *A Classical Introduction to Modern Number Theory*. New York, etc.: Springer-Verlag.

LAGRANGE, Joseph-Louis. 1770-1771. Réflexions sur la résolution algébrique des équations. *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-lettres de Berlin, années 1770 et 1771* (1772), 134–215; (1773), 138–253. Repr. in *Œuvres*, ed. J.-A Serret, vol. III, pp. 203–421. Paris: Gauthier-Villars, 1869; repr. Hildesheim, New York: G. Olms, 1973.

———. 1808. *Traité de la résolution des équations numériques de tous les degrés*. 2nd ed. Paris: Courcier. Repr. in *Œuvres*, ed. J.-A Serret, vol. VIII, pp. 1–370. Paris: Gauthier-Villars, 1879; repr. Hildesheim, New York: G. Olms, 1973.

LEBESGUE, Henri. 1955. L'œuvre mathématique de Vandermonde. *L'Enseignement mathématique* 11e ser. 1, 203–223.

LEMMERMEYER, Franz. 2000. *Reciprocity Laws. From Euler to Eisenstein*. Berlin, etc.: Springer.

LOEWY, Alfred (ed.). 1900. *Abhandlung über eine besondere Klasse algebraisch auflösbarer Gleichungen. Von N. H. Abel.* Ostwald's Klassiker 111. Leipzig: Engelmann.

———. 1918. Inwieweit kann Vandermonde als Vorgänger von Gauss bezüglich der Auflösung der Kreisteilungsgleichungen $x^n = 1$ angesehen werden? *Jahresbericht der DMV* 27, 189–195.

———. 1921. Über eine algebraische Behauptung von Gauss. II. *Jahresbericht der DMV* 30, 155–158.

LÜTZEN, Jesper. 1990. *Joseph Liouville 1809–1882: Master of Pure and Applied Mathematics.* New York, etc.: Springer.

MASER, Hermann (ed.). 1889a. *Abhandlungen über die algebraische Auflösung der Gleichungen von N. H. Abel und E. Galois.* Berlin: Julius Springer.

———. 1889b. *Untersuchungen über höhere Arithmetik von Carl Friedrich Gauss.* Berlin: Julius Springer. Repr. New York: Chelsea, 1969, 1981.

NETTO, Eugen (ed.). 1913. *Die vier Gauss'schen Beweise für die Zerlegung ganzer algebraischer Functionen in reelle Factoren ersten oder zweiten Grades (1799–1849).* Ostwald's Klassiker 14. 3rd ed. Leipzig, Berlin: Engelmann.

NEUMANN, Olaf. 1980. Zur Genesis der algebraischen Zahlentheorie. Bemerkungen aus heutiger Sicht über Gauss' Beiträge zu Zahlentheorie, Algebra und Funktionentheorie. 2. und 3. Teil. *NTM-Schriftenreihe* 17:1, 32–48; 17:2, 38–58.

———. 1997. Die Entwicklung der Galois-Theorie zwischen Arithmetik und Topologie (1850 bis 1960). *Archive for History of Exact Sciences* 50:3–4, 291–329.

———. 2005. Carl Friedrich Gauss's *Disquisitiones Arithmeticae* (1801). In *Landmark Writings in Western Mathematics, 1640–1940*, ed. I. Grattan-Guinness, pp. 303–315. Amsterdam: Elsevier.

———. 2006. The 17-Gon and Vandermonde. In *Festschrift für Karin Reich*, ed. G. Wolfschmidt, S. Kirschner. Algorismus. München: Institut für Geschichte der Naturwissenschaften, to appear.

———. 2007. Cyclotomy: from Euler through Vandermonde to Gauss. To appear in a volume commemorating the 300th anniversary of Leonard Euler's birthday, ed. R. E. Bradley and E. Sandifer.

NOVÝ, Luboš. 1973. *Origins of Modern Algebra.* Prague: Academia.

REICH, Karin. 1996. Frankreich und Gauss, Gauss und Frankreich. Ein Beitrag zu den deutsch-französichen Wissenschaftsbeziehungen in den ersten Jahrzehnten des 19. Jahrhunderts. *Berichte zur Wissenschaftsgeschichte* 19, 19–34.

———. 2000. Die Entdeckung und frühe Rezeption der Konstruierbarkeit des regelmäßigen 17-Ecks und dessen geometrische Konstruktion durch Johannes Erchinger (1825). In *Mathesis. Festschrift zum siebzigsten Geburtstag von Matthias Schramm*, ed. R. Thiele, pp. 101–118. Berlin: Diepholz.

———. 2003. Gauss' "Übersicht der Gründe der Constructibilität des Siebenzehnecks" (1801). *Mitteilungen der Gauss-Gesellschaft Göttingen* 40, 85-91.

SCHARLAU, Winfried. 1982. Unveröffentlichte algebraische Arbeiten Richard Dedekinds aus seiner Göttinger Zeit 1855–1858. *Archive for History of Exact Sciences* 27:4, 335–367.

Scholz, Erhard (ed.). 1990. *Geschichte der Algebra. Eine Einführung*. Mannheim, Wien, Zürich: B.I. Wissenschaftsverlag.

Serret, Joseph-Alfred. 1849. *Cours d'algèbre supérieure*. Paris: Gauthier-Villars.

Sylow, Ludwig. 1902. Les études d'Abel et ses découvertes. In *Niels Henrik Abel. Mémorial publié à l'occasion du centenaire de sa naissance*, part IV, 59 p. Kristiana: Jacob Dybwad; Paris: Gauthier-Villars; Leipzig: Teubner; London: Williams & Norgate.

Tignol, Jean-Pierre. 1988. *Galois' Theory of Algebraic Equations*. Burnt Mill, Harlow: Longman Scientific and Technical. 2nd rev. ed., Singapore: World Scientific, 2001.

Toti Rigatelli, Laura. 1989. *La mente algebrica. Storia dello sviluppo della Teoria di Galois nel XIX secolo*. Siena: Bramante Editrice.

Umemura, Hiroshi. 1984. Resolution of algebraic equations by theta constants. Appendix to D. Mumford, *Tata Lectures on Theta*, vol. II, pp. 261–272. Boston, Basel, Stuttgart: Birkhäuser.

Vandermonde, Alexandre-Théophile. 1770-1771. Mémoire sur la résolution des équations. *Histoire de l'Académie royale des sciences. Année 1771* 88 (1774), Mémoires, 365–416. German transl. in *Abhandlungen aus der reinen Mathematik von N. Vandermonde*, ed. C. Itzigsohn, pp. 1–64. Berlin: Springer, 1888.

van der Waerden, Bartel Leendert. 1985. *A History of Algebra*. Berlin: Springer.

Waring, Edward. 1770. *Meditationes algebraicae*. Canterbury: Nicholsom. 2nd ed. enlarged, 1782. English transl. D. Weeks: Providence R.I.: AMS, 1991.

Weber, Heinrich. 1898. *Lehrbuch der Algebra*, vol. 1. 2nd ed. Braunschweig: Vieweg. Repr., 1961; New York: Chelsea, 1979.

———. 1912. *Lehrbuch der Algebra. Kleine Ausgabe in einem Bande*. Braunschweig: Vieweg.

Wiman, Anders. 1900. Endliche Gruppen linearer Substitutionen. In *Encyklopädie der mathematischen Wissenschaften*, vol. I, part. 1, art. IB3 f, pp. 522–554. Leipzig: Teubner.

Yuškevič, Adolph Andrei Pavlovič (ed.). 1972. *Istoriya matematiki. Tom tretii'. Matematika XVIII stoletiya* (History of Mathematics. Vol. 3. Mathematics of XVIIIth century). Moskva: Nauka.

II.2

Composition of Binary Quadratic Forms and the Foundations of Mathematics

HAROLD M. EDWARDS

Writing to Leopold Kronecker on June 14, 1846, Ernst Kummer said of his newly created theory of ideal prime factors:

> Dirichlet strongly urged me to work the theory out completely and submit it to Crelle for publication as soon as possible. He also told me and showed me, from oral and written indications of Gauss himself, that when Gauss was completing the section of *Disqu. arith.* on composition of forms he had something similar to ideal factors for his private use, but that he had not put it on firm ground. Specifically, Gauss says in a note to his treatise on the factorization of integral rational functions into linear factors something like: "Had I been willing to use imaginaries in the way that earlier mathematicians did, I would have been able to simplify substantially one of my researches which, as it is, is quite difficult." Gauss later told Dirichlet that the reference here was to the composition of forms.[1]

William Waterhouse has convincingly argued that Gauss was referring in the footnote Kummer mentions *not* to the composition of forms in sec. 5 but to the unfinished sec. 8 of *Disquisitiones Arithmeticae*.[2] One should not, however, allow

[1] [Kummer 1846/1910]: *Dirichlet hat mich sehr ermahnt die Theorie bald fertig auszuarbeiten und Crelle zum Drucke zu übergeben. Auch hat er mir erzählt und gezeigt, nämlich aus mündlichen und schriftlichen Aeußerungen von Gauss, daß Gauss schon bei Anfertigung des Abschnittes* de compositione formarum *aus den* Disqu. arith. *etwas ähnliches wie ideale Factoren zu seinem Privatgebrauche gehabt hat, daß er dieselben aber nicht auf sicheren Grund zurückgeführt hat, er sagt nämlich in einer Note seiner Abhandlung über die Zerfällung der ganzen rat. Functionen in lineäre Factoren ohngefähr so: „Wenn ich hätte auf dieselbe Weise verfahren wollen wie die früheren Mathematiker mit dem imaginären, so würde eine andere meiner Untersuchungen die sehr schwierig ist sich auf sehr leichte Weise haben machen lassen.“ Daß hier die* compositio formarum *gemeint ist, hat Dirichlet später mündlich von Gauss erfahren.*

[2] See [Waterhouse 1984]. The eighth section is discussed by G. Frei in chap. II.4 of the

this important correction to cancel the remaining, more interesting part of Kummer's assertion. Although one of the three men, Gauss or Dirichlet or Kummer, appears to have misremembered or misunderstood what had occasioned a footnote published 47 years earlier, they all seem to have thought in 1846 that Gauss used "something similar to ideal prime factors" for his own calculations of compositions of forms when he was composing the *Disquisitiones*, but that he had not put it on "firm ground." Consideration of such a possibility raises an interesting question about the *Disquisitiones*: What was Gauss's conception of "firm ground" in 1801, and – regardless of what he might have left out – what firm ground underlay the theories that he did include?

There are no statements about the foundations of mathematics in the *Disquisitiones.* A glimpse of Gauss's views appears in his statement in the preface that all of mathematical analysis is the study of general properties and relations of numerical[3] quantities, whereas number theory (arithmetic) studies just *whole* numbers. This attitude implies that he thought of mathematics as being founded on the notion of "number," but he seems never to have discussed, in the *Disquisitiones* or elsewhere, his conception of "numbers."[4] In sec. 7 he certainly computes with irrational numbers – for example, the values of the trigonometric functions for arguments of the form $2\pi p/q$ with integral p and q in art. 336 – but he gives no explanation of them. He does not even justify his use of them in a book on arithmetic other than to say that "the exposition will make abundantly clear that this subject is linked to higher arithmetic in an intimate connection."[5] I infer from these few remarks that Gauss's view of mathematics was that it deals with *computations* with *numbers,* and that, like many other mathematicians since, his interest lay in pursuing mathematics itself, not in investigating its metaphysical underpinnings in the notion of number.

1. The Composition of Forms in the *Disquisitiones*

The difficult theory of composition of forms in sec. 5 is indeed closely related to Kummer's ideal prime factors, so it is not surprising that Kummer, Dirichlet and Gauss would have discussed connections between the two. Kummer explicitly mentioned binary quadratic forms in his first paper on ideal prime factors, [Kummer 1847], saying that the theory of numbers of the form $x+y\sqrt{D}$ leads to a theory of ideal factors, and that the natural way of partitioning these ideal factors into equivalence classes corresponds exactly to Gauss's way of partitioning binary quadratic forms into equivalence classes. He saw this as a powerful validation of his theory because the

present book [Editors' note].

[3] Gauss does not refer specifically to *numerical* quantities, but I am told that Maser's use of this term in his 1889 German translation correctly describes the way in which Gauss's contemporaries would have understood his phrase.

[4] A small note by Gauss on his conception of magnitudes, "Zur Metaphysik der Mathematik," published in vol. XII of his *Werke*, is discussed by J. Boniface in chap. V.1 of the present book [Editors' note].

[5] Gauss's *Disquisitiones Arithmeticae*, art. 335: *Tractatio ipsa abunde declarabit, quam intimo nexu hoc argumentum cum arithmetica sublimiori coniunctum sit.*

Gaussian classification of forms, although it appeared artificial from the standpoint of the theory of forms, had been demonstrated by Gauss to be more fruitful than the obvious classification. Unfortunately, Kummer gave no detailed explanation, and he never returned to the subject of ideal prime factors of numbers $x + y\sqrt{D}$ and binary quadratic forms.

A great obstacle for modern students of Gauss's theory of composition of forms (arts. 234–251) is Gauss's use of the word "composition" to denote an operation that is *not a binary operation.* Modern treatments normally ignore the composition of forms altogether and deal only with the composition of *equivalence classes* of forms, which *is* a binary operation. Even André Weil, [Weil 1984], p. 334, says the Gaussian theory was a "stumbling-block" until Dirichlet "restored its simplicity," without noting that Dirichlet only composed forms that satisfy certain *additional conditions* (conditions of "concordance"). Dirichlet in fact made no attempt to compose forms, as Gauss had done, but instead focussed on the question of determining which numbers were represented by which forms; in this study, it is natural to replace a form by an equivalent form whenever it is convenient to do so, and that is what Dirichlet did. In other words, he did not compose the two given forms, but instead replaced them, when necessary, with equivalent forms in order to find forms that were easy to compose. In this way, he solved the problems that interested him and avoided the complications of Gauss's theory, but he left aside the challenging problem Gauss had successfully solved, the problem of composing arbitrarily given forms. (See [Dirichlet 1851] or §146 of [Dirichlet-Dedekind 1879].)

Composition of forms is an elaboration of the ancient formula

$$(x^2 - Dy^2)(u^2 - Dv^2) = (xu + Dvy)^2 - D(xv + yu)^2, \tag{0}$$

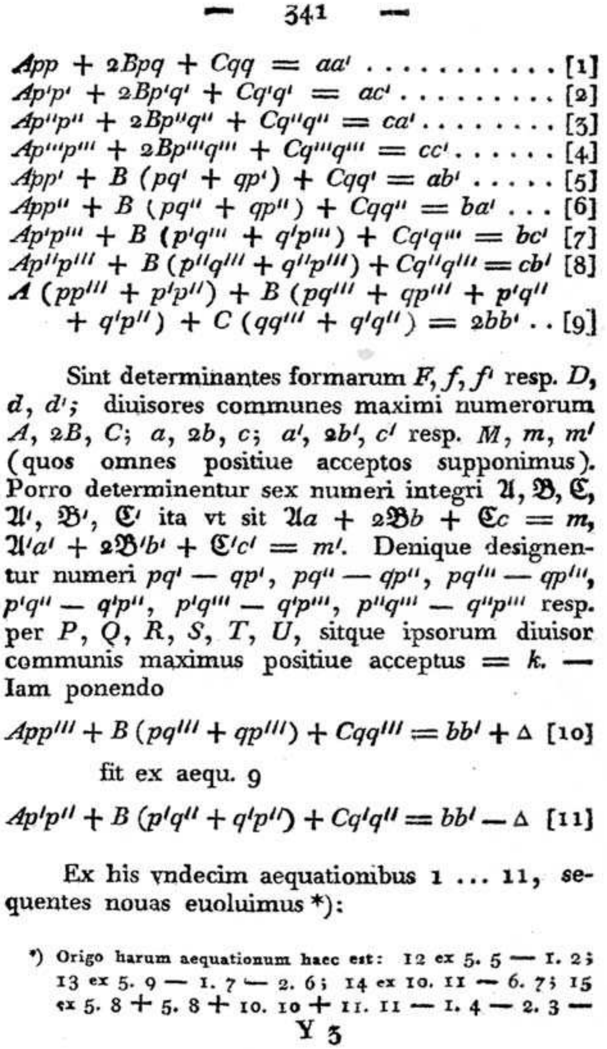
where D is a specified integer. Given three binary quadratic forms f, ϕ, and F (in the ancient example, all three are the form $X^2 - DY^2$), a *transformation* formula is a formula $f(x, y)\phi(u, v) = F(X, Y)$ where X and Y are linear functions

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} a_{11} & a_{12} & a_{13} & a_{14} \\ a_{21} & a_{22} & a_{23} & a_{24} \end{bmatrix} \begin{bmatrix} xu \\ xv \\ yu \\ yv \end{bmatrix}$$

of the four monomials xu, xv, yu and yv. (Gauss did not, of course, write the transformation equations in the matrix form used here.) A transformation is a *composition* (art. 235) if (1) the six 2×2 minors of the matrix $[a_{ij}]$ have greatest common divisor 1 and (2) the first two minors, that is, $a_{11}a_{22} - a_{21}a_{12}$ and $a_{11}a_{23} - a_{21}a_{13}$, are both positive. In the example (0), the transformation is given by the matrix

$$\begin{bmatrix} 1 & 0 & 0 & D \\ 0 & 1 & 1 & 0 \end{bmatrix}$$

so it is a composition because the six minors are 1, 1, 0, 0,$-D$ and $-D$. Actually, Gauss only imposes the technical condition (2) at a later stage in the development of the theory (art. 239).



— 341 —

$$App + 2Bpq + Cqq = aa' \ldots\ldots [1]$$
$$Ap'p' + 2Bp'q' + Cq'q' = ac' \ldots\ldots [2]$$
$$Ap''p'' + 2Bp''q'' + Cq''q'' = ca' \ldots\ldots [3]$$
$$Ap'''p''' + 2Bp'''q''' + Cq'''q''' = cc' \ldots\ldots [4]$$
$$App' + B(pq' + qp') + Cqq' = ab' \ldots\ldots [5]$$
$$App'' + B(pq'' + qp'') + Cqq'' = ba' \ldots [6]$$
$$Ap'p''' + B(p'q''' + q'p''') + Cq'q''' = bc' \; [7]$$
$$Ap''p''' + B(p''q''' + q''p''') + Cq''q''' = cb' \; [8]$$
$$A(pp''' + p'p'') + B(pq''' + qp''' + p'q'' + q'p'') + C(qq''' + q'q'') = 2bb' \ldots [9]$$

Sint determinantes formarum F, f, f' resp. D, d, d'; diuisores communes maximi numerorum $A, 2B, C$; $a, 2b, c$; $a', 2b', c'$ resp. M, m, m' (quos omnes positiue acceptos supponimus). Porro determinentur sex numeri integri $\mathfrak{A}, \mathfrak{B}, \mathfrak{C}, \mathfrak{A}', \mathfrak{B}', \mathfrak{C}'$ ita vt sit $\mathfrak{A}a + 2\mathfrak{B}b + \mathfrak{C}c = m$, $\mathfrak{A}'a' + 2\mathfrak{B}'b' + \mathfrak{C}'c' = m'$. Denique designentur numeri $pq' - qp'$, $pq'' - qp''$, $pq''' - qp'''$, $p'q'' - q'p''$, $p'q''' - q'p'''$, $p''q''' - q''p'''$ resp. per P, Q, R, S, T, U, sitque ipsorum diuisor communis maximus positiue acceptus $= k$. — Iam ponendo

$$App''' + B(pq''' + qp''') + Cqq''' = bb' + \Delta \; [10]$$

fit ex aequ. 9

$$Ap'p'' + B(p'q'' + q'p'') + Cq'q'' = bb' - \Delta \; [11]$$

Ex his vndecim aequationibus 1 … 11, sequentes nouas euoluimus *):

*) Origo harum aequationum haec est: 12 ex 5. 5 — 1. 2; 13 ex 5. 9 — 1. 7 — 2. 6; 14 ex 10. 11 — 6. 7; 15 ex 5. 8 + 5. 8 + 10. 10 + 11. 11 — 1. 4 — 2. 3 —

Y 3

Fig. II.2A. Computations at the core of Gauss's composition of forms: an extract from art. 235 in the 1801 edition of the *Disquisitiones arithmeticae*.

Gauss sets down in equations [1]-[9] the equations that describe a composition formula and begins the long solution of the problem, "Given two forms, determine whether there is a third form that composes them, and, if so, find all such forms."

Note that this definition rests on the firm ground of computation with whole numbers. The forms f, ϕ and F are described by triples of integers, and a composition is described by equations of the form given above. Composition is not a binary operation, but a ternary *relation.* Given f and ϕ, there may not be any F at all for which there is a composition formula, so it is meaningless to talk about "*the* composite of two given forms."[6] To make matters worse, if there *is* an F there are certainly *infinitely many* of them, because X and Y can be subjected to an arbitrary unimodular change of variables.

Gauss says (art. 234) "thus far no one has considered this topic." Small wonder. Ever since Gauss, mathematicians have struggled with it. The first theorem he proves states: If f and ϕ can be composed, the ratio of their determinants must be a ratio of squares. The proof is a display of algebraic virtuosity that occupies a few pages. Just as demanding and lengthy is his proof of the converse: if the ratio of the determinants of two forms is a ratio of squares, a third form can be written as a composite of them. His proof of this theorem is of course a construction; given two forms, and given that the ratio of their determinants is equal to a ratio of squares, his proof (art. 236) is an algorithm for constructing a third form and a 2×4 matrix that fulfills the conditions that define compositions. (In fact, in his masterly fashion, he shows how to construct *all possible* compositions of them.)

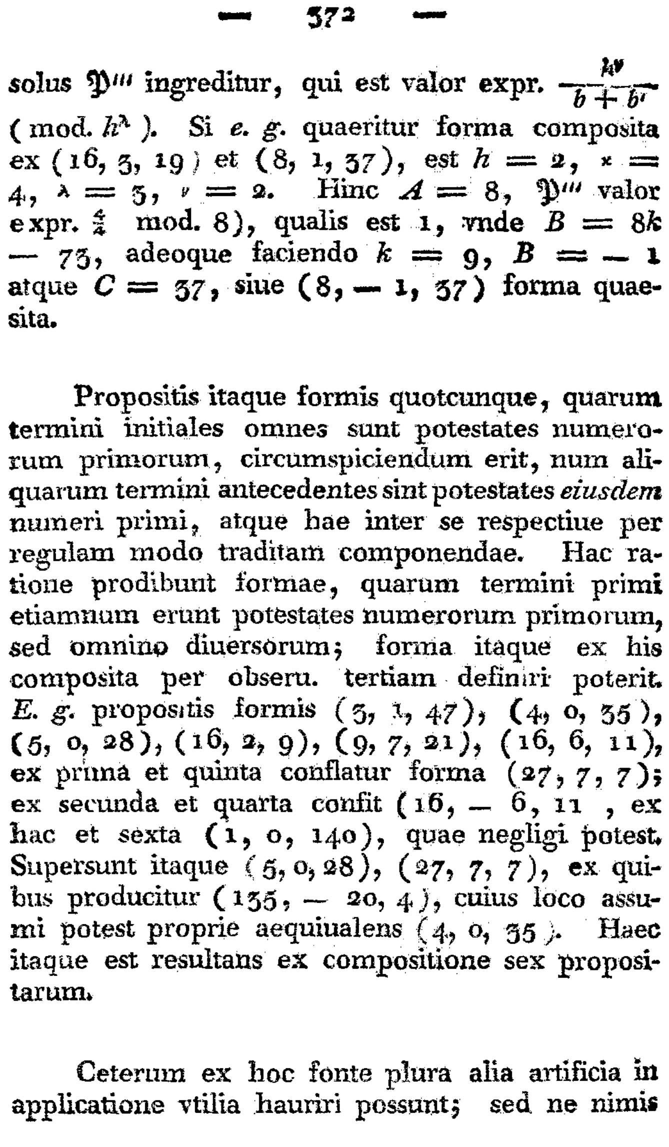
This is lengthy and daunting, but Gauss has only begun to do what he needs to do. Earlier (art. 158) he has defined what it means for two forms to be *equivalent.* In the main this definition is the natural one – each form can be obtained from the other by a change of variables with integer coefficients – but, as Gauss was the first to realize, addition of the seemingly unnatural requirement for the determinant of the change of variables to be *positive* improves the theory. He next proves that compositions of equivalent forms are equivalent. More precisely, if a form F can be expressed as a composite of two forms f and f', and if f'' is a form equivalent to f', then there is a form F' that is a composite of f and f'', and any such F' is equivalent to F. Note that the second statement implies, when $f' = f''$, that two compositions of the same pair of forms are equivalent.

And more: He needs to prove that this binary operation on equivalence classes is *associative,* a theorem that requires several more pages of work. Because he deals with composition of forms rather than of classes of forms, his statement of this associative law in art. 240 needs to be rather lengthy:

> If from the forms f, f' the form F is composed, from F, f'' the form $\mathfrak{F}$, from f, f'' the form F' and from F', f' the form $\mathfrak{F}'$, then the forms $\mathfrak{F}$ and $\mathfrak{F}'$ are equivalent.

Finally, after eight long and difficult articles (arts. 234–241) dealing with composition of forms in complete generality, Gauss turns in art. 242 to the specific problem of computing composites of given forms. Again I would like to emphasize that he composes *forms,* not equivalence classes. For example, in art. 243 he gives himself the problem of finding a form that is a composite of the forms $(3, 1, 47)$, $(4, 0, 35)$,

[6] Both the English and the German translations of the *Disquisitiones* wrongly translate the theorem of art. 249 when they use definite articles rather than indefinite ones; the original Latin of course has no articles.



— 372 —

solus $\mathfrak{P}'''$ ingreditur, qui est valor expr. $\frac{h^{\nu}}{b+b'}$ (mod. h^{λ}). Si *e. g.* quaeritur forma composita ex (16, 3, 19) et (8, 1, 37), est $h = 2$, $\varkappa = 4$, $\lambda = 3$, $\nu = 2$. Hinc $A = 8$, $\mathfrak{P}'''$ valor expr. $\frac{4}{4}$ mod. 8), qualis est 1, vnde $B = 8k - 73$, adeoque faciendo $k = 9$, $B = -1$ atque $C = 37$, siue (8, — 1, 37) forma quaesita.

Propositis itaque formis quotcunque, quarum termini initiales omnes sunt potestates numerorum primorum, circumspiciendum erit, num aliquarum termini antecedentes sint potestates *eiusdem* numeri primi, atque hae inter se respectiue per regulam modo traditam componendae. Hac ratione prodibunt formae, quarum termini primi etiamnum erunt potestates numerorum primorum, sed omnino diuersorum; forma itaque ex his composita per obseru. tertiam definiri poterit. *E. g.* propositis formis (3, 1, 47), (4, 0, 35), (5, 0, 28), (16, 2, 9), (9, 7, 21), (16, 6, 11), ex prima et quinta conflatur forma (27, 7, 7); ex secunda et quarta confit (16, — 6, 11 , ex hac et sexta (1, 0, 140), quae negligi potest. Supersunt itaque (5, 0, 28), (27, 7, 7), ex quibus producitur (135, — 20, 4), cuius loco assumi potest proprie aequiualens (4, 0, 35). Haec itaque est resultans ex compositione sex propositarum.

Ceterum ex hoc fonte plura alia artificia in applicatione vtilia hauriri possunt; sed ne nimis

Fig. II.2B. A composite of 6 forms:
an extract from art. 243 in the 1801 edition of the *Disquisitiones arithmeticae*.

$(5, 0, 28)$, $(16, 2, 9)$, $(9, 7, 21)$ and $(16, 6, 11)$, all of which have determinant -140. The form he finds is $(135, -20, 4)$.

He goes on to mention that $(135, -20, 4)$ is equivalent to $(4, 0, 35)$ – a fact that follows easily from the presence of 4 in both and the divisibility of the middle terms in both by 4 – perhaps because $(4, 0, 35)$ is a simpler representative of the equivalence class of the result, and, as was noted above, if F is a composite of f and f', then any form equivalent to F is also a composite of f and f'. The result $(4, 0, 35)$ can also be found in the following way: as Gauss states, $(27, 7, 7)$ is a composite of the first and fifth forms, $(3, 1, 47)$ and $(9, 7, 21)$; and, as is easily found (see below), $(4, 0, 35)$ is a composite of the fourth and sixth forms, $(16, 2, 9)$, and $(16, 6, 11)$. Since $(20, 0, 7)$ is a composite of $(4, 0, 35)$ and $(5, 0, 28)$ – easily found because 4 and 5 are relatively prime – a composite of all six forms but the second is found by using the fact that 27 and 20 are relatively prime to conclude that $(540, -20, 1)$ is a composite of $(27, 7, 7)$ and $(20, 0, 7)$ and therefore is a composite of the five forms other than $(4, 0, 35)$. This form $(540, -20, 1)$ is equivalent to the principal form $(1, 0, 140)$, as the last coefficient 1 shows, so any composite of all six forms must be equivalent to the composite of $(1, 0, 140)$ and $(4, 0, 35)$ and must therefore be equivalent to $(4, 0, 35)$.

My main point is that *computations* of this sort are the core of Gauss's theory of composition of forms. Gauss has gone to great lengths to describe in full generality the ways in which they may be done and the properties they have. His immediate purpose is, as the following sections of the *Disquisitiones* show, the proof of the law of quadratic reciprocity, which he extracts from simple facts about composition of primitive equivalence classes of forms for various determinants.[7] This marvellous proof leaves the reader with an impression that the theory is a powerful tool that will open the way to other realms of arithmetic, as indeed it has.

2. Revisiting the Composition of Forms

I would now like to describe a simple method of accomplishing the composition of forms that I hope will give some insight into the operations involved and into the way in which Gauss's approach, cumbersome as it is, does place the theory on the firm ground of computations with integers in an admirable and rather natural way.

Let an integer D, not a square, be fixed. I will take the addition and multiplication of numbers $x + y\sqrt{D}$, where x and y are integers, for granted. By a *module* of numbers of the form $x + y\sqrt{D}$, where x and y are integers, I will mean a list of (a finite number of) such numbers written between square brackets, $[x_1 + y_1\sqrt{D}, x_2 + y_2\sqrt{D}, \ldots, x_n + y_n\sqrt{D}]$. The term "module" is motivated by the following definition: a module is *congruent to zero* modulo another module, written

$$[x_1 + y_1\sqrt{D}, \ldots, x_n + y_n\sqrt{D}] \equiv 0 \bmod [x_1' + y_1'\sqrt{D}, \ldots, x_m' + y_m'\sqrt{D}]$$

[7] A form is said to be primitive if the coefficients (a, b, c) have no common divisor; if there is a primitive form in an equivalence class, all the forms of the class are primitive and the class is said to be primitive.

if each of its entries is a sum of multiples of entries of the other module in the sense that for each $i = 1, 2, \ldots, n$ there are integers $u_1, u_2, \ldots, u_m, v_1, v_2, \ldots, v_m$ such that

$$x_i + y_i\sqrt{D} = \sum_{\sigma=1}^{m}(u_\sigma + v_\sigma\sqrt{D})(x'_\sigma + y'_\sigma\sqrt{D}).$$

Two modules are by definition *equal* if each is congruent to zero modulo the other. As is easily seen, two modules are equal if and only if each can be transformed into the other by a sequence of operations of three types: (1) Rearrange terms. (2) Annex or delete zeros. (3) Add a multiple of one entry in the module to another entry – the multiplier being a number of the form $x + y\sqrt{D}$. We can then find a simple, uniquely determined representation of a given module:

Theorem. Let an integer D, not a square, be fixed, and let a list $x_1 + y_1\sqrt{D}$, $x_2 + y_2\sqrt{D}, \ldots, x_n + y_n\sqrt{D}$ of numbers of the form $x + y\sqrt{D}$ be given. Provided at least one of the listed numbers is not zero, there are nonnegative integers e, f and g for which $ef \neq 0$, $g < f$, $g^2 \equiv D \bmod f$ and

$$[x_1 + y_1\sqrt{D}, x_2 + y_2\sqrt{D}, \ldots, x_n + y_n\sqrt{D}] = [ef, eg + e\sqrt{D}].$$

Two modules in this form $[ef, eg + g\sqrt{D}]$, where e, f and g are nonnegative integers, $ef \neq 0$, $g < f$, and $g^2 \equiv D \bmod f$, are equal only if they are identical.

Proof. Let a module be called *full* if $\sqrt{D}$ times any entry in the module can be written as a sum of *integer* multiples of entries in the module. Every module is equal to a full module, as one can prove as follows: Double the length of the module by annexing to the end a number of zeros equal to the number of terms in the module. To each of the zeros in the second half, add $\sqrt{D}$ times the corresponding term in the first half. Then $\sqrt{D}$ times any term in the second half is equal to D times the corresponding term in the first half, so the new module is both full and equal to the original one.

Since every module is equal to a full module, it will suffice to prove that every full module that is not equal to [0] is equal to one in the required form $[ef, eg + g\sqrt{D}]$. This will be done in two stages.

Stage one: Because reversing the sign of an entry in a module obviously gives an equal module, one can assume without loss of generality that the coefficient of $\sqrt{D}$ in each term listed in the module is nonnegative. Because the module is assumed to be full and not equal to [0], at least one entry must contain $\sqrt{D}$ with a positive coefficient. (Use is made here of the assumption that $\sqrt{D}$ is not an integer.) If only one entry does, pass to stage two. Otherwise, choose an entry in which the coefficient of $\sqrt{D}$ is positive but otherwise as small as possible and subtract this entry from each other entry in which the coefficient of $\sqrt{D}$ is positive. The new module obtained in this way is equal to the old one, and the coefficients of $\sqrt{D}$ are all nonnegative. The new module is also full. (A number $x + y\sqrt{D}$ is a sum of integer multiples of the entries in the old module if and only if it is a sum of integer multiples of entries in the new module, and $\sqrt{D}$ times an entry in the new module is either $\sqrt{D}$ times an entry in the old module or it is a difference of two such, so it is certainly a sum of integer multiples of entries in either the old or the new module.) Such a step reduces the total of the coefficients of $\sqrt{D}$ (by $(k-1)$ times the smallest of the nonzero coefficients, where k is the number of nonzero coefficients), so repetition of the step eventually reaches a full module in which all entries but one are integers, and the one entry that is not an integer contains $\sqrt{D}$ with a positive coefficient, at which point one passes to stage two.

Stage two: Given a full module in which all terms but one are integers, one can again reverse signs, if necessary, to find an equal full module in which all terms but one are *nonnegative* integers. Delete all zeros from the module. At least one positive integer remains, because the module is assumed to be full and not equal to [0] (and D is not a square, so $(x + y\sqrt{D})\sqrt{D} = \mu(x + y\sqrt{D})$ is impossible for integer μ). If only one remains, a module of the form $[a, b + \sqrt{D}]$ that is full and equal to the original module has been reached. Otherwise, among the integers in the module (now all positive) choose one that is as small as possible, subtract it from each of the other integers in the module, and delete all zeros that result. Since each step of this type reduces the total of the integers in the module, repetition of it eventually results in a full module of the form $[a, b + c\sqrt{D}]$ equal to the original module.

Thus, given any module that is not equal to [0], one can construct a full module of the form $[a, b+c\sqrt{D}]$ that is equal to it. Moreover, one can assume without loss of generality that a and c are positive. Because $a\sqrt{D} = \mu \cdot a + \nu \cdot (b + c\sqrt{D})$ where μ and ν are integers, $a = \nu \cdot c$. Moreover, $b\sqrt{D} + cD = \sigma \cdot a + \tau \cdot (b + c\sqrt{D})$, so $b = \tau \cdot c$ and $cD = \sigma a + \tau b = \sigma \nu c + \tau^2 c$. Thus, with $e = c$, $f = \nu$ and $g = \tau$, the module is $[ef, eg + e\sqrt{D}]$, where $g^2 + \sigma f = D$, so $g^2 \equiv D \bmod f$. Since eg can be changed by any multiple of ef, g can be replaced by any integer congruent to it mod f, and one can assume without loss of generality that $0 \le g < f$, in which case the module has the required form.

Suppose now that both $[ef, eg+e\sqrt{D}]$ and $[e'f', e'g'+e'\sqrt{D}]$ have the required form, and suppose they are equal. Since $[ef, eg + e\sqrt{D}]$ is full, the statement that $[e'f', e'g'+e'\sqrt{D}] \equiv 0 \bmod [ef, eg+e\sqrt{D}]$ implies $e'f' = \mu \cdot ef + \nu \cdot (eg+e\sqrt{D})$ and $e'g' + e'\sqrt{D} = \sigma \cdot ef + \tau \cdot (eg + e\sqrt{D})$. Since ν must be zero, $e'f'$ must be a multiple of ef. By symmetry, ef must also be a multiple of $e'f'$. Since they are both positive integers, $ef = e'f'$. Similarly, since $e' = \tau \cdot e$ and, by symmetry, e is also a multiple of e' and both are positive, $e = e'$. Thus, $f = f'$. Since τ must then be 1, $eg' = e'g' = \sigma \cdot ef + eg$, so g' must be congruent to g mod f. Since both are nonnegative and less than f, $g = g'$, and the proof is complete.

A module of this form $[ef, eg + \sqrt{D}]$ will be said to be in *canonical form.* (The integers e, f and g are nonnegative, $ef \neq 0$, $g < f$, and $g^2 \equiv D \bmod f$.) The Theorem solves the problem: "Given two modules, determine whether they are equal." Each is equal to one in canonical form, and two in canonical form are equal only if they are identical.

Modules can be *multiplied* in a natural way: the entries of the product module are the products of two factors in which the first factor is from the first module and the second factor is from the second. This definition depends, of course, on the fact that it is consistent with the definition of equality of modules, which is to say that if one of the two modules is replaced by an equal module, the product module is replaced by an equal module. This is easy to prove.

Thus, every module can be written as a product $[e][f, g+\sqrt{D}]$ in which the first factor is $[e]$ for a positive integer e and the second factor is $[f, g+\sqrt{D}]$, where f is a positive integer and g is a square root of D mod f. Multiplication of any module by $[e]$ is easy, so the multiplication of two modules in canonical form, say $[e][f, g+\sqrt{D}]$ and $[e'][f', g'+\sqrt{D}]$ comes down to the computation of $[f, g+\sqrt{D}][f', g'+\sqrt{D}]$ which is to say the reduction of $[ff', f(g'+\sqrt{D}), f'(g+\sqrt{D}), gg'+D+(g+g')\sqrt{D}]$ to canonical form. *This operation contains the essence of the idea of the composition of forms.*

For example, Gauss's statement, mentioned above, that (27, 7, 7) is a composite of (3, 1, 47) and (9, 7, 21) follows from

$$\begin{aligned}
&[3, 1+\sqrt{-140}][9, 7+\sqrt{-140}] \\
&\qquad = [27, 3(7+\sqrt{-140}), 9(1+\sqrt{-140}), -133+8\sqrt{-140}] \\
&\qquad = [27, 21+3\sqrt{-140}, 9+9\sqrt{-140}, 2+8\sqrt{-140}] \\
&\qquad = [27, 21+3\sqrt{-140}, 7+\sqrt{-140}, 2+8\sqrt{-140}] \\
&\qquad = [27, 0, 7+\sqrt{-140}, -54] = [27, 7+\sqrt{-140}].
\end{aligned}$$

(These two forms (3, 1, 47) and (9, 7, 21) are concordant in Dedekind's sense, which is to say that the greatest common divisor of $a = 3$, $\alpha = 9$ and $b+\beta = 1+7$ is 1. Therefore the composite (27, 7, 7) is determined, as Dedekind showed, by the fact that $B = 7$ must be 1 mod 3 and 7 mod 9 and must be a square root of -140 mod 27.)

Similarly, the above statement that (4, 0, 35) is a composite of (16, 2, 9) and (16, 6, 11) follows from

$$\begin{aligned}
&[16, 2+\sqrt{-140}][16, 6+\sqrt{-140}] \\
&\qquad = [256, 16(6+\sqrt{-140}), 16(2+\sqrt{-140}), -128+8\sqrt{-140}] \\
&\qquad = [8][64, 12+2\sqrt{-140}, 4+2\sqrt{-140}, -16+\sqrt{-140}] \\
&\qquad = [8][64, 8, 4+2\sqrt{-140}, -16+\sqrt{-140}] \\
&\qquad = [8][8, 4+2\sqrt{-140}, \sqrt{-140}] = [8][4, \sqrt{-140}].
\end{aligned}$$

(This is a composition of forms that are not concordant in Dedekind's sense, which is to say that the greatest common divisor of $a = 16$, $\alpha = 16$, and $b+\beta = 8$ is not equal to 1. Therefore, Dedekind's method does not produce a composite.)

If f and f' are relatively prime, the product $[f, g+\sqrt{D}][f', g'+\sqrt{D}]$ of two modules in canonical form with $e = 1$ is simply $[ff', G+\sqrt{D}]$, where G is determined mod ff' by $G \equiv g$ mod f and $G \equiv g'$ mod f'. This is a consequence of the fact that there are integers σ and τ for which $\sigma f + \tau f' = 1$; since both

$\sigma f(G+\sqrt{D})$ and $\tau f'(G+\sqrt{D})$ are zero mod $[f, G+\sqrt{D}][f', G+\sqrt{D}]$, so is their sum $G+\sqrt{D}$, and

$$\begin{aligned}[f, g+\sqrt{D}][f', g'+\sqrt{D}] &= [f, G+\sqrt{D}][f', G+\sqrt{D}]\\ &= [ff', f(G+\sqrt{D}), f'(G+\sqrt{D}), (G+\sqrt{D})^2]\\ &= [ff', f(G+\sqrt{D}), f'(G+\sqrt{D}), (G+\sqrt{D})^2, G+\sqrt{D}]\\ &= [ff', G+\sqrt{D}].\end{aligned}$$

Explicitly, multiplication of modules can be used to construct composites of given forms[8] in the following way (assuming, of course, that the ratio of their determinants is a ratio of squares):

Theorem. Let $ax^2+2bxy+cy^2$ and $\alpha u^2+2\beta uv+\gamma v^2$ be given forms, and suppose that the ratio of their determinants is a ratio of squares, but that the determinants themselves are not squares. An explicit composition formula

$$(ax^2+2bxy+cy^2)(\alpha u^2+2\beta uv+\gamma v^2) = AX^2+2BXY+CY^2 \qquad (1)$$

can be constructed as follows. Choose positive integers s and σ for which $s^2(b^2-ac)$ and $\sigma^2(\beta^2-\alpha\gamma)$ are equal. Let D denote their common value, which is by assumption not a square. Put the module $[sa, sb+\sqrt{D}][\sigma\alpha, \sigma\beta+\sqrt{D}]$ in canonical form, say $[sa, sb+\sqrt{D}][\sigma\alpha, \sigma\beta+\sqrt{D}] = [E][F, G+\sqrt{D}]$. Then formula (1) holds for

$$AX^2+2BXY+CY^2 = \pm\frac{m\mu}{M}(FX^2+2GXY+HY^2) \qquad (2)$$

when the sign is the sign of $a\alpha$, when $H=(G^2-D)/F$, when m, μ and M are the positive integers defined by $[m]=[a, 2b, c]$, $[\mu]=[\alpha, 2\beta, \gamma]$ and $[M]=[F, 2G, H]$ (in short, they are the "contents" of the forms $ax^2+2bxy+cy^2$, $\alpha u^2+2\beta uv+\gamma v^2$ and $FX^2+2GXY+HY^2$) and when X and Y are the linear functions of xu, xv, yu and yv determined implicitly by

$$(sax+(sb+\sqrt{D})y)(\sigma\alpha u+(\sigma\beta+\sqrt{D})v) = E(FX+(G+\sqrt{D})Y). \qquad (3)$$

Proof. Reversing the sign of either of the given forms merely reverses the signs of both sides of (1) (the sign of the right side is reversed because the sign of (2) is reversed), so there is no loss of generality in assuming that a and α are both positive. Neither a nor α can be zero because the determinants are by assumption not squares. The definition (3) of X and Y obviously implies $sax v+\sigma\alpha yu+(sb+\sigma\beta)yv = EY$, after which it implies $EFX = sa\sigma\alpha xu+sa\sigma\beta xv+\sigma\alpha sbyu+(sb\sigma\beta+D)yv -$

[8] The degenerate case in which the given forms factor over the rationals – which is to say that their determinants are squares – will be ignored.

$G(saxv + \sigma\alpha yu + (sb + \sigma\beta)yv)$ so the explicit expression of X and Y in terms of xu, xv, yu and yv is

$$\begin{bmatrix} X \\ Y \end{bmatrix} = \begin{bmatrix} \frac{sa\sigma\alpha}{EF} & \frac{sa(\sigma\beta - G)}{EF} & \frac{\sigma\alpha(sb - G)}{EF} & \frac{sb\sigma\beta + D - G(sb+\sigma\beta)}{EF} \\ 0 & \frac{sa}{E} & \frac{\sigma\alpha}{E} & \frac{sb+\sigma\beta}{E} \end{bmatrix} \begin{bmatrix} xu \\ xv \\ yu \\ yv \end{bmatrix}. \tag{4}$$

Multiplication of the defining equation (3) by its conjugate $(sax + (sb - \sqrt{D})y)$ $(\sigma\alpha u + (\sigma\beta - \sqrt{D})v) = E(FX + (G - \sqrt{D})Y)$ – which is the same statement as (3) – gives $((sax + sby)^2 - (s^2b^2 - s^2ac)y^2)((\sigma\alpha u + \sigma\beta v)^2 - (\sigma^2\beta^2 - \sigma^2\alpha\gamma)v^2) = E^2((FX + GY)^2 - (G^2 - FH)Y^2)$, that is,

$$s^2\sigma^2 a\alpha(ax^2 + 2bxy + cy^2)(\alpha u^2 + 2\beta uv + \gamma v^2) = E^2F(FX^2 + 2GXY + HY^2).$$

Division by $s^2\sigma^2 a\alpha$ gives equation (1) with $A = \frac{E^2F^2}{s^2\sigma^2 a\alpha}$, $2B = \frac{2E^2FG}{s^2\sigma^2 a\alpha}$ and $C = \frac{E^2FH}{s^2\sigma^2 a\alpha}$. Thus, the theorem will be proved[9] if $\frac{E^2F}{s^2\sigma^2 a\alpha}$ is shown to be equal to $\frac{m\mu}{M}$, if the entries of the matrix in (4) are shown to be integers and if the greatest common divisor of the 2×2 minors of this matrix is shown to be 1. (The first two minors $\frac{(sa)^2\sigma\alpha}{E^2F}$ and $\frac{sa(\sigma\alpha)^2}{E^2F}$ are positive because s, σ, a, α and F are all positive.)

By definition, $[sa, sb + \sqrt{D}][\sigma\alpha, \sigma\beta + \sqrt{D}] = [E][F, G + \sqrt{D}]$. Thus, E, F and G are found by putting $[sa\sigma\alpha, sa\sigma\beta + sa\sqrt{D}, \sigma\alpha sb + \sigma\alpha\sqrt{D}, sb\sigma\beta + D + (sb + \sigma\beta)\sqrt{D}]$ in canonical form. Let $\mathfrak{P}'$, $\mathfrak{P}''$, and $\mathfrak{P}'''$ (Gauss's notation) be such that $\mathfrak{P}'sa + \mathfrak{P}''\sigma\alpha + \mathfrak{P}'''(sb + \sigma\beta)$ is the greatest common divisor of sa, $\sigma\alpha$, and $sb + \sigma\beta$, call it d. Then d clearly divides both coefficients of all four numbers in the product module $[sa\sigma\alpha, sa\sigma\beta + sa\sqrt{D}, \sigma\alpha sb + \sigma\alpha\sqrt{D}, sb\sigma\beta + D + (sb + \sigma\beta)\sqrt{D}]$ with the possible exception of $sb\sigma\beta + D$, and it divides this coefficient as well because $D \equiv (sb)^2 \bmod sa$, so $sb\sigma\beta + D \equiv sb\sigma\beta + (sb)^2 \equiv sb(\sigma\beta + sb) \equiv 0 \bmod d$. Let G_0 be defined by the equation $d(G_0 + \sqrt{D}) = \mathfrak{P}'sa(\sigma\beta + \sqrt{D}) + \mathfrak{P}''\sigma\alpha(sb + \sqrt{D}) + \mathfrak{P}'''(sb\sigma\beta + D + (sb + \sigma\beta)\sqrt{D})$. In other words,

$$G_0 = \frac{1}{d}(\mathfrak{P}'sa\sigma\beta + \mathfrak{P}''\sigma\alpha sb + \mathfrak{P}'''(sb\sigma\beta + D)).$$

Then

$$\begin{aligned}
&[sa, sb + \sqrt{D}][\sigma\alpha, \sigma\beta + \sqrt{D}] \\
&= [sa\sigma\alpha, sa\sigma\beta + sa\sqrt{D}, \sigma\alpha sb + \sigma\alpha\sqrt{D}, sb\sigma\beta + D + (sb + \sigma\beta)\sqrt{D}, d(G_0 + \sqrt{D})] \\
&= [sa\sigma\alpha, sa\sigma\beta - saG_0, \sigma\alpha sb - \sigma\alpha G_0, sb\sigma\beta + D - (sb + \sigma\beta)G_0, d(G_0 + \sqrt{D})].
\end{aligned}$$

This module is full because it can be found by starting with the full module $[sa, sb + \sqrt{D}][\sigma\alpha, \sigma\beta + \sqrt{D}]$ (full because each factor is full), annexing a zero, and adding

[9] By the definition of M, the coefficients A, $2B$, C of the composite form are integers. For (1) to be a composition in the Gaussian sense, $2B$ must be proved to be *even,* but, for reasons explained below, this point will be ignored and (1) will be accepted as a "composition" without a proof that $2B$ is even.

integer multiples of other entries to this zero – namely, adding $\mathfrak{P}'$, $\mathfrak{P}''$ and $\mathfrak{P}'''$ times the appropriate entries. Let F_0 be defined by

$$[dF_0] = [sa\sigma\alpha, sa\sigma\beta - saG_0, \sigma\alpha sb - \sigma\alpha G_0, sb\sigma\beta + D - (sb + \sigma\beta)G_0].$$

Then the module $[dF_0, dG_0 + d\sqrt{D}]$ can be reached by successively subtracting integer multiples of entries of $[sa\sigma\alpha, sa\sigma\beta - saG_0, \sigma\alpha sb - \sigma\alpha G_0, sb\sigma\beta + D - (sb + \sigma\beta)G_0, d(G_0 + \sqrt{D})]$ to reduce the integers in this module to their greatest common divisor dF_0 while leaving $d(G_0 + \sqrt{D})$ unchanged, so it is full, as well as equal to the product module.

Because $[dF_0, dG_0 + d\sqrt{D}]$ is full and d and F_0 are positive, it is in canonical form, except that G_0 may not be in the range $0 \le G_0 < F_0$. Because $[dF_0, dG_0 + d\sqrt{D}] = [E][F, G + \sqrt{D}]$, it follows that $E = d$, $F = F_0$, and $G \equiv G_0 \bmod F$.

In particular, E is the greatest common divisor of sa, $\sigma\alpha$ and $sb + \sigma\beta$, which shows that the entries in the second row of the matrix in (4) are integers. Moreover, $EF = dF_0$ is the greatest common divisor of $sa\sigma\alpha$, $sa\sigma\beta - saG_0$, $\sigma\alpha sb - \sigma\alpha G_0$ and $sb\sigma\beta + D - (sb + \sigma\beta)G_0$, from which it follows, because $G_0 \equiv G \bmod F$, that the entries in the first row of the matrix in (4) are integers.

The product of $[sa, sb + \sqrt{D}]$ with its conjugate $[sa, sb - \sqrt{D}]$ is $[sa, sb + \sqrt{D}][sa, sb - \sqrt{D}] = [(sa)^2, sa(sb - \sqrt{D}), sa(sb + \sqrt{D}), s^2b^2 - s^2(b^2 - ac)] = [sa][sa, sb + \sqrt{D}, sb - \sqrt{D}, sc] = [sa][sa, 2sb, sc, sb + \sqrt{D}] = [sa][sm, sb + \sqrt{D}]$, where m is as in the statement of the theorem. Similar calculations apply to the other two modules in the equation $[sa, sb+\sqrt{D}][\sigma\alpha, \sigma\beta+\sqrt{D}] = [E][F, G+\sqrt{D}]$, so multiplication of this equation by its conjugate gives

$$[sa][sm, sb + \sqrt{D}][\sigma\alpha][\sigma\mu, \sigma\beta + \sqrt{D}] = [E^2][F][M, G + \sqrt{D}].$$

Since $sb \equiv -sb \bmod sm$, $\sigma\beta \equiv -\sigma\beta \bmod \sigma\mu$ and $G \equiv -G \bmod M$, the modules in this equation are self-conjugate and multiplication of the equation with its conjugate amounts to squaring and results in

$$[sa\sigma\alpha]^2[sm][sm, sb + \sqrt{D}][\sigma\mu][\sigma\mu, \sigma\beta + \sqrt{D}] = [E^2F]^2[M][M, G + \sqrt{D}]$$

which combines with the previous equation to give

$$[sa\sigma\alpha][sm\sigma\mu][E^2F][M, G + \sqrt{D}] = [E^2F]^2[M][M, G + \sqrt{D}].$$

When G is reduced mod M (the result must be 0 or $\frac{1}{2}M$) the modules on either side are in canonical form, and $sa\sigma\alpha \cdot sm\sigma\mu = E^2F \cdot M$ follows. In other words, $\frac{E^2F}{s^2\sigma^2a\alpha} = \frac{m\mu}{M}$, as was to be shown.

Finally, let Δ_{ij} for $0 < i < j \le 4$ be the minor of the matrix in (4) that uses columns i and j. It remains to show that the greatest common divisor of the Δ_{ij} is equal to 1. By direct computation,

$$\begin{aligned}&[E^2F][\Delta_{12}, \Delta_{13}, \Delta_{14}, \Delta_{23}, \Delta_{24}, \Delta_{34}]\\ &\qquad = [sa\sigma\alpha][sa, \sigma\alpha, sb + \sigma\beta, \sigma\beta - sb, sc, \sigma\gamma].\end{aligned}$$

(The calculation is simplified when one observes that adding G times the second row to the first does not change the minors.) What is to be proved, then, is that $[E^2F] = [sa\sigma\alpha][sa, \sigma\alpha, sb + \sigma\beta, \sigma\gamma, sc]$, which is to say

$$\begin{aligned}&[E][sa\sigma\alpha, sa(\sigma\beta - G_0), \sigma\alpha(sb - G_0), sb\sigma\beta + D - (sb + \sigma\beta)G_0]\\ &\qquad = [sa\sigma\alpha][sa, \sigma\alpha, sb + \sigma\beta, \sigma\beta - sb, \sigma\gamma, sc].\end{aligned}$$

The first three terms on the right – that is, $sa\sigma\alpha$ times sa, $\sigma\alpha$ and $sb + \sigma\beta$ – are all divisible by $Esa\sigma\alpha$ and are therefore zero modulo the module on the left. The remaining three are zero modulo the module on the left by virtue of

$$sa\sigma\alpha(\sigma\beta - sb) = \frac{\sigma\alpha}{E} \cdot Esa(\sigma\beta - G_0) - \frac{sa}{E} \cdot E\sigma\alpha(sb - G_0)$$

$$\begin{aligned}sa\sigma\alpha\sigma\gamma &= \frac{sb + \sigma\beta}{E} \cdot Esa(\sigma\beta - G_0) - \frac{sa}{E} \cdot E(sb\sigma\beta + D - (sb + \sigma\beta)G_0)\\ sa\sigma\alpha sc &= \frac{sb + \sigma\beta}{E} \cdot E\sigma\alpha(sb - G_0) - \frac{\sigma\alpha}{E} \cdot E(sb\sigma\beta + D - (sb + \sigma\beta)G_0).\end{aligned}$$

Finally, the four terms in the module on the left are zero modulo the module on the right by virtue of

$$\begin{aligned}Esa\sigma\alpha &= \mathfrak{P}'s^2a^2\sigma\alpha + \mathfrak{P}''sa\sigma^2\alpha^2 + \mathfrak{P}'''(sb + \sigma\beta)sa\sigma\alpha\\ Esa(\sigma\beta - G_0) &= \mathfrak{P}''sa\sigma\alpha(\sigma\beta - sb) + \mathfrak{P}'''sa\sigma\alpha\sigma\gamma\\ E\sigma\alpha(sb - G_0) &= \mathfrak{P}'sa\sigma\alpha(sb - \sigma\beta) + \mathfrak{P}'''sa\sigma\alpha sc\\ E(sb\sigma\beta + D - (sb + \sigma\beta)\sigma\beta) &= \mathfrak{P}'sa\sigma\alpha\sigma\gamma + \mathfrak{P}''sa\sigma\alpha sc,\end{aligned}$$

(the last three equations are obtained by eliminating one of the $\mathfrak{P}$s from $E = \mathfrak{P}'sa + \mathfrak{P}''\sigma\alpha + \mathfrak{P}'''(sb + \sigma\beta)$ and $EG_0 = \mathfrak{P}'sa\sigma\beta + \mathfrak{P}''\sigma\alpha sb + \mathfrak{P}'''(sb\sigma\beta + D)$) and the proof is complete.

Allowing forms to have odd middle coefficients permits the theorem to take the more natural form

$$\frac{ax^2 + 2bxy + cy^2}{m} \cdot \frac{\alpha u^2 + 2\beta uv + \gamma v^2}{\mu} = \frac{FX^2 + 2GXY + HY^2}{M} \tag{5}$$

of a composition of two *primitive* forms (forms in which the greatest common divisor of the coefficients is 1) in which the composite is also primitive. One can obviously compose *arbitrary* forms if one can compose *primitive* forms, so it is natural to restate the theorem in the form: Given two primitive forms $ax^2 + bxy + cy^2$ and $\alpha u^2 + \beta uv + \gamma v^2$, if the ratio of $b^2 - 4ac$ to $\beta^2 - 4\alpha\gamma$ is a ratio of squares, the obvious modification of the construction of the theorem gives a composition formula for them in which the composite form is primitive.

For example, to compose $x^2 + xy - y^2$ with itself, the theorem replaces it with $2x^2 + 2xy - 2y^2$ and computes $[2, 1 + \sqrt{5}][2, 1 + \sqrt{5}] = [2][2, 1 + \sqrt{5}]$ to find the composition $(2x^2 + 2xy - 2y^2)(2u^2 + 2uv - 2v^2) = 2(2X^2 + 2XY - 2Y^2)$, where

X and Y are defined by $(2x+(1+\sqrt{5})y)(2u+(1+\sqrt{5})v) = 2(2X+(1+\sqrt{5})Y)$, which is to say $X = xu + vy$ and $Y = xv + yu + yv$. The more natural way to state this composition formula is of course

$$(x^2+xy-y^2)(u^2+uv-v^2) = X^2+XY-Y^2.$$

Formula (5) can be used to construct a composition of any two forms, when the ratio of their determinants is a ratio of squares, whether or not they are primitive and whether or not their middle coefficients are even. Once a *single* composition is known, all others are obtained by taking unimodular changes of variables $X' = pX + qY$, $Y' = rX + sY$, where p, q, r and s are integers with $ps - qr = 1$.

From Gauss's point of view the theorem does not provide a composition of two given forms until B is proved to be an integer, or, in the terms of the modified theorem, until it is proved that if the middle coefficients of the given primitive forms are both even, the middle coefficient of the composite form given by the theorem is even. This statement is true, as follows from Gauss's construction of art. 236, but it is a matter of little importance unless there is a reason to restrict consideration to forms with even middle coefficients, a point on which I and many other of Gauss's readers remain unconvinced.

3. Conclusion

I hope that the use of module multiplication in some measure simplifies Gauss's theory of composition of forms. For example, it clarifies the difficult associativity property described and proved by Gauss in art. 240. Multiplication of modules is *obviously* an associative binary operation, and this property easily translates into the property Gauss uses.[10]

But, more importantly, I hope that by focussing attention on Gauss's composition of actual forms – as opposed to equivalence classes of forms as in the modern theory – I have highlighted Gauss's great achievement in giving a rigorous treatment of the composition of binary quadratic forms in the greatest possible generality.

His theory is "rigorous," not only in the usual sense that it is mathematically convincing, but also in the literal sense that it makes great demands on the reader. The second kind of rigor has caused succeeding generation of mathematicians to devote some of their best efforts to avoiding it. But it is the first kind of rigor that makes Gauss the great master. It is based on his mastery of the computational structure of his subject and his ability to explain that structure in the most general circumstances. While they may seek to avoid the difficulties of Gauss's theory, succeeding generations should never cease to admire it.

[10] Since multiplication of modules can be used to establish the theory of composition of forms, Gauss's proof of quadratic reciprocity using composition of forms can be deduced in this way. However, quadratic reciprocity can be proved working directly with multiplication of modules. Therefore, if the goal is quadratic reciprocity, one can dispense with quadratic forms altogether. Other aspects of Gauss's theory can be revisited in a similar way. See [Edwards 2005].

References

DIRICHLET, Johann Peter Gustav LEJEUNE-. 1851. *De Formarum Binariarum Secundi Gradus Compositione*. Berlin: Akademie Verlag. Repr. with changes in *Journal für die reine und angewandte Mathematik* 47 (1854), 155–160. Repr. in *Werke*, ed. L. Fuchs and L. Kronecker, vol. 2, pp. 107–114. Berlin: Reimer, 1889-1897.

———. 1879. *Vorlesungen über Zahlentheorie*, ed. with supplements by R. Dedekind. 3rd ed. Braunschweig: Vieweg.

EDWARDS, Harold M. 2005. *Essays in Constructive Mathematics*. New York: Springer.

KUMMER, Ernst Eduard. 1846. Letter to Leopold Kronecker, June 14, 1846. *Festschrift zur Feier des 100 Geburtstages Eduard Kummer mit Briefen an seine Mutter und an Leopold Kronecker*, ed. K. Hensel. Berlin and Leipzig: Teubner, 1910. Repr. in [Kummer 1975], vol. 1, p. 68.

———. 1847. Zur Theorie der complexen Zahlen. *Journal für die reine und angewandte Mathematik* 35, pp. 319–326. Repr. in [Kummer 1975], vol. 1, pp. 203–210.

———. 1975. *Collected Papers*, ed. A. Weil. 2 vols. New York: Springer.

WATERHOUSE, William. 1984. A note by Gauss referring to ideals? *Historia Mathematica* 11, 142–146.

WEIL, André. 1984. *Number Theory. An Approach Through History from Hammurapi to Legendre*. Boston: Birkhäuser.

II.3

Composition of Quadratic Forms: An Algebraic Perspective

Della D. Fenster and Joachim Schwermer

When it comes to the arithmetic theory of binary quadratic forms, Carl Friedrich Gauss's systematic treatment of the reduction of forms in arts. 171–175 of the *Disquisitiones Arithmeticae* stands as one of the masterpieces of this work.[1] Composition of forms, dealt with in arts. 235–240, represents the second core of his investigations of integral forms. Gauss's treatment presented a major challenge to mathematicians of subsequent generations. On the arithmetic side, particularly after Richard Dedekind had given his reinterpretation of certain results in terms of orders of quadratic number fields, the Gaussian theory proved crucial in the development of algebraic number theory. The recent work of Manjul Bhargava, for example, testifies to the continued inspiration of the original constructive style of Gauss.

On the algebraic side, Martin Kneser considered the possibility of a theory of the composition of binary quadratic forms over an arbitrary commutative ring with unity. In this general context, the subsequent theory hinged on a consideration of the natural structure of a given quadratic R–module (M, q) as a module under the (even) Clifford algebra attached to M. This new point of view resolved the difficult issue of "orientation" faced by Gauss and others, and we will use it here to highlight key aspects of Gauss's work. Adolf Hurwitz provides an intermediary step between Gauss and Kneser. We will look first at Gauss's theory through the eyes of Hurwitz in 1898. The structural approach outlined by Hurwitz in his personal notebooks makes Gauss's work far more accessible. Moreover, the sheer record of his mathematical thoughts allows a very personal indication of the reception of Gauss's *Disquisitiones Arithmeticae*. Once we gain an understanding of the six main "conclusions" of Gauss (with some help from Hurwitz), we turn our attention to the question of proper equivalence that will play a significant role in the work of Kneser. We provide a brief overview of various attempts to simplify and enhance our understanding of

[1] For a discussion of these results we refer to J. Schwermer's chap. VIII.1 in this volume.

Gauss's theory of the composition of integral quadratic forms. We next turn our attention to the ideas that served as our starting point, namely, an algebraic approach to the composition of binary quadratic forms. This highly technical section of the paper focuses on Kneser's efforts to recast Gauss's work in terms of Clifford algebras, thereby extending the theory considerably.

1. Hurwitz's Thoughts on Gauss's Composition of Forms

While completing his Habilitation in Göttingen in 1882, Adolf Hurwitz began to enter his mathematical investigations and thoughts in a notebook.[2] Sixteen years later, this former student of Felix Klein who now held a position at the Eidgenössische Polytechnicum in Zürich, was still at it. On October 20, 1898, in particular, he recorded a seven-page entry titled "On Gauss, Disquisitiones Arithmeticae, Art. 235 ff. Composition of Forms." There, Hurwitz examined in detail Gauss's composition of forms, the fundamental focus of his theory of binary quadratic forms with integral coefficients.

Gauss's work is an elaboration of classical formulas such as, for example, the sum of two squares $(x^2 + y^2)(x'^2 + y'^2) = (xx' \pm yy')^2 + (xy' \mp yx')^2$ or, more generally,

$$(ax^2 + cy^2)(x'^2 + acy'^2) = a(xx' - cyy')^2 + c(axy' + yx')^2.$$

This portion of Gauss's work contains a large number of carefully worked out investigations based on explicit manipulations of equations. It is difficult to follow, and, perhaps, does not represent Gauss's initial approach to the composition of forms.[3] These highly computational investigations form the basis for a proof of the law of quadratic reciprocity in the following articles of the *Disquisitiones Arithmeticae*. Thus in the *Disquisitiones Arithmeticae*, Gauss links the composition of forms with the *Theorema fundamentale* in the theory of quadratic residues. The strength of this latter result lies in its ability to compare congruences modulo different primes.

Following Gauss, Hurwitz began to consider the most general problem of the transformation of a binary form $F = AX^2 + 2BXY + CY^2$ into the product of two forms $f = ax^2 + 2bxy + cy^2$, $f' = a'x'^2 + 2b'x'y' + c'y'^2$, by means of a bilinear substitution (Σ):

[2] The mathematical notebooks of Adolf Hurwitz are held in his Nachlass at the ETH – Bibliothek, Archives, Zürich. This collection now holds 31 notebooks ranging from April 1882 to May 1918. These notebooks contain beautiful, truly elegant entries that tend not to reflect any of the tension involved in working out an idea but, rather, a complete understanding of that idea.

[3] The historical record now contains substantial evidence to suggest that the published presentation of Gauss's composition of forms in the *Disquisitiones Arithmeticae* may not accurately reflect its actual development. Neumann argued in [Neumann 1980] that Gauss's initial approach was based on what can be described in modern terms as a multiplication of modules (or lattices) in the quadratic field $\mathbf{Q}(\sqrt{d})$. His analysis relies on a footnote of Gauss to sec. 8.3 of his thesis (see [Gauss 1866], p. 14) and a letter of Kummer to Kronecker on June 14, 1846, [Kummer 1975], vol. 1, p. 98–99. See also H. Edwards's chap. II.2 above.

$$\begin{array}{rcll} X & = & pxx' + p'xy' + p''yx' + p'''yy' & = \alpha'x + \beta'y = \alpha x' + \beta y' \\ Y & = & qxx' + q'xy' + q''yx' + q'''yy' & = \gamma'x + \delta'y = \gamma x' + \delta y'. \end{array}$$

Gauss and Hurwitz confined the coefficients of this substitution to the integers (as well as those of F, f, f', of course). As usual, Hurwitz denoted the determinants of F, f, f' by $D = B^2 - AC$, $d = b^2 - ac$, $d' = b'^2 - a'c'$ respectively, and he put

$$n = \sqrt{\frac{d}{D}}, \qquad n' = \sqrt{\frac{d'}{D}}.$$

Note that this definition relies on a subtle point, that is, a choice of a sign for the root. This point plays an important role in the following discussion. As in Gauss, Hurwitz denoted the determinants [his notation!] $(pq'-qp') = (pq'), (pq''), (pq'''), (p'q'')$, $(p'q''')$, $(p''q''')$ by P, Q, R, S, T, U respectively. With this notation established, however, Hurwitz followed a different course than Gauss in dealing with the question of a possible transformation of F into the product of two forms f and f'. By interpreting x', y' as fixed but arbitrary constants (not unlike as we do it today), Hurwitz stated that, under the assumption $F = f \cdot f'$ by means of (Σ), the form F is transformed by the substitution $\begin{pmatrix} \alpha' & \beta' \\ \gamma' & \delta' \end{pmatrix}$ into $f'ax^2 + f'2bxy + f'cy^2$. As a consequence Hurwitz obtained the identity $D(\alpha'\delta' - \beta'\gamma')^2 = df'^2$, or

$$nf' = \alpha'\delta' - \beta'\gamma' = Qx'^2 + (R+S)x'y' + Ty'^2. \tag{I}$$

Along with this equation (I), Hurwitz obtained in an analogous way an equation

$$n'f = \alpha\delta - \beta\gamma = Px^2 + (R-S)xy + Uy^2. \tag{II}$$

After a very lucid two-page manipulation, he drew as his conclusion what he called the "foundation of Gauss's theory of composition": If F is transformed into the product $f \cdot f'$ by means of the substitution (Σ) then the following three equations hold:

$$n'f = \begin{vmatrix} px + p''y & p'x + p'''y \\ qx + q''y & q'x + q'''y \end{vmatrix}$$

$$nf' = \begin{vmatrix} px' + p'y' & p''x' + p'''y' \\ qx' + q'y' & q''x' + q'''y' \end{vmatrix}$$

$$nn'F = \begin{vmatrix} q''X - p''Y & q'''X - p'''Y \\ qX - pY & q'X - p'Y \end{vmatrix}.$$

In addition, Hurwitz noted, $d = n^2D$ and $d' = n'^2D$ respectively. In reverse, when n, n' are non-zero numbers, these three equations imply that F can be transformed into $f \cdot f'$ by a substitution of the form

$$\begin{pmatrix} p & \cdots \\ q & \cdots \end{pmatrix}.$$

With this result, Hurwitz took up his apparent aim for this entry in his private notebook, namely, a clearer explanation of the six conclusions stated by Gauss in art. 235 of the *Disquisitiones Arithmeticae*. Since n and n' are rational, Hurwitz easily established the first conclusion that the determinants of F, f, f' are in "ratio of squares" (i. e. they are equal up to square factors).[4]

Next Hurwitz deduced that if m and m' denote the greatest common divisor of the coefficients of f and f' respectively, then $m'n$ and mn' are integers since $n'f$ and nf' are integral forms. Thus, by the very definition of n and n', one obtains

$$D(m'n)^2 = dm'^2, \qquad D(mn')^2 = d'm^2,$$

that is, D divides dm'^2 and $d'm^2$ respectively. This is Gauss's second conclusion.

As Hurwitz noted, the third conclusion coincides with the first two equations above,[5] that is,

$$n'f = \begin{vmatrix} px + p''y & p'x + p'''y \\ qx + q''y & q'x + q'''y \end{vmatrix}$$

$$nf' = \begin{vmatrix} px' + p'y' & p''x' + p'''y' \\ qx' + q'y' & q''x' + q'''y' \end{vmatrix}.$$

The fourth conclusion of Gauss established that Dk^2 is the greatest common divisior of dm'^2 and $d'm^2$ where k is the greatest commmon divisor of the determinants extracted from

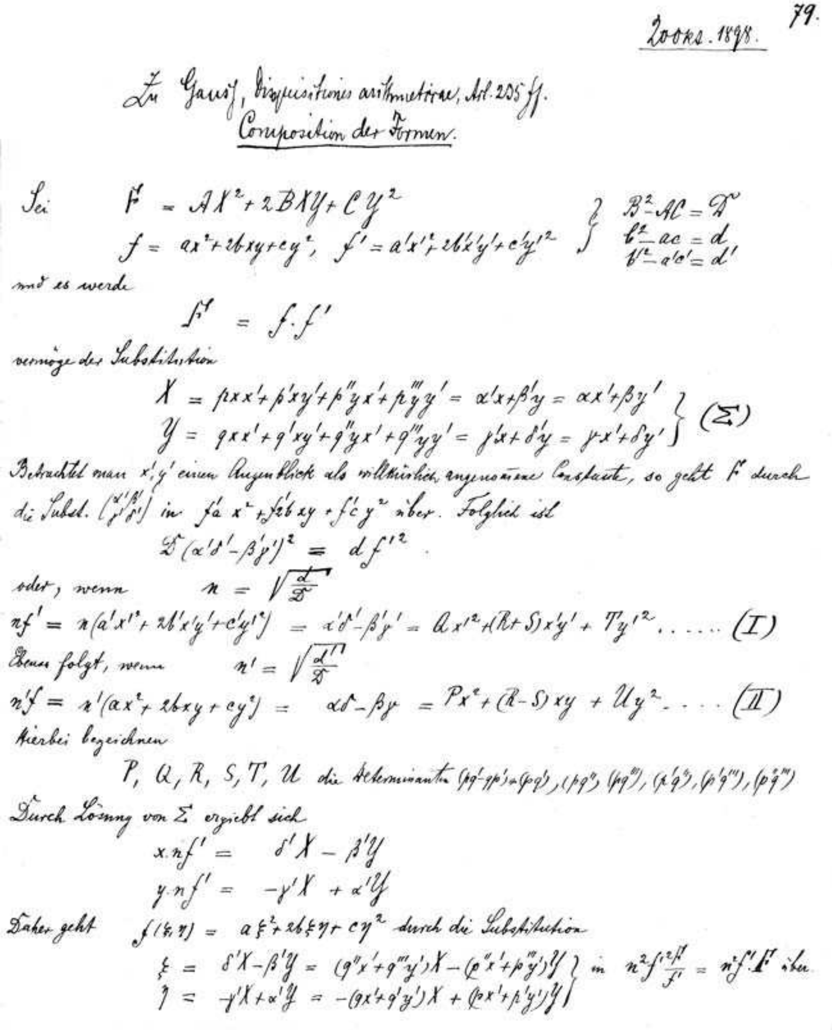
$$\begin{pmatrix} p & p' & p'' & p''' \\ q & q' & q'' & q''' \end{pmatrix}.$$

That is, by definition, k is the greatest common divisor of P, Q, R, S, T, U. Hurwitz gave the following deduction of this result of Gauss. First, the equations (I) and (II) imply that k divides nm' and $n'm$. Conversely, a common divisor of nm' and $n'm$ also divides P, Q, $R+S$, $R-S$, T, U, hence, it also divides $2R$ and $2S$. But one has $4RS = 4(a'c'n^2 - acn'^2)$ so that a common divisor divides R and S as well. It follows that k is the greatest common divisor of nm' and $n'm$. This implies that Dk^2 is the greatest common divisor of $Dn^2m'^2 = dm'^2$ and $Dn'^2m^2 = d'm^2$.

In a similarly straightforward way, Hurwitz deduced that $(mm')/M$ is an integer where M denotes the divisor of F. Moreover, this integral value $(mm')/M$ divides k^2. This result accounted for Gauss's fifth conclusion. For the sixth conclusion, however, Hurwitz did not see a more direct way to show that mm' divides Mk^2 other than to rely on the explicit formulas of Gauss.

[4] As Hurwitz states it, "Die Determinanten von F, f, f' stehen im Verhältnis von Quadratzahlen."

[5] Gauss's formulation, however, is slightly different. He stated that the coefficients of f are proportional to the numbers P, $R-S$, U. If one puts the proportion of the former to the latter as the ratio $1/n'$ then n' is the square root of d'/D. Gauss made an analogous statement for the coefficients of f'. This is how Gauss introduced the terms n and n' respectively.



20 Okt. 1898. 79.

Zu Gauss, Disquisitiones arithmeticae, Art. 235 ff.
Composition der Formen.

Sei
$$F = AX^2 + 2BXY + CY^2$$
$$f = ax^2 + 2bxy + cy^2,\quad f' = a'x'^2 + 2b'x'y' + c'y'^2 \Bigg\}\quad \begin{array}{l} B^2 - AC = \mathfrak{D} \\ b^2 - ac = d \\ b'^2 - a'c' = d' \end{array}$$
und es werde
$$F = f\cdot f'$$
vermöge der Substitution
$$\left.\begin{array}{l} X = pxx' + p'xy' + p''yx' + p'''yy' = \alpha' x + \beta' y = \alpha x' + \beta y' \\ Y = qxx' + q'xy' + q''yx' + q'''yy' = \gamma' x + \delta' y = \gamma x' + \delta y' \end{array}\right\}\ (\Sigma)$$
Betrachtet man x', y' einen Augenblick als willkürlich angenommene Constante, so geht F durch die Subst. $\begin{pmatrix}\alpha' & \beta' \\ \gamma' & \delta'\end{pmatrix}$ in $f'a\,x^2 + f'2b\,xy + f'c\,y^2$ über. Folglich ist
$$\mathfrak{D}(\alpha'\delta' - \beta'\gamma')^2 = d f'^2 .$$
oder, wenn $n = \sqrt{\frac{d}{\mathfrak{D}}}$
$$nf' = n(a'x'^2 + 2b'x'y' + c'y'^2) = \alpha'\delta' - \beta'\gamma' = Qx'^2 + (R+S)x'y' + Ty'^2 \ldots\ldots (I)$$
Ebenso folgt, wenn $n' = \sqrt{\frac{d'}{\mathfrak{D}}}$
$$n'f = n'(ax^2 + 2bxy + cy^2) = \alpha\delta - \beta\gamma = Px^2 + (R-S)xy + Uy^2 \ldots\ldots (II)$$
Hierbei bezeichnen

P, Q, R, S, T, U die Determinanten $(pq' - qp') = (pq'), (pq''), (pq'''), (p'q''), (p'q'''), (p''q''')$

Durch Lösung von Σ ergiebt sich
$$x.nf' = \delta' X - \beta' Y$$
$$y.nf' = -\gamma' X + \alpha' Y$$
Daher geht $f(\xi,\eta) = a\xi^2 + 2b\xi\eta + c\eta^2$ durch die Substitution
$$\left.\begin{array}{l} \xi = \delta' X - \beta' Y = (q''x' + q'''y')X - (p''x' + p'''y')Y \\ \eta = -\gamma' X + \alpha' Y = -(qx' + q'y')X + (px' + p'y')Y \end{array}\right\}\ \text{in}\ n^2 f'^2 \frac{F}{f'} = n^2 f' F\ \text{über}$$

Fig. II.3. Hurwitz's comments on Gauss's composition of forms
(Courtesy of ETH-Library, Archives, Zürich)

Whereas Gauss dealt in art. 235 with the most general question of a transformation of a form F into a product $f \cdot f'$ of forms f and f' by means of a substitution (Σ), he focused his attention in the next article to the case where $k = 1$, that is, the greatest common divisor of the determinants P, Q, R, S, T, U equals one. In such a case, F is said to be compounded of f and f', or, F is a composite of f and f'. Gauss showed in art. 236 that, given integral binary forms f and f' as above with determinants that differ by a square factor, there exists a form F which can be compounded of f and f'. Note that such a form F cannot be uniquely determined since the variables X, Y can always be transformed with a unimodular substitution. More precisely, if F is transformed into the product of f and f' by (Σ) and if the variables X and Y of F are transformed under some unimodular substitution $T = \begin{pmatrix} r & s \\ u & v \end{pmatrix}$, that is, there are new variables $X^* = rX + sY$, $Y^* = uX + vY$, then the new form F^* with the variables X^* and Y^* is transformed into the product of f and f' by the substitution $T \cdot (\Sigma)$.

Based on his alternative approach to Gauss's theory, which relied less on explicit computations and more on insights gained from an awareness of the theory of linear transformations, Hurwitz could infer this result as well. Like Gauss, he followed a constructive argument. The equations

$$n'(ax^2 + 2bxy + cy^2) = Px^2 + (R - S)xy + Uy^2$$

$$n(a'x'^2 + 2b'x'y' + c'y'^2) = Qx'^2 + (R + S)x'y' + Ty'^2$$

served as a starting point for Hurwitz's investigation. He found the entities P, Q, R, S, T, U as integers in an explicit way. The next step ahead was to find a system of numbers of the form $\begin{pmatrix} p & p' & p'' & p''' \\ q & q' & q'' & q''' \end{pmatrix}$ so that the extracted determinants (pq'), (pq''), (pq'''), $(p'q'')$, $(p'q''')$, $(p''q''')$ coincided with the integral values of P, Q, R, S, T, U. With these determinants at hand, the equation

$$nn'F = \begin{vmatrix} q''X - p''Y & q'''X - p'''Y \\ qX - pY & q'X - p'Y \end{vmatrix}$$

gives rise to a form F which is compounded of f and f'. Note that this equation is the third one in Hurwitz's basic result. For this final step, Hurwitz largely relied on the methods of Gauss to pass over from the integers P, Q, R, S, T, U to the system of numbers that form the entries of (Σ).

Hurwitz concluded his reading of Gauss's composition of forms by examining the content of art. 240. There, Gauss had proved that given three integral binary forms f, f', f'', a composite $(f \cdot f') \cdot f''$ is equivalent to a composite $f \cdot (f' \cdot f'')$ where $f \cdot f'$, resp. $(f \cdot f') \cdot f''$, etc., denote a composite of f and f', resp. of $(f \cdot f')$ and f'', etc. Gauss's treatment of this associative type of behaviour required several pages of computations, some of which he left to the reader. Hurwitz was able to deal with this statement within his alternative approach in an insightful way. Without going into details we just mention his basic step: a composite $(f \cdot f') \cdot f'' = F$ is obtained by means of a substitution of variables where the variables X, Y of F depend on the eight monomials $xx'x''$, $xx'y''$, $xy'x''$, $xy'y''$, ... As above, this can be written as

$$X = \alpha x + \beta y = \alpha' x' + \beta' y' = \alpha'' x'' + \beta'' y''$$

$$Y = \gamma x + \delta y = \gamma' x' + \delta' y' = \gamma'' x'' + \delta'' y''.$$

These equations imply

$$\alpha\delta - \beta\gamma = \sqrt{\frac{d}{D}} f' \cdot f'', \quad \alpha'\delta' - \beta'\gamma' = \sqrt{\frac{d'}{D}} f \cdot f'', \quad \alpha''\delta'' - \beta''\gamma'' = \sqrt{\frac{d''}{D}} f \cdot f'$$

in obvious notation. These identities prove decisive in Hurwitz's following argument to show associativity up to equivalence since they relate the values of all the determinants of the underlying substitution to the coefficients of f, f' and f''. In this proof, Hurwitz had to make the crucial choice that these roots $\sqrt{d/D}$, $\sqrt{d'/D}$, $\sqrt{d''/D}$ are positive.

In the record of his study of Gauss's *Disquisitiones Arithmeticae* on October 20, 1898, Hurwitz gave his attention to arts. 235, 236 and 240. He apparently considered these articles the most relevant for his own work. Hurwitz made extensive use of the insights gained from linear transformations and determinants to recast Gauss's work in a way he – and we after him – could understand better.

2. Historical Remarks

There have been many attempts to simplify Gauss's theory of composition of integral quadratic forms and to make transparent the underlying concepts.[6] In the previous section we discussed how Hurwitz revisited Gauss's constructive treatment of 1801 in his private, unpublished notebook nearly a century later. At the end of the XIX$^{\text{th}}$ century, the question of composition of forms had already moved beyond the theory of binary quadratic forms with integral coefficients. Hurwitz, for example, had just published his paper "Ueber die Composition der quadratischen Formen von beliebig vielen Variablen," [Hurwitz 1898]. There he proved that a theory of composition for non-degenerate quadratic forms with real coefficients in n variables only exists in the cases where $n = 2, 4$, and 8. Thus Hurwitz brought the long discussion about the known product formulas for sums of two, four or eight squares to an end. The case was closed. The complex numbers, quaternions and octonions are, in contempory terms, the only composition algebras.[7] Hurwitz's line of argument for this proof relied on the theory of linear transformations and matrices as developed by Cayley.

As we have seen, if a given integral form F is a composite of integral forms f and f' then the determinants of f and f' differ from the one of F by an integral

[6] Henry J. S. Smith covers this topic in [Smith 1862] and Leonard E. Dickson gives a survey of the literature up to 1920 in [Dickson 1923], chap. 3.

[7] The theory of composition algebras contains Hurwitz's result as a special case. We refer to [Jacobson 1958] and [Springer, Veldkamp 2000].

quadratic factor. Gauss's treatment of more specific situations, however, had a more visible impact on the theory of numbers. In particular, for the case where the three determinants coincide, Gauss made an observation that played a key role in subsequent developments. In general, two quadratic forms with the same determinant permit two essentially different types of composites. This is related to the choice of the roots $n = \sqrt{d/D}$ and $n' = \sqrt{d'/D}$ respectively in a coherent way. (Notation as in section 1.) Gauss already took up this point in art. 235 of the *Disquisitiones Arithmeticae* in the discussion of the third conclusion where he distinguished the types of substitutions (Σ) by the very choices of n, n' as positive or negative. This issue is particulary important for the case where the greatest common divisor, k, of the determinants of (Σ) equals 1.

This crucial obervation led Gauss to introduce the notion of proper equivalence for binary quadratic forms. Recall that two integral forms f and g (in the variables x, y and x', y' respectively) are equivalent if one can be transformed into the other by a substitution of the form

$$x' = px + qy, \qquad y' = rx + sy$$

where p, q, r, s are integers with $ps - rq = 1$ or $= -1$. The concept of proper equivalence requires a substitution with $ps - rq = 1$. Gauss could prove that the proper equivalence class of F is uniquely determined by the proper equivalence classes of f and f', both primitive integral forms of the same determinant.[8]

Gauss's results, in contemporary terms, provide a parametrization of pairs of arithmetic rings N which are (oriented) free $\mathbf{Z}$–modules of rank two and classes of invertible fractional ideals in N by means of the set $V_{\mathbf{Z}}$ of integral binary quadratic forms modulo proper equivalence. This latter notion of equivalence comes via the action of the special linear group $SL_2(\mathbf{Z})$ of (2×2)-matrices with determinant 1 on the set $V_{\mathbf{Z}}$. This characterization has turned out to be quite useful in dealing with class groups of arithmetic rings in a more algorithmic context. Classical examples include results concerning the density of discriminants for quadratic algebraic number fields.

Manjul Bhargava takes up precisely this arithmetic aspect in his recent work, [Bhargava 2004]. He situates the parametrization above within the theory of prehomogenous vector spaces. This approach, combined with the classification of prehomogenous vector spaces, leads to a number of generalizations of Gauss's theory of composition of forms.

Again, roughly speaking, an orbit space of the form $V_{\mathbf{Z}}/G_{\mathbf{Z}}$ (with $G_{\mathbf{Z}}$ the integral points of a reductive algebraic $\mathbf{Q}$-group acting on a vector space V) parametrizes

[8] It is exactly this result of Gauss which forms the core of Dedekind's reinterpretation of the Gaussian theory. Dedekind, however, was not interested in this theory in its full generality [Editors'note: see H. Edwards's chap. II.2 above]. Then there is a correspondence between proper equivalence classes of binary integral quadratic forms as above and narrow classes of invertible fractional ideals in orders of a quadratic number field, and composition of forms (up to proper equivalence) is interpreted as multiplication of ideals. For a fixed determinant the set of proper equivalence classes is endowed with the structure of a finite abelian group. This is a consequence of Gauss's general theory of composition of forms.

pairs $(N, *)$ where N is an isomorphism class of arithmetic orders of small rank and $*$ stands for a supplementary structure, usually an N-module. It is possible to define a "law of composition" on an appropriate subset of $V_{\mathbf{Z}}/G_{\mathbf{Z}}$. In turn, one can interpret this composition in terms of the class group attached to the algebraic object N involved.

Despite the unifying idea that underlies his new approach, Bhargava depends on very explicit computations and constructions to deal with the specific cases at hand. These constructions echo the spirit of the original work of Gauss in 235ff. in the *Disquisitiones Arithmeticae*. Bhargava, however, obtains new results on the densities of quartic and quintic algebraic number fields, [Bhargava 2005].[9]

3. Composition of Binary Quadratic Forms: An Algebraic Approach

What can be said about composition of forms if you allow the coefficients to come from an arbitrary ring rather than just the integers? Quite a number of authors have considered an extension of the Gaussian theory of composition of integral binary quadratic forms to a more general class of commutative rings with unity.[10] These broader investigations replace the studies of a binary quadratic form $ax^2+bxy+cy^2$, a, b, c in $\mathbf{Z}$, with a so-called binary quadratic R-module (see below)[11] . These new investigations had to contend with the existence of units in R other than ± 1 as in the case of quadratic forms over the ring $\mathbf{Z}$. If one changes the basis of the corresponding quadratic module, the determinant of a quadratic form is multiplied by the square of a unit. In the integral theory, the emergence of the concept of proper equivalence of quadratic forms is closely related to this fact. Coherent choices of specific square roots of the determinants of forms involved in a composition arose as a crucial issue to be resolved.

In a most elegant way, the theory of composition of binary quadratic R-modules as developed by Kneser overcomes these difficulties, see [Kneser 1982]. In his approach, he makes the decisive observation that the underlying binary quadratic R-module (M, q) comes equipped with an additional structure. Namely, he naturally considers (M, q) as a module under an R-algebra C isomorphic to the even Clifford algebra $C^+(M, q)$ of (M, q). This C-module structure replaces the classical "orientation" (that is, the choice of signs) of (M, q). Morphisms (between quadratic R-modules) that preserve this C-module structure serve then as substitutes for the aforementioned proper equivalences. Finally, the isomorphism classes of primitive quadratic R-modules of type C for a fixed R-algebra C make up an abelian group under composition.

Let R be a commutative ring with identity element 1. A projective R-module (M, q) of rank two endowed with a quadratic form $q : M \to R$ (i. e., we have

[9] Karim Belabas gives an elaborate account of the work of Bhargava and related results of others in [Belabas 2005].

[10] Among these are [Dulin, Butts 1972], [Kaplansky 1968], and [Towber 1980]. In particular, Towber provides a carefully written, far-reaching text, enriched with historical remarks.

[11] This essentially geometric concept goes back to Ernst Witt, [Witt 1937]. It is, by now, the method of choice in the study of quadratic forms over rings.

$q(\lambda x) = \lambda^2 q(x)$ for all $\lambda \in R, x \in M$) and associated R-bilinear form $b : M \times M \to R$, $b(x, y) := q(x + y) - q(x) - q(y)$ is called a binary quadratic module. Suppose that (M, q) is non-degenerate, that is, its radical rad $M = \{x \in M \mid b(x, M) = 0\}$ is (0). A module (M, q) is said to be primitive if the R-ideal $Rq(M)$ generated by $q(M)$ coincides with R. A morphism $f : (M, q) \to (M', q')$ between two binary quadratic modules is, by definition, a R-linear map $f : M \to M'$ such that $q = q' \circ f$. The graded Clifford algebra attached to a module (M, q) is denoted by $C(M, q)$.[12] It is given as the quotient of the tensor algebra $T_R(M)$ by the ideal generated by all elements $x \otimes x - q(x)1$, $x \in M$. We denote by $C^+(M, q)$ (resp. $C^-(M, q)$) the subalgebra of $C(M, q)$ generated by tensors of even (resp. odd) degree. Since M is a projective R-module, the canonical homomorphism $M \to C(M, q)$ is injective, and we can identify M with its image in $C(M, q)$.

In fact, in the case of binary quadratic modules, $C^-(M, q)$ coincides with M, and $C^+(M, q)$ has the structure of a quadratic R-algebra, that is, an R-algebra with identity which is projective of rank two as an R-module and such that $R.1$ is a direct factor as an R-module. Such a quadratic R-algebra C is commutative and has a unique automorphism: $C \to C$, $y \mapsto \overline{y}$ such that its trace $tr(y) := y + \overline{y}$ and norm $n(y) := y\overline{y}$ take values in R. It is crucial that multiplication in $C(M, q)$ endows M with a structure of a left $C^+(M, q)$-module. For the case where $C = C^+(M, q)$, this unique morphism $^-$ is the restriction to $C^+(M, q)$ of the standard antiautomorphism of $C(M, q)$ that induces the identity on M. Thus, we have

$$q(cx) = n(c)q(x) \quad \text{for all} \quad c \in C^+(M, q),\ x \in M = C^-(M, q). \tag{1}$$

If one twists this natural $C^+(M, q)$-module structure on M by the automorphism $^-$ on $C^+(M, q)$, one obtains a new $C^+(M, q)$-module structure on M. Thus we have to distinguish two structures, the $C^+(M, q)$-module M and the twisted $C^+(M, q)$-module M.

[12] A Clifford algebra of a quadratic R-module (M, q) is essentially a non-commutative R-algebra $C(M)$ that contains M and the quadratic form q is determined by the equation $x^2 = q(x) \cdot 1_C$, $x \in M$. For instance, let (M, q) be a quadratic module over a field K of characteristic $\neq 2$, and let $e_1, e_2, \ldots, e_n$ be an orthogonal basis of M with $q(e_i) = a_i$, $i = 1, \ldots, n$, where the a_i are non-trivial elements of K. Then the Clifford algebra is generated by $e_1, \ldots, e_n$ and 1, subject to the relations $e_i^2 = a_i$, for $i = 1, \ldots, n$ and $e_ie_j + e_je_i = 0$ for $i \neq j$. In particular, if $n = 2$, that is, (M, q) is a non-degenerate quadratic module of rank two, then $C(M)$ has the basis $1, e_1, e_2, e_1e_2$ as a K-vector space, subject to the relations $e_1^2 = a_1, e_2^2 = a_2$ and $e_1e_2 = -e_2e_1$. This is a so-called generalized quaternion algebra. These algebras are in important cases the building blocks of all Clifford algebras. Note that for $K = \mathbf{R}$, the field of real numbers, and $a_1 = a_2 = -1$, one obtains the Hamilton quaternion algebra. For a given module (M, q), a Clifford algebra always exists. This algebra is uniquely determined up to isomorphism. We refer to [Kneser 2002] or [Hahn, O'Meara 1989], chap. 7, for the construction of $C(M)$ and its basic properties. The Clifford algebras are now indispensable tools in the study of quadratic forms. They prove decisive in questions of classifications of quadratic forms as well as in the construction of the two-fold covering group of the orthogonal group attached to (M, q).

Given quadratic R-modules (M_1, q_1), (M_2, q_2), and (M, q), a composition map is, by definition, a bilinear map

$$\mu : M_1 \times M_2 \to M, \qquad (x_1, x_2) \mapsto \mu(x_1, x_2) \tag{2}$$

such that $q(\mu(x_1, x_2)) = q_1(x_1)q_2(x_2)$ for all $x_1 \in M_1$, $x_2 \in M$.

The following result of Kneser establishes a close relationship between composition maps and homomorphisms of Clifford algebras. Suppose that the modules (M_1, q_1), (M_2, q), and (M, q) are primitive, then, given a composition map $\mu : M_1 \times M_2 \to M$, there are uniquely determined algebra morphisms $\gamma_i : C^+(M_i, q_i) \to C^+(M, q)$, $i = 1, 2$, such that

$$\mu(c_1x_1, c_2x_2) = \gamma_1(c_1)\gamma_2(c_2)\mu(x_1, x_2) \tag{3}$$

for all $c_i \in C^+(M_i, q_i)$, $x_i \in M_i$, $i = 1, 2$. The existence of these morphisms γ_i is connected with Gauss's first and second conclusion in art. 235 where Gauss considered the most general problem of the transformation of a form F into a product of two forms f and f'.

In the general case of a ring R with 1, the construction of a composition of quadratic R-modules is a difficult matter. The principal ideal domain $\mathbf{Z}$ of integers is replaced by a ring with a more complicated structure. In particular, the group R^* of units in R is generally larger then $\mathbf{Z}^* = \{\pm 1\}$. Recall that squares of units played an important role in comparing determinants under a change of basis in the $\mathbf{Z}$-module underlying a form f. The subtle point to choose signs in a coherent manner strongly influenced the concept of proper equivalence of forms in the work of Gauss.

The notion of a quadratic R-module (M, q) of type C, as introduced by Kneser, [Kneser 1982], takes care of these issues in the general case. It is suggested by the natural $C^+(M, q)$-module structure on M discussed above. A quadratic R-module (M, q) is said to be of type C if C is a quadratic R-algebra, M a projective C-module of rank one, and if the identity $q(cx) = n(c)q(x)$ is satisfied for all $c \in C$, $x \in M$. It turns out that, if (M, q) is primitive, the C-structure given by $C^+(M, q)$ on M is essentially unique.

More generally, if (M, q) is a quadratic R-module of type C so that the annihilator of $q(M)$ in R (i. e., $\{s \in R \mid sq(M) = 0\}$) vanishes, then there is a unique homomorphism of quadratic R-algebras

$$\beta : C^+(M, q) \to C \tag{4}$$

with $\beta(c)x = cx$ for all $c \in C^+(M, q)$, $x \in M$. The morphism β is an isomorphism if and only if the quadratic module (M, q) is primitive.

Regarding existence and uniqueness of composition of quadratic R–modules is then the following result due to Kneser, [Kneser 1982].

Theorem. Given quadratic R-algebras C_1, C_2, and C, given quadratic R-modules (M_1, q_1) and (M_2, q_2) of type C_1 and C_2 respectively, and given homomorphisms $\gamma_i : C_i \to C$, $(i = 1, 2)$ of quadratic R-algebras, then there are a quadratic R-module (M, q) of type C and a composition map $\mu : M_1 \times M_2 \to M$ so that $\mu(c_1x_1, c_2x_2) = \gamma_1(c_1)\gamma_2(c_2)\mu(x_1, x_2)$ for all $c_i \in C_i$, $x_i \in M_i$, $i = 1, 2$. The quadratic R-module (M, q) is uniquely determined up to isomorphism.

There is an explicit way to construct (M, q). Let (M, q) be a quadratic module of type C, and let $\gamma : C \to C'$ be a homomorphism of quadratic R-algebras. Then $C' \otimes_C M =: M^\gamma$ is an R-module. There exists a unique quadratic form $q' : M^\gamma \to R$ with $q'(c' \otimes x) = n(c')q(x)$ for all $c' \in C'$, $x \in M$. Endowed with this form (M^γ, q') is a quadratic module of type C'. In view of this construction, the modules $M_i^{\gamma_i}$ (under the assumptions in the theorem) are quadratic modules of type C and we can put $M := M_1^{\gamma_1} \otimes_C M_2^{\gamma_2}$. It carries a unique quadratic form $q : M \to R$ which satisfies $q(x_1 \otimes x_2) = q_1'(x_1)q_2'(x_2)$, $x_i \in M_i^{\gamma_i}$, $i = 1, 2$. Then, (M, q) is a quadratic R-module of type C. The composition map μ is then defined by

$$\mu(x_1, x_2) = (1 \otimes x_1) \otimes (1 \otimes x_2).$$

In view of Gauss's initial treatment of composition it might be interesting to reformulate this general result in the case where (M_1, q_1), (M_2, q_2), and (M, q) are quadratic R-modules with the same determinant and there exists a composition $\mu : M_1 \times M_2 \to M$. Under these assumptions there exist a quadratic R-algebra C and C-type structures on M_1, M_2, and M respectively such that $M \cong M_1 \otimes_C M_2$ and the composition map turns into the multiplication of tensors in this case.

Moreover, the isomorphism classes of primitive quadratic R-modules of type C for a fixed quadratic R-algebra C form an abelian group. The laws of commutativity and associativity follow from the corresponding properties of the tensor product. The quadratic module (C, n) endowed with the norm form serves as the identity element. Given an element (M, q) in that group, its inverse, as a quadratic R-module, is isomorphic to M but now endowed with a different C-structure. The previous map $(c, x) \mapsto cx$ is replaced by $(c, x) \mapsto \bar{c}x$, $x \in C$, $x \in M$. The assignment $M \otimes_C M' \to C$, $x \otimes y \mapsto \beta(xy)$, where $\beta : C^+(M, q) \to C$ is the unique isomorphism of (4), defines an isomorphism.

Kneser used his algebraic approach to understand and clarify the difficult work of Heinrich Brandt, [Brandt 1913], [Brandt 1924], regarding the theory of composition of quaternary quadratic forms, see [Kneser *et al.* 1984]. A few years later, Kneser explained his own work, in his own words, to reach a wider audience [Kneser 1987].[13]

4. Conclusion

There are many ways to measure the reception – and success – of a text, or, more precisely, the ideas of a text. We have elaborated here, in part, on Martin Kneser's personal remarks and contributions at Oberwolfach, in June 2001. That Gauss's

[13] W. Waterhouse suggested an extension of Kneser's approach to other specific forms of higher degree, the so-called norm-type forms, see [Waterhouse 1984].

question on the composition of forms could lead to the construction of a complex, yet stunningly elegant, algebraic theory of composition for binary quadratic modules over an arbitrary commutative ring with unity certainly testifies – again – to the breadth and depth of Gauss's original ideas. Hurwitz's private thoughts on Gauss's composition of forms at the close of the nineteenth century, Bhargava's more contemporary results on the arithmetic of number fields and Kneser's extension of the theory via Clifford algebras provide further evidence of the lasting impact of the *Disquisitiones Arithmeticae*.

References

BELABAS, Karim. 2005. Paramétrisation de structures algébriques et densité de discriminants (d'après Bhargava). In *Séminaire Bourbaki. Vol. 2003–2004*, exposé 935, pp. 267–299. Astérisque 299. Paris: Société mathématique de France.

BHARGAVA, Manjul. 2004. Higher composition laws. I. A new view on Gauss composition, and quadratic generalizations. *Annals of Maths* 159, 217–250. II. On cubic analogues of Gauss composition. *Annals of Maths* 159, 865–886. III. The parametrization of quartic rings. *Annals of Maths* 159, 1329–1360.

———. 2005. The density of discriminants of quartic rings and fields. *Annals of Maths* 162, 1031–1062.

BRANDT, Heinrich. 1913. Zur Komposition der quaternären quadratischen Formen. *Journal für die reine und angewandte Mathematik* 143, 106–129.

———. 1924. Der Kompositionsbegriff bei den quaternären quadratischen Formen. *Mathematische Annalen* 91, 300–315.

DICKSON, Leonard E. 1923. *History of the Theory of Numbers,* vol. III. Washington D.C.: Carnegie Institution of Washington.

DULIN, Bill J., BUTTS, Hubert S. 1972. Composition of binary quadratic forms over integral domains. *Acta Arithmetica* 20, 223–251.

GAUSS, Carl Friedrich. 1866. *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. III. Göttingen: Universitäts-Druckerei.

HAHN, Alexander, O'MEARA, O. Timothy. 1989. *The Classical Groups and K-Theory.* Grundlehren der mathematischen Wissenschaften 291. Berlin, Heidelberg: Springer.

HURWITZ, Adolf. 1898. Über die Komposition der quadratischen Formen von beliebig vielen Veränderlichen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen, Mathematisch-Physikalische Klasse*, 309–316. Repr. *Mathematische Werke*, vol. II, pp. 565–571. Basel, Stuttgart: Birkhäuser, 1963.

JACOBSON, Nathan. 1958. Composition algebras and their automorphisms. *Rendiconti del Circolo Matematico di Palermo* 2nd ser. 7, 55–80.

KAPLANSKY, Irving. 1968. Composition of binary quadratic forms. *Studia Mathematica* 31, 523–530.

KNESER, Martin. 1982. Composition of binary quadratic forms. *Journal of Number Theory* 15, 406–413.

———. 1987. Komposition quadratischer Formen. *Wissenschaftliche Beiträge der Martin-Luther-Universität Halle-Wittenberg.* 1987/33 (M48), 161–173.

———. 2002. *Quadratische Formen.* Berlin, Heidelberg, New York: Springer.

Kneser, Martin, Knus, Max-Albert, Ojanguren, Manuel, Parimala, Raman, Sridharan, Raja. 1986. Composition of quaternary quadratic forms. *Compositio Mathematica* 60, 133–150.

Kummer, Ernst Eduard. 1975. *Collected Papers,* ed. A. Weil. 2 vols. Berlin: Springer.

Neumann, Olaf. 1979. Bemerkungen aus heutiger Sicht über Gauß' Beiträge zur Zahlentheorie, Algebra und Funktionentheorie. *NTM-Schriftenreihe* 16:2, 22–39.

———. 1980. Zur Genesis der algebraischen Zahlentheorie. Bemerkungen aus heutiger Sicht über Gauss' Beiträge zu Zahlentheorie, Algebra und Funktionentheorie. 2. und 3. Teil. *NTM-Schriftenreihe* 17:1, 32–48; 17:2, 38–58.

Smith, Henry J. S. 1862. Report on the Theory of Numbers, part IV. *Report of the British Association for the Advancement of Science for 1862*, 503–526. Repr. in *Collected Mathematical Papers*, ed. J. W. L. Glaisher, vol. I, pp. 229–262. Oxford: Clarendon, 1894.

Springer, Tonny Albert, Veldkamp, Ferdinand D. 2000. *Octonions, Jordan Algebras and Exceptional Groups.* Berlin, Heidelberg, New York: Springer.

Towber, James. 1980. Composition of oriented binary quadratic form-classes over commutative rings. *Advances in Mathematics* 36, 1–107.

Waterhouse, William C. 1984. Composition of norm–type forms. *Journal für die reine und angewandte Mathematik* 353, 85–97.

Weil, André. 1984. *Number Theory. An Approach through History from Hammurapi to Legendre*. Boston, Bastel, Stuttgart: Birkhäuser.

———. 1986. Gauss et la composition des formes quadratiques binaires. In *Aspects of Mathematics and its Applications*, ed. J.A. Barroso, pp. 895–912. North-Holland Mathematical Library 34. Amsterdam: North-Holland, Elsevier.

Witt, Ernst. 1937. Theorie der quadratischen Formen in beliebigen Körpern. *Journal für die reine und angewandte Mathematik* 176, 31–44.

II.4

The Unpublished Section Eight: On the Way to Function Fields over a Finite Field

GÜNTHER FREI

To my dear friend and inspiring teacher, Peter HILTON,
on the occasion of his eightieth birthday.

The starting point for these investigations of the little known and only posthumously published Section Eight of Gauss's *Disquisitiones Arithmeticae* was a study of how Emil Artin was led to his reciprocity law in abelian extensions of algebraic number fields. I naturally began with Artin's thesis on the theory of quadratic extensions of function fields over a finite field of constants. There, Artin refers to Richard Dedekind's paper [Dedekind 1857a]. The first sentence of this paper states that the subject, that is, the theory of higher congruences modulo a prime number, was initiated by Gauss.[1] An examination of Gauss's *Disquisitiones Arithmeticae* showed that the subject is not treated there, but that Gauss refers to a Section Eight which, however, is missing from the published book. An early fragmentary version of this Section Eight, written in Latin apparently in 1797, was found after Gauss's death (1855) in his papers under the title *Disquisitiones generales de congruentiis*.[2] It was published by Dedekind in 1863 in the second volume of Gauss's *Werke*. A second printing of this volume appeared in 1876.

In our first section, we shall discuss the relation of the *Disquisitiones generales*

[1] See [Dedekind 1857a], p. 1: *von Gauß zuerst angeregt.*

[2] We shall usually refer to the *Disquisitiones generales de congruentiis* by the article, which we label §, following Dedekind and distinguishing in this way from the articles of the *Disquisitiones Arithmeticae* which are referred to as “art.” The corresponding page is then easy to find, either in the Latin original [Gauss 1863b], pp. 212–240, or in the German translation [Maser 1889], pp. 602–629.

de congruentiis to the *Disquisitiones Arithmeticae*. In section 2 we try to put the *Disquisitiones generales de congruentiis* into historical perspective, in section 3 we shall present the content of the *Disquisitiones generales de congruentiis*, using modern mathematical terminology and concepts.[3] In section 4 we shall comment on a few entries in Gauss's mathematical diary related to the *Disquisitiones generales de congruentiis*, and in the conclusion we shall sketch how Gauss's investigations on higher congruences gradually evolved.

1. The D.A. and the *Disquisitiones Generales de Congruentiis*

1.1. The Disquisitiones Arithmeticae

It has been said that the final Section Seven of the *Disquisitiones Arithmeticae* – the book will often be abbreviated as "D.A." in the sequel – is alien to the other sections since it is not arithmetic in character but rather algebraic or even analytic. But we shall see that this is not so. Gauss seems to defend himself against this impression, in the opening paragraph of art. 335, by insisting that the development of the theory will demonstrate its arithmetic character:

> The readers might be surprised to find such an investigation [on the division of the circle], notably in the present work which deals with a subject apparently so unrelated; but the treatment itself will make it abundantly clear that there is an intimate connection between this subject and higher arithmetic.[4]

As a matter of fact, the theory of the division of the circle developed by Gauss in Section Seven, which algebraically can be reduced to the solution of the equation $f(x) = x^n - 1 = 0$, had been initiated by Gauss's number theoretic investigations into the congruence $x^n - 1 \equiv 0 \bmod p$, in particular $x^{p-1} - 1 \equiv 0 \bmod p$, where p is an odd prime number.[5] Gauss's fundamental discovery was that the set of solutions of the congruence $x^{p-1} - 1 \equiv 0 \bmod p$, and the set of permutations that send a fixed primitive root of the equation

$$F(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + \cdots + x + 1 = 0$$

to another – i.e. in today's terminology, the Galois group of $F(x)$ – both form what we call today a cyclic group of order $p - 1$.[6] Gauss used this fact in Section Seven to

[3] A more detailed discussion of the mathematical content of the *Disquisitiones generales de congruentiis* is given in [Frei 2001].

[4] D.A., art. 335: *Mirari possent lectores, talem disquisitionem in hocce potissimum opere, disciplinae primo aspectu maxime heterogeneae imprimis dicato, institui; sed tractatio ipsa abunde declarabit, quam intimo nexu hoc argumentum cum arithmetica sublimiori coniunctum sit.*

[5] See our section 4 below for the corresponding entry in Gauss's diary.

[6] See also [Bachmann 1911], pp. 33–34: *Wie Gauss zu seiner Theorie [der Kreisteilung] geführt sein mag? Kaum wohl von Seiten der Geometrie ..., wahrscheinlicher durch algebraische Studien. ... Bedenkt man aber, dass in Kap[itel] 6 der* A[nalysis] R[esiduorum] *die Theorie der* Gleichung $x^p = 1$ *erst derjenigen der* Kongruenz $x^p \equiv 1$ *nachfolgt und*

present the $p-1$ roots of $F(x)$ in a purely abstract algebro-arithmetic way, without using complex numbers in the form introduced by Euler – see D.A., art. 343.

The cyclic structure of the roots of $F(x)$ and the possibility of grouping them into what Gauss called "periods" in a way to allow the solution of the equation $F(x) = 0$ became clear to Gauss on March 29, 1796, i.e., one day before he discovered the construction of the 17-gon with straightedge and compass, which made him start his mathematical diary – see [Gauss 1796–1814], entry 1. This can be deduced from a letter of Gauss, written on January 6, 1819, to his former student Christian Ludwig Gerling, where Gauss describes what happened March 29, 1796:

> Already earlier I had found everything related to the separation of the roots of the equation $\frac{x^p-1}{x-1} = 0$ into *two* groups on which the beautiful theorem in the D. A. on p. 637 depends, in the winter of 1796 (during my first semester in Göttingen), without having recorded the day. By thinking with great effort about the relation of all the roots to each other with respect to their arithmetic properties, I succeeded, while I was on a vacation in Braunschweig, on that day (before I got out of bed) in seeing this relation with utmost clarity, so that I was able to make on the spot the special application to the 17-gon and to verify it numerically.[7]

The "beautiful theorem in the D. A. on p. 637" refers to art. 357 of the D.A., where Gauss uses the two (Gaussian) periods ω_1 and ω_2 of length $\frac{p-1}{2}$ of the roots of the cyclotomic polynomial $F(x) = \frac{x^p-1}{x-1}$ (p an odd prime number) to split $F(x)$ into two factors with integral rational coefficients in ω_1 and ω_2. He obtains the decomposition $4F(x) = G(x)^2 - p^*H(x)^2$, $G(x)$ and $H(x)$ being polynomials with integral rational coefficients and $p^* = +p$ if $p = 4t+1$, $p^* = -p$ if $p = 4t-1$. Furthermore, Gauss shows that ω_1 and ω_2 are the two roots of the polynomial $x^2 + x + \frac{1}{4}(1-p^*)$ – see D.A., art. 356 –, and that on this fact a third and

dass die Methode zur Auflösung dieser Kongruenz das genaue Vorbild für die Auflösung der Kreisteilungsgleichung ist, so darf man wohl auf den rein arithmetischen *Ursprung von Gauss' Beschäftigung mit der letzteren schliessen. ... Die Wurzeln ... der Gleichung* $X = \frac{x^p-1}{x-1} = 0$, *die, wenn wir* $r = \cos\frac{2\pi}{p} + \sqrt{-1}\sin\frac{2\pi}{p}$ *setzen, durch die Potenzen* $r, r^2, \dots, r^{p-1}$ *dargestellt sind, zeigen, wenn p als eine ungerade Primzahl vorausgesetzt wird, auf Grund des arithmetischen Satzes, dass die Potenzen* $1, g, g^2, \dots, g^{p-2}$ *einer primitiven Wurzel g (mod. p) den Resten* $1, 2, 3, \dots, p-1$, *von der Ordnung abgesehen, kongruent sind, das eigentümliche Verhalten, dass bei der zyklischen Anordnung* $r, r^g, r^{g^2}, \dots, r^{g^{p-2}}$ *jede die gleiche rationale Funktion (nämlich die* g^te^ *Potenz) der vorhergehenden ist.* Mit dieser Einsicht war der schöpferische Gedanke gewonnen, aus welchem die ganze Gausssche Theorie der Kreisteilungsgleichung entsprang.

[7] [Gauss 1917], p. 125: *Schon früher war alles was auf die Zertheilung der Wurzeln der Gleichung* $\frac{x^p-1}{x-1} = 0$ *in* zwei *Gruppen sich bezieht, von mir gefunden, wovon der schöne Lehrsatz D.A. p. 637 unten abhängt u[nd] zwar im Winter 1796 (meinem ersten Semester in Göttingen), ohne dass ich den Tag aufgezeichnet hätte. Durch angestrengtes Nachdenken über den Zusammenhang aller Wurzeln unter einander nach arithmetischen Gründen, glückte es mir bei einem Ferienaufenthalt in Braunschweig, am Morgen des gedachten Tages (ehe ich aus dem Bette aufgestanden war) diesen Zusammenhang auf das klarste anzuschauen, so dass ich die specielle Anwendung auf das 17-Eck und die numerische Bestätigung auf der Stelle machen konnte.*

completely new proof of the quadratic reciprocity law can be based. It is remarkable that Gauss already announced this theorem on the decomposition of $F(x)$ in art. 124 of the D.A. where he analysed the quadratic character of 7 and -7 mod p.

All this gives us a better understanding of Gauss's announcement in the foreword of the *Disquisitiones Arithmeticae*:

> The theory of the division of a circle or of a regular polygon treated in sec. 7 *of itself* does not pertain to Arithmetic but the *principles* involved depend uniquely on Higher Arithmetic. This will perhaps prove unexpected to geometers, but I hope they will be equally pleased with the new results that derive from this treatment.[8]

In the next section, we shall see that Section Seven is not only based on arithmetic, namely on the solutions of the congruence $x^{p-1} - 1 \equiv 0 \bmod p$, and the consequent representation of the Gaussian periods, but that it was also meant to serve as preparation for the sequel: a eighth section or a second part of the *Disquisitiones Arithmeticae* on the theory of polynomials mod p (as well as for another treatise on elliptic functions):

> Moreover, the principles of the theory which we are about to explain reach much farther than they will be extended here. For they can be applied not only to circular functions but just as well to many other transcendental functions, e.g. to those which depend on the integral $\int \frac{dx}{\sqrt{(1-x^4)}}$ and also to various types of congruences. Since, however, we are preparing a substantial special work on these transcendental functions and since on the other hand we shall treat congruences at length in the continuation of the D.A., it appears to be justified to consider only circular functions here. And although we could discuss them in all their generality, we reduce the methods to the simplest case in the following article, both for the sake of brevity and in order that the new principles of this theory may be more easily understood.[9]

This fact is of crucial importance in order to fully understand and appreciate the *Disquisitiones Arithmeticae* as a whole.

[8] D.A., *praefatio*: *Theoria divisionis circuli, sive polygonorum regularium, quae in Sect. VII tractatur,* ipsa *quidem* per se *ad Arithmeticam non pertinet, attamen eius* principia *unice ex Arithmetica Sublimiori petenda sunt: quod forsan geometris tam inexpectatum erit, quantum veritates novas, quas ex hoc fonte haurire licuit, ipsis gratas fore spero.*

[9] D.A., art. 335: *Ceterum principia theoriae, quam exponere aggredimur, multio latius patent, quam hic extenduntur. Namque non solum ad functiones circulares, sed pari successu ad multas alias functiones transscendentes applicari possunt, e.g. ad eas, quae ab integrali* $\int \frac{dx}{\sqrt{(1-x^4)}}$ *pendent, praetereaque etiam ad varia congruentiarum genera: sed quoniam de illis functionibus transscendentibus amplum opus peculiare paramus, de congruentiis autem in continuatione disquisitionum arithmeticarum copiose tractabitur, hoc loco solas functiones ciculares considerare visum est. Imo has quoque, quas summa generalitate amplecti liceret, per subsidia in art. sq. exponenda ad casum simplicissimum reducemus, tum brevitati consulentes, tum ut principia plane nova huius theoriae eo facilius intellegitur.*

1.2. The Disquisitiones Generales de Congruentiis

This second volume of Gauss's treatise was to contain in particular a detailed treatment of the "Theory of higher congruences with respect to a prime number" or "Theory of double congruences," paving the way to a theory of function fields over a finite field of constants. The first hint of Gauss's plans can be found in the preface of the *Disquisitiones Arithmeticae*:

> Finally, since the book came out much larger than I expected, owing to the size of sec. 5, I shortened much of what I first intended to do and, especially, I omitted the whole of Section *Eight* (even though I refer to it at times in the present volume; it was to contain a general treatment of algebraic congruences of arbitrary degree). All this, which will easily fill another volume of equal size as the present one, will be published at the first opportunity.[10]

And in a letter to János Bolyai dated November 29, 1798, we read regarding the sections of the *Disquisitiones Arithmeticae* as they were being written at the time:

> The sixth [section] is not big; the seventh (which contains the theory of polygons) is somewhat larger but essentially already finished, and only the last will still keep me occupied for a considerable time, since it contains the most difficult matters.[11]

This unpublished draft of the planned Section Eight of *Disquisitiones Arithmeticae* entitled *Disquisitiones generales de congruentiis* (General Treatise on Congruences) was found in Gauss's papers as Chapter Eight of a manuscript bearing the title *Analysis residuorum* (Theory of Residues) and containing three chapters, labelled Chapter Six through Eight. Two portions of this manuscript were edited by Dedekind in 1863, the second one being the *Disquisitiones generales de congruentiis. Analysis residuorum: Caput Octavum* (General Investigations on Congruences. Theory of Residues: Chapter Eight).[12] It is divided up into articles running from § 330 up to § 375, in a way similar to those in the *Disquisitiones Arithmeticae* which already indicates that it belonged to an earlier version of a part of this book.[13] This is con-

[10] D.A., *praefatio*: *Denique quum liber praesertim propter amplitudinem Sect. V in longe maius quam exspectaveram volumen excresceret, plura quae ab initio ei destinata erant, interque ea totam Sectionem* octavam *(quae passim iam in hoc volumine commemoratur, atque tractationem generalem de congruentiis algebraicis cuiusvis gradus continet) resecare oportuit. Haec omnia, quae volumen huic aequale facile explebunt, publici iuris fient, quamprimum occasio aderit.*

[11] See [Gauss & Bolyai 1899], pp. 11-12: *Der sechste [Abschnitt] ist von keinem grossen Umfange; der* 7$^{\text{te}}$ *(der die Theorie der Polygone enthält) etwas grösser aber im Wesentlichen schon fertig, u[nd] nur der letzte wird mich noch eine beträchtliche Zeit beschäftigen da er die schwersten Materien enthält.*

[12] See [Gauss 1863b/1876], pp. 212–240; cf. [Maser 1889], pp. 602-629. On the other portion, see our section 4 below.

[13] Hints at earlier stages of the *Disquisitiones Arithmeticae* have been recorded and commented by Dedekind (in [Gauss 1863b/1876], p. 240f, where he also mentions evidence of the way that Gauss's plans for the second volume changed over time) and Bachmann, see [Bachmann 1911]. The paper [Merzbach 1981] gives a global comparison of the early and the published version of the *Disquisitiones Arithmeticae*.

firmed by a mathematical analysis of the contents of the *Disquisitiones Arithmeticae* and of the *Disquisitiones generales de congruentiis*, as well as by Gauss's diary and by scattered remarks made by Gauss in both works.[14]

Gauss's theory of polynomials mod p in the *Caput Octavum* was planned to run parallel to the theory of rational integers as treated in the seven sections of the D.A. In particular, it was also to contain a theory of cyclotomy (division of the circle) modulo p. For these reasons, many proofs in the *Disquisitiones Arithmeticae* are formulated in such a way that they are not only valid for the domain of rational integers but also for the domain of polynomials over the integers or rationals or over a "finite field" with p elements, and even, as we would say today, for integral domains. This is one reason why the *Disquisitiones Arithmeticae* appeared so advanced and abstract for many readers – see also below in our section 3.1 what concerns § 330.

What Gauss noticed was that what he called the two periods of length $\frac{p-1}{2}$, belonging to the *cyclotomic congruence* $x^p - 1 \equiv 0 \bmod q$, where p and q are two distinct odd prime numbers, furnish a *third proof* and a *fourth proof* of the quadratic reciprocity law. It was this discovery of the third proof of the quadratic reciprocity law, made on or before September 2, 1796, which stimulated Gauss to go deeper into the theory of polynomials over a finite field. The connection of the quadratic reciprocity law with his theory of polynomials mod p, however, had been discovered by Gauss three weeks earlier, on the August 13, 1796.[15] The third and the fourth proofs are presented in the §§ 360–366 of the *Disquisitiones generales de congruentiis* – see our section 3.5 below. On the other hand, the two periods also give, as Gaussian sums of the cyclotomic equation $x^p - 1 = 0$, yet another determination of the quadratic character $\left(\frac{-1}{p}\right)$ of -1, i.e., another proof of what one calls the first complementary law of quadratic reciprocity. Gauss included this proof in D.A., art. 356. The other proofs were given in arts. 108, 109 and 262. It is remarkable that it was exactly this solution of the congruence $x^2 + 1 \equiv 0 \bmod p$, which led Gauss, according to his own testimony, to his investigations on number theory in the beginning of the year 1795 – see D.A., preface. From the letter to Gerling of January 6, 1819 cited in our section 1.1 above, we learn that Gauss had already discovered the structure and importance of the two periods of length $\frac{p-1}{2}$ belonging to the cyclotomic equation $x^p - 1 = 0$ on or before March 29, 1796.[16]

Thus from the beginning, Gauss's study of the theory of polynomials mod p was the driving force for his investigations and discoveries in number theory.

[14] In the preface, but also, among others, in arts. 11, 44, 61, 62, 65, 84 of the D.A. and by remarks in § 338 and § 366 of the *Disquisitiones generales de congruentiis*. Cf. [Frei 2001].

[15] See [Gauss 1796–1814], entries 23 and 30.

[16] Later, in 1811, Gauss found another proof of the quadratic reciprocity law based on Gaussian sums ([Gauss 1863b/1876], pp. 9–45, in particular § 33; or [Maser 1889], pp. 463–495, in particular p. 493) and in 1817–1818 still another one, closely related to the theory of polynomials mod p ([Gauss 1863b/1876], pp. 47–64, in particular pp. 55–59; or [Maser 1889], pp. 496–510, in particular pp. 501–505). See also [Frei 1994], pp. 79–81.

In the same way that Gauss's discovery of the third proof of the quadratic reciprocity law gave rise to a detailed theory of functions mod p, Gauss's discovery of his second proof of the quadratic reciprocity law by means of his theory of the genus of quadratic forms, made on June 27, 1796,[17] was the stimulus for Gauss to develop a detailed theory of quadratic forms in Section Five of the *Disquisitiones Arithmeticae*. From the letter to Bolyai cited above we know that Gauss had rewritten this Section Five four times, each time improving on the former version in a way which "exceeded his boldest hopes."[18] Let us recall that Gauss already discovered the quadratic reciprocity law, called by him *"theorema fundamentale"* in March 1795.[19] The first proof for it was found by Gauss a year later on April 8, 1796,[20] it is the one he presented in art. 131–144 of the *Disquisitiones Arithmeticae*. That Gauss considered the quadratic reciprocity law as being the central theorem of number theory is also underlined by the fact that he turned back to the theorem again and again, finally leaving eight different proofs, most of them completely different from one another.[21]

We shall now discuss the origin and influence of the *Disquisitiones generales de congruentiis*, before describing their mathematical content in section 3 below.

2. Origin and Influence of the *Disquisitiones Generales de Congruentiis*

2.1. Origin of the Disquisitiones Generales de Congruentiis

The theory of functions, i.e., polynomials, over a prime field of characteristic p must be seen as Gauss's genuine creation. However, Gauss might have been motivated towards such a theory by the theorem of Lagrange asserting that a polynomial of degree n whose leading coefficient is not divisible by the prime number p has at most n roots mod p. Gauss proved this theorem in § 338 of the *Disquisitiones generales de congruentiis* by showing that if a polynomial $f(x)$ with integer coefficients has the integer a as a root mod p, then $f(x)$ is divisible mod p by $x - a$, a theorem which goes back to Descartes in the ordinary case where $f(x)$ is a polynomial and a is a root belonging to the rational, real or complex numbers. Gauss adds in this same § 338, after having given his proof, that "this is the proof of this theorem we had promised." This refers to art. 43 of the D.A., where the same theorem is proved by induction on the degree n, and a different proof is announced for Section Eight.

In his commentaries in the following art. 44 of the D.A., Gauss attributes this theorem to Lagrange. Lagrange had proved the theorem in essentially the same way as Gauss did in art. 43 of the D.A., i.e., by induction.[22] The theorem in art. 43 of the D.A. is one of several results appearing in arts. 38–44 of the D.A. under the heading "various theorems" (*Theoremata varia*). Lagrange's theorem is the last theorem proved in Section Two. This and Gauss's commentaries in art. 44 suggest that Gauss

[17] See [Bachmann 1911], p. 25.

[18] See [Gauss & Bolyai 1899], p. 11.

[19] See [Bachmann 1911], p. 5; and [Gauss 1863a], p. 475, Zu Art. 131.

[20] See [Gauss 1796–1814], entry 2; cf. [Gauss 1863a], p. 475, Zu Art. 130 and Zu Art. 131. See also [Bachmann 1911], pp. 15–16.

[21] See [Frei 1994].

[22] See [Lagrange 1770], p. 667, art. 10, Cor. V.

considered it a key theorem for the theory of polynomials mod p, a theory he would eventually develop later. In fact, he also mentions Euler who proved the theorem in the particular case where the polynomial is $f(x) = x^n - 1$, in a paper presented to the St. Petersburg Academy on May 18, 1772. Euler was then already blind and was not aware of the more general result by Lagrange published two years earlier.[23] That Gauss considered it a key theorem is underlined by the fact that Gauss gives some extensive historical commentary on this theorem. This compares with that given on the quadratic reciprocity law in art. 151 of the *Disquisitiones Arithmeticae*, the law he considered to be the most fundamental theorem of arithmetic.

That Lagrange's theorem might have been a motivation for Gauss's theory of functions mod p is also indicated by what Gauss says in § 338 of the *Disquisitiones generales de congruentiis*, following his second proof of Lagrange's theorem:

> But at the same time one sees from this that the solution of congruences constitutes only a part of a much higher [more advanced] investigation, namely the investigation of the decomposition of functions [i.e., polynomials] into factors.[24]

And art. 44 of the D.A. seems to hint in the same direction when Gauss says that this theorem of Lagrange is considered here only as a lemma, and that this is not the occasion for a detailed elaboration. This could mean that Gauss was planning a more detailed treatment for Part Two of the *Disquisitiones Arithmeticae*.

Under the same heading *Theoremata varia* in art. 42 of the D.A., immediately before the theorem of Lagrange, Gauss proved another isolated important theorem on polynomials which later was to play a fundamental rôle for Kronecker's theory of divisors: If a monic polynomial $f(x)$ with integral coefficients is decomposable into two monic polynomials $g(x)$ and $h(x)$ with rational coefficients, then the coefficients of $g(x)$ and $h(x)$ must necessarily be integers. So we might guess that an elaboration on this theorem was also to be part of a detailed theory of polynomials reserved for the planned Part Two of the *Disquisitiones Arithmeticae*.

2.2. *Influence of the Disquisitiones Generales de Congruentiis*

2.2.1. *Dedekind*

The *Disquisitiones generales de congruentiis* did not exert any immediate influence; as mentioned earlier, it was published by Dedekind only in 1863. By then, works on the same subject by Evariste Galois (1830), Theodor Schönemann (1846), Joseph-Alfred Serret (1854) and Dedekind himself (1857) had already appeared. In addition, Gauss's manuscript was in Latin, a language which was beginning to fall out of use as the language for mathematical papers after 1850. It was translated into a modern language (German) only in 1889 by Hermann Maser, see [Maser 1889], pp. 602–629.

[23] See [Euler 1774/1917], art. 28, p. 248. An even more special case had been considered by Euler in 1754 in connection with his proof of Fermat's theorem asserting that every prime number p of the form $4n + 1$ is the sum of two squares, see [Euler 1760].

[24] Our translation from *Disquisitiones generales de congruentiis* § 338, [Gauss 1863b/1876], p. 217 (cf. Fig. II.4A): *Sed simul hinc perspicitur, quomodo congruentiarum solutio partem tantummodo constituat multo altioris disquisitionis, scilicet de resolutione functionum in factores.*

By that time, the main interest in number theory had shifted to the fundamental works of Kummer, Dedekind, and Kronecker on the new theory of algebraic number fields. Later authors, such as Heinrich Kornblum and Emil Artin, only refer to Dedekind's paper [Dedekind 1857a] as a source for the theory of higher congruences modulo a prime number p. Hence Gauss's posthumously published treatise has remained largely unnoticed up to recent times.

In the introduction to [Dedekind 1857a], Dedekind referred to Gauss by saying that Gauss initiated the subject of functions mod p. He also mentioned that Galois, Serret, and Schönemann had taken it up afterwards:

> It is my intention to give a simple and coherent presentation of the subject given in the title, which was first initiated by *Gauss*[25] and later taken up with success by *Galois, Serret, Schönemann*,[26] a presentation which shall be strongly related by the analogy with the elements of number theory. This analogy is, in fact, so sweeping that only a change of words is needed in the proofs of number theory, except for some investigations which are peculiar to our subject. I follow exactly the path taken by *Dirichlet* in his lectures on number theory[27] (or in his short presentation of the theory of complex numbers in volume 24 of this journal).[28] Taking this into account, one will not blame me for stressing mostly only the main points of the proofs, since a more detailed presentation would necessarily be tedious for the expert in number theory, a theory which is assumed here.[29]

Let us indicate several reasons why the reference Dedekind made here to Gauss must refer to the remarks made by Gauss in the *Disquisitiones Arithmeticae*, and cannot have meant the *Disquisitiones generales de congruentiis*.

[25] In his commentary in [Dedekind 1930–1932], vol. 1, p. 40, Ore refers here to [Gauss 1863b], p. 212–240. But it is doubtful, as we shall see presently, that Dedekind already knew Gauss's manuscript *Disquisitiones generales de congruentiis* when he wrote his paper [Dedekind 1857a] in October 1856.

[26] In [Dedekind 1930–1932], vol. 1, p. 40, Ore adds here references to [Galois 1830/1897], pp. 15–23; to [Serret 1854], pp. 343-370; as well as to [Schönemann 1845] and [Schönemann 1846].

[27] Dirichlet's lectures had been given in 1856–1857, and were in turn inspired by the D.A., see [Dirichlet 1863].

[28] The reference is to [Dirichlet 1842].

[29] See [Dedekind 1857a], p. 1: *Es ist meine Absicht, dem in der Überschrift bezeichneten Gegenstand, welcher, von* Gauß *zuerst angeregt, später mit Erfolg von* Galois, Serret, Schönemann *wieder aufgenommen ist, eine einfache zusammenhängende Darstellung zu widmen, welche sich streng an die Analogie mit den Elementen der Zahlentheorie binden soll. Diese ist in der Tat so durchgreifend, daß es mit Ausnahme einiger unserem Gegenstand eigentümlicher Untersuchnungen nur einer Wortänderungen in den Beweisen der Zahlentheorie bedarf. Ich folge genau dem Gange, welchen* Dirichlet *in seinen Vorlesungen über die Zahlentheorie (oder in seiner kurzen Darstellung der Theorie der komplexen Zahlen im 24. Band dieses Journals) eingeschlagen hat. In Rücksicht hierauf wird man es nicht tadeln, daß ich meist nur die Hauptmomente der Beweise hervorhebe, da größere Ausführlichkeit für den Kenner der Zahlentheorie, welche hier vorausgesetzt wird, ermüdend sein müßte.*

Firstly, by October 1856 Dedekind could hardly have seen the unpublished Section Eight *Disquisitiones generales de congruentiis* by Gauss (who had died just 20 months before, on February 23, 1855). In fact, a letter from Dedekind to Jacob Henle, dated February 29, 1860, seems to indicate that Dedekind saw Gauss's manuscript for the first time in the spring of 1860.[30]

Secondly, Dedekind's paper treats the subject in a way so similar to Gauss that Dedekind would hardly have published it, had he known Gauss's manuscript already in 1856, or he would have at least mentioned this manuscript of Gauss, a manuscript Dedekind was going to publish later.

Thirdly, from the content of Dedekind's paper itself it is obvious that Dedekind did not yet know Gauss's Section Eight, since he reproves several theorems that had already been proved by Gauss in his unpublished manuscript. Again Dedekind would at least have mentioned that these theorems had already been stated and proved by Gauss in an unpublished manuscript.

Fourthly, in his paper [Dedekind 1857b], written at the same time, in October 1856, Dedekind refers to Schönemann's paper [Schönemann 1845] for a theorem which corresponds to the theorem stated by Gauss in the §§ 348–350 of the *Disquisitiones generales de congruentiis*. Again, Dedekind would have mentioned that the same theorem is already stated and proved in a manuscript of Gauss, had he known this manuscript.

It therefore seems certain that Dedekind did not know the Gauss manuscript when he wrote his paper [Dedekind 1857a]; but he knew from the *Disquisitiones Arithmeticae* that Gauss had planned a work on this subject (this is also mentioned in also [Schönemann 1845], see 2.2.3. below).

Dedekind had been Gauss's student in Göttingen from 1850 until 1852, where he followed, among other things, Gauss's lectures on the method of least squares. In 1852, he graduated under the direction of Gauss with the doctoral thesis *Über die Theorie der Eulerschen Integrale* (On the Theory of Eulerian Integrals). In 1854, Dedekind submitted his *Habilitation* thesis *Über die Transformationsformeln für rechtwinklige Koordinaten* (On the Transformation Formulae for Rectangular Coordinates), and on June 30, 1854, Dedekind presented his inaugural lecture *Über die Einführung neuer Funktionen in der Mathematik* (On the Introduction of New Functions in Mathematics); both thesis and lecture were examined by Gauss. Having thus aquired the status of *Privatdozent*, Dedekind taught his first lecture course at Göttingen in the Winter term 1854–1855, on "Probability and Geometry." So it is conceivable, albeit not likely, that Dedekind learned directly from Gauss about the latter's investigations on polynomials modulo a prime number p. Alternatively, Dirichlet may have communicated it to Dedekind: after Gauss's death in 1855,

[30] From this letter we learn that Wilhelm Weber, Professor of Physics in Göttingen, had asked Dedekind through Jacob Henle, Professor of Anatomy in Göttingen, to collaborate on the edition of Gauss's *Werke* and that Dedekind should come to Göttingen in order to look over Gauss's manuscripts and perhaps edit part of them for the edition. See [Dedekind 1985], pp. 335–336. I would like to thank Ralph Haubrich for giving me the reference to this letter.

Dirichlet was in charge of Gauss's manuscripts in order to prepare the edition of Gauss's works. Dirichlet died in 1859, and Dedekind left Göttingen in 1858 and went to Zürich.

Be that as it may, the references Gauss made in the *Disquisitiones Arithmeticae* to the unpublished Section Eight *Disquisitiones generales de congruentiis* on higher congruences made it sufficiently clear to Dedekind that Gauss was in the possession of a theory of polynomials mod p running parallel to Gauss's theory of rational numbers and thus must have been an important inspiration for Dedekind's paper. The references given to Gauss by Galois in [Galois 1830/1897], p. 15, and by Schönemann in [Schönemann 1845], p. 270, may also have had some influence on Dedekind. However, Dedekind's own testimony seems to indicate that the direct motivation for his paper actually came from the series of papers by Kummer on ideal numbers in cyclotomic fields which appeared in Crelle's *Journal* (*Journal für die reine und angewandte Mathematik*) in the years 1846 and 1847,[31] and that Dedekind's paper was meant as a preparation for establishing a solid foundation to Kummer's ideal numbers by Dedekind's ideal theory, which Dedekind was to develop 14 years later in the Supplement X of the second edition of Dirichlet's lectures on number theory, [Dirichlet 1863/1871], §§ 159–170. In fact, Dedekind later recalled:

> I developed first the new principles by which I got a rigorous theory of ideals without exceptions seven years ago in the second edition of the *Lectures on Number Theory by Dirichlet* (§§ 159–170) … Stimulated by Kummer's great discoveries I had already studied the same subject earlier during a long series of years, whereby I started from a completely different foundation, namely from the theory of higher congruences.[32]

Dedekind went on to explain that, since Zolotarev in 1874 also had developed a theory of ideal numbers based on the theory of higher congruences,[33] he thought that it would be sufficiently interesting to elaborate on the connection between the two different ways of establishing a solid foundation for Kummer's ideal numbers, namely between Dedekind's theory of ideals and the theory of higher congruences, and Dedekind continued,

> Hereby I have to presume as known my theory of ideals as well as the theory of higher congruences of which I have given a concise presentation some time ago in Borchardt's Journal. [34]

[31] See [Kummer 1975], pp. 193–251.

[32] [Dedekind 1878], p. 1: *Die neuen Prinzipien, durch welche ich zu einer ausnahmelosen und strengen Theorie der Ideale gelangt bin, habe ich zuerst vor sieben Jahren in der zweiten Auflage der Vorlesungen über Zahlentheorie von Dirichlet (§§ 159-170) entwickelt … Mit demselben Gegenstand hatte ich mich schon vorher, durch die große Entdeckung Kummers angeregt, eine lange Reihe von Jahren hindurch beschäftigt, wobei ich von einer ganz anderen Grundlage, nämlich von der Theorie der höheren Kongruenzen ausging.*

[33] This theory is presented in P. Piazza's chap. VII.2 below [Editors' note].

[34] See also [Dedekind 1878], p. 2: *Hierbei muß ich sowohl meine Theorie der Ideale, als auch die Theorie der höheren Kongruenzen, von welcher ich früher in Borchardts Journal (Bd. 54, S. 1) eine gedrängte Darstellung gegeben habe, als bekannt voraussetzen.*The reference is to [Dedekind 1857a].

Indeed, Kummer had introduced and defined an ideal number and the divisibility by an ideal number by means of higher congruences;[35] and the fundamental decomposition theorem on the factorization of a prime number p into prime ideals in the cyclotomic field $\mathbf{Q}(\zeta_q)$ is expressed by the factorization of the cyclotomic polynomial $F(x) = \frac{x^q-1}{x-1}$ mod p.[36] Let us add here that Eduard Selling has also, following Kummer, worked out a definition for Kummer's ideal numbers in an algebraic number field by means of the theory of higher congruences.[37]

Gauss, in his *Disquisitiones generales de congruentiis*, and Dedekind, in his paper [Dedekind 1857a], both first establish the fundamental theorem of arithmetic for polynomials mod p, that is, in today's terminology, for the ring $\mathbf{F}_p[x]$, via the existence of a Euclidean algorithm, thus following the presentation given by Gauss in the *Disquisitiones Arithmeticae* for the rational integers. Like Gauss, Dedekind always works within the domain of polynomials with rational integer coefficients, taken mod p. After proving the fundamental theorem of arithmetic for these polynomials, he treats the theory of congruences in this domain, and then the theory of quadratic residues. He finally deduces the analogue of Gauss's lemma for this domain and sketches how to obtain the analogue of the quadratic reciprocity law, following Gauss's fifth proof of the law for the rational numbers. Dedekind writes:

> The proof of our theorem [i.e., the quadratic reciprocity law for polynomials] can be established completely analogously to *Gauss*'s fifth proof of *Legendre's* theorem [i.e., the quadratic reciprocity law for the rational integers] and is based on the lemma [i.e., Gauss's lemma] proved at the end of the preceding article ... Its consequences, up to the last result which contains the proof of the theorem, are so similar to the ones in the cited treatise of *Gauss*[38] that no one can fail to find the complete proof. Herewith, we shall leave our theory, since its further development follows automatically.[39]

2.2.2. Galois

We have seen that Dedekind referred to Galois in his article [Dedekind 1857a], which was written in 1856. In his paper "Sur la théorie des nombres," Galois said:

[35] See [Kummer 1975], pp. 204–206 and 226–228.

[36] See [Dedekind 1878], § 1, pp. 4-5 and § 2, in particular Theorem I, pp. 11-12.

[37] See [Selling 1865]. Selling's paper is also based on [Dedekind 1857a] as well as on [Schönemann 1845], [Schönemann 1846], and its presentation is influenced by Galois as treated in [Serret 1854] – see [Selling 1865], p. 23.

[38] I.e., [Gauss 1863b], pp. 51–54; cf. the German translation in [Maser 1889], pp. 497–501.

[39] See [Dedekind 1857a], § 17: *Der Beweis unseres Theorems kann ganz analog dem fünften Gaußschen für den Satz von Legendre geführt werden und stützt sich dann auf das am Schlusse des vorigen Artikels bewiesene Lemma ... die Schlußfolgerungen daraus bis zu dem letzten Resultat hin, in welchem der Beweis des Theorems enthalten ist, sind denen der zitierten Abhandlung von Gauß so ähnlich, daß die vollständige Durchführung Niemandem entgehen kann. Und hiermit wollen wir diesen Teil unserer Theorie verlassen, da seine weitere Entwicklung sich von selbst ergibt.* For more details on Dedekind's paper, we refer to [Frei 2001] and [Frei 2004].

> If in the algebraic calculations, one agrees to consider as zero all quantities which are multiples of a given prime number p, and if one looks for the solutions of an algebraic equation $Fx = 0$ with respect to this convention, which Gauss denotes by $Fx \equiv 0$, then it is customary to consider only the integer solutions of this kind of question. After having been led by special investigations to consider the incommensurable solutions, I arrived at some results which I believe to be new.[40]

Galois refers of course to Gauss's *Disquisitiones Arithmeticae*, since in 1830 he could not have known Gauss's unpublished *Disquisitiones generales de congruentiis*. And further down, after having proposed to introduce imaginary symbols for the incommensurable, i.e., irrational, solutions of $F(x) \equiv 0 \bmod p$, Galois writes:

> It is the classification of these imaginaries and their reduction to the smallest number possible which will occupy us [in this paper].[41]

It is in this language that Galois then set out to establish what we would describe today as the additive and multiplicative structure of the finite algebraic field extensions of the prime field $\mathbf{F}_p$ of characteristic p. He thus worked with an (imaginary) root of a polynomial $F(x)$ of a certain degree ν which, in today's language, is irreducible over $\mathbf{F}_p$. Galois then illustrated his theory in detail with the example where $p = 7$ and $\nu = 3$. The discoveries of Galois are essentially the same as those of Gauss's §§ 351–352 of the *Disquisitiones generales de congruentiis*. However, Gauss worked with the irreducible polynomial $F(x)$ itself instead of an (imaginary) root of $F(x)$. And Gauss explicitly said in § 338 of the *Disquisitiones generales de congruentiis* that he could have shortened considerably his investigations, had he wanted to introduce such imaginary quantities; but he preferred to deduce everything from first principles – see the end of section 3.2 below for the precise quote. Not only in the *Disquisitiones generales de congruentiis* did Gauss avoid imaginary roots, but also in the *Disquisitiones Arithmeticae*:[42] in Section Seven on Cyclotomy, he refrained from deducing the properties of the roots of unity and of the Gaussian periods generated by them from the fact that the former are complex numbers. He instead obtained these properties by representing them arithmetically in a formal way and solely using the fact that they are roots of the cyclotomic polynomial and of real (abelian) polynomials of lower degree – cf. section 1.1 above and section 3.3 below.

[40] [Galois 1830/1897], p. 15: *Quand on convient de regarder comme nulles toutes les quantités qui, dans les calculs algébriques, se trouvent multipliées par un nombre premier donné p, et qu'on cherche, dans cette convention, les solutions d'une équation algébrique* $Fx = 0$, *ce que M. Gauss désigne par la notation* $Fx \equiv 0$, *on n'a coutume de considérer que les solutions entières de ces sortes de questions. Ayant été conduit par des recherches particulières à considérer les solutions incommensurables, je suis parvenu à quelques résultats que je crois nouveaux.*

[41] See [Galois 1830/1897], p. 15:*C'est la classification de ces imaginaires, et leur réduction au plus petit nombre possible, qui va nous occuper.*

[42] On this issue, see also H. Edwards's chap. I.2 in this volume [Editors' note].

2.2.3. Schönemann and Kronecker

As well as to Galois, Dedekind [Dedekind 1857a] also referred to Schönemann. Like Galois, Schönemann also mentions Gauss in the preface:

> The famous author of the *Disquisitiones Arithmeticae* had intended a general theory of higher congruences for Section Eight of his work. Since, however, this Section Eight did not appear, and also, as far as I know, the author did not publish anything on this subject, nor indicate anything precisely, I do not dare to decide whether, and how closely, this present paper is related to the investigations of the famous master. In case I have perhaps dedicated my research partially to the same theorems as the profound creator of the theory of congruences, then the loss of the first discovery would be compensated by my knowledge of having met on my own independently the endeavour of such a [great] spirit.[43]

Schönemann also mentions in his preface that he was led to his investigations by the discovery of the theorem asserting that the polynomial $F(x)$, whose roots mod p are the p^{th} powers of the roots mod p of a given polynomial $f(x)$ with integral coefficients, is congruent to this given polynomial $f(x)$ mod p, if p is a prime number.[44] Gauss established this crucial theorem in § 350 of the *Disquisitiones generales de congruentiis* – see the theorem 3 and our comments in section 3.2 below. Schönemann found what we would describe today as the properties of finite fields in terms of congruences modulo a prime number p and modulo an "expression" $f(\alpha)$, where $f(x)$ is an irreducible polynomial mod p, and α is a root of $f(x)$ mod p. Schönemann called this double congruence a congruence according to the modulus (p, α). However, unlike Gauss, Schönemann did not realize the importance, for the structure of finite fields, of what we know as the related Frobenius automorphism. In addition, Schönemann's presentation lacks clarity and precision compared to Gauss who essentially works in $\mathbf{F}_p[x] \bmod f(x)$ (see below), and also to Galois who considers α as being an algebraic irrational and works in $\mathbf{F}_p(\alpha)$. Schönemann's principal result is the following *Hauptsatz*:[45]

[43] See [Schönemann 1845], p. 270: *Der berühmte Verfasser der* Disquisitiones Arithmeticae *hatte für den achten Abschnitt seines Werkes eine allgemeine Theorie der höheren Congruenzen bestimmt. Da indessen dieser achte Abschnitt nicht erschienen, und auch, so viel ich weiss, über diesen Gegenstand sonst nichts von dem Herrn Verfasser bekannt gemacht oder nur bestimmt angedeutet worden ist (denn die Untersuchungen über imaginäre Moduln gehören in ein anderes Gebiet), so wage ich nicht, zu entscheiden, ob und wie weit die vorliegende Arbeit mit den Untersuchungen des berühmten Meisters in Berührung stehe. Sollte ich vielleicht zum Theil denselben Sätzen meine Forschung gewidmet haben, wie der tiefsinnige Begründer der Lehre von den Congruenzen, so würde mich über die Einbusse der ersten Entdeckung das Bewusstsein schadlos halten, auf selbstständigem Wege mit dem Streben eines solchen Geistes zusammengetroffen zu sein.* Theodor Schönemann (1812–1868) had published this paper already a year before, in 1844, in a publication (*Programm*) of the Brandenburg *Gymnasium* (high school) at Brandenburg on the Havel, where he taught.

[44] He proved this theorem in § 13 of [Schönemann 1845], pp. 269, 287.

[45] See § 18 of [Schönemann 1845], p. 292. We present the result in a modernized form.

Main Theorem. If $f(x)$ is an irreducible monic polynomial of degree n modulo a prime number p, and if α is a root of $f(x)$ modulo p, then $f(x)$ splits as follows modulo p:

$$f(x) \equiv (x-\alpha)(x-\alpha^p)(x-\alpha^{p^2})\dots(x-\alpha^{p^{n-1}}) \quad \mathrm{mod} p.$$

Furthermore: $\alpha^{p^n-1} \equiv 1 \,\mathrm{mod} p$.

Schönemann (p. 288)[46] views this as a generalization of Lagrange's theorem: $x^{p-1}-1 \equiv (x-1)(x-2)\cdots(x-(p-1))$ mod p, which can also be written as $x^{p-1}-1 \equiv (x-a)(x-a^2)\cdots(x-a^{p-1})$ mod p if a is a primitive root mod p, as well as of Fermat's theorem: $a^{p-1} \equiv 1$ mod p.

Schönemann then goes on to study what we would call today the polynomial ring $\mathbf{F}_p(\alpha)[x]$, where α is a root of an irreducible monic polynomial $f(x)$ in $\mathbf{F}_p[x]$. He establishes (p. 297) the unique decomposition of polynomials into irreducibles. Then he passes to iterated algebraic extensions $\mathbf{F}_p(\alpha)(\beta)$, where β is a root of an irreducible monic polynomial $g(x) = g(x,\alpha)$ in $\mathbf{F}_p(\alpha)[x]$ (pp. 302–305). For q a prime number and α a root of an irreducible monic polynomial $f(x)$ in $\mathbf{F}_p[x]$, he determines (p. 319) the number of irreducible polynomials of degree q^ν in $\mathbf{F}_p(\alpha)[x]$. Finally, Schönemann essentially finds part of Kummer's decomposition law, in terms of congruences mod p, of a prime number p in the cyclotomic field $\mathbf{Q}(\zeta_q)$, where q is a prime (pp. 323–325); namely, if $q \neq p$ and f is the smallest natural number such that $p^f \equiv 1$ mod q, then $\psi(x) = x^{q-1} + x^{q-2} + \cdots + x + 1$ splits mod p into $\frac{q-1}{f} = e$ irreducible factors of degree f; and if $q = p$, then $\psi(x) \equiv (x-1)^{p-1}$ (mod p).[47] From there he obtains (p. 325), by means of Dirichlet's theorem on primes in an arithmetic progression, the theorem that the polynomial $\psi(x) = x^{q-1} + x^{q-2} + \cdots + x + 1$ is irreducible in $\mathbf{Q}[x]$. Gauss had proved this result in D.A., art. 341.

In a subsequent paper [Schönemann 1846], Schönemann extended his investigations from a prime number p to a prime power p^m. Thereby he discovered an early version of what we call today Hensel's lemma.[48] He then obtained a new and simple proof for the cyclotomic polynomial $\psi(x) = x^{q-1} + x^{q-2} + \cdots + x + 1$ to be irreducible in $\mathbf{Q}[x]$ if q is a prime number.[49] In this context, Schönemann also used and proved the irreducibility criterion which Barteel L. van der Waerden in his book on modern algebra would call "Eisenstein's criterion."[50]

Let us also mention Leopold Kronecker who seems to have been the first to quote Gauss's *Disquisitiones generales de congruentiis* after these had been published by Dedekind. Kronecker wrote:

[46] The page numbers in brackets given in this and the following paragraph all refer to the paper [Schönemann 1845].

[47] Cf. [Kummer 1847], p. 321.

[48] See [Schönemann 1846], §§ 58–59, pp. 97–98.

[49] See [Schönemann 1846], § 61, p. 100.

[50] See [Schönemann 1846], § 61, pp. 100-101 and [van der Waerden 1930], pp. 77–79. It was proven independently by Eisenstein in [Eisenstein 1850], pp. 166–167.

> This consideration [i.e., the theory of algebraic functions of several variables] shows the theory of higher congruences in a new light and relates this theory with other quite different number theoretic fields. One also finds in this theory, not only in the manuscript from *Gauss's* legacy published by Herr *Dedekind* but also in *Schönemann's* previously published articles, the first indication to divisor systems of level two, although from a more restricted point of view. The natural and far reaching distinction of module systems according to their different levels, the separation of the *truly* manifold divisor systems from those representing only simple divisors, could only emerge with the arithmetic treatment of integer functions of *several* variables, and on those nothing has been made known up to now as far as I know.[51]

This seems to indicate that Schönemann's papers as well as Gauss's *Disquisitiones generales de congruentiis* have had some influence on Kronecker's foundation of the theory of divisors.[52]

2.2.4. Later Authors: Kühne, Kornblum, Artin, F.K. Schmidt

Of the later authors working on function fields $\mathbf{F}_q[x]$ of characteristic p, where $q = p^m$, we first mention Hermann Kühne,[53] who, in [Kühne 1902], proved the general n^{th} power reciprocity law in $\mathbf{F}_q[x]$ for $n = 3$ and $n = 4$, and for general n in the case where the constant field $\mathbf{F}_q$ contains the n^{th} roots of unity. This theorem was rediscovered and reproved later in 1925 independently by Friedrich Karl Schmidt.

[51] See [Kronecker 1882], § 21. *Diese Betrachtung zeigt die Theorie der höheren Congruenzen in einem neuen Lichte und bringt dieselbe mit ganz anderen zahlentheoretischen Gebieten in Verbindung. Es finden sich auch in dieser Theorie, sowohl in der von Herrn* Dedekind *aus* Gauss' *Nachlass publicirten Arbeit als in den* Schönemann'*schen früher veröffentlichten Aufsätzen die ersten Andeutungen von Divisoren-Systemen zweiter Stufe, wenngleich nur unter beschränkterem Gesichtspunkte. Die naturgemässe und weitreichende Unterscheidung der Modulsysteme nach ihren verschiedenen Stufen, die Sonderung der in* Wahrheit *mehrfaltigen Divisoren-Systeme von denjenigen, die nur einfache Divisoren vertreten, konnte sich erst bei der arithmetischen Behandlung ganzer Functionen* mehrerer *Variabeln ergeben, und über diese ist bisher meines Wissens nichts bekannt gemacht worden.*

[52] We do not go into more details here, since we shall study the relation between Kronecker's theory of divisors and the theory of higher congruences more closely in a separate paper.

[53] Hermann Ernst Gustav Eduard Kühne was born on November 25, 1867 in Berlin and died on May 21, 1907 in Dortmund. He studied from 1886 until 1892 in Berlin where he obtained his Dr. phil. with a thesis on n-manifolds. The thesis was directed by Lazarus Fuchs – Herman Amandus Schwarz was the second examiner, but the suggestion for the topic seems to have come from Kronecker – see [Biermann 1988], p. 160 (I thank Herbert Pieper for this information). In 1896, Kühne became a high school (*Gymnasium*) teacher in Königsberg in der Neumark (Brandenburg; now Krzywka in Poland), and in 1897 in Herford in Westfalen. From 1899 until his early retirement in 1907, he was *Oberlehrer* at the *Maschinenbauschule* in Dortmund. His papers, published between 1892 and 1904 in *Mathematische Annalen* and *Archiv der Mathematik und Physik*, concern the theory of manifolds.

Kühne does not give any reference to his predecessors, but surely he must have been aware of Dedekind's paper [Dedekind 1857a], where Dedekind proves the quadratic reciprocity law. It seems to me also most likely that Kühne knew Schönemann's articles, and also Gauss's *Disquisitiones generales de congruentiis*, which had been published in the meantime in 1863 and reprinted in 1876. If we take for granted that Kühne's papers on functions of several variables were initiated by a suggestion from Kronecker,[54] we may conclude that Kühne was familiar with Kronecker's monumental *Grundzüge* [Kronecker 1882], and hence that Kühne was also aware of Schönemann's articles and of Gauss's *Disquisitiones generales de congruentiis* both mentioned in [Kronecker 1882] – see the quotation at the end of section 2.2.3. Another reason why Kühne must have known these predecessors is that he does not repeat anything contained in the paper of Dedekind, the articles of Schönemann, or the treatise of Gauss, but rather takes this material for granted and starts where these three authors stopped. For example, Kühne's iterated construction of the finite algebraic extension $K = \mathbf{F}_p(\alpha_1, \dots, \alpha_n)$ over $\mathbf{F}_p$ resembles the one given by Schönemann. From there, Kühne goes on to study the polynomials in $K[x]$.

Kühne first introduces, following the tradition of Kronecker,[55] the domain $\mathcal{B} = \mathbf{Z}[x_1, \dots, x_n]$ modulo the "prime module system"

$$P = \big(p, f_1(x_1), f_2(x_2; x_1), \dots, f(x_n; x_1, \dots, x_{n-1})\big),$$

where p is a prime number and $f_1(x_1)$ is a monic irreducible integral polynomial mod p, $f_2(x_2; x_1)$ is a monic irreducible integral polynomial mod $(p, f_1(x_1))$, etc. That is, in today's terminology, he considers the finite algebraic extension $\mathbf{F}_q = \mathbf{F}_p(\alpha_1, \dots, \alpha_n)$ of $\mathbf{F}_p$, where $f_1(\alpha_1) = 0$, $f_2(\alpha_2; \alpha_1) = 0$, etc. Then he deduces the general n^{th} power reciprocity law in $\mathbf{F}_q[x]$ for n dividing $q - 1$, that is, when the field $\mathbf{F}_q$ contains the n^{th} roots of unity: If f and g are two different monic irreducible polynomials in $\mathbf{F}_q[x]$ of degree μ and ν respectively, then

$$\left(\frac{f}{g}\right)_n = \left(\frac{g}{f}\right)_n (-1)^{\mu\nu\frac{q-1}{n}}$$

where $(\frac{}{g})_n$ is the n^{th} power Legendre symbol of g in $\mathbf{F}_q[x]$.[56]

Kühne then derives also the cubic and biquadratic reciprocity law in the cases where $n = 3, 4$ is not a divisor of $q - 1$. In both cases, he finds:[57]

$$\left(\frac{f}{g}\right)_n = \left(\frac{g}{f}\right)_n .$$

[54] See [Biermann 1988], p. 160. The way in which Kühne treats the subject and the terminology and concepts he uses confirm this hypothesis.

[55] See for instance [Kronecker 1882], § 21. We shall study more closely elsewhere the relationship between Kronecker's theory of divisors and the theory of higher congruences, as well as Kühne's papers.

[56] See [Kühne 1902], p. 129.

[57] See [Kühne 1902], pp. 132–133.

In a subsequent paper, Kühne studied the units in $\mathbf{F}_q[x]$ and obtained the analogue of Dirichlet's unit theorem for $\mathbf{F}_q[x]$ – see [Kühne 1903], p. 115. For that purpose Kühne also states and proves what we would refer to as Hensel's lemma – see [Kühne 1903], p. 105. Gauss had already stated and proved a version of Hensel's Lemma in his *Disquisitiones generales de congruentiis* – see section 3.6 below for more details – and Schönemann found an early version in his paper [Schönemann 1846]. We have explained why we have strong reasons to believe that Kühne did know the *Disquisitiones generales de congruentiis* and also the papers by Schönemann. Hence it is quite probable that Kühne got the idea for this lemma directly from Gauss.[58] So it is possible that Hensel's lemma goes back all the way to Gauss's *Disquisitiones generales de congruentiis*, even though neither Kühne nor Hensel mention any predecessors related to this lemma.[59] It is, of course, no accident, that Gauss's proof of Hensel's Lemma – see section 3.6 below – and Hensel's introduction of p-adic numbers both emerged in connection with higher ramification.[60]

According to p. 130 of [Kühne 1902], he had the intention to study also the theory of quadratic forms over $\mathbf{F}_q[x]$, probably following the exposition given by Gauss in Section Five of the *Disquisitiones Arithmeticae*, but it seems that Kühne did not live to publish anything on this subject. He took an early retirement in 1907 at the age of 40, probably because of bad health, and died the same year. His last paper appeared in 1904.

Although not directly influenced by Gauss, another author we want to mention is Heinrich Kornblum who, in the paper [Kornblum 1919], carried Dirichlet's theorem on primes in arithmetic progressions from the ring of integers $\mathbf{Z}$ to the ring $\mathbf{F}_p[x]$ of integral polynomials mod p. Heinrich Kornblum (1890–1914) was a student of Landau in Göttingen. He was killed in the First World War in October 1914 at the age of 24 near Poël-Capelle. Kornblum's paper is based on his doctoral dissertation on prime functions (irreducible polynomials) in arithmetical progressions and was edited in 1919 after the war by Edmund Landau. Kornblum's starting point was also Dedekind's paper [Dedekind 1857a]. Kornblum discovered, after having introduced L-functions for $\mathbf{F}_p[x]$, that the classical proof of Dirichlet for the non-vanishing of $L(s, \chi)$ at $s = 1$ for non-principal characters χ can be adapted to function fields $\mathbf{F}_p(x)$. However, Kornblum did not introduce algebraic extensions of $\mathbf{F}_p(x)$.

[58] Starting with volume 125 (1903) until 1936, Hensel was the editor of Crelle's *Journal* and used to read all submitted articles. So he must have known Kühne's paper. Whether this may have influenced his work on p-adic numbers, gradually taking shape from 1897, and his discovery of Hensel's lemma (see [Hensel 1904], § 4, in particular p. 81) remains to be analysed.

[59] Hensel does mention, in his paper [Hensel 1904], p. 69, the name of Gauss in connection with Gauss's theorem and proof on primitive functions, to the effect that the product of two primitive functions is again primitive, but without giving a precise reference to Gauss: *Nach dem Vorgange von Gauß beweist man leicht, daß das Produkt zweier primitiven Funktionen … wieder primitiv ist.*

[60] We shall discuss in a separate paper the history of p-adic numbers in connection with higher ramification in the works of Gauss, Schönemann, Kummer, Dedekind, Kronecker and Hensel. For the history of p-adic numbers, see also [Arigoni 1984], [Ullrich 1998].

An important step in the theory of function fields of characteristic p was taken by Emil Artin in his thesis [Artin 1924] where he introduces and studies systematically the arithmetic of a quadratic extension $\mathcal{K}$ of the function field $\mathbf{F}_p(x)$ over a finite field of prime order p, that is, the theory of hyper-elliptic curves over a finite prime field $\mathbf{F}_p$. The focus of his study was the analytic class number formula for $\mathcal{K}$ which led him to introduce the ζ-function for the function field $\mathcal{K}$ and to formulate and conjecture the Riemann Hypothesis for $\mathcal{K}$. The thesis was sent for publication to the *Mathematische Zeitschrift* on October 14, 1921, but appeared only in 1924. Like Kornblum, Artin does not mention Gauss in his dissertation but refers to the article [Dedekind 1857a], and also to Kornblum's paper which had appeared just two years before Artin's thesis was written and sent to the same journal as Kornblum's. It was Artin's thesis advisor Gustav Herglotz who suggested to Artin that he study quadratic algebraic extensions of a function field $\mathbf{F}_p(x)$, after having seen Kornblum's thesis in the *Mathematische Zeitschrift* of which Herglotz was a scientific adviser (*wissenschaftlicher Beirat*).[61]

Finally, let us mention F.K. Schmidt who continued the theory of function fields of characteristic p where Artin had left it in 1924, by generalizing Artin's theory from quadratic extensions of $\mathbf{F}_p(x)$ to arbitrary finite algebraic extensions $\mathcal{K}$ of $\mathbf{F}_q(x)$, where q is a power of p. This was done first in Schmidt's thesis [Schmidt 1925] where he derived the fundamental arithmetical properties of the ring of integers $\mathcal{R} = \mathfrak{o}_{\mathcal{K}}$ in $\mathcal{K}$, that is, properties of the discriminant, units and class number of $\mathcal{R}$. However, the thesis was never published, probably because similar results had been obtained at the same time and independently by Paul Sengenhorst and Herbert Rauter, a doctoral student of Helmut Hasse – see [Roquette 2001], p. 564. We have already mentioned that the n^{th} power reciprocity law in $\mathbf{F}_q[x]$, found by Schmidt in his thesis, had previously been obtained by Kühne in 1902.

In his next papers, however, Schmidt goes into completely new territory by deriving class field theory for function fields of characteristic p, in analogy to Hasse's report on class field theory of algebraic number fields.[62] To do this, Schmidt had first to develop the analytic theory of the ζ-function and of the L-functions of $\mathcal{K}$ in order to obtain the first inequality of class field theory. Thereby Schmidt discovered that the functional equation of the ζ-function, introduced by him in 1926 for a congruence function field $\mathcal{K}$ – see [Schmidt 1926–1927] – is equivalent to the theorem of Riemann-Roch in $\mathcal{K}$ – see [Schmidt 1931a]. This theorem had been translated by Schmidt from the case of characteristic zero (which had been studied by Dedekind and Weber in their fundamental article [Dedekind, Weber 1882]) to the case of characteristic p.

Schmidt's theory was fundamental for Hasse's investigations on the Riemann Hypothesis for function fields in one variable over finite fields, for Hasse's proof in the elliptic case (1933), for André Weil's proof of the general case (1948), and for the proof of the Weil conjectures (1949) by Bernard Dwork (1960), Alexandre

[61] This has been confirmed by Peter Roquette – see [Roquette 2002], p. 85. For more details on Artin's thesis we refer to [Frei 2001] and [Frei 2004].

[62] See [Schmidt 1931b], cf. [Hasse 1926–1930].

Grothendieck and Pierre Deligne (1973).[63] For more details on F.K. Schmidt's work, see [Roquette 2001].

3. Content of the *Disquisitiones Generales de Congruentiis*

3.1. Fundamental Theorem and Main Problem

Let us now indicate the content of Gauss's *Disquisitiones generales de congruentiis* in abbreviated form and with the help of modern notation and terminology. In particular, instead of working with polynomials with integral coefficients taken modulo p, as Gauss does, we shall freely speak of polynomials belonging to $\mathcal{R} := \mathbf{F}_p[x]$. We shall also number the key theorems from 1 to 10. A more detailed discussion of the mathematical content of the *Disquisitiones generales de congruentiis* will appear in [Frei 2001].

§ 330. Gauss opens his investigation by saying that, what he has communicated on congruences in the preceding sections [that is, in an early version of the *Disquisitiones Arithmeticae*] concerns only the simplest cases and was mostly found by special methods. He announces that in the present section he will try to base the theory of congruences, at least as far as this is possible at present, on higher principles, following the salient analogy with the theory of [algebraic] equations, an analogy he has observed many times.[64] We have already seen in 2.1 the example of Lagrange's theorem, and shall encounter that of Fermat's theorem below.

From the numerous remarks Gauss made on his new methods and the "higher principles" based on this analogy and governing his investigations, let us quote what Gauss writes in the preface of the D.A.:

> When I decided after some time to publish the fruits of my efforts, I let myself be persuaded, following the wish expressed by several people, not to omit anything of these early investigations, so much the more so since at that time there was no book from which the works of other mathematicians on this subject could have been learnt, scattered as they were among Commentaries of learned Academies; but also since many of these are treated in an altogether new way and for the most part with new methods, and finally since all of them are so closely connected with each other as well as with [my] later investigations, that also the new results could not be explained appropriately enough without repeating the remaining results from the beginning.[65]

[63] See [Hasse 1933]; [Weil 1948], pp. 60–70; [Dieudonné 1985], IX 8, art. 123–139, pp. 151–158.

[64] See [Gauss 1863b], p. 212: *Quae in Sectionibus praecedentibus de congruentiis sunt tradita, simplicissimos tantum casus attinent methodisque particularibus plerumque sunt eruta. In hac Sectione periculum faciemus congruentiarum theoriam, quantum quidem adhuc licet, ad altiora principia reducere, simili fere modo ut* aequationum *theoria considerari solet, quacum insignis intercedit analogia, uti iam saepius observavimus.*

[65] D.A., *praefatio*: *Postquam interiecto tempore consilium de fructibus vigiliarum in publicum edendis cepi: eo lubentius, quod plures optabant, mihi persuaderi passus sum, ne quid vel ex illis investigationibus prioribus supprimerem, quod tum temporis liber non habetur, ex quo aliorum geometrarum labores de his rebus, in Academiarum Commentariis sparsi, edisci potuissent; quod multae ex illis omnino novae et pleraeque per methodos*

In the final version of the D.A. these higher principles and the analogy between the arithmetic of rational integers and polynomials, that is, between $\mathbf{Z}$ and $\mathbf{Q}[x]$, or $\mathcal{R} = \mathbf{F}_p[x]$, already appear so clearly that Dedekind in [Dedekind 1857a] could write: "the deductions ... up to the last result which contains the proof of the theorem are so similar to the ones in the cited treatise by *Gauss* that no one can fail to find the complete proof" – see 2.2.1 above for the full quote.

§ 333. Gauss begins the theory with the theorem: If a is a root of a polynomial $P(x)$ in $\mathcal{R} = \mathbf{F}_p[x]$, then $P(x)$ is divisible in $\mathcal{R}$ by $x - a$.

§ 334. Gauss develops the Euclidean algorithm in $\mathcal{R}$.

§ 335. Gauss proves the theorem: Given two polynomials $A(x)$ and $B(x)$ in $\mathcal{R}$, prime to each other, there exist polynomials $P(x)$ and $Q(x)$ in $\mathcal{R}$ such that $A(x)P(x) + B(x)Q(x) = 1$.[66]

§ 340. From there Gauss gets the fundamental theorem on unique factorization in $\mathcal{R}$.

§ 341–347. Gauss treats what he calls the "Main Problem": to determine the number of (monic) irreducible polynomials[67] $P(x)$ in $\mathcal{R}$ of a given degree m. He first gets this number by combinatorial counting arguments and by recursion starting from polynomials of degree one to polynomials of higher degree (§§ 343–346). Then he obtains an explicit formula (§ 347).[68]

3.2. *An Early Parent of the Theory of Finite Fields*

§ 348. Gauss opens this section with the following question: Given an equation $P(x) = 0$, where $P(x)$ is a monic polynomial of degree m, with roots $\alpha_1, \ldots, \alpha_m$, find an equation $P^{(t)}(x) = 0$ whose roots are $\alpha_1^t, \ldots, \alpha_m^t$, i.e., the t^{th} powers of the roots of $P(x)$.

Gauss compares two different methods. The first one applies Newton's formulae relating the coefficients of $P(x)$ to the sums of powers $s_\nu = \alpha_1^\nu + \cdots + \alpha_m^\nu$, for $\nu = 1, 2, 3, \ldots$ This, he says, works well in practice and proves the first key result:
Theorem 1. The coefficients of $P^{(t)}$ can be expressed rationally in those of P.
However, the first method makes it hard to see that the coefficients of $P^{(t)}$ are integers when those of P are. The second method makes use – for the first time – of cyclotomy, i.e., of Section Seven of the *Disquisitiones Arithmeticae*. If ϑ is a primitive t^{th} root of unity, then Gauss forms the product $\prod(x - \vartheta^\tau \alpha_i)$ over all $\tau = 1, \ldots, t$ and $i = 1, \ldots m$ and puts $x^t = y$. This gives $P^{(t)}(y)$, and shows
Theorem 2. The coefficients of $P^{(t)}$ are integers when those of P are.

novas tractatae erant; denique quod omnes tum inter se tum cum disquisitionibus posterioribus tam arcto nexu cohaerebant, ut ne nova quidem satis commode explicari possent, nisi reliquis ab initio repetitis.

[66] Cf. [Gauss 1796–1814], entry 27 (August 19, 1796).

[67] Gauss uses the term *functio prima* (*Primfunktion* in Maser's German translation) for "irreducible polynomial."

[68] Cf. [Gauss 1796–1814], entry 75 (August 26, 1797).

The two entries from Gauss's diary related to the two solutions discussed are [Gauss 1796–1814], entry 6 (May 23, 1796), and entry 28 (August 21, 1796).

§ 350. Next Gauss proves the following remarkable property:[69]

Theorem 3. If t is a prime number, then $P^{(t)}(x) = P(x)$ for $P(x)$ belonging to $\mathbf{F}_t[x]$.

Looked at from today's vantage point, this suggests that raising to the t^{th} power induces a permutation of the roots of a given polynomial $P(x)$ of $\mathbf{F}_t[x]$. Following Hasse, [Hasse 1926-1930], this permutation is today called the Frobenius automorphism of the field $E = \mathbf{F}_t(\alpha_1, \ldots, \alpha_m)$ over the base field $\mathbf{F}_t$.

That Gauss was perfectly aware of operations on the roots of equations and was thinking of what we call the Frobenius automorphism appears very clearly in § 348, where Gauss writes: "Since we shall often use this operation in the sequel, we shall denote by (P, ρ^τ) the polynomial whose roots are the τ^{th} powers of the roots of P."[70] And he notes that (P, ρ^τ) has not only rational but integral coefficients if P has integral coefficients, and that, if P and Q are two polynomials and $P \equiv Q$ with respect to a modulus, then also $(P, \rho^\tau) \equiv (Q, \rho^\tau)$. In § 356 – see below – Gauss speaks explicitly of permutations[71] of the quantities x^τ and of the invariance of expressions[72] of these quantities under these permutations.

Gauss explicitly mentions the point of view of adjoining algebraic quantities to $\mathbf{F}_p$ in § 338 where he proves Lagrange's theorem (see 2.1 above) to the effect that a polynomial $P(x)$ in $\mathbf{F}_p[x]$ of degree m cannot have more than m distinct roots (a theorem he deduced from Descartes's theorem):

> From this it becomes clear that the number of roots [of a polynomial congruence] cannot exceed the dimension [i.e., degree] of the congruence ... But at the same time, one sees from this how the solution of congruences constitutes only a part of a much higher [more advanced] investigation, namely on the decomposition of functions [i.e., polynomials] into factors. It is clear that the congruence $\xi \equiv 0$ does not have real roots if ξ has no factors of dimension one; but nothing prevents us from decomposing ξ, nevertheless, into factors of two, three or more dimensions, whereupon, in some sense, *imaginary* roots could be attributed to them. Indeed, we could have shortened incomparably all our following investigations, had we wanted to introduce such imaginary quantities by taking the same liberty some more recent mathematicians have taken; but nevertheless, we have preferred to deduce everything from [first] principles. Perhaps, we shall explain our view on this matter in more detail on another occasion.[73]

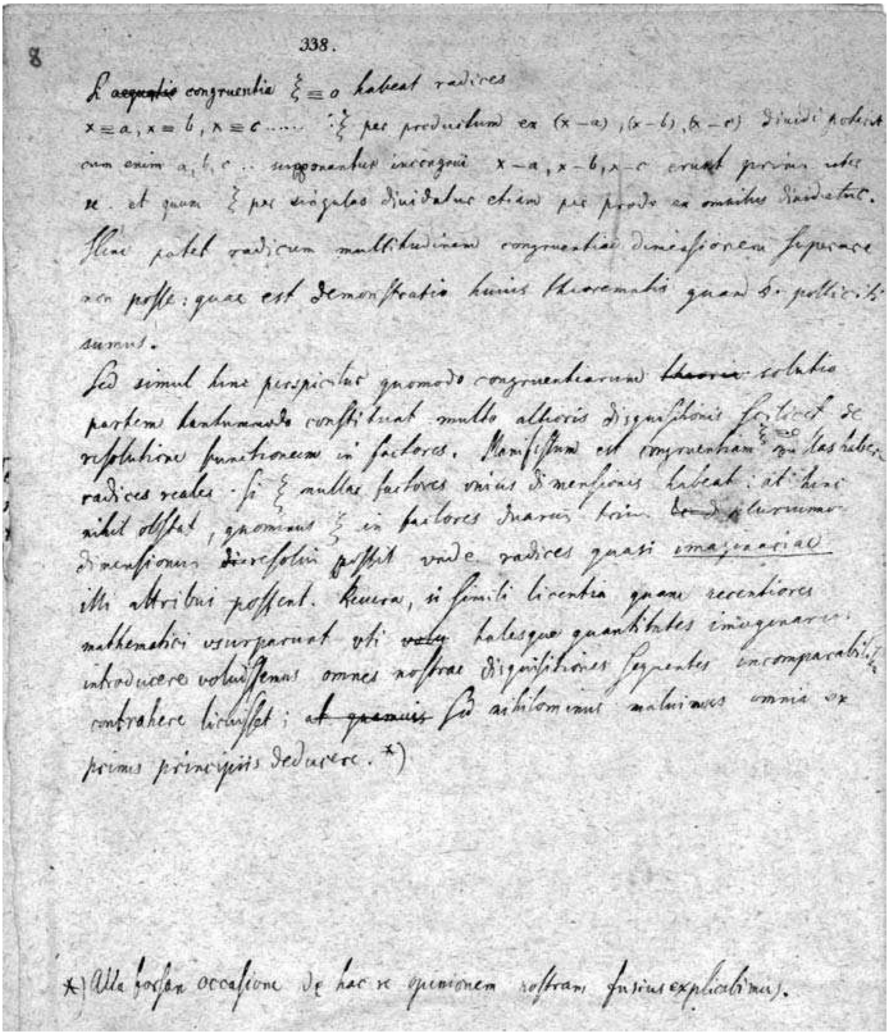
[69] According to his diary, Gauss discovered this theorem in order to establish his third proof of the quadratic reciprocity law. See [Gauss 1796–1814], entry 26 (August 18, 1796). He had got the principal idea for this proof five days before, on August 13, 1796, see [Gauss 1796–1814], entry 23.

[70] See [Gauss 1863b], pp. 223-224: *Quoniam hac operatione in sequentibus saepe utemur, per* (P, ρ^τ) *indicabimus functionem, qua cifrae aequali posita aequatio proveniens habeat radices, quae sunt potestates* τ^{tae} *radicum aequationis* $P = 0$.

[71] ... *quomodocunque eae inter se permutentur* ...

[72] ... *quae eadem maneat* ...

[73] Our translation from [Gauss 1863b], p. 217f; see Fig. II.4A.



8

338.

Si ~~aequatio~~ congruentia $\xi \equiv 0$ habeat radices $x \equiv a, x \equiv b, x \equiv c \ldots\ldots$ ξ per productum ex $(x-a), (x-b), (x-c)$ dividi poterit cum enim a, b, c .. ſupponantur incongrui $x-a, x-b, x-c$ erunt primi inter ſe. et quum ξ per ſingulos dividatur etiam per prodᵗ ex omnibus dividetur. Hinc patet radicum multitudinem congruentiae dimenſionem ſuperare non poſſe: quae eſt demonſtratio huius theorematis quam s. polliciti ſumus.

Sed ſimul hinc perſpicitur quomodo congruentiarum ~~theoria~~ ſolutio partem tantummodo conſtituat multo altioris diſquiſitionis ſcilicet de reſolutione functionum in factores. Manifeſtum eſt congruentiam $\xi \equiv 0$ nullas habere radices reales ſi ξ nullos factores unius dimenſionis habeat: at hinc nihil obſtat, quominus ξ in factores duarum trium ~~[illegible]~~ pluriumve dimenſionum ~~dis~~reſolvi poſſit unde radices quaſi imaginariae illi attribui poſſent. Revera, ſi ſimili licentia quam recentiores mathematici uſurparunt uti ~~voly~~ taleſque quantitates imaginarias introducere voluiſſemus omnes noſtrae diſquiſitiones ſequentes incomparabiliter contrahere licuiſſet; at ~~quamvis~~ ſed nihilominus maluimus omnia ex primis principiis deducere. *)

*) Alia forſan occaſione de hac re opinionem noſtram fuſius explicabimus.

Fig. II.4A. Manuscript of § 338 of Gauss's *Disquisitiones generales de congruentiis.* (Courtesy of NSUB Göttingen)

3.3. Finite Fields and their Subfields via the "Frobenius Automorphism"

Next Gauss studies, with the help of the "Frobenius automorphism," the theory of cyclotomy modulo a prime number p, that is, the factorization of $x^{p^m-1} - 1 \bmod p$ and obtains fundamental properties of what we would call the theory of finite fields of characteristic p.

§ 351–353. First Gauss proves:

Theorem 4. Every irreducible polynomial $P(x) \neq x$ of degree m in $\mathbf{F}_p[x]$ is a divisor of $x^{p^m-1} - 1$ in $\mathbf{F}_p[x]$.

Interpreting this in terms of roots, it means that

Theorem 4'. All roots of $P(x)$ are $(p^m - 1)^{\text{th}}$ roots of unity with respect to $\mathbf{F}_p$.

Even though Gauss formulates and deduces what we call Theorem 4 in terms of divisibility of polynomials only, with no references to roots, he was of course aware of its interpretation somewhere along the lines of our Theorem 4' – cf. the passage § 338 quoted above. We know for instance that at the same time Gauss was working on the proof of the fundamental theorem of algebra, published in 1799 in his thesis. There he proved that every polynomial admits a complex root, yet avoiding very carefully dealing explicitly with roots or with complex numbers, whose existence was still somewhat mysterious. Gauss had recognized their importance in connection with his studies on the lemniscatic function – see D.A., art. 335 – and on the algebraic-geometric mean.[74] Instead of dealing with complex numbers, Gauss talked in his thesis of the decomposition of polynomials into real factors of degree one and two, quite similar to what he is doing in the *Disquisitiones generales de congruentiis.*

In order to deduce Theorem 4, Gauss first proves in § 352 the following theorem: If $P(x) \neq x$ is an irreducible polynomial of degree m in $\mathbf{F}_p[x]$, and if t is the smallest natural number such that $x^t - 1$ is divisible by P in $\mathbf{F}_p[x]$, then t is equal to $p^m - 1$ or is a divisor of $p^m - 1$.

Gauss mentions that this theorem is proved with the same method as the theorem[75] in art. 49 of the *Disquisitiones Arithmeticae* which states: if p is a prime not dividing the integer a, and if t is the smallest natural number such that $a^t \equiv 1 \bmod p$, then t is equal to $p - 1$ or is a divisor of $p - 1$. From this last theorem Gauss deduces immediately Fermat's theorem in art. 50 of the *Disquisitiones Arithmeticae*: If p is a prime not dividing the integer a, then $a^{p-1} \equiv 1 \bmod p$. In § 353 of the *Disquisitiones generales de congruentiis* it becomes clear that Gauss

[74] Compare with the later *Anzeige* of his papers on biquadratic residues [Gauss 1863b] p. 175, where Gauss says: *Der Verf[asser] hat diesen hochwichtigen Theil der Mathematik seit vielen Jahren aus einem verschiedenen Gesichtspunkt aus betrachtet, wobei den imaginären Grössen eben so gut ein Gegenstand untergelegt werden kann, wie den negativen: es hat aber bisher an einer Veranlassung gefehlt, dieselbe öffentlich bestimmt auszusprechen, wenn gleich aufmerksame Leser die Spuren davon in der 1799 erschienenen Schrift über die Gleichungen, und in der Preisschrift über die Umbildung der Flächen leicht wiederfinden werden.*

[75] Gauss does not give the specific number of the article, but Dedekind in [Gauss 1863b], p. 242 explains that the reference can be to art. 49. This is also cleared up by what Gauss says in the following § 353 of the *Disquisitiones generales de congruentiis.*

viewed Theorem 4 as a generalization of Fermat's theorem, namely the case $m = 1$. The reference to art. 49 of the *Disquisitiones Arithmeticae* is another instance where Gauss hints at the analogy of methods in the theory of numbers and the theory of polynomials.

Furthermore Gauss obtains:[76]

Theorem 5. $x^{p^m-1} - 1$ is equal to the product over all monic irreducible polynomials in $\mathbf{F}_p[x]$ whose degree d is a divisor of m.

3.4. The Residue Field $\mathbf{F}_p[x]/P(x)$ *over* $\mathbf{F}_p$

In § 356, Gauss deduces the following important result:[77]

Theorem 6. If $P(x)$ is an irreducible polynomial in $\mathbf{F}_p[x]$ of degree m, and $Q(x)$ is another polynomial in $\mathbf{F}_p[x]$ which is invariant under all permutations of $x, x^p, x^{p^2}, x^{p^3}, \ldots, x^{p^{m-1}}$, then $Q(x) \equiv a$ (mod $P(x)$, for some a in $\mathbf{F}_p$.

This means in modern Galois-theoretic terminology:

Theorem 6'. Let ϑ be a root of $P(x)$ and $E = \mathbf{F}_p(\vartheta)$. If $Q(\vartheta)$ is invariant under the Frobenius automorphism $\sigma : \alpha \mapsto \alpha^p$ of $E/\mathbf{F}_p$, then $Q(\vartheta)$ lies in the ground field $\mathbf{F}_p$.

§ 357. From this, Gauss deduces a result which, in terms of a root, amounts to:

Theorem 7. Let $P(x) = x^m - a_1x^{m-1} + a_2x^{m-2} - a_3x^{m-3} + \ldots + (-1)^m a_m$ be an irreducible polynomial in $\mathbf{F}_p[x]$ of degree m and ϑ a root of P. Then $E_i(\vartheta) = a_i$, where $E_i(x)$ is the i^{th} elementary symmetric function of $x, x^p, x^{p^2}, x^{p^3}, \ldots, x^{p^{m-1}}$.

§ 358–359. The following theorem is also quite remarkable and suggests that Gauss had a deep insight into the structure of finite fields and their Galois theory:

Theorem 8. Let $P(x)$ be an irreducible polynomial in $\mathbf{F}_p[x]$ and let x^ν be the smallest power of x such that $x^\nu \equiv 1 \bmod P(x)$. If $P(x) = P^{(n)}(x)$, then $n \equiv p^t \bmod \nu$ for some t.

This translates into the following statement in terms of roots:

Theorem 8'. If ϑ^n is a conjugate of ϑ, then there is a certain power σ^t of the Frobenius automorphism σ which maps ϑ onto ϑ^n.

From this it is only a small step to the assertion that, in today's language, the group of automorphisms of $\mathbf{F}_p(\vartheta)$ over $\mathbf{F}_p$ is cyclic, generated by the Frobenius automorphism.

3.5 Gauss's Third Proof of the Quadratic Reciprocity Law

The last part of the *Disquisitiones generales de congruentiis*, i.e., §§ 360–375, is entitled: "On finding the prime divisors of the function $x^\nu - 1$ with respect to a prime modulus." As we have observed before, to determine all the irreducible factors of $F(x) = x^\nu - 1$ in $\mathbf{F}_p[x]$ means to determine all the sub-fields of the splitting field of $F(x) = x^\nu - 1$ over $\mathbf{F}_p$.

[76] In our field theoretic reading, this theorem determines all the sub-fields of $\mathbf{F}_p(\vartheta)$, where ϑ is a root of an irreducible polynomial $P(x)$ in $\mathbf{F}_p[x]$. Cf. [Gauss 1796–1814], entry 30 (September 2, 1796).

[77] Cf. [Gauss 1796–1814], entry 76 and 77 (August 30 and 31, 1797).

§§ 362–364. In analogy with Section Seven of the *Disquisitiones Arithmeticae*, Gauss sketches the theory of cyclotomy for the polynomial $F(x) = x^{\nu} - 1$ over the field $\mathbf{F}_p$ with ν not divisible by p. That is, Gauss essentially develops the Galois theory over the finite field $\mathbf{F}_p$ by explicitly constructing the subfields of the splitting field of $F(x) = x^{\nu} - 1$ over $\mathbf{F}_p$, by means of Gaussian periods.

§§ 365–366. If $\nu = q$ is a prime number, Gauss obtains a new proof for the quadratic reciprocity law in $\mathbf{Z}$, his third proof (Proof VII, in the official counting). Gauss makes the following comment:

> Thus, this is the third complete proof of the fundamental theorem of Chapter IV [sec. 4 of the D.A.] which is all the more noteworthy since the principles from which it is derived are completely different from those we have used for the earlier [proofs]. From the very same source, but going in the opposite direction, we shall deduce a fourth proof.[78]

The main idea of the proof, from the modern point of view, is this: The field $\mathbf{F}_p(\sqrt{q^*})$ is viewed as contained in the cyclotomic field $\mathbf{F}_p(\zeta_q)$. Here $q^* = \left(\frac{-1}{q}\right) q$, where $\left(\frac{\ }{q}\right)$ is the Legendre symbol for the prime number q, and ζ_q is a primitive q^{th} root of unity over $\mathbf{F}_p$. Then the reciprocity law follows from the fact that the degree t of $\mathbf{F}_p(\zeta_q)$ over $\mathbf{F}_p(\sqrt{q^*})$ is a divisor of $\frac{q-1}{2}$. The subfield $\mathbf{F}_p(\sqrt{q^*})$ is constructed within $\mathbf{F}_p(\zeta_q)$ by means of Gaussian periods of length $\frac{q-1}{2}$.

Hence this proof has some similarity with Gauss's sixth proof of the quadratic reciprocity law.[79] There Gauss uses Gaussian sums in $\mathbf{Q}[x]$ mod $G(x) = x^{q-1} + \cdots + x + 1$;[80] or in $\mathbf{Q}(\zeta_q)$, as Eisenstein has pointed out in [Eisenstein 1847], p. 274. That $\mathbf{Q}[x]$ mod $G(x) = x^{q-1} + \cdots + x + 1$ is isomorphic to $\mathbf{Q}(\zeta_q)$ was also clear to Gauss.

3.6. Generalizations and Hensel's Lemma

In the remaining nine articles, Gauss goes on to indicate generalizations of his investigations in different directions.

§ 367. First, he says that analogous theorems hold for composite ν:[81]

> Although we have restricted ourselves here to the case where ν is a prime number, however, if ν is composite, analogous theorems can be established without much effort, which, for the sake of brevity, we cannot discuss now in more detail.[82]

[78] See [Gauss 1863b], § 366, p. 234: *Haec igitur est tertia theorematis fundamentalis Capitis IV completa demonstratio, eo magis attentione digna, quod principia, e quibus est petita, ab iis quibus ad priores usi sumus, prorsus sunt diversa. At ex eodem hoc fonte, sed via opposita quartam deducamus.*

[79] See Gauss's 1817 paper "Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et amplificationes novae" in [Gauss 1863b], pp. 55–59; cf. [Maser 1889], pp. 501–505.

[80] See [Frei 1994].

[81] Cf. [Gauss 1796–1814], entry 77 and 78 (August 31, September 4, 1797)

[82] See [Gauss 1863b], § 367, p. 235: *Quamvis ad casum, ubi ν est numerus primus, hic nos retrinxerimus, tamen etiam, si ν sit compositus, theoremata analoga haud magno negotio*

Then Gauss starts to prepare a proof of a higher reciprocity law by means of periods of arbitrary length. He first considers a prime q of the form $q = 3t + 1$ and constructs periods of length $\frac{q-1}{3}$ in $\mathbf{F}_p(\zeta_q)$, cf. [Gauss 1796–1814], entry 39 (October 1, 1796):

> It would not be difficult for us to enrich this Chapter with many other observations, if the limits imposed on us did not forbid it. For those who want to advance further, these principles can at least indicate the way.[83]

§ 368–369. After this he starts studying the case where $P(x)$ in $\mathbf{F}_p[x]$ has multiple roots.[84] He first proves:

Theorem 9. $P(x)$ in $\mathbf{F}_p[x]$ has no multiple roots, if $P(x)$ and its derivative $P'(x)$ have no common non-trivial factor in $\mathbf{F}_p[x]$.

He says and shows that this is done in the same way as for polynomials (with rational or real coefficients).

§ 373–375. Next, he opens up another important chapter, the study of the case where the modulus p^k is a power of a prime p.[85] Gauss says that this case not only merits attention in itself, but also in order to remove doubts related to other arguments,[86] referring to articles he planned to include later in the manuscript. We shall see in § 374 that these "doubts" refer to the difficult problem of ramification, namely the problem of multiple roots, a subject Gauss intended to study in more detail later in the manuscript.

As a preparation he proves what we may interpret as a version of Hensel's Lemma, cf. [Gauss 1796–1814], entry 79 (September 9, 1797). He states:

Theorem 10. There is a factorization of a polynomial $P(x)$ mod p^k for any $k \geq 0$, once a factorization of $P(x)$ is known mod p, under the hypothesis that the factors of $P(x)$ are relatively prime mod p.

Gauss shows explicitly how to pass from a factorization $P(x) \equiv Q(x)R(x)$ mod p to a factorization $P(x) \equiv Q'(x)R'(x)$ mod p^2, such that the degrees of $P(x)$ and $Q(x)$ are equal to the degrees of $P'(x)$ and $Q'(x)$ respectively. Then he shows more generally how to pass from a factorization mod p^m to a factorization mod p^{m+k} for $0 < k < m + 1$. These steps are done with the help of § 336 (Bezout's theorem). He thus obtains a factorization modulo all powers $p^3, p^4, \ldots$ analogous to the factorization mod p.[87]

§ 374. Gauss goes on by saying:

determinari possunt, quod fusius exponere brevitatis gratia nunc non licet.

[83] See [Gauss 1863b], § 367, p. 235: *Non difficile nobis foret hoc Caput multis aliis observationibus locupletare, nisi limites, intra quos restringi oportet, vetarent. Iis qui ulterius progredi amant, haec principia viam saltem addigitare poterunt.*

[84] Cf. [Gauss 1796–1814], entry 68 (July 1, 1797).

[85] Cf. [Gauss 1796–1814], entry 77 and 78 (August 31, and September 4, 1797).

[86] See [Gauss 1863b], p. 237: *Praesertim vero hic ille casus attentione dignus est, ubi modulus est numeri primi potestas, tum per se tum quod ad aliqua dubia removenda (§.§...) necessarius sit.*

[87] The construction is essentially identical with the one given by Hensel in [Hensel 1904], § 4, pp. 80–81.

> From this one sees that if the function X does not have equal factors with respect to the modulus p, it can be decomposed into factors mod p^k in a similar way as mod p. But if X has equal factors, then things get much more complicated and, even from the preceding principles, they cannot be extracted in a straightforward way. For this reason, since we cannot communicate everything pertinent to this subject, we shall consider only a single case, the one which occurs most often and which requires clarification in order to resolve certain doubts in the preceding. That is where only equal factors of dimension one will be considered. This case can also be applied in an appropriate way to find the roots of congruences. We shall treat this subject in a general way on another occasion.[88]

§ 375. In the last article, Gauss sets out to study this very case: If $P(x) \equiv Q(x)(x-a)^m$ mod p, where $Q(x)$ is prime to $(x-a)$, to find all factors of $P(x)$ of degree one which are congruent to $(x-a)$ mod p and congruent to $P(x)$ modulo all powers of p,[89] whereby $(x-a)$ is not a divisor of $P(x)$. But after having made a linear transformation and having started to develop a linear factor modulo p^2 and modulo p^3 to obtain $x-a+\alpha p+\beta p^2$, he stops his pen after a few lines in the middle of his exposition, indeed in the middle of a formula. According to what Gauss says in § 374, he encountered serious obstacles related to the problem of multiple factors. Notes from his mathematical diary can give us an idea of the direction in which Gauss was looking for a solution to these problems.

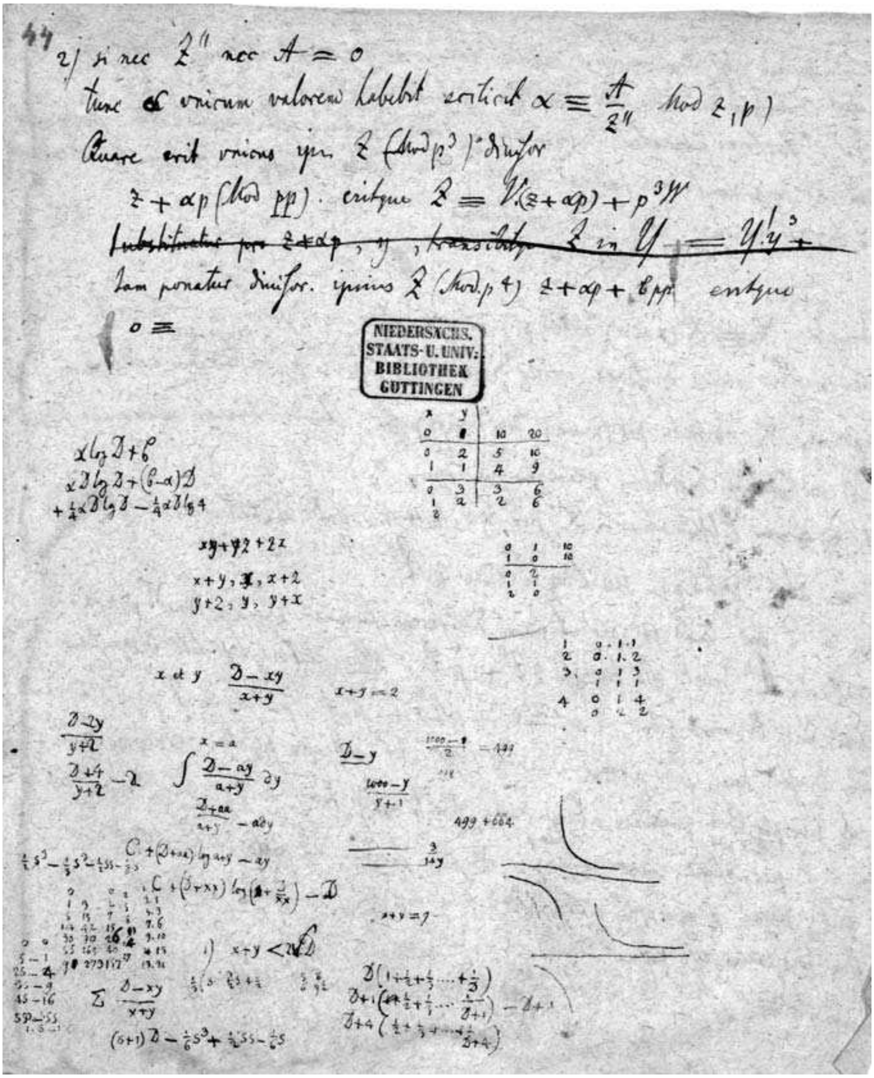
4. Gauss's Mathematical Diary and the *Disquisitiones Generales de Congruentiis*

We have often referred to what we consider as being the corresponding entries in Gauss's mathematical diary [Gauss 1796-1814]. These entries shed some more light on the *Disquisitiones generales de congruentiis* and allow us to gain a deeper insight into Gauss's theory of polynomials modulo a prime number p. They also put us in a position to watch closely how Gauss gradually arrived at his remarkable discoveries in the theory of polynomials and how these relate to his other discoveries connected with them. Our analysis of the *Disquisitiones generales de congruentiis* will also allow us on the other hand to get a better understanding of the diary and to interpret several entries that have not been correctly understood up to now.[90]

[88] See [Gauss 1863b], § 374, p. 239: *Ex his perspicitur, si functio X aequales non habeat divisores secundum modulum p, eam secundum modulum p^k similiter in factores discerpi posse, uti secundum modulum p. At si X divisores aequales habeat, res fit multo magis complicata neque adeo ex principiis praecedentibus prorsus exhauriri potest. Quare quum quae huc pertineant cuncta communicare non possimus, unicum casum tantummodo considerabimus, qui plurimum occurit cuiusque enodatio ad quaedam in praecedentibus dubia solvenda requiritur. Hic est, si factores aequales unius dimensionis tantum respiciantur. Hic proprie etiam ad congruentiarum radices inveniendas adhiberi potest. Generaliter alia occasione hanc rem pertractabimus.*

[89] We denote by $P(x)$ and $Q(x)$ what Gauss denotes by X and X' – see [Gauss 1863b], p. 239: *desiderantur omnes divisores unius dimensionis huic $x-a$ secundum modulum p congrui ipsius X secundum modulos pp, p^3 etc.*

[90] The original Latin text together with a facsimile and a German translation can be found in



44

2) si nec Z'' nec $A = 0$

tunc α unicum valorem habebit scilicet $\alpha \equiv \frac{A}{Z''}$ (Mod z, p)

Quare erit unicus ips. Z (Mod p^3) divisor

$z + \alpha p$ (Mod pp). eritque $Z = V.(z + \alpha p) + p^3 W$

~~Substituatur pro $z+\alpha p$, y, transibitque Z in $Y = Y'.y^3 +$~~

Iam ponatur divisor ipsius Z (Mod p^4) $z + \alpha p + \beta pp$ eritque

$0 \equiv$

x y
0 1 | 10 20
0 2 | 5 10
1 1 | 4 9
0 3 | 3 6
1 2 | 2 6
2

$\alpha \lg \mathfrak{Z} + \beta$

$\alpha \mathfrak{Z} \lg \mathfrak{Z} + (\beta - \alpha)\mathfrak{Z}$

$+ \frac{1}{4}\alpha \mathfrak{Z} \lg \mathfrak{Z} - \frac{1}{4}\alpha \mathfrak{Z} \lg 4$

$xy + yz + zx$

$x + y, z, x + z$

$y + z, y, y + x$

0 1 10
1 0 10
0 2
1 1
2 0

1 0.1.1
2 0.1.2
3. 0 1 3
1 1 1
4 0 1 4
0 2 2

x et y $\frac{\mathfrak{Z} - xy}{x + y}$ $x + y = 2$

$\frac{\mathfrak{Z} - 2y}{y + 2}$

$\frac{\mathfrak{Z} + 4}{y + 2} - 2$ $\int^{x = a} \frac{\mathfrak{Z} - ay}{a + y} \partial y$

$\frac{\mathfrak{Z} + aa}{a + y} - a \partial y$

$\mathfrak{Z} - y$ $\frac{1000 - 1}{2} = 499$

$\frac{1000 - y}{y + 1}$

$499 + 664$

$\frac{3}{3 + y}$

$\frac{1}{6}s^3 - \frac{1}{3}s^2 - \frac{1}{2}ss - \frac{1}{3}s$ $C + (\mathfrak{Z} + aa)\lg a + y - ay$

$C + (\mathfrak{Z} + xx)\lg\left(1 + \frac{\mathfrak{Z}}{xx}\right) - \mathfrak{Z}$

$x + y = 7$

1) $x + y < 2\sqrt{\mathfrak{Z}}$

$\Sigma \frac{\mathfrak{Z} - xy}{x + y}$

$(s + 1)\mathfrak{Z} - \frac{1}{6}s^3 + \frac{1}{2}ss - \frac{1}{3}s$

$\mathfrak{Z}\left(1 + \frac{1}{2} + \frac{1}{3} \ldots + \frac{1}{\mathfrak{Z}}\right)$

$\mathfrak{Z} + 1\left(\frac{1}{2} + \frac{1}{3} \cdots \frac{1}{\mathfrak{Z} + 1}\right) - \mathfrak{Z} + 1$

$\mathfrak{Z} + 4\left(\frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{\mathfrak{Z} + 4}\right)$

Fig. II.4B. Last page of Gauss's manuscript of the *Disquisitiones generales de congruentiis*. (Courtesy of NSUB Göttingen)

[Gauss 1796–1814/1985], an English translation in [Gauss 1796–1814/1984]. However, we shall have to correct a few errors in both translations. For lack of space, we shall only present a few significant examples of our findings here. For more details we refer to [Frei 2001] and a future publication.

The starting point of Gauss's investigations on $\mathbf{F}_p[x]$ seems to be the study of the cyclotomic equation $x^m \equiv 1$ modulo a prime number p, where m is a prime or a power of a prime. A manuscript by Gauss entitled *Solutio congruentiae* $X^m - 1 \equiv 0$. *Analysis residuorum. Caput Sextum. Pars Prior* (Solution of the Congruence $X^m - 1 \equiv 0$. The Theory of Residues. Chapter Six. Part One)[91] is published (posthumously) in the second volume of Gauss's *Werke*, just before the manuscript *Disquisitiones generales de congruentiis. Analysis residuorum: Caput Octavum.* In the former manuscript, which we shall henceforth refer to as *Solutio*, Gauss studies in detail how to find the roots of the cyclotomic polynomial $X^m - 1$ modulo a prime number p in terms of Gaussian periods, all expressed by means of a primitive root mod p. That these investigations seem to be the starting point for Gauss's study of the ring $\mathbf{F}_p[x]$ leading to a new proof of the quadratic reciprocity law is also indicated by Gauss's first entry in his diary related to this subject, the theory of polynomials modulo a prime number p. It is entry 22, made on August 3, 1796:[92]

> $a^{2^n \mp 1}\ {}^{(p)} \equiv 1$ can always be solved by a power.[93]

In his commentary in [Gauss 1917], Bachmann conjectured that Gauss meant by this that he discovered how to factor the polynomial $X^m - 1$ modulo a prime number q into irreducible polynomials, if $m = p$ is a prime number of the form $p = 2^n \mp 1$ for some n. Bachmann refers to the last section of the *Solutio*, § 252, where Gauss treats the example with the exponent $p = 31 = 2^5 - 1$ and the prime modulus $q = 331$.[94] In that same § 252, Gauss says that he will add this example in order to clarify his general theory on the roots of $X^m - 1 \equiv 0$ modulo a prime q, and he remarks that much more will be said later on the solutions of $X^m - 1 \equiv 0$ mod q.

In addition, we conjecture that *in potestate* means that $a^p \equiv 1$ mod q always has a solution which is a $(q^m - 1)^{\text{th}}$ root of unity over $\mathbf{F}_q$ for some m, that is, a power of a primitive $(q^m - 1)^{\text{th}}$ root of unity mod q. This would correspond to Theorem 4 in our section 3 (§§ 351–351 in the *Disquisitiones generales de congruentiis*).

That Bachmann is very probably on the right track is confirmed by a commentary made by Schlesinger in [Gauss 1917] who pointed out that the entries 22, 23, 25, 26, 27 must refer to the same topic since they are all underlined in red. Indeed, all these entries deal with the theory of polynomials over a finite field of constants, as treated in Gauss's *Disquisitiones generales de congruentiis*. There, in addition, we find in § 360 the example with $m = 63 = 2^6 - 1$ and $q = 13$, by which Gauss illustrates how to determine for each degree the number of irreducible polynomials $P(x)$ of $X^m - 1$

[91] See [Gauss 1863b/1876], pp. 199–211 or [Maser 1889], pp. 589–601.

[92] A lot of confusion seems to surround this entry 22 of Gauss's diary. The editors of [Gauss 1796–1814/1985] say in their commentary *Unklarer Sachverhalt* (unclear state of affairs), but they write $a^{2n \mp 1} \equiv 1\ (p)$ instead of $a^{2^n \mp 1}\ {}^{(p)} \equiv 1$. J. Gray in [Gauss 1796–1814/1984] calls this entry "obscure", but he writes $a^{2^{n \mp 1}}\ {}^{(p)} \equiv 1$ instead of $a^{2^n \mp 1}\ {}^{(p)} \equiv 1$. In neither of these editions are the words *in potestate* translated.

[93] $a^{2^n \mp 1}\ {}^{(p)} \equiv 1$ *semper solvere in potestate.*

[94] [Gauss 1863b/1876], p. 209. Here Gauss uses the notation $n = 31$ and $p = 331$ instead.

modulo a prime number q. And in § 364, Gauss takes the example $m = 15 = 2^4 - 1$ and the prime modulus $q = 17$ in order to illustrate how to determine explicitly all the irreducible polynomials $P(x)$ of $X^m - 1 \bmod q$, although in both cases m is not a prime.[95] These two examples are also in agreement with what Gauss had promised about $X^m - 1 \bmod q$ in § 252 of the *Solutio*. All these examples clearly seem to confirm Bachmann's conjecture as well as our conjecture saying that entry 22 corresponds to Theorem 4 above.

From his method of factoring the polynomial $X^m - 1$ modulo a prime number q by means of periods as described by Gauss in the *Solutio*, we can see why Gauss first investigated the case where m is a prime p of the form $m = p = 2^n + 1$. In this case, $\lambda = p - 1$ becomes a power of 2: $\lambda = p - 1 = 2^n$. Hence $X^m - 1 \equiv 0 \bmod q$ is solved successively by quadratic equations, that is, by periods which are all square roots. The method is completely analogous to the one developed by Gauss in the *Disquisitiones Arithmeticae*, where Gauss showed in art. 354 that $X^{17} - 1$ can be solved successively by square roots, from where he concludes in art. 365 that the regular polygon of 17 sides can be constructed with straightedge and compass.[96] It looks as if Gauss, who always calculated typical examples first, had been guided by the examples $m = 63 = 2^6 - 1$, $q = 13$ and $m = 15 = 2^4 - 1$, $q = 17$ in order to find the general theory of factorization of $X^m - 1 \equiv 0 \bmod q$ as developed in the *Disquisitiones generales de congruentiis*.

After the reference to his third proof of the quadratic reciprocity law in entry 23 (August 13, 1796) and entry 25 (August 16, 1796), Gauss mentions an essential tool for his investigations, namely the discovery of the *Frobenius automorphism*, as treated in § 350 of the *Disquisitiones generales de congruentiis*. He notes this as follows in entry 26, dated August 18,1796:

> $(a^p) \equiv (a)$ mod. p, a the root of an arbitrary irrational equation.[97]

Here (a) stands for a rational expression in a, that is an element in $\mathbf{F}_p(a)$, and (a^p) for the image of (a) under the map $a \mapsto a^p$. Thus (a) and (a^p) both are roots of the same irreducible polynomial over $\mathbf{F}_p$.

On August 21, 1796, Gauss discovered the algebraic relations between the coefficients of a polynomial $P(x)$ and of the polynomial $P^{(t)}(x)$ having as roots the t^{th} powers of the roots of $P(x)$. This refers to what we have called Theorem 1 in our section 3, i.e., the problem formulated and solved in § 348 of the *Disquisitiones generales de congruentiis*. Indeed, Gauss writes in entry 28, dated August 21, 1796:

[95] In the discussion of § 364, the notation is different: in particular, ν is what is m here, p the prime modulus (here q) and m denotes the smallest positive integer such that $p^m \equiv 1 \bmod \nu$. In the German translation [Maser 1889], Maser writes $m = 5$ when dealing with the example $\nu = 15$ and a prime modulus 17. This should be corrected to $m = 4$.

[96] In fact, it seems that Gauss at first only wrote $a^{2^n+1}\ (p) \equiv 1$ in his diary and then added the minus sign "$-$" on top of the plus sign "$+$", when he realized that his method for congruences was also valid in the case of $m = p = 2^n - 1$ and even in the case of an arbitrary prime p, or in the still more general case where p is a power of a prime t: $p = t^\nu$. Indeed, in the *Solutio*, Gauss treats this general case.

[97] $(a^p) \equiv (a)$ *mod. p, a radix aequationis cuiusvis quomodocunque irrationalis.*

> The sums of powers of the roots of a given equation are expressed by a very simple law in terms of the coefficients of the equation (with other geometric [matters] in the Exercitationes).[98]

Here, Gauss was not merely referring to Newton's formulae which he used in his first proof of the theorem in § 348 of the *Disquisitiones generales de congruentiis* (Theorem 1 above). He had already discovered the *explicit* form of Newton's or Girard-Waring's formulae in entry 6 on May 23, 1796. Because of this, and in view of entry 27, entry 28 implicitly means that he had discovered more, namely the theorem itself.

Finally, on September 2, 1796, Gauss obtained most of his third proof (Proof VII) of the quadratic reciprocity law. He writes in entry 30:

> Except for some details, I have happily attained the goal, namely if $p^n \equiv 1 \pmod{\pi}$, then $x^\pi - 1$ will be composed of factors not exceeding the degree n and *therefore the conditional equation will become solvable*; from there I have deduced two proofs of the golden theorem [i.e., of the quadratic reciprocity law].[99]

By "conditional equation," Gauss means what is called "auxiliary equation" in § 365 of the *Disquisitiones generales de congruentiis* and also in entry 68 of the diary, namely an equation whose roots are the periods of length e associated to $X^\pi - 1$, for a divisor e of $\pi - 1$. These periods and their equation are treated in detail in the D.A., art. 339–356, in particular art. 342–343, where they are used to solve $X^\pi - 1$, that is, to factor $X^\pi - 1$ into smaller factors. How this is done for $X^\pi - 1$ over $\mathbf{F}_p$ is indicated in § 362 and § 363 of the *Disquisitiones generales de congruentiis*, in which Gauss refers to Chapter Six for the details. We have seen earlier that this Chapter Six of the *Disquisitiones generales de congruentiis* went into Section Seven of the *Disquisitiones Arithmeticae*. The "details" mentioned by Gauss which caused him some trouble are also mentioned at the end of § 363 of the *Disquisitiones generales de congruentiis* and again in entry 68 of the diary. They refer to the case where the auxiliary equation has multiple factors mod p.

The entries of the following 10 and a half months show Gauss mostly occupied with the theory of equations, the fundamental theorem of algebra, the theory of elliptic integrals and the division of the lemniscate.

Gauss was continuing to think about general congruences, as is testified by entry 68, dated July 21, 1797, where Gauss announces that he now knows, after having worked hard on the problem for a long time, how to handle the case of multiple factors of the auxiliary equation of $X^m - 1 \equiv 0$ modulo a prime p by going to higher and higher powers of p, that is, by p-adic methods. It is in this context that he proved Hensel's lemma, as we have seen in §§ 373-374 of the *Disquisitiones generales de congruentiis*. Gauss writes:

[98] *Exprimuntur potestates radicum aequationis propositae aggregatae per coefficientes aequationis lege perquam simplici (cum aliis quibusdam geometr. in Exerci.).*

[99] *Minutiis quibusdam exceptis feliciter scopum attigi scil[icet] si* $p^n \equiv 1 \pmod{\pi}$, *fore* $x^\pi - 1$ *compositum e factoribus gradum n non excedentibus et* proin aequationem conditionalem fore solubilem*; unde duas theor[ematis] aurei demonstr[ationes] deduxi.*

> We have overcome the particular case of the solution of the congruence $x^n - 1 \equiv 0$ (namely when the auxiliary congruence has equal roots), which troubled us for so long, with most happy success, via the solution of congruences when the modulus is a *power* of a prime number.[100]

A month later, after having made a deeper study of the auxiliary equations and the periods related to them (entries [69], 70, 71, 73, 74), Gauss made several discoveries about general congruences, some of which we have already encountered in the *Disquisitiones generales de congruentiis*. On August 26, 1797, he notes in entry 75 of the diary that he had found the number of irreducible polynomials of any given degree m in $\mathbf{F}_p[x]$ by an easy method:

> I have found the number of prime functions [i.e. irreducible polynomials] by a most simple analysis.[101]

We have seen in §§ 342-347 of the *Disquisitiones generales de congruentiis* that Gauss first obtained this number by induction and then he found an explicit formula for it.

Four days later Gauss discovered the central rôle played by the *Frobenius automorphism* in the study of the sub-fields of $\mathbf{F}_{p^\mu}$. The importance of this discovery is emphasized by the fact that Gauss formulates it as a *Theorem* and underlines the word "Theorem." It is the theorem stated and proved in § 356 of the *Disquisitiones generales de congruentiis* which says, translated into modern terms, that if ϑ is a root of the irreducible polynomial $P(x) = 1 + ax + bx^2 + \cdots + mx^\mu$, and if $Q(\vartheta)$ is a rational expression of ϑ which is invariant under the Frobenius automorphism $\sigma : x \mapsto x^p$ of $\mathbf{F}_p(\vartheta)/\mathbf{F}_p$, e.g. $Q(x) = x + x^p + x^{p^2} + \cdots + x^{p^{\mu-1}}$, then $Q(\vartheta)$ is equal to some element $-d$ in the ground field $\mathbf{F}_p$. This is expressed by Gauss as follows in entry 76, dated August 30, 1797:

> Theorem: If $1 + ax + bx^2 + \cdots + mx^\mu$ is a prime function [i.e., an irreducible polynomial] with respect to the modulus p, then $d + x + x^p + x^{p^2} + \cdots + x^{p^{\mu-1}}$ is divisible by this function with respect to this modulus, etc. etc.[102]

In entry 77, dated August 31, 1797, i.e., the day after, Gauss goes on by noting that the preceding theorem is proved and that he is now advancing into new territory by introducing moduli which are the powers of a prime number. He writes:

> This is proved, and the way to many greater things is paved by the introduction of multiple moduli [i.e. moduli which are the powers of a prime number].[103]

[100] *Casum singularem solutionis congruentiae $x^n - 1 \equiv 0$ (scilicet quando cong[ruentia] aux[iliaris] radices aequales habet), qui tam diu nos vexavit, felicissimo succesu vicimus, ex congruentiarum solutione, si modulus est numeri primi* potestas.

[101] *Functionum primarum multitudinem per analysin simplicissimam erui.*

[102] Theorema: *Si $1 + ax + bx^2 + \cdots + mx^\mu$ est functio secundum modulum p prima, erit: $d + x + x^p + x^{p^2} + \cdots + x^{p^{\mu-1}}$ per hanc f[un]ct[io]nem s[e]c[un]d[u]m hunc modulum divisibilis etc. etc.* E. Schuhmann in [Gauss 1796–1814/1985] erroneously translates *secundum modulum* by "zweiter Modul" instead of "nach dem Modul." The same error is repeated in entry 79.

[103] *Demonstratum, viaque ad multa maiora per introd[uctionem] modulorum multiplicium*

This means that Gauss had discovered a way to extend the key theorem in entry 76 to moduli which are the powers of a prime number. Our discussion of §§ 373–375 (in our section 3.6 above) strongly suggests that the "way" he had discovered it was some kind of p-adic method; it thus looks as if Gauss had some concept about the key role of the Frobenius automorphism in a p-adic extension. In fact, entry 76 corresponds to what Gauss says in § 372 of the *Disquisitiones generales de congruentiis*:

> We proceed to another chapter, namely to the consideration of congruences when the modulus is not a prime number, as we have always supposed up to here. Indeed, in particular that case deserves here the attention where the modulus is the power of a prime number, on the one hand in itself, on the other hand because it is necessary in order to remove some doubts (§.§....).[104]

The same "doubts" appear also at the end of § 363 of the *Disquisitiones generales de congruentiis*, where they refer to the difficulties that arise when an auxiliary equation of the congruence $X^m - 1 \equiv 0 \bmod p$, having as its roots Gaussian periods belonging to this congruence, has multiple factors. They appear again in § 374 – Gauss announces here that he is going to remove the doubts concerning the problem of multiple factors by means of his method. Finally Gauss notes, still on the same topic, in entry 78, dated September 4, 1797, that the result mentioned in entry 77, i.e., the proof of the key theorem of entry 76 of the August 30, is now generalized to any modulus:

> [The result of] August 31 more generally is adapted to arbitrary moduli.[105]

And in entry 79 of September 9, 1797, Gauss writes:

> I have uncovered principles by which the resolution of congruences with respect to multiple moduli is reduced to congruences with respect to a linear modulus.[106]

We read this as saying that he could reduce the resolution of congruences with respect to a prime power modulus, to congruences with respect to a prime modulus. This corresponds to what Gauss is treating in the §§ 373–375 of the *Disquisitiones*

strata. E. Schuhmann in [Gauss 1796–1814/1985] translates "modulorum multiplicium" by "zusammengesetzter Moduln" (of composite moduli). But this is not correct and misses the important point that the moduli are just powers of a prime number. Arbitrary composite moduli appear only in entry 78 as "quosvis modulos." The same inappropriate translation is given in entry 79.

[104] See [Gauss 1863b/1876], p. 237: *Progredimur ad aliud caput, scilicet ad considerationem congruentiarum, si modulus non est numerus primus, uti hactenus semper supposuimus. Praesertim vero hic ille casus attentione dignus est, ubi modulus est numeri primi potestas, tum per se tum quod ad aliqua dubia removenda (§.§....) necessarius sit.*

[105] *Aug. 31. generalius ad quosvis modulos adaptatur.* (Gauss actually wrote "Aug. 1." instead of "Aug. 31" – see the commentary made by Bachmann in [Gauss 1917], p. 523. The editors of [Gauss 1796–1814/1985] write 30. Aug. This reading still refers to the same theorem, namely the key theorem in entry 76.)

[106] *Principia detexi, ad quae congruentiarum secundum modulos multiplices resolutio ad congruentias secundum modulum linearem reducitur.* See our footnotes above concerning the German translations of entry 76 and entry 77 in [Gauss 1796–1814/1985].

generales de congruentiis, where he starts to handle the case where an auxiliary equation of the congruence $X^m - 1 \equiv 0 \bmod p$ has multiple factors.

At this point Gauss seems again to have met a situation to which he refers in a letter to Wilhelm Olbers, dated February 19, 1826:

> In my scientific life I have often encountered the case where, due to external circumstances, I have put aside investigations that were not successful, which however were successful later, e.g. my proof of the main theorem of the theory of equations [i.e. the fundamental theorem of algebra] published in volume 3 of our Commentationes; but I had to make a 10fold effort just to get again to the point, where I had been earlier more than once.[107]

5. The Genesis of Gauss's Theory of Function Fields over a Finite Field

Our analysis of Gauss's *Disquisitiones generales de congruentiis* and of Gauss's diary permits us to describe the gradual evolution of Gauss's investigations on function fields over a finite field. Gauss's starting point for parts of his work on number theory and on algebra was the study of the congruence $x^m - 1 \equiv 0$ modulo a prime number p, in particular the factorization of $x^m - 1 \bmod p$. It led him to his theory of function fields over a finite field presented in the *Disquisitiones generales de congruentiis*, to parts of his theory of congruences as it is presented in the first four Sections of the D.A., to the theory of cyclotomy presented in the last one, and to Gauss's doctoral thesis on the Fundamental Theorem of Algebra. As said above, a basic result for the beginning of these investigations was Lagrange's theorem on the number of roots of a polynomial $P(x) \bmod p$, a particular case of which, where $P(x) = x^m - 1$, had been treated by Euler – see our section 2.1, as well as § 338 of the *Disquisitiones generales de congruentiis*.

A first important discovery about polynomials over a finite field $\mathbf{F}_p$ was the theorem that every root of a polynomial over $\mathbf{F}_p$ of degree m, and hence of any degree d which divides m, can be viewed as being contained in the same extension field $\mathbf{C}_m$, that of the $p^m - 1^{\text{th}}$ roots of unity over $\mathbf{F}_p$ (entry 22 and §§ 351–353 of the *Disquisitiones generales de congruentiis*). At the same time Gauss discovered how the polynomial $x^m - 1$ could be decomposed step by step via auxiliary polynomials whose roots are Gaussian periods belonging to $x^m - 1$. This applies to $x^m - 1$ over $\mathbf{Q}$ in the same way as it applies to $x^m - 1$ over $\mathbf{F}_p$ (entry 23 and also entry 1; cf. entry 11). The case $x^m - 1$ over $\mathbf{Q}$ is treated in detail in the D.A. when m is an odd prime number q. At the same time, Gauss discovered that the quadratic Gaussian sums of length $\frac{q-1}{2}$ furnish a third proof of the quadratic reciprocity law. This led to the idea that Gaussian sums of length $\frac{q-1}{e}$, where e divides $q - 1$, might furnish a proof for

[107] [Gauss 1796-1814], p. 570: *Ich habe in meinem wissenschaftlichen Leben öfters den Fall gehabt, dass ich durch äussere Umstände veranlasst, Beschäftigungen, die nicht glückten, bei Seite legte, und die allerdings später glückten, z.B. mein Beweis für das Haupttheorem der Lehre von den Gleichungen, der im 3. Bande unsrer Comment[ationes] steht; aber ich habe nachher die 10fache Anstrengung gehabt, nur erst wieder auf den Punkt zu kommen, auf dem ich schon früher mehr als einmahl gewesen war.*

an e^{th} power reciprocity law. The crucial part consisted in constructing explicitly the corresponding auxiliary equation of degree e and in determining whether it is solvable mod p or not. Only a few days later, Gauss discovered an essential tool for finding such an equation and for constructing the factors of $x^m - 1$, and more generally the factors of any polynomial of degree m over $\mathbf{F}_p$. The essential tool is given by what we now call the Frobenius automorphism over $\mathbf{F}_p$ (entries 23, 25, 26, 28 and 30; also entry 6, 34, and 35). All these discoveries were made within a very short period between August 3 and September 2, 1796.

In the next period, between September 2, 1796 and July 21, 1797, Gauss went on to look for an analogous proof of a cubic reciprocity law and to study the case where an auxiliary equation has multiple factors. The second problem could not be solved immediately; Gauss put it aside and concentrated on the first problem (entries 39, [47], 55, 67). This led to a deeper algebraic study of cyclotomy, i.e., of the Galois theory of $x^m - 1$ over $\mathbf{Q}$, and as a consequence also over $\mathbf{F}_p$ (entries 34, 35, 36, 37, 38, 40). In particular it led him to investigate the solution of $x^m - 1$ by pure equations (entries 37, 38, 41, 55) and to the corresponding generalization to arbitrary polynomials and equations over these domains (entries 34, 35, 36, 37, 41, 42, 43). This also gave rise to the study of the Fundamental Theorem of Algebra (entry 80). In addition, other problems related to the theory of cyclotomy were tackled, such as the theory of the lemniscate and of elliptic functions as generalizations of the theory of cyclotomy (entries 32, 33, 48, 50, 51, 53, 54, 59, 60, 61, 62, 63). On July 17, 1797, Gauss came back to the study of the solution of $x^m - 1$ by means of pure equations related to the first unsolved problem (entries 65, 66). Three days later he settled the question of the auxiliary equation of degree 3, which was an important step towards a cubic reciprocity law (entry 67). The day after, on July 21, 1797, he wrote that he had solved the problem of multiple factors via congruences modulo powers of a prime number, that is by means of a p-adic method (entry 68).

In the next period between July 21 and September 9, 1797, Gauss analysed more closely the auxiliary equations of $x^m - 1$ (entries [69], 70, 71, 73, 74) and the crucial role played by the Frobenius automorphism for the study of these auxiliary equations. It led to what amounts to the determination of the structure of the finite algebraic field extensions of a finite prime field (entry 76) as well as to some sort of p-adic extension thereof (entries 77 and 78) for which Gauss proved a version of Hensel's Lemma (entry 79). The following entry 80 from October 1797, where Gauss noted that he had proved the Fundamental Theorem of Algebra by a genuine method, might indicate where Gauss expected to get some help for the solution of the problem of multiple factors. It looks almost as if Gauss thought of some kind of algebraic closure of finite fields or some kind of p-adic version of the complex numbers. Unfortunately he did not leave us more details of these ideas than what he started to treat in the §§ 373–375 of the *Disquisitiones generales de congruentiis*. After entry 80, Gauss occasionally continued to work on higher reciprocity laws, on the Fundamental Theorem of Algebra and on the theory of cyclotomy, but he never came back to the theory of polynomials over a finite field.

Acknowledgements

This paper is a by-product of a project, jointly with Peter Roquette, on the Artin-Hasse correspondence and on the work of Helmut Hasse. It is a pleasure to thank Peter Roquette for his hospitality, his support and for the many interesting discussions. My thanks also go to the University of Heidelberg and to the Deutsche Forschungsgemeinschaft for their generous practical and financial support. I would also like to thank Urs Stammbach and Franz Lemmermeyer for their comments and suggestions.

References

ARIGONI, Coralia. 1984. *Sur le développement des nombres p-adiques.* Diplôme, direc. Günther Frei. ETH Zürich. 61 p.

ARTIN, Emil. 1924. Quadratische Körper im Gebiete der höheren Kongruenzen I, II. *Mathematische Zeitschrift* 19, 153–246. Repr. in *Collected Papers*, ed. S. Lang, J.T. Tate, pp. 1–94. New York, Berlin, etc.: Springer, 1965.

BACHMANN, Paul. 1911. *Über Gauß' zahlentheoretische Arbeiten.* Leipzig: Teubner. Repr. and slightly revised in [Gauss 1922–1933], Abhandlung 1.

BIERMANN, Kurt Reinhard. 1988. *Die Mathematik und ihre Dozenten an der Berliner Universität 1810–1933. Stationen auf dem Wege eines mathematischen Zentrums von Weltgeltung.* 2$^{\text{nd}}$ rev. ed. Berlin: Akademie-Verlag.

DEDEKIND, Richard. 1857a. Abriß einer Theorie der höheren Kongruenzen in bezug auf einen reellen Primzahl-Modulus. *Journal für die reine und angewandte Mathematik* 54, 1–26. Repr. in [Dedekind 1930–1932], vol. 1, pp. 40–67.

———. 1857b. Beweis für die Irreduktibilität der Kreisteilungs-Gleichungen. *Journal für die reine und angewandte Mathematik* 54, 27–30. Repr. in [Dedekind 1930–1932], vol. 1, pp. 68–71.

———. 1878. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen* 23, 1–23. Repr. in [Dedekind 1930–1932], vol. 1, pp. 202–232.

———. 1930–1932. *Gesammelte mathematische Werke*, ed. R. Fricke, E. Noether, O. Ore. 3 vols. Braunschweig: Vieweg.

———. 1985. *Vorlesung über Differential- und Integralrechnung 1861/62 in einer Mitschrift von Heinrich Bechtold*, ed. M.-A. Knus, W. Scharlau. Braunschweig, Wiesbaden: Vieweg.

DEDEKIND, Richard, WEBER, Heinrich. 1882. Theorie der algebraischen Funktionen einer Veränderlichen. *Journal für die reine und angewandte Mathematik* 92, 181–290. Repr. in [Dedekind 1930–1932], vol. 1, pp. 238–350.

DIEUDONNÉ, Jean. 1985. *History of Algebraic Geometry.* Monterey, Cal.: Wadsworth. Originally published as *Cours de géométrie algébrique I*. Paris: Presses Universitaires de France, 1974.

DIRICHLET, Johann Peter Gustav LEJEUNE-. 1842. Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. *Journal für die reine und angewandte Mathematik* 24, 291–371. Repr. in *Werke*, vol. 1, ed. L. Kronecker, pp. 533–618. Berlin: Reimer, 1889.

———. 1863. *Vorlesungen über Zahlentheorie*, ed. R. Dedekind. 1st ed. Braunschweig: Vieweg. 2nd ed., 1871.

EISENSTEIN, Gotthold. 1847. Genaue Untersuchung der unendlichen Doppelproducte, aus welchen die elliptischen Functionen als Quotienten zusammengesetzt sind, und der mit ihnen zusammenhängenden Doppelreihen (als eine neue Begründungsweise der Theorie der elliptischen Functionen, mit besonderer Berücksichtigung ihrer Analogie zu den Kreisfunctionen). *Journal für die reine und angewandte Mathematik* 35, 153–274. Repr. in *Mathematische Werke*, vol. 1, pp. 357–478. New York: Chelsea, 1975.

———. 1850. Über die Irreductibilität und einige andere Eigenschaften der Gleichung, von welcher die Theilung der ganzen Lemniscate abhängt. *Journal für die reine und angewandte Mathematik* 39, 160–179. Repr. in *Mathematische Werke*, vol. 2, pp. 536–555. New York: Chelsea, 1975.

EULER, Leonhard. 1760. Demonstratio theorematis FERMATIANI omnem numerum primum formae $4n + 1$ esse summam duorum quadratorum. *Novi Commentarii Academiae Scientiarum Petropolitanae* 5, 3–13. Repr. in *Opera Omnia, Series Prima* II, ed. F. Rudio, E. 241, pp. 328–337. Leipzig, Berlin: Teubner, 1915.

———. 1774. Demonstrationes circa residua ex divisione potestatum per numeros primos resultantia. *Novi Commentarii Academiae Scientiarum Petropolitanae* 18, 85–135. Repr. in *Opera Omnia, Series Prima* III, ed. F. Rudio, E. 449, pp. 240–281. Leipzig, Berlin: Teubner, 1917.

FREI, Günther. 1994. The Reciprocity Law from Euler to Eisenstein. In *The Intersection of History and Mathematics*, ed. Ch. Sasaki, M. Sugiura, J.W. Dauben, pp. 67–88. Basel: Birkhäuser.

———. 2001. On the Development of the Theory of Function Fields over a Finite Field from Gauss to Dedekind and Artin. Preprint. 62 pages.

———. 2004. On the History of the Artin Reciprocity Law in Abelian Extensions of Algebraic Number Fields: How Artin was led to his Reciprocity Law. In *The Legacy of Niels Henrik Abel (The Abel Bicentennial, Oslo 2002)*, ed. O.A. Laudal, R. Piene, pp. 267–294. Berlin, Heidelberg, etc.: Springer.

GALOIS, Évariste. 1830. Sur la théorie des nombres. *Bulletin des Sciences mathématiques de M. Férussac* 13, 428–435. Repr. in *Œuvres mathématiques*, pp. 15–23. Paris: Gauthier-Villars, 1897.

GAUSS, Carl Friedrich. 1796–1814. Mathematical Diary. Original manuscript in Latin: Handschriftenabteilung Niedersächsische Staats- und Universitätsbibliothek Göttingen, Cod. Ms. Gauß Math. 48 Cim. Ed. (Latin with German annotations): Abdruck des Tagebuchs (Notizenjournals), in [Gauss 1917], pp. 483–575. French annotated transl. by P. Eymard, J.-P. Lafon: Le journal mathématique de Gauss. *Revue d'histoire des sciences et de leurs applications* 9 (1956), 21–51. English commented transl. by J. Gray: A commentary on Gauss's mathematical diary, 1796-1814, with an English translation. *Expositiones Mathematicae* 2 (1984), 97–130. German translation by E. Schuhmann, with a historical introduction by K.-R. Biermann, and annotations by H. Wußing und O. Neumann: *Mathematisches Tagebuch 1796–1814*. 4th ed. Ostwalds Klassiker der exakten Wissenschaften 256. Leipzig: Akademische Verlagsgesellschaft Geest & Portig; Frankfurt a.M., Thun: Harry Deutsch, 1985.

———. 1863a. *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. I, *Disquisitiones arithmeticæ*. Göttingen: Universitäts-Druckerei. 2nd ed., 1876.

———. 1863b. *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. II, *Höhere Arithmetik*. Göttingen: Universitäts-Druckerei. 2nd ed., 1876.

———. 1917. *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. X.1, *Nachtraege zur reinen Mathematik*. Leipzig: Teubner.

———. 1922–1933. *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. X.2, *Abhandlungen ueber Gauss' wissenschaftliche Taetigkeit auf den Gebieten der reinen Mathematik und Mechanik*. Berlin: Springer.

Gauss & Bolyai. 1899. *Briefwechsel zwischen Carl Friedrich Gauss und Wolfgang Bolyai*, ed. F. Schmidt, P. Stäckel. Leipzig: Teubner.

Hasse, Helmut. 1926–1930. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper I; Ia; II. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 35, 1–55; 36, 233–311; Ergänzungsband 6, 1–204.

———. 1933. Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Vorläufige Mitteilung. *Nachrichten Gesellschaft der Wissenschaften Göttingen* 1, Nr. 42, 253–262.

Hensel, Kurt. 1904. Neue Grundlagen der Arithmetik. *Journal für die reine und angewandte Mathematik* 127, 51–84.

Kronecker, Leopold. 1882. Grundzüge einer arithmetischen Theorie der algebraischen Grössen. *Journal für die reine und angewandte Mathematik* 92, 1–122. Repr. in *Werke*, ed. K. Hensel, vol. 2, pp. 237–387. Leipzig: Teubner, 1897; repr. New York: Chelsea, 1968.

Kornblum, Heinrich. 1919. Über die Primfunktionen in einer arithmetischen Progression. *Mathematische Zeitschrift* 5, 100–111.

Kühne, Hermann. 1902. Eine Wechselbeziehung zwischen Functionen mehrerer Unbestimmten, die zu Reciprocitätsgesetzen führt. *Journal für die reine und angewandte Mathematik* 124, 121–133.

———. 1903. Angenäherte Auflösung von Congruenzen nach Primmodulsystemen in Zusammenhang mit den Einheiten gewisser Körper. *Journal für die reine und angewandte Mathematik* 126, 102–115.

Kummer, Ernst Eduard. 1847. Zur Theorie der complexen Zahlen. *Journal für die reine und angewandte Mathematik* 35, 319-326. Repr. in [Kummer 1975], vol. I, pp. 203–210.

———. 1975. *Collected Papers*, ed. A. Weil. 2 vols. Berlin, Heidelberg, New York: Springer.

Lagrange, Joseph-Louis. 1770. Nouvelle méthode pour résoudre les problèmes indéterminés en nombres entiers. *Mémoires de l'Académie Royale des Sciences et Belles-Lettres de Berlin. Année 1768* 24, 181–250. Repr. in *Œuvres*, ed. J.-A. Serret, vol. 2, pp. 655–726. Paris: Gauthier-Villars, 1868.

Maser, Hermann. 1889. *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*. Berlin: Julius Springer.

Merzbach, Uta C. 1981. An Early Version of Gauss's *Disquisitiones Arithmeticae*. In *Mathematical Perspectives*, ed. J. W. Dauben, pp. 167–177. New York: Academic Press.

Roquette, Peter. 2001. Class Field Theory in Characteristic p, its Origin and Development. In *Class Field Theory: Its Centenary and Prospect*, ed. K. Miyake, pp. 549–631. Advanced Studies in Pure Mathematics 30. Tokyo: Mathematical Society of Japan.

———. 2002. The Riemann hypothesis in characteristic p, its origin and development. *Mitteilungen der mathematischen Gesellschaft in Hamburg* 21/2, 79–157.

SCHÖNEMANN, Theodor. 1845. Grundzüge einer allgemeinen Theorie der höheren Congruenzen, deren Modul eine reelle Primzahl ist. *Journal für die reine und angewandte Mathematik* 31, 269–325.

———. 1846. Von denjenigen Moduln, welche Potenzen von Primzahlen sind. *Journal für die reine und angewandte Mathematik* 32, 93–105.

SCHMIDT, Friedrich Karl. 1925. *Allgemeine Körper im Gebiet der höheren Kongruenzen.* Inauguraldissertation zur Erlangung der Doktorwürde. Naturwissenschaftliche Mathematische Fakultät der Universität Freiburg. 52 p.

———. 1926–1927. Zur Zahlentheorie in Körpern der Charakteristik p. Vorläufige Mitteilung. *Sitzungsberichte der Physikalisch-medizinischen Sozietät zu Erlangen* 58/59, 159–172.

———. 1931a. Analytische Zahlentheorie in Körpern der Charakteristik p. *Mathematische Zeitschrift* 33, 1–32.

———. 1931b. Die Theorie der Klassenkörper über einem Körper algebraischer Funktionen in einer Unbestimmten und mit endlichem Koeffizientenbereich. *Sitzungsberichte der Physikalisch-medizinischen Sozietät zu Erlangen* 62, 267–284.

SELLING, Eduard. 1865. Ueber die idealen Primfactoren der complexen Zahlen, welche aus den Wurzeln einer beliebigen irreductiblen Gleichung rational gebildet sind. *Zeitschrift für Mathematik und Physik* 10, 17–47

SERRET, Joseph-Alfred. 1854. *Cours d'algèbre.* 2nd ed. Paris: Mallet-Bachelier.

ULLRICH, Peter. 1998. The Genesis of Hensel's p-adic Numbers. In *Karl der Grossen und sein Nachwirken. 1200 Jahre Kultur und Wissenschaft in Europa*, ed. P.L Butzer, H. Th. Jongen, and W. Oberschelp, vol. 2, pp. 163-178. Turnhout: Brepols.

VAN DER WAERDEN, Bartel Leendert. 1930. *Moderne Algebra.* Berlin: Springer.

WEIL, André. 1948. *Sur les courbes algébriques et les variétés qui s'en déduisent.* Actualités scientifiques et industrielles 1041, Publications de l'Institut de Mathématique de l'Université de Strasbourg VII. Paris: Hermann.

Part III

The German Reception of the *Disquisitiones Arithmeticae:* Institutions and Ideas

Viel Politischer Tierkreis gelesen. Herr Gauß bringt mich um meinen Kaffee indem er von 3 bis um 5 sitzt. Heute um 12 Uhr mittags streift der Schatten meines Gartenhauses die südliche Spitze des Ziegenstalls.

Georg Christoph Lichtenberg
Staatskalender entry for October 28, 1796

III.1

A Network of Scientific Philanthropy: Humboldt's Relations with Number Theorists

Herbert Pieper

This text is dedicated to Prof. K.-R. Biermann (1918–2002), for many years the director of the Alexander-von-Humboldt-Forschungsstelle. More than anyone else he has investigated in editions, monographs, and articles, the relations of A. von Humboldt to Gauss in the first place, and to Dirichlet and Eisenstein.

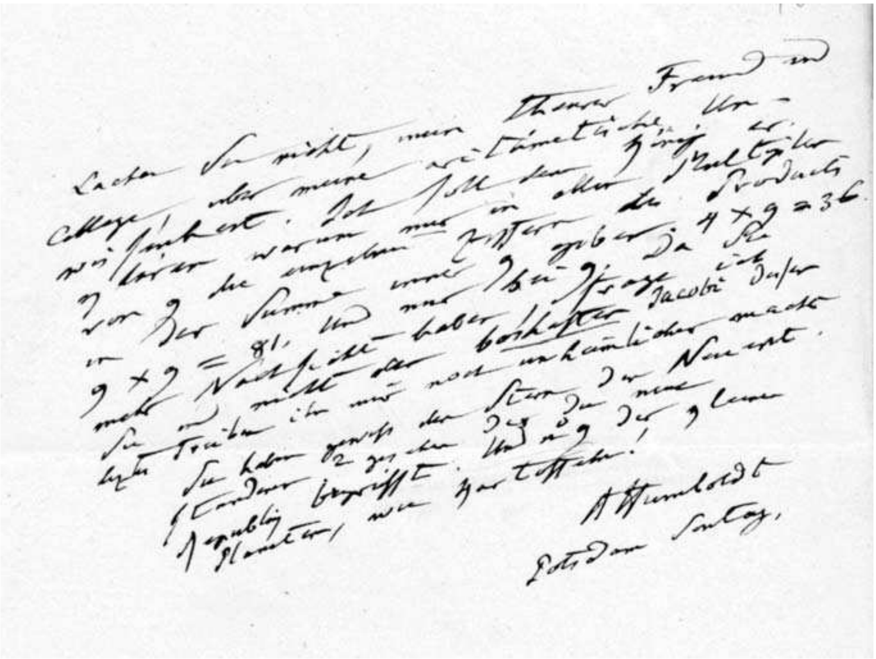
When Alexander von Humboldt[1] (1769–1859) returned from his research trip to the Americas to Paris in 1804, he found Gauss's name "in every mouth … because of the publication of the Theory of Numbers."[2] A year later, Humboldt replied to the invitation from the Prussian King, Friedrich Wilhelm III, to enter the Berlin Academy of Sciences, that his own presence would be "very insignificant" [*sehr unbedeutsam*], but one man could give the Academy back its lustre: Gauss.[3] We shall here illuminate the relations between C.F. Gauss and Alexander von Humboldt through selected episodes. We shall see how young mathematicians drew the attention of Gauss or Humboldt on the basis of number-theoretical works, usually related to Gauss's work, and in particular to the *Disquisitiones Arithmeticae*. With the discovery of new talent an ever-widening circle of number-theorists grew around Gauss and Humboldt. A communication network was set up which served not only to exchange knowledge,

[1] On Humboldt's life and work, see for instance [Bruhns 1872], [Biermann 1981a], [Biermann 1983], [Biermann 1991].

[2] Humboldt to Dirichlet, June 2(?), 1855. See [Humboldt & Dirichlet 1982], p. 123: *… wegen der Erscheinung der Zahlentheorie … in aller Mund.*

[3] Humboldt to Schumacher, April 2, 1836, [Humboldt & Schumacher 1979], p. 65 (letter 39): *aber ein Mann könne der Akademie den Glanz wiedergeben, er heisse Karl Friedrich Gauss.*

but also to support newly-discovered talent and to protect colleagues belonging to this circle from the vicissitudes of life and work.



Lachen Sie nicht, mein theurer Freund und College, über meine arithmetische Unwissenheit. Ich soll dem König erklären, warum nur in allen Multiplen von 9 die einzelnen Ziffern des Products in der Summe immer 9 geben. 4×9=36. 9×9=81. Und nur bei 9. Da Sie mit mir Nachsicht haben, frage ich Sie. [illegible] Jacobi Dase [illegible] boshafter [illegible] unheimlicher [illegible] Nun erst [illegible] Sie haben [illegible] Und [illegible] begriffe [illegible]

A Humboldt

Potsdam Sontag.

Fig. III.1A. Humboldt to Encke: "Do not laugh, my dear friend…"
Nachlaß Encke, Archiv der Berlin-Brandenburgischen Akademie der Wissenschaften
(Courtesy of ABBAW)

One could be surprised to find Alexander von Humboldt, the famous scientific traveller, natural scientist, and geographer, in such a circle of number-theorists. "Do not laugh, my dear friend and colleague, at my arithmetical ignorance," Humboldt (then almost eighty) begged Johann Franz Encke, director of the Berlin observatory:

> I am supposed to explain to the King [Friedrich Wilhelm IV] why *only* in the multiples of 9 the sum of the individual digits of the product always gives 9, 4 × 9 = 36.9 × 9 = 81. And only with 9. Since you are indulgent with me, I am asking you.[4]

Not only knowledge, but also mathematical understanding seemed to be rather

[4] [Pieper 1991], p. 98; [Encke NL], Band 52, II/70: *Lachen Sie nicht, mein theurer Freund und College, über meine arithmetische Unwissenheit. Ich soll dem König erklären, warum* nur *in allen Multiplen von* 9 *die einzelnen Ziffern des Products in der Summe immer* 9 *ergeben,* 4*x*9 = 36. 9*x*9 = 81. *Und nur bei 9. Da Sie mit mir Nachsicht haben, frage ich Sie.*

foreign to the older Humboldt.[5] In a letter to Humboldt, Jacobi wrote:

> The theorem to the effect that in mathematics there is only one sort of impossibility introduced by the special relationship between the given magnitudes, to wit the equation $xx + 1 = 0$, is the most profound result of analysis. Through it, this impossibility acquires a definite form and may be inserted into the calculation. Almost all recent progress stems from it, and the practice, which for a long time defended itself against it, has profited from it as much as the theory.[6]

Humboldt's summary of this passage reads : "The theorem that $xx + 1 = 0$ is the deepest of analysis. Thanks to it, impossibility acquires a definite form."[7]

However, through his long-term acquaintance with leading French mathematicians, while in Paris, Humboldt developed a high esteem for the achievements of the mathematicians:

> In spite of my very limited mathematical knowledge ..., and of my ignorance which I am happy to confess, the long acquaintance with La Grange, Laplace, and Fourier has given me some idea of the relative value of my contemporaries.[8]

In turn, he would act to support talented mathematicians.[9]

1. Humboldt and Gauss: 1804–1827

On November 16, 1805, Humboldt returned to Berlin again. During his American trip, in 1800, he had become an extraordinary member of the Berlin *Académie royale*

[5] Humboldt had been introduced to mathematics in his youth by Ernst Gottfried Fischer, Professor at the Berlin *Gymnasium zum Grauen Kloster*, who was convinced in 1789 that Humboldt "could have made a very good mathematician out of himself," if "he could have concentrated exclusively or chiefly on mathematics," [Bruhns 1872], vol. 1, p. 76. As a student in Göttingen and in his autodidactic studies, Humboldt acquired at least the mathematical knowledge that he needed as a scientific traveller for geographical localizations on an astronomical basis, for the barometric measurement of heights, and for geomagnetic measurements.

[6] [Humboldt & Jacobi 1987], p. 91 : *Der Satz, daß es in der Mathematik nur eine einzige Art durch die besonderen Größenverhältnisse der zu Grunde liegenden Data herbeigeführter Unmöglichkeit giebt, nämlich die Gleichung* $xx + 1 = 0$, *ist der tiefste der Analysis. Dadurch erhält dies Unmögliche eine bestimmte Form und kann in die Rechnung eingeführt werden. Hiervon datieren fast alle Fortschritte der neueren Zeit, und die Praxis, die lange Zeit sich dagegen gewehrt hat, hat ebensoviel Nutzen daraus gezogen als die Theorie.*

[7] [Humboldt & Jacobi 1987], p. 157: *Der Satz, daß* $xx + 1 = 0$ *[ist], ist [der] tiefste der Analysis. Dadurch erhielt [die] Unmöglichkeit eine bestimmte Form.*

[8] [Humboldt & Jacobi 1987], p. 109: *Bei einer sehr geringen mathematischen Kenntnis, ... bei der Unwissenheit, die ich so gern eingestehe, hat mir doch der lange Umgang mit La Grange, Laplace und Fourrier [sic] einiges Ahndungsvermögen über den relativen Werth meiner Zeitgenossen eingeflösst.*

[9] On the influence of Alexander von Humboldt on the development of mathematics, see [Biermann 1959b], [Hofmann 1959], [Biermann 1969], [Biermann 1970], [Biermann 1981], [Pieper 2004], and furthermore [Dunken 1958], [Schubring 1981a], [Schubring 1981b], [Schubring 1982], [Humboldt & Jacobi 1987].

des sciences et belles-lettres,[10] and he was now made an ordinary member, with an annual pension. As Humboldt would describe it later to Gotthold Eisenstein:

> I had asked the King a few months after my return to appoint the young Gauss from Braunschweig to the Berlin Academy, and to use the 500 *Thaler* set aside for myself as a payment towards Gauss's pension.[11]

After a visit to Berlin, Olbers wrote to Gauss on July 12, 1806: "Humboldt has not abandoned his praiseworthy intentions towards your appointment to the Academy. But he complained that things did not move ahead in Berlin."[12] Indeed, in July 1806, Humboldt proposed a reorganization of the Academy which would allow an increase in the number of foreign members in accordance with "the present state of European culture." The list he proposed included Laplace, Legendre, Monge, and Gauss – see [Biermann 1991], p. 108. Gauss was finally appointed to the Berlin Academy in 1810 as a foreign member. He could have instead accepted a position at the newly founded Berlin University, implying an ordinary membership.[13]

Meanwhile, in November 1807, Humboldt had left again Berlin for Paris, where he stayed and worked until 1827, except for two short visits to Berlin. It was on his

[10] Extraordinary members did not receive any pension: they were considered honorary members who would be made ordinary members when a place became free.

[11] Humboldt to Eisenstein, April 17, 1846, [Biermann 1959b], p. 127: *Ich hatte einige Monate nach meiner Rückkunft ... den König gebeten, den jungen Gauß aus Braunschweig für die Berliner Akademie zu berufen und die mir bestimmten 500 Thaler als Zuschuß zu der Pension von Gauß zu nehmen.*

[12] [Gauss & Olbers 1900–1909], vol. 1, p. 303, also quoted in [Humboldt & Gauss 1977], p. 28: *Humboldt hat seine lobenswürdigen Absichten in Ansehung Ihrer Aufnahme in die Akademie nicht aufgegeben; klagte aber, daß man in Berlin zu nichts kommen könne.*

[13] For the details on these proposals and Gauss's reasons to reject the offer from Berlin University in 1810, see [Humboldt & Gauss 1977], p. 125–127. Renewed attempts to convince him were made in vain between 1822 and 1824; see [Pieper 2004], pp. 46–58. Later, the situation seemed to evolve; according to Schumacher's interpretation, the reluctance to nominate Gauss reflected the anxiety of other professors to confront Gauss's intellectual superiority: *Es ist mir vorgekommen, als ob man im Allgemeinen keineswegs Ihre Anstellung in Berlin wünscht. Ich nehme Herrn v[on] Humboldt und die wenigen, die sich würklich dort auszeichnen, natürlich von dieser Behauptung aus, die nur von dem gros der Gelehrten gelten soll. Jeder dieser Herren ... hat seine eigenen Gesellschaftscirkel, in denen er als Orakel gilt, und keiner ist gesonnen seinem Ansehen, durch die Erscheinung eines gewaltigen und als solches allgemein anerkannten Genies einen Abbruch zuzufügen. Wären Sie nicht, der Sie sind, sondern ein mittelmäßiger Kopf mit einigem Ruf, so würden diese Herren Sie mit offenen Armen empfangen, da jeder dann die Hoffnung hätte, seine Superiorität über einen berühmten Mann zu zeigen und seine Autorität in Gesellschaften noch fester zu begründen. ... Bei der Vermischung der Stände in Berlin, und dem freien Zutritt, den die Gelehrten zu den ersten Personen des Staates haben, kann die von mir vorausgesetzte Stimmung dieser Herren gegen Sie einen wesentlichen Einfluss auf Ihre Berufung haben, dem vielleicht selbst Humboldts Autorität nur mit Mühe das Gegengewicht halten kann.* (Schumacher to Gauss, September 7, 1828, [Gauss & Schumacher 1860–1865], vol. 2, p. 185.)

way to Berlin during one of these visits in the fall of 1826 that Humboldt met Gauss for the first time.[14]

> A few months ago, I had the great pleasure to get to know Humboldt here personally, and I am thus doubly pleased now that he will take his future permanent residence in Berlin.[15]

And when Humboldt did return to Berlin for good a few months later,[16] Gauss wrote:

> I am convinced that Humboldt's return to Berlin will be most advantageous for the flourishing of the exact sciences in Germany. He takes the most vivid interest in encouraging each excellent talent.[17]

To such talents, and to Humboldt's efforts to promote them, we will now turn.

2. An "Excellent Talent": Peter Gustav Lejeune-Dirichlet

In March, 1849, Humboldt wrote to the Prussian Minister of culture:

> In the circles of higher mathematical knowledge, in which I cannot claim to have a personal judgement, I do feel securely guided by those whom Europe recognizes to be first rate. Upon Laplace's suggestion, I have then … strongly recommended the then 22-year old Le Jeune Dirichlet to the ministry. … Le Jeune Dirichlet has become one of the main pillars, a bright star of our university.[18]

Lejeune-Dirichlet,[19] born in 1805 as the son of the post-office director in Düren, spent two years at the *Gymnasium* in Bonn, then in Köln. But from May 1822, he

[14] They entertained a correspondence much earlier. The first among the 32 letters we have from Humboldt to Gauss is dated July 14, 1807. Only 12 letters from Gauss to Humboldt are extant.

[15] Gauss to Olbers, January 14, 1827, [Gauss & Olbers 1900–1909], vol. II, pp. 467–468, see also [Humboldt & Gauss 1977], p. 31: *Eine große Freude habe ich vor mehreren Monaten gehabt, Humboldt hier persönlich kennen zu lernen, und doppelt angenehm ist es mir nun, daß er künftig seinen bleibenden Aufenthalt in Berlin nehmen wird.*

[16] In May 1827, Humboldt returned from Paris to Berlin. One of Humboldt's aims was the advancement of mathematics in Prussia. See [Biermann 1968], [Pieper 2004].

[17] Gauss to Olbers, March 1, 1827, [Gauss & Olbers 1900–1909], vol. II, p. 472, also quoted in [Humboldt & Gauss 1977], p. 31: *Ich bin überzeugt, daß Humboldt's Rückkehr nach Berlin dem Gedeihen der exakten Wissenschaften in Deutschland die grössten Vortheile bringen wird. Auf das Lebhafteste interessiert er sich dafür, daß jedes ausgezeichnete Talent aufgemuntert werde.*

[18] Humboldt to Ladenberg, March 11, 1849, [Biermann 1985], p. 124: *In den Kreisen des höheren mathematischen Wissens, über das ich mir kein Urtheil anmaßen kann, glaube ich sicher durch die geleitet zu werden, die Europa als auf der ersten Stelle stehend erkennt. Durch La Place dazu aufgefordert, habe ich dem Ministerium den damals kaum 22-jährigen Le Jeune Dirichlet … dringend empfohlen. … Le Jeune Dirichlet ist eine der Hauptstützen, ein Glanzpunkt unserer Berliner Universität geworden.*

[19] On Dirichlet's life and work, see [Kummer 1860], [Biermann 1959a], [Biermann 1959d], [Biermann 1960b], [Reichardt 1963], [Koch 1981], [Ore 1981], [Humboldt & Dirichlet 1982], [Schubring 1984], [Biermann 1988], [Koch 1998].

studied in Paris, attending lectures at the *Collège de France* and the *Sorbonne*, while intensely studying Gauss's *Disquisitiones Arithmeticae* on his own. Three years later, he submitted his results on Fermat Last Theorem for the exponent 5 to the Paris Academy of Sciences, [Dirichlet 1889–1897], vol. 1, pp. 1–46. Around the same time, he became acquainted with Joseph Fourier and Alexander von Humboldt, who both, for different reasons, would exert a decisive influence on his life: the French mathematician for the future orientation of Dirichlet's work and Humboldt for encouraging Dirichlet's wish to return to Prussia and helping him to fulfill it. In 1826, indeed, Dirichlet wrote to the Prussian *Kultusminister*,[20] to the Berlin Academy of Sciences, and to Gauss, accompanying his letters with his Academy memoir and with a letter of recommendation by Humboldt. To the Minister, he offered his services on May 14, 1826. Later, he wrote:

> I had come to Paris at the age of 18, as a complete unknown and only with the intention to further my education in the mathematical sciences in order to one day be useful to my homeland, Prussia, in an academic career. … Through my efforts and perseverance in my studies, I have managed within a few years to gain the sympathy and the kind encouragement of the more well-known mathematicans here.[21]

In an accompanying letter, written to Altenstein on May 14, 1826, Humboldt emphasized that "this young man full of genius" whose analytical works "have drawn since his 19th year the attention of the *Institut*" recommended himself for "his conduct, his modesty and his poverty," [Biermann 1959a], p. 14. The exchange with Gauss, whom Dirichlet referred to as "the author of the immortal *Disquisitiones Arithmeticae*," provides us with interesting hints at the situation of number theory at that time. Dirichlet wrote:

> In view of the gracious recommendation by Herr Baron von Humboldt, I trust I may hope that you will receive and judge this first work of a young German with gracious indulgence. … In having worked mainly on higher arithmetic, I have completely followed my personal inclination. … Although I convince myself more with every day of the difficulties implied by such investigations, I have become too much used to these occupations, and I'd almost say that I am too passionately involved with them that I could easily decide to abandon the investigations once started. … But since even among the best mathematicians – as I have the opportunity to convince myself here [in Paris] – only very few are familiar with indeterminate analysis, it is to be feared that my memoir will receive a less favourable reception than it might

[20] The *Kultusministerium*, more precisely ministery of the spiritual, educational, and medical affairs, was founded in 1817; from 1817 to 1840, the Minister in charge was Karl Freiherr von Stein zum Altenstein, who was Humboldt's friend of youth.

[21] Dirichlet to Altenstein, August 13, 1826, [Biermann 1959a], pp. 15–16: *Ich bin in meinem achtzehnten Jahre ganz unbekannt und blos in der Absicht nach Paris gekommen, mich in den mathematischen Wissenschaften weiter auszubilden, um einst meinem Vaterlande Preußen in der akademischen Laufbahn nützlich werden zu können. … Durch Anstrengung und Beharrlichkeit im Studium ist es mir nach wenigen Jahren gelungen, mir die Zuneigung und das aufmunternde Wohlwollen der hiesigen berühmteren Mathematiker zu erwerben.*

> have earned if, of the same inherent quality, it was devoted to a problem from a better known part of science, like astronomy or integral calculus.[22]

Meanwhile, Humboldt also wrote directly to Gauss to support his "promising compatriot." Relying, as he said, on the mathematical judgements of the Parisian geometers, particularly Fourier and Poisson, he asked for Dirichlet "the protection of [Gauss's] great name," [Humboldt & Gauss 1977], pp. 28–29.

Both Gauss[23] and Humboldt contacted the Academy of Sciences on Dirichlet's behalf; Gauss wrote to Encke, one of his former students, and now Secretary of the mathematical class of the Berlin Academy of Sciences:

> A young German from Aachen, Dirichlet, currently in Paris, recently sent me a short memoir on higher arithmetic which shows excellent talent. This phenomenon makes me all the happier, since it is rare that someone acquires a familiarity with these objects – I know of none in Germany – and I am convinced that this is one of the best ways to sharpen the mathematical talent also for other, totally different, branches of mathematics; it would be all the more regrettable if his homeland Prussia lets the occasion pass, and France appropriates this excellent talent too.[24]

[22] Dirichlet to Gauss, May 28, 1826, [Dirichlet 1889–1897], vol. 2, pp. 373–374: *Bei der gütigen Empfehlung des Herrn Baron von Humboldt glaube ich mir mit der Hoffnung schmeicheln zu dürfen, dass Sie diese erste Arbeit eines jungen Deutschen mit gütiger Nachsicht aufnehmen und beurtheilen werden. … Indem ich mich bisher hauptsächlich mit der höheren Arithmetik beschäftigt habe, bin ich ganz meiner Neigung gefolgt …. Obgleich ich mich nun täglich mehr von den Schwierigkeiten überzeuge, womit Untersuchungen dieser Art verbunden sind, so ist mir doch diese Beschäftigung zu sehr zur Gewohnheit und ich möchte fast sagen, zu sehr zur Leidenschaft geworden, als dass ich mich so leicht entschliessen könnte, die einmal begonnenen Untersuchungen aufzugeben. … Da aber selbst unter den ausgezeichnetsten Mathematikern – wie ich mich hier zu überzeugen Gelegenheit habe – nur sehr wenige mit der unbestimmten Analysis vertraut sind, so steht zu fürchten, dass meine Abhandlung eine weniger günstige Aufnahme finden werde, als derselben vielleicht zu Theil werden dürfte, wenn dieselbe bei übrigens gleichem inneren Werthe eine Aufgabe aus einem bekanntern Theile der Wissenschaft, z.B. der Astronomie oder Integralrechnung zum Gegenstande hätte.*

[23] To Dirichlet, Gauss answered that he was very pleased to discover Dirichlet's inclination for such a dear topic, although since the publication of the D.A., he had been distracted from it by other tasks; he also mentioned his new arithmetical focus, namely the theory of biquadratic and cubic residues – see [Dirichlet 1889–1897], vol. 2, pp. 375–376 and [Gauss 1863–1933], vol. II, pp. 514–515.

[24] Gauss to Encke, July 9, 1826, [Gauss 1863–1933], vol. XII, p. 70: *Ein junger Deutscher aus Aachen[,] Dirichlet, der sich in Paris aufhält, hat mir vor kurzem eine kleine Abhandlung aus der höheren Arithmetik zugesandt, welche ein ausgezeichnetes Talent verräth. Je seltener die Beispiele sind daß Jemand sich mit diesen Gegenständen vertraut macht – in Deutschland weiß ich gar keines – und jemehr ich überzeugt bin daß dieses eines der besten Mittel ist, das mathematische Talent auch für andere ganz verschiedene Zweige der Mathematik zu schärfen, um so erfreulicher ist mir das Phaenomen, und um so betrübender würde es seyn, wenn sein Vaterland, Preußen, sich zuvorkommen ließe und Frankreich sich auch dieses ausgezeichnete Talent zueignete.*

Only a few days later, Encke turned to the ministry, quoting from Gauss's as well as Humboldt's letters, to draw attention again to Dirichlet's talent. At the end of August, and after other letters, Humboldt summarized his efforts to Dirichlet:

> I acted differently from what you wished, but in your best interest. I wrote long letters to M. Altenstein and M. Encke. I enclosed your letters and I sent everything off to Berlin with the Embassy's mail *this morning*. Why let this occasion slip away! I still spoke of Gauss, Fourier, and the *Institut*, and warned them that you would be abducted here, in spite of your patriotism, to teach at a French military school. And finally I told them all that a beautiful talent like yours inspires.[25]

Another half year and more pressures were necessary before Dirichlet received his *Habilitation* at the University of Breslau and a yearly income of 400 *Thaler*. "On his trip to Breslau, [Dirichlet] chose to pass through Göttingen, in order to meet Gauss personally, and paid him a visit on March 18, 1827," [Kummer 1975], vol. 2, p. 731. Humboldt's activities in Dirichlet's favour, however, did not stop then, for he wanted to secure him "a pleasant position in Berlin," [Humboldt & Dirichlet 1982], p. 41. In October 1828, Dirichlet indeed began to teach at the Royal Military School, and in July 1831, he was appointed extraordinary professor at Berlin University.

3. A "Very Talented Young Man": Jacob Jacobi

Quite a similar story, with interesting variants, has Jacobi as its hero. Jacob Jacobi[26] was born in 1804 in Potsdam, in a Jewish family. He studied at Berlin University from 1821 on, dropping his first interests, philosophy and philology, for mathematics. As the 1812 decree authorizing Jews to obtain academic positions was withdrawn in December 1822, the only way to an academic career for Jacobi was through baptism, [Pieper 1995]. After his doctorate and habilitation during the summer of 1825, he settled as *Privatdozent* at the *Albertina*, i.e., at Königsberg University, in May, 1826.

Gauss's first results on biquadratic residues, already alluded to above, appeared as a short announcement in the *Göttinger gelehrte Anzeigen* in 1825, [Gauss 1863–1933], vol. 2, pp. 165–168. According to Kummer:

> This announcement, which contained some of Gauss's results whose proofs were said to be based on an entirely new principle of the theory of numbers, kindled strongly both Jacobi's and Dirichlet's curiosity. Both tried to penetrate the Gaussian mystery in quite different ways, and both succeeded in finding a wealth of new theorems

[25] Humboldt to Dirichlet, August 25, 1826, [Humboldt & Dirichlet 1982], pp. 31–32: *J'ai agi autrement que Vous le vouliez, Monsieur, mais dans Vos intérêts. J'ai écrit longuement à Mr. Alt[enstein] et à Mr. Encke, j'ai inclus Vos lettres et j'ai fait partir le tout par le courrier de l'Ambassade qui est parti* ce matin *pour Berlin. Pourquoi négliger cette occasion ! J'ai parlé encore de Gauss, Fourier et de l'Institut, j'ai fait craindre que Vous seriez enlevé ici [à Paris], malgré Votre patriotisme, pour une Ecole française militaire … enfin j'ai dit ce qu'inspire un beau talent comme le Vôtre.*

[26] On Jacobi's life and works, see [Dirichlet 1852]; [Jacobi 1881–1891]; [Koenigsberger 1904]; [Jacobi & Jacobi 1907]; [Klein 1926–1927], vol. 1, pp. 108–114, 203–207; [Scriba 1981]; [Humboldt & Jacobi 1987]; [Knobloch, Pieper, Pulte 1995]; [Jacobi & Legendre 1975/1998]; [Pieper 1995]; [Pieper 1998]; [Pieper 2005].

> in this realm of higher power residues, although the new principle which consisted in the introduction of complex numbers still remained concealed from them at the time.[27]

At the end of October 1826, Gauss received a letter from Jacobi, communicating some of his investigations about power residues.

> When following a few considerations in your *Disquisitiones Arithmeticae*, I recently chanced upon a simple and direct method of researching the reciprocity laws for power residues. When I mentioned this subject to Professor Bessel, he gave me the interesting note extracted from a paper on biquadratic residues submitted to the Göttingen Academy which your Excellency has communicated in the *Göttinger Anzeigen*. I took this opportunity to check my method.[28]

A few weeks later, Gauss enquired with Bessel about the exact situation of this "very talented young man,"[29] and at the beginning of 1827, he wrote to Humboldt about the remarkable mathematical competencies of Jacobi. Humboldt replied:

> Those are not many who keep the 'holy fire' burning, and I will always be infinitely grateful if you continue to draw my attention to the young talents who are worthy of your protection.[30]

While studying the D.A., Jacobi also came upon Gauss's hint in sec. 7, art. 335, according to which the principles of the theory of equations used in the division of the circle could be extended from the cyclotomic functions to "many other transcendental functions." It was a decisive stimulus for his research on elliptic integrals and their inverse functions, which he started in the winter of 1826–1827.[31] "The application of

[27] [Kummer 1975], vol. 2, pp. 732–733: *Diese Ankündigung, welche einige der Gauss'schen Resultate gab, deren Beweis auf einem ganz neuen Prinzip der Zahlentheorie beruhen sollte, erregte zugleich Jacobis und Dirichlets Wißbegierde in hohem Grade, beide suchten auf ganz verschiedenem Wege in das Gaußsche Geheimnis einzudringen, und beiden gelang es auch, in diesem Gebiete der höheren Potenzreste eine Fülle neuer Sätze zu finden, obgleich das neue Prinzip, welches in der Einführung der komplexen Zahlen bestand, ihnen damals noch verborgen blieb.*

[28] Jacobi to Gauss, October 27, 1826, [Jacobi 1881–1891], vol. 7, pp. 391–392: *Ich gerieth nämlich zufällig, als ich einige in Ihren Disquisitiones angestellte Betrachtungen verfolgte, auf eine einfache und directe Methode, die Fundamentaltheoreme über die Reste der Potenzen zu erforschen. Als ich dieses Gegenstandes gegen den Herrn Prof. Bessel erwähnte, gab er mir die interessante Notiz von dem Auszuge, den Ew. Hochwohlgeboren in den Göttinger Anzeigen von einer der Göttinger Societät über die biquadratischen Reste vorgelegten Abhandlung gegeben haben. Ich nahm die Gelegenheit meine Methode zu prüfen.*

[29] Gauss to Bessel, November 20, 1826, [Gauss & Bessel 1880], p. 463: ... *diesen ... sehr talentvollen jungen Mann.*

[30] Humboldt to Gauss, February 16, 1827, [Humboldt & Gauss 1977], p. 30: *Es giebt der Menschen nicht viele, die das 'heilige Feuer' bewahren und ich werde Ihnen stets unendlich dankbar sein, wenn Sie fortfahren, mich auf die jungen Talente aufmerksam zu machen, die Ihres Schutzes werth sind.*

[31] See chap. I.1, § 3.4, and C. Houzel's chap. IV.2 in this book [Editors' note].

higher arithmetic to the division of the elliptic transcendents," he wrote hopefully to Gauss, "has been promised in the *Disquisitiones Arithmeticae*. If only the promise would be fulfilled!"[32]

Jacobi also benefited from Legendre's research on elliptic integrals and communicated his first results to him, [Jacobi & Legendre 1875/1998], pp. 13–19, 91–98. Thus Humboldt was for the second time alerted to Jacobi's talent, this time from Legendre. In his very positive evaluation of Jacobi's achievements, the Parisian mathematician expressed his satisfaction to see at last the fruits of the theory on which he himself had worked for forty years. He concluded:

> As for you, Sir, who are not only one of the most exquisitely learned men in Europe, but who also like to spread the sciences and to find influential patrons for them, I have nothing to request, but simply rely on your well-known zeal which, given the circumstances, will certainly not be in vain.[33]

Legendre had also, as he informed Humboldt, reported on Jacobi's work to the French Academy, and Humboldt in turn transmitted Legendre's recommendation to the *Kultusminister* and to the Berlin Academy.[34] He apparently also informed other protagonists; in fact, we know at least of one further reaction, by Encke, who commented on the situation to Bessel:

> Legendre has written to Humboldt a very nice letter on Jacobi's discovery which honours both of them. It honours Legendre all the more as he had been distant from Humboldt, and now wants to see this letter used to push Jacobi at the ministry here.[35]

The exact impact of each letter is of course difficult to determine. However, Jacobi was appointed extraordinary professor at Königsberg University in December 1827. Besides their correspondence, Humboldt and Jacobi also met personally on various occasions and Humboldt pursued his efforts to secure Jacobi a better financial situation and subsidies. For instance, at the occasion of the Königsberg celebration of his

[32] Jacobi to Gauss, February 8, 1827 [Jacobi 1881–1891], p. 400: *Die Anwendung der höheren Arithmetik auf die Teilung der elliptischen Transzendenten ist in den Disquisitiones versprochen, o würde doch das Versprechen erfüllt!*

[33] Legendre to Humboldt, November 29, 1827 [Humboldt & Jacobi 1987], pp. 165: *Pour Vous, Monsieur, qui n'êtes pas seulement un des savants les plus distingués de l'Europe, mais qui prenez un vrai plaisir à propager les sciences et à leur susciter de puissants protecteurs, je n'ai aucune demande à Vous former et me repose entièrement sur Votre zèle bien connu qui dans cette circonstance ne restera sûrement pas infructueux.*

[34] *Herrn Le Gendre's Brief, welcher die ehrenvollsten Lobsprüche Ihrer Entdeckungen enthält, habe ich dem Ministerium des Cultus geschickt, ich denke, eine Abschrift davon in dieser Woche der Akademie der Wissenschaften vorzulegen. Es ist mir eine angenehme Pflicht, Ihnen diesen Beweis meines lebhaftesten Antheils an Ihren Arbeiten zu geben*, wrote Humboldt to Jacobi on February 4, 1828, [Humboldt & Jacobi 1987], p. 47.

[35] Encke to Bessel, January 21, 1828, [Humboldt & Jacobi 1987], p. 166: *Legendre hat an Humboldt einen sehr hübschen und für beide Theile sehr ehrenvollen Brief über Jacobis Entdeckung geschrieben, um so ehrenvoller für Legendre, als er sonst von Humboldt entfernt stand und diesen Brief wünscht benutzt zu wissen, um Jacobi bei dem hiesigen Ministerium zu poussieren.*

coronation, the new King Friedrich Wilhelm IV was again made aware by Humboldt of Jacobi's merits, and rewarded him with an annual bonus of 500 *Thaler* – see also [Bruhns 1872], vol. 2, p. 326.

Humboldt and Dirichlet also supported plans for a prolonged cure for Jacobi when he had fallen ill with diabetes in the 1840s: "Jacobi will be sent to Italy," Humboldt wrote to Schumacher in May 1843, [Humboldt & Schumacher 1979], p. 113, see also [Jacobi & Jacobi 1907], p. 99. After this trip, Jacobi was authorized by the king to transfer from Königsberg to Berlin (again for medical reasons) and was received at the Berlin Academy of sciences in September 1844. However, Humboldt intervened again several times, with moderate success, to obtain royal support for Jacobi at the end of the 1840s, when the mathematician was too ill to hold his courses and foresaw financial problems for his large family; at that time, Jacobi's republican activities made state protection more difficult to obtain and he was resigned to accept an offer from Vienna, [Pieper 2005], when Humboldt's intervention allowed him to stay in Berlin.

Dirichlet and Jacobi had known each other since 1829 and had developed a close friendship, both personal and mathematical – see [Kummer 1975], vol. 2, p. 747. On a 1832 trip to his home town of Potsdam, Jacobi met his brother as well as Dirichlet and Steiner in a Berlin inn. Moritz Hermann Jacobi reported in his diary

> that Jacob hardly said hello to me and immediately retreated to a corner with Dirichlet in order to discuss under which conditions *a* would be a prime number.[36]

Dirichlet and his wife Rebecca, the younger sister of the composer Mendelssohn-Bartholdy, also accompanied Jacobi during part of his health trip in Italy. Reciprocally, Jacobi was influential in keeping Dirichlet in Berlin; when still in 1846, his friend did not get the expected income of an ordinary professor, and was ready to accept a position in Heidelberg, Jacobi wrote directly to the King, while at the same time providing Humboldt with useful arguments for his own intervention. To Friedrich Wilhelm IV, Jacobi wrote:

> His disappearance would leave me all by myself in my discipline, and there is no substitute in sight since, except for Gauss in Göttingen and Cauchy in Paris, I am not aware of any living mathematician who would be his equal.[37]

His description for Humboldt of Dirichlet's specific strengths is worth a full quotation:

> Scientifically, Dirichlet has two sides that constitute his peculiar nature. He alone, not myself, not Cauchy, not Gauss, knows what a completely rigorous proof is, we only know it from him. If Gauss says he has proved something, I think it is likely. If

[36] [Jacobi & Jacobi 1907], p. 10: *dass Jacques mich kaum begrüsste und sich sogleich mit Dirichlet in eine Ecke stellte um zu untersuchen unter welcher Bedingung a eine Primzahl würde.*

[37] December 12, 1846, [Biermann 1959a], pp. 54–55, [*Kultusministerium*], Vf Litt D Nr 4, Bl. 193–194: *Sein Abgang würde mich in meinem Fache gänzlich vereinsamen und an einen Ersatz ist nicht zu denken, da außer Gauß in Göttingen und Cauchy in Paris, mir unter den heutigen Mathematikern keiner der ihm gleichzustellen, bekannt ist.*

> Cauchy says it, one may bet as much in favour as against it. If Dirichlet says it, it is for sure. I for my part prefer not to enter into these delicate issues. Secondly, Dirichlet has created a new mathematical discipline, the application of those infinite series to the theory of prime numbers which Fourier has introduced into the theory of heat. He then found a great number of theorems which will last for science and constitute the basic pillars of new theories. Dirichlet has preferred to deal mainly with the subjects which present the greatest difficulties. This is why his works may not lie on the broad avenue of science, and therefore may have found much recognition that they deserve, but not all. Had he stayed in Paris, he would now reign there without competitor, and how different would his ostensible situation be![38]

And thus, Dirichlet's income was raised and he remained in Berlin.

4. Humboldt and Gauss Again: 1828–1855

Between September 18 and 24, 1828, the Seventh Meeting of German Scientists and Physicians (*Versammlung deutscher Naturforscher und Ärzte*) took place in Berlin with Humboldt as chairman. Gauss received an invitation from him and H. Lichtenstein, to which Humboldt added:

> I live in the pleasant hope to be able to welcome in my house Europe's first mathematician and profound astronomer, to put him up and to look after him as well as I can.[39]

Gauss replied positively, expressing his wish to see "Berlin, and above all, you in Berlin," [Humboldt & Gauss 1977], p. 33. He spent the conference at his friend's house. During the conference, both Humboldt and Gauss met the 24 year old physicist Wilhelm Eduard Weber, then extraordinary professor in Halle, who reported on acoustics. Characteristically, a few years later, using their memories of this meeting, both would support Weber's appointment as ordinary professor and successor of

[38] Jacobi to Humboldt, December 21, 1846, [Humboldt & Jacobi 1987], p. 99: *Dirichlet hat in der Wissenschaft zwei Seiten, die seine Spezialität ausmachen. Er allein, nicht ich, nicht Cauchy, nicht Gauß weiß, was ein vollkommen strenger mathematischer Beweis ist, sondern wir kennen es erst von ihm. Wenn Gauß sagt, er habe etwas bewiesen, ist es mir wahrscheinlich, wenn Cauchy es sagt, ist es eben so viel pro als contra zu wetten, wenn Dirichlet sagt, ist es gewiß, ich lasse mich auf diese Delicatessen lieber gar nicht ein. Zweitens hat D[irichlet] eine neue Disziplin der Mathematik geschaffen, die Anwendung derjenigen unendlichen Reihen, welche Fourier in die Wärmetheorie eingeführt hat, auf die Erforschung der Eigenschaften der Primzahlen. Dann hat er eine Menge Theoreme gefunden, welche in der Wissenschaft bleiben und die Grundpfeiler neuer Theorien bilden. D[irichlet] hat es vorgezogen, sich hauptsächlich mit solchen Gegenständen zu beschäftigen, welche die größten Schwierigkeiten darbieten; darum liegen seine Arbeiten vielleicht nicht so auf der breiten Heerstraße der Wissenschaft und haben daher, wenn auch große Anerkennung, doch nicht alle die gefunden, welche sie verdienen. Wäre er in Paris geblieben, so würde er dort jetzt ohne Nebenbuhler herrschen, und wie anders würde seine äußere Stellung sein!*

[39] [Humboldt & Gauss 1977], p. 32: *Ich lebe noch der angenehmen Hoffnung, den ersten Mathematiker Europas, den tiefsinnigen Astronomen in meinem Hause in Berlin zu empfangen, ihn zu beherbergen und (wie ich kann) zu pflegen.*

Tobias Mayer at Göttingen.[40] The various commentaries made by both men on the occasion of this visit are quite revealing of their different personalities. Gauss expressed his pleasure warmly, first to Humboldt himself after his return to Göttingen:

> You have, most honoured friend, rendered my stay in every respect so pleasurable and instructive by your selfabnegating kindness that I am unable to express my gratitude in words. I count these unforgettable days among the happiest of my life,[41]

then, even more convincingly, to an outsider, three months later:

> My journey to Berlin, where I was housemate of the incomparable Humboldt for almost three weeks, has offered me rich pleasures in every respect. Life in Berlin is very comfortable. The contrast with the calm life in Göttingen is very big. For the mind it is like passsing from the earth's atmosphere into pure oxygen.[42]

As for Humboldt, he wrote to Schumacher, on October 18, a few days after Gauss's thanks:

> I found Gauss charming in day-to-day contact; and he seemed happy. At the beginning, however, and towards strangers, he is cold as a glacier, and does not take part in almost anything which lies outside of the circles he has already touched upon.[43]

Nonetheless, the relations between the two scholars seemed to have cooled, from Humboldt's side at least, when Humboldt, a world expert on earth magnetism, got the impression that this visit had been the launching factor for Gauss's later interest in this topic, a factor that the mathematician did not acknowledge satisfactorily [Humboldt & Gauss 1977], pp. 44, 46–47. Yet they were reconciled in 1837 when

[40] Gauss (positively) wrote in his official evaluation that Weber had then seemed to live more in science than in the outside world, see [Michling 1997], p. 102. Humboldt, as often, used Gauss's opinions to promote Weber: *Der Mann, der bei dem Vereine der 400 nomadischen Freunde am meisten Scharfsinn und Geist gezeigt hat nach Gaussens eigenem Zeugnis, empfiehlt sich durch mich ... Ihrer schützenden Wohlgewogenheit. Er wird gewiß einmal einer der wichtigsten Physiker Deutschlands werden.* Humboldt an Schumacher, January 20, 1829, [Humboldt & Schumacher 1979], p. 37.

[41] Gauss to Humboldt, October 12, 1828, [Humboldt & Gauss 1977], p. 37: *Sie haben mir, mein Verehrtester Freund, meinen Aufenthalt in Berlin mit so großer aufopfernder Güte in jeder Beziehung so genußreich und lehrreich gemacht, daß ich meine Dankbarkeit mit Worten nicht ausdrücken kann. Ich zähle diese mir unvergeßlichen Tage zu den glücklichsten meines Lebens,*

[42] Gauss to Gerling, December 18, 1828, [Gauss & Gerling 1927], p. 329, [Humboldt & Gauss 1977], p. 40: *Meine Reise nach Berlin, wo ich fast drei Wochen Hausgenosse des unvergleichlichen Humboldt war, hat mir in jeder Beziehung reichen Genuß gewährt. Man lebt in Berlin sehr angenehm. Der Abstrich gegen das stille Leben in G[öttingen] ist sehr groß. Es ist für den Geist fast wie der Übertritt aus atmosphärischer Luft in Sauerstoffgas.*

[43] [Humboldt & Schumacher 1979], pp. 34–35: *Über G[auß] bin ich in nahem Umgange entzückt gewesen; auch schien er zufrieden. Anfangs und gegen Unbekannte ist er freilich gletscherartig kalt und untheilnehmend fast für alles, was außer den von ihm schon berührten Kreisen liegt.*

Humboldt met Gauss in Göttingen (it was to be their last meeting), and Gauss sent Humboldt a reprint of his 1839 *Allgemeine Theorie des Erdmagnetismus*, a treatise which Humboldt welcomed with admiration and set off to try and understand, at least intuitively, as he described it, with Jacobi's help.[44]

They remained in contact until Gauss's death in 1855; their correspondence in the 1840s and 1850s concerns mainly the nomination of mathematicians for various honours, in particular the Order *pour le mérite* in sciences.[45] But there was also the "Eisenstein case" to which we shall soon return.

5. A Highschool Teacher, Who Would Be an "Ornament for Any University": Ernst Eduard Kummer

In 1834, a 24-year old highschool teacher drew the attention of the 29-year old Königsberg professor Jacobi, by sending him some of his first publications ([Kummer 1975], vol. 2, pp. 33-41; pp. 75–166; pp. 47–74). After his doctorate in 1831,[46] Kummer had intensively studied the works of Gauss, Abel, and Jacobi, in particular Jacobi's monography *Fundamenta nova theoriae functionum ellipticarum* and Gauss's article on the hypergeometrical series.[47] Kummer was serving a year in the army when he entered in contact with Jacobi, who is told to have commented:

> There we are; now the Prussian musketeers even enter into competition with the professors by way of mathematical works.[48]

[44] [Humboldt & Jocobi 1987], pp. 49–62, [Humboldt & Gauss 1977], pp. 75–82. Humboldt wrote to Gauss on June 18, 1839, [Humboldt & Gauss 1977], p. 76: *Was ich von dem tieferen algebraischen Zusammenhang nicht gleich verstand, hat mir Jacobi, mit dem ich selbst schriftlich darüber verhandelt und den ich stets bei meinem Aufenthalte in Potsdam besuche, zur Intuition gebracht. Zuversicht und Glaube erleichtern die Einsicht und stärken das Fassungsvermögen. Die grossen Geister üben eine anziehende Kraft aus. Ihre 'allgemeine Theorie' hat mich nun seit 6 Wochen fast ununterbrochen beschäftigt. Das Büchlein ist mir überall gefolgt und ich lebe in der frohen Täuschung, daß ich die Theorie besitze, ja vollkommen verstehe, wie in derselben die Mittel liegen, eine Menge spezieller physikalischer Nebenfragen auf das gründlichste beantworten zu können. Siebzigjährig im nächsten September versteinere ich langsam.*

[45] The King created in 1842 within the Order *pour le merite* a specific class for services in the sciences and the arts. Humboldt was its first chancellor, Gauss and Jacobi among the first nominated. Gauss wrote in favour of choosing Dirichlet, underlining that although the young mathematician had not yet published an extended treatise, all of his articles were jewels. But Dirichlet was only nominated after Gauss's death, as Gauss's successor, which he also was to Gauss's Göttingen chair – see [Humboldt & Gauss 1977].

[46] Kummer, born in 1810, in Sorau, the son of a doctor, studied in Halle, first theology, then mathematics. He spent his probationary year as highschool teacher in his home town, then, from 1832 on, was teaching in Liegnitz. On his life and work, see [Kummer 1975], [Hensel 1910], [Biermann 1981c], [Pieper 1988], [Edwards 1998].

[47] See respectively [Jacobi 1881–1891], vol. 1, pp. 49–239 and [Gauss 1863–1933], vol. III, pp. 123–162.

[48] [Kummer 1975], vol. 1, p. 18: *Sieh da, jetzt machen schon preußische Musketiere mit ihren mathematischen Arbeiten den Professoren Concurrenz!*

He was sufficiently impressed by Kummer's results to answer him directly:

> It would certainly be a great gain for the sciences if you would embark on a career giving you full time for your scientific work, although your example also shows how genius overcomes all hurdles. … If you think that I could be of any help with obtaining an academic position, I would be happy to offer my humble services – less because I think that you would need them, or that they would be significant, but as a token of my great respect for your talent and your works.[49]

He praised the "deepness and the originality" of Kummer's achievements, stating that Kummer would be "the ornament of any university."[50] And of course, he finally suggested requiring Humboldt's help:[51]

> I also draw your attention to the fact that A. von Humboldt could easily be useful for you. He has the double passion, firstly for things he does not understand, which is easily forgiven in a man who grasps so many things, and secondly for serving others, which would make his character likeable and even more praiseworthy if he differentiated more keenly. Both, you see, can be profitable for you, or rather, for all of us, since your interest in this case is at the same time that of science itself.[52]

As expected, Humboldt was set to action. On November 21, 1840, he informed Jacobi that he had already accompanied Kummer's request for a position with an "urgent recommendation"[53] for the minister, then Eichhorn; he added:

> How could I forget somebody who has been recommended so urgently by you and Dirichlet. I relied mostly on your testimony, and therefore implore you to write

[49] Jacobi to Kummer, July 13, 1834, [Pieper 1988], p. 27: *Es wäre sicher ein großer Gewinn für die Wissenschaften, wenn Sie eine Carrriere ergriffen, welche Ihnen Ihre volle Zeit zu Ihren wissenschaftlichen Arbeiten gewährte, obgleich man an Ihrem Beispiel wieder sieht, wie das Genie alle ihm entgegenstehenden Hindernisse überwindet. … Wenn Sie glauben, daß ich Ihnen zur Erlangung einer akademischen Thätigkeit von Nutzen sein könnte, so würde ich Ihnen gern meine geringen Dienste anbieten, weniger weil Sie meiner Meinung nach derselben bedürften oder sie von Bedeutung sein könnten, als Ihnen die große Achtung, die ich vor Ihrem Talent und Ihren Arbeiten hege, zu beweisen.*

[50] [Pieper 1988], p. 32 and p. 25: resp. *Tiefe und Originalität* and *eine Zierde jeder Universität.*

[51] Dirichlet also intervened in the same sense. For instance, he proposed Kummer jointly with Steiner and Crelle as a corresponding member of the Berlin Academy as early as 1839. Later, he proposed him as his own successor at Berlin University – see also their correspondence, [Dirichlet NL], n$^\circ$ 48. According to Hensel, Dirichlet was Kummer's teacher in the highest sense, although Kummer never attended any of his lectures, [Kummer 1975], vol. 1, pp. 42–43.

[52] Jacobi to Kummer, June 1, 1838, [Dirichlet NL], n$^\circ$ 49: *Auch mache ich Sie darauf aufmerksam, daß Al. v. Humboldt leicht Ihnen von Nutzen sein könnte, er hat die zwiefache Leidenschaft, erstens für Dinge, die er nicht versteht, was man einem der so vieles umfaßt, gern nachsieht, und zweitens, andern zu dienen, was seinen Charakter liebenswürdig und noch mehr verehrungswürdig machen würde, wenn er mehr unterschiede. Beides, wie Sie sehn, kann Ihnen von Vortheil sein oder vielmehr uns allen, da ihr Vortheil hier zugleich der der Wissenschaft ist.*

[53] [Humboldt & Jacobi 1987], p. 65: *mit einer dringenden Empfehlung.*

> yourself 3 lines to the minister Eichhorn, starting with the words: "A. v. Humboldt just asks me to report to your Excellency about Professor Kummer and the total neglect of mathematical education in Breslau." … Minister Eichhorn will not be able to consider this initiative as indiscreet because I asked you to take it, and because a man in your high position has the right to speak up truly and freely.[54]

As a result of all these efforts by Humboldt, Jacobi, and Dirichlet, Kummer was appointed professor of mathematics at Breslau University in 1841. At that time, he had already begun his work on number-theoretical questions, finding his inspiration in Gauss's writings, mainly the D.A. and Gauss's articles on biquadratic residues. To his student and friend Leopold Kronecker, he wrote:

> From the moment … I recognized that Breslau might be serious, I sat down at home and worked diligently in order to put together something like a dissertation for my habilitation. I started with something completely new: the cubic residues of the primes $6n + 1$. I have since found some remarkable things there, but I am totally ignorant of earlier, and in fact all previous, work of others in this domain, and in order not to remain that ignorant, I ask you to inquire with Dirichlet about it some time.[55]

Following Kronecker's suggestion, Kummer also read Jacobi's relevant articles[56] and communicated his results on cubic residues[57] to Jacobi, who thanked him in December 1842:

> I have to thank you … for your paper on cubic residues. You seem to be pursuing a goal once fixed with terrible perseverance.[58]

[54] [Humboldt & Jacobi 1987], p. 65: *Wie sollte ich jemand vergessen, der mir von Ihnen und Dirichlet so dringend empfohlen ist. Ich habe mich auf Ihr Zeugnis hauptsächlich gestützt und bitte Sie daher inständigst, 3 Zeilen selbst noch in dieser Sache an Minister Eichhorn zu schreiben mit den Worten anhebend: Ich werde soeben durch A[lexander] v[on] H[umboldt] aufgefordert, Ew. Excell[enz] über den Prof[essor] Kummer und die gänzliche Vernachlässigung des mathem[atischen] Unterrichts in Breslau zu berichten … Minister Eichhorn wird diesen Schritt nicht für indiscret halten können, da Sie durch mich aufgefordert sind und es einem so hoch gestellten Mann wie Ihnen ansteht, wahr und frei zu reden.*

[55] Kummer to Kronecker, February 9, 1842, [Kummer 1975], vol. 1, p. 79: *Seit ich … merkte, es könne mit Breslau Ernst werden, so setzte ich mich zu Hause hin und arbeitete sehr fleißig, um so etwas wie eine Dissertation zur Habilitirung zu [er]arbeiten, und ich fing bei etwas mir ganz neuem an, nämlich bei den Cubischen Resten der Primzahlen* $6n+1$. *Ich habe seitdem einige bemerkenswerthe Dinge darin gefunden, bin aber mit den früheren oder vielmehr bisherigen Leistungen Anderer in diesem Fache ganz unbekannt, und um damit nicht unbekannt zu bleiben, so richte ich an Sie die Bitte, einmal Dirichlet hierüber zu befragen.*

[56] See [Jacobi 1881–1891], vol. 6, pp. 233–237, 254–274.

[57] [Kummer 1975], vol. 1, pp. 145–163.

[58] [Pieper 1988], p. 26: *Ich habe Ihnen … für Ihre Abhandlung über kubische Reste zu danken. Sie scheinen mit ungeheurer Hartnäckigkeit ein einmal vorgestecktes Ziel zu verfolgen..* [Editors'note: on this goal and its effects on the development of number theory, see R. Bölling's chap. IV.1 in this book.]

6. A Talent "That Nature Bestows on Only a Few Men in Each Century": Gotthold Eisenstein

During the summer of 1843, Helene Eisenstein applied to the *Kultusministerium* for financial support for her son's studies.[59] The police were asked to report on the situation of the applicant. From this report, we learn a few things about the life of Gotthold Eisenstein,[60] born in Berlin in 1823. His parents, of Jewish origin, converted to Christianity the year of his birth, and spent some time in England, in the hope of improving their income.

> G. Eisenstein first attended a higher *Bürgerschule* here in Berlin, then the *Werdersches Gymnasium* until the last year. He is now, after the interruption due to his trip to England, taking his graduation exam before the commission.[61] According to his teachers, in particular Dirichlet whose lecture courses he has taken, the young man has an excellent gift for the mathematical sciences, and commands an admirable wealth of knowledge, considering his age.[62]

Despite this impressive recognition, the request failed. Eisenstein, who had already attended lectures by Dirichlet and Martin Ohm as a highschool pupil and who had met Hamilton while in Dublin, studied mathematics at Berlin University[63] from the winter 1843–1844 onwards. He then renewed his application for a stipend. His mother also turned to the Queen for protection:

> Even if the most pressing worries about food already assail me in this desperate situation, my heart is humiliated even more deeply by the unspeakable pain of seeing my son deprived of his studies for lack of means, in particular in mathematics to which he has devoted himself not only following his chief inclination, but also with dominating talent and, up to now, with such rare success that he justifies the highest expectations for the future, according to the testimonies of such excellent

[59] I am preparing the edition of the whole "Akte Eisenstein", [*Kultusministerium*] Vf Litt E Nr 6, together with the (recovered) original letters of Humboldt to Eisenstein.

[60] More information can be found in [Biermann 1959b], [Biermann 1959c], [Biermann 1961], [Biermann 1964], [Eisenstein 1975], [Biermann 1981b], [Biermann 1992], and [Schappacher 1998].

[61] He attended the Friedrich-Wilhelms-Gymnasium from 1837 onwards, the Werdersches Gymnasium from 1840 to 1842. He obtained his final certificate on September 22, 1843 at the Friedrich-Wilhelms-Gymnasium on Berlin.

[62] [*Kultusministerium*], Vf Litt E Nr 6, pp. 3–8: *[G. Eisenstein] hat hier [in Berlin] eine höhere Bürgerschule, sodann das Werdersche Gymnasium bis Prima besucht und ist jetzt, da sein Cursus durch den Aufenthalt in England unterbrochen war, beschäftigt, die Abiturienten-Prüfung vor der Commission abzulegen. Nach dem Zeugniß seiner Lehrer, insbesondere des Professor Dirichlet bei welchem er Vorlesungen gehört, hat der junge Mann eine hervorragende Anlage für die mathematischen Wissenschaften, und einen für sein Alter bewunderungswürdigen Umfang von Kenntnissen.*

[63] Besides Dirichlet, Steiner, and the *Privatdozent* Minding, the professors were still the ones whose lectures Jacobi had attended as a student: Grüson, Lubbe, Dirksen, M. Ohm. After his election to the Berlin Academy of Sciences in 1844, Jacobi himself used the right thus obtained to lecture at the University several times.

> judges as the professors Dirichlet, Jacobi, Schellbach, Hamilton in Dublin.[64]

The Queen recommended Eisenstein to the *Kultusminister* who, after further information from the University, supported the request to the King on April 1, 1844. Meanwhile, Humboldt had been made aware of Eisenstein's precocious talents by Crelle or by Dirichlet, or both, and predictably wrote to the King as well. These efforts succeeded at last: from May 1, 1844, Eisenstein received an annual stipend of 250 *Thaler* – see [*Kultusministerium*], Vf Litt E Nr 6, pp. 41–46. A few days later, Humboldt explained to Eisenstein:

> Human life is a conditional equation, and the securing of some of its material needs is one of the most important conditions to satisfy. … Do not be surprised by the small sum. There are limits which cannot easily be crossed, because the noble will of the monarch to help a young man with such rich gifts is counteracted by those cooling influences of the financial bureaucrats who calculate, which however does not render them more positively inclined towards the theory of numbers.[65]

One may weigh this against the mathematical production of the young man; the two volumes of Crelle's journal of the same year 1844 contain altogether 25 articles by Eisenstein (including two collections of exercises)! On January 25, 1844, he had already submitted to the Berlin Academy of Sciences a long memoir containing some of his results on cubic forms with two variables. In his accompanying letter, he explained:

> Since everything that has been produced in the theory of numbers up to now is limited to the consideration of forms of the second degree, this first step into the realm of higher forms may not be completely useless for science. The results found by me seem to be all the more interesting as they express an intimate connection between the theory of cubic forms and another part of higher arithmetic, of which the famous Gauss says that it seems to depend on the deepest mysteries of the science of numbers, to wit, the theory of multiplication of quadratic forms. Without going into details I just note that in a way the role played by the quadratic residues with

[64] [*Kultusministerium*], Vf Litt E Nr 6, pp. 20–22: *[W]enn mich in dieser trostlosen Lage schon die drückendsten Nahrungssorgen bedrängen, so wird mein Herz doch noch weit tiefer gebeugt durch den unaussprechlichen Schmerz, meinen Sohn dem Studium, besonders der Mathematik, aus Mangel an Mitteln entrissen zu sehen, welchem er sich nicht nur mit vorherrschender Neigung sondern auch nach dem Zeugnisse ausgezeichneter competenter Beurtheiler, wie der Professoren Dirichlet, Jacobi, Schellbach, Hamilton in Dublin, mit so überwiegendem Talent und bis hieher mit so seltenem Erfolge gewidmet hat, daß er für die Zukunft zu den glänzendsten Erwartungen berechtigt.*

[65] Humboldt an Eisenstein, Mai 11, 1844, [Biermann 1959b], pp. 122–123, [Biermann 1992], pp. 127–128: *Das menschliche Leben ist eine Bedingungsgleichung, und Sicherheit eines Theils der materiellen Bedürfnisse ist eine der Bedingungen, deren Erfüllung am wichtigsten ist. … Wundern Sie sich nicht über die Kleinheit der Summe. Es giebt Grenzen, die hier schwer überschritten werden, da dem edeln Willen, den der Monarch hat, einem so reichbegabten jungen Manne hülfreich zu werden, erkältende Einflüsse der rechnenden, aber deshalb der "Zahlen-Theorie" nicht holderen Finanzmänner entgegentreten.*

> the forms of the second degree is here taken over, not by the cubic residues, but by certain classes of quadratic forms which may be generated by "triplication" of other classes, so that the analogy is, so to speak, shifted over to other territory. In the second half of the fifth section of the *Disquisitiones Arithmeticae*, Gauss has established a very nice theory of the duplication of classes, not so much for its own sake, but with a view towards application to other things. The results of this theory, which are scattered over the work, may be condensed in the statement "that for every given determinant, those classes which may be obtained by duplication are precisely those of the *genus principale*, and that each of them may be obtained by duplicating as many classes as there are *genera*."[66] Nothing is to be found, however, about the triplication of classes.[67]

On Encke's advice, Eisenstein also sent some of his papers to Gauss before visiting him personally in Göttingen in June 1844. Encke wrote to Humboldt:

> Especially for a young talent this meeting seems to me to be most important. Our great mathematicians here may feel a bit jealous, or just uncomfortable, when a new talent arises at the same place, particularly in an excited city like Berlin, and at such an excited time. For Gauss in the tranquility of Göttingen it is easier to control possible unpleasant reactions, and he has a special gift of encouraging others. Besides, nothing is more beneficial to Gauss than to have somebody to talk to.[68]

[66] See F. Lemmermeyer's chap. VIII.3 below [Editors'note].

[67] [Biermann 1961], p. 10: *Da Alles, was bis jetzt auf dem Gebiete der Zahlentheorie in Beziehung auf die homogenen ganzen Funktionen geleistet worden ist, sich auf die Betrachtung der Formen des zweiten Grades beschränkt, so möchte dieser mein erster Schritt in das Gebiet der höheren Formen vielleicht nicht ganz ohne Nutzen für die Wissenschaft sein. Die von mir gefundenen Resultate scheinen ein um so größeres Interesse darzubieten, als sie eine innige Beziehung aussprechen zwischen der Theorie der cubischen Formen und einem andern Theile der höheren Arithmetik, von welchem der berühmte Gauss sagt, daß er von den tiefsten Mysterien der Zahlenlehre abzuhängen scheint, nämlich der Theorie der Multiplication der quadratischen Formen. Ohne mich auf Einzelheiten einzulassen, bemerke ich nur, daß gewissermaßen die Rolle, welche die quadratischen Reste bei den Formen des zweiten Grades spielen, hier nicht etwa von den cubischen Resten übernommen werden, sondern von gewissen Klassen quadratischer Formen, welche durch die 'Triplication' anderer Klassen erzeugt werden können, so daß die Analogie, um mich so auszudrücken, auf ein anderes Feld hinübergespielt wird. Gauss hat in der letzten Hälfte des fünften Abschnittes seiner Disquisitiones Arithmeticae weniger um der Sache selbst willen, als wegen der Anwendung auf andere Gegenstände, eine sehr schöne Theorie der Duplication der Klassen aufgestellt, deren Resultate, im Werke zerstreut, sich in dem Satz zusammendrängen lassen, "daß für jede bestimmte Determinante diejenigen Klassen, welche durch Duplication entstehen können, die Klassen des genus principale sind, und daß jede derselben aus der Duplication so vieler Klassen entstehen kann, als es genera giebt." Über die Triplication der Klassen findet sich dagegen noch nichts.*

[68] [Biermann 1959b], pp. 114–115: *Gerade bei einem jungen Talente scheint mir dieses Zusammensein von der größten Wichtigkeit. Unsere großen Mathematiker hier fühlen (vielleicht) eine kleine Eifersucht oder doch ein Mißbehagen wenn an dem Orte selbst u. noch dazu in einer so erregten Stadt wie Berlin u. einer so erregten Zeit ein neues Ta-*

Again, a network of letters was efficiently set to action: Humboldt provided an introductory letter for Eisenstein in Göttingen, Gauss wrote to Encke about Eisenstein's papers, Encke transmitted at least part of it to Humboldt along with his own letter, and Humboldt could use it, when he asked the *Kultusminister* Eichhorn for a additional support to send Eisenstein for a few weeks to a cure in Alexisbad:

> As testimony to the importance of Eisenstein's knowledge and talent by the biggest authority in Europe, next to Jacobi, I quote from the letter of *Hofrath* Gauss to Encke: "I have only had the time so far to peruse one of the papers, but it made me encounter an *extraordinarily ingenious* author. This work bestows the *highest honour* on Eisenstein. I would be very glad to meet such an outstanding young man in person. I could not be of any use to him through instruction because he has *obviously* passsed that stage *long ago and by far*."[69]

A day later, Crelle also wrote to Eichhorn with the same aim, and much the same line of argument:

> For an extraordinary new talent has emerged here recently, the student Herr G. Eisenstein. … Herr Eisenstein, although barely more than 20 years old, has already made some real discoveries in analysis, especially in the theory of numbers, and he has penetrated the most difficult problems with awesome energy. He has produced a series of papers on reciprocity laws for real and complex numbers, on quadratic and cubic forms, on biquadratic residues, on cyclotomy, on elliptic and Abelian transcendents, etc. They contain many new things, and some of them advance on almost uncharted territory. A first series of his papers is printed in the 27th volume of the *Journal der Mathematik*, and a second series is currently in press for the 28th volume. Also … *Herr Hofrath Gauss in Göttingen* has taken notice of the first papers of Herr Eisenstein, and has also received his personal visit, and as far as I heard has

lent sich aufmacht. Gauß in dem ruhigen Göttingen kann leichter etwaige unangenehme Berührungen abhalten u. hat eine besondere Gabe Andere anzuspornen. Nebenbei ist für Gauß selbst nichts wohlthätiger als Jemand zu haben mit dem er sich unterhalten kann. Let us also record Encke's further comments on Eisenstein's personality and on precocious mathematical talent in general: *Es ist eine eigene Sache mit diesen mathematischen Talenten daß sie immer so jung sich hervorthun, daher auch ein gewißer Uebermuth von dem Eisenstein ebenfalls nicht frei ist. Auch liegt in der beständigen Spannung mit welcher der Mathematiker prüft ob auch Alles richtig sei, eine Anstrengung, welche den Umgang mit ihm schwer macht. Es sind häufig etwas eigensinnige und manchmal auch einseitige Männer, von denen die Klügeren nur dieses Selbstbewußtsein des eigenen Werthes zu bemänteln wissen. … Der Ehrgeiz wird bei diesem isolirenden Studium entsetzlich angeregt.*

[69] Humboldt to Eichhorn, July 5, 1844, [Biermann 1985], pp. 110–111: *Um die Wichtigkeit der Kenntnisse und Anlage des p. Eisenstein durch eine Autorität zu bezeugen, die mit Jacobi die größte in Europa ist, ziehe ich folgende Stelle aus dem Briefe des Hofrath Gauß an Encke aus: "Ich habe bisher nur eine der Abhandlungen durchnehmen können, habe aber den Verf[assser] als einen* überaus genialischen *Kopf daraus kennen gelernt. Die Arbeit gereicht dem Eisenstein zur* größten Ehre. *Es würde mich freuen, die nähere Bekanntschaft eines so trefflichen jungen Mannes zu machen. Durch Unterricht könnte ich ihm nicht nützlich werden, da er über diesen* offenbar längst *und* weit hinaus *ist."* (Humboldt's emphasis.)

> welcomed these works as well as their author with approval. … It therefore seems beyond doubt that Herr Eisenstein has to be regarded as a very promising young scientist who therefore deserves all possible promotion and support for his endeavours. … As his teacher he especially venerates Professor Lejeune-Dirichlet.[70]

Through these combined efforts, Eisenstein got his exceptional support. Gauss had not inflated his opinion of Eisenstein for tactical reasons; he told for instance Gerling and Schumacher about the visit of the young mathematician:

> I have recently made the acquaintance of a young mathematician from Berlin who came here with a letter of recommendation from Humboldt. This still very young man shows excellent talent and will certainly achieve something big.[71]

And to Schumacher, he wrote similarly:

> I have had the occasion the other day to meet personally a young mathematician who came here with a recommendation by Humboldt and who has a highly excellent talent. His name is Eisenstein and he seems to be of Jewish origin. The 27th volume of Crelle's journal contains a lot of articles by him, mainly belonging to higher arithmetic, which are however, as far as I have been able to look at them, of uneven value. But even the weakest among them would arouse favourable expectations, considering that they come from a 21-year old young man, while some of it is of the sort that the first master would not have to disown. I expect great things from him. He seems to come from modest circumstances, but he has a yearly stipend from the King of Prussia which seems to be sufficient for the time being.[72]

[70] Crelle to Eichhorn, July 6, 1844, [Biermann 1959c], pp. 70–71; [*Kultusministerium*] Vf Litt E Nr 6, p. 49–52: *Es hat sich nämlich so eben in der letzten Zeit hier in der Person des Studiosus Herrn G. Eisenstein ein neues außerordentliches Talent hervorgethan. … Herr Eisenstein hat schon, obgleich erst wenig über 20 Jahre alt, mehrere wirkliche Entdeckungen in der Analysis gemacht, besonders in der Theorie der Zahlen und ist in die schwierigsten Aufgaben mit einer Energie gedrungen, welche Staunen erregt. Er hat über die Gesetze der Reciprocität bei reellen und complexen Zahlen, über die quadratischen und cubischen Formen, über die biquadratischen Reste, über die Kreistheilung, über die elliptischen und Abelschen Transcendenten u.s.w. eine Reihe von Abhandlungen geliefert, die gar manches Neue enthalten und zum Theil auf fast unbetretenen Wegen vordringen. Eine erste Reihe dieser seiner Abhandlungen ist in dem 27. Bande des "Journals der Mathematik" gedruckt, und eine zweite Reihe ist im 28. Bande so eben in der Presse. Auch … Herr Hofrath Gauß in Göttingen hat von den ersten Arbeiten des Herrn Eisenstein, der sich ihm persönlich vorgestellt hat, Kenntnis erhalten und hat dem Vernehmen nach diese Arbeiten und ihren jungen Verfasser mit Beifall aufgenommen. … Es dürfte daher Herr Eisenstein wohl unzweifelhaft als ein für die Wissenschaft viel versprechender junger Mann zu betrachten sein und folglich in seinen Bestrebungen alle nur mögliche Förderung und Unterstützung verdienen. … Als seinen Lehrer insbesondere verehrt er den Herrn Professor Lejeune-Dirichlet.*

[71] Gauss to Gerling, June 14, 1844, [Gauss & Gerling 1927], p. 701–703: *Ich habe unlängst einen jungen Mathematiker, Eisenstein aus Berlin, kennengelernt, der mit einem Empfehlungsschreiben von Humboldt hieher kam. Dieser noch sehr junge Mann zeigt sehr ausgezeichnetes Talent und wird gewiß Großes leisten.*

[72] [Gauss & Schumacher 1860–1865], vol. 4, pp. 265–266: *Ich habe dieser Tage Gelegenheit*

And when Gauss proposed Dirichlet for the Order *pour le mérite* (see above), he recognized that the choice between Dirichlet and Eisenstein had been difficult.[73]

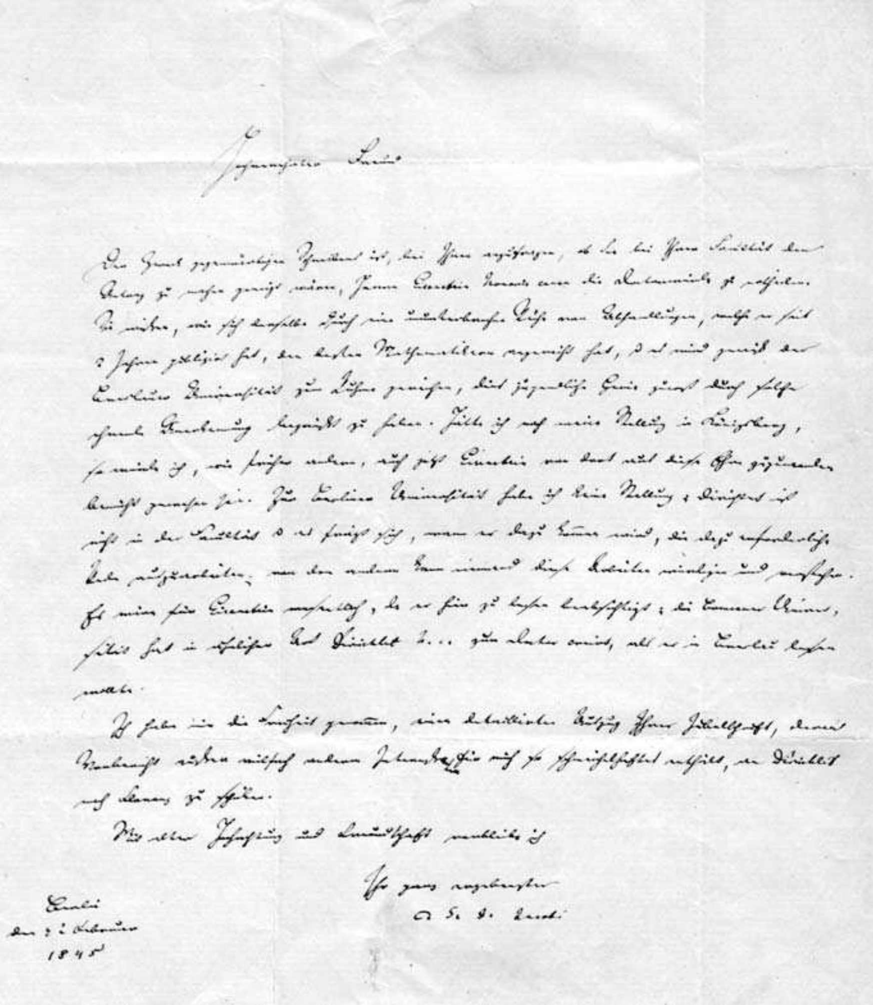
Jacobi, too, acted in favour of Eisenstein. First of all, in February 1845, he asked for a financial support of 300 *Thaler* from the Academy of Sciences, "to put Eisenstein in a position to finish a work on the theory of complex numbers which promises a new enrichment for science," [Biermann 1959b], p. 110. Interestingly, the Academy offered only half of the promised sum immediately; the second half was to be given after completion of the work, and was, indeed, in October of the same year ([*Kultusministerium*], Vf Litt E Nr 6, p. 88). Also, Jacobi was influential in obtaining a doctorate *honoris causa* for Eisenstein. He wrote to this effect to Kummer:

> The purpose of the present letter is to ask you if you would be inclined to apply to your Faculty to award an honorary doctorate to Herr Eisenstein. You know how he has added his name to the list of the best mathematicians by the uninterrupted series of papers which he has published over the last two years. It will certainly be a point of honour for the Breslau University to have been the first to have welcomed the youthful genius with such an honourable distinction. If I still had my position in Königsberg, I would have made an effort, as I did in other cases at the time, to bestow this honour on Eisenstein from there. But I have no official connection with Berlin University. Dirichlet is not a member of the Faculty, and there is also the question of when he would find the time to write up the necessary speech. None of the other colleagues can appreciate and understand those papers.[74]

gehabt, einen jungen Mathematiker, der mit einer Empfehlung von Humboldt hieher kam, persönlich kennen zu lernen, der ein höchst ausgezeichnetes Talent besitzt. Sein Name ist Eisenstein, und er scheint aus jüdischem Stamme zu sein. Der 27. Band des Crelleschen Journals enthält eine Menge von Aufsätzen von ihm, grösstentheils zur höhern Arithmetik angehörig, die allerdings, so weit ich bisher sie habe beachten können, von ungleichem Werth sind, aber auch die schwächsten darunter, würden in Erwägung, dass sie von einem 21jährigen jungen Menschen herrühren, günstige Erwartungen erregen, während manches der Art ist, dass der erste Meister es nicht zu desavouiren haben würde. Ich verspreche mir grosses von ihm. Er scheint, von Haus aus in beschränkten Umständen zu sein, hat aber eine, ihm vor der Hand genügende, jährliche Unterstützung vom Könige von Preussen.

[73] Gauss to Humboldt, [Humboldt & Gauss 1977], p. 88. Humboldt transmitted the letter to Dirichlet: *Man stellt Ihren Schüler Ihnen so nahe! Das ist der Lauf der Welt, der eigentlichen Geisteswelt. Wie viele habe ich als Kinder gesehen, die jetzt über mir stehen und deren Arbeiten leben werden, wenn mein Ruf längst verschollen ist*, [Humboldt & Dirichlet 1982], p. 67. Dirichlet's reaction to this is not known.

[74] [Humboldt & Jacobi 1987], p. 25; [Dirichlet NL], n° 61: *Der Zweck gegenwärtigen Schreibens ist, bei Ihnen anzufragen, ob Sie bei Ihrer Facultät den Antrag zu machen geneigt wären, Herrn Eisenstein honoris causa die Doctorwürde zu ertheilen. Sie wissen, wie sich derselbe durch eine ununterbrochene Reihe von Abhandlungen, welche er seit zwei Jahren publizirt hat, den besten Mathematikern angereiht hat, und es wird gewiß der Breslauer Universität zum Ruhme gereichen, dies jugendliche Genie zuerst durch solche ehrende Anerkennung begrüßt zu haben. Hätte ich noch meine Stellung in Königsberg, so würde ich, wie früher andern, auch jetzt Eisenstein von dort aus diese Ehre zuzuwenden*



Hochgeschätzter Freund

Der Grund gegenwärtigen Schreibens ist, Sie aufzufordern, ob Sie bei Ihrer Facultät den Antrag zu machen geneigt wären, Herrn Eisenstein honoris causa die Doctorwürde zu ertheilen. Sie wissen, wie sich derselbe durch eine wunderbare Reihe von Abhandlungen, welche er seit 2 Jahren publicirt hat, den ersten Mathematikern angereiht hat, so daß es gewiß der Breslauer Universität zur Ehre gereichen, dies jugendliche Genie zuerst durch solche seine Auszeichnung begrüßt zu haben. Hätte ich noch meine Stellung in Königsberg, so würde ich, wie früher andern, auch jetzt Eisenstein von dort aus diese Ehre zuzuwenden bemüht gewesen sein. Zur Berliner Universität habe ich keine Stellung; Dirichlet ist nicht in der Facultät und es fragt sich, wann er dazu kommen wird, die dazu erforderliche Rede auszuarbeiten; von den andern kann niemand diese Arbeiten würdigen und verstehn. Es wäre für Eisenstein wünschenswerth, da er hier zu bleiben beabsichtigt; die hiesige Universität, [illegible] Dirichlet [illegible] zu [illegible] wird, als er in Breslau [illegible] werde.

Ich habe mir die Freiheit genommen, eine lithographirte Abschrift Ihrer Jubelschrift, deren [illegible] auf so schmeichelhafte Weise erhielt, an Dirichlet [illegible] zu schicken.

Mit aller Hochachtung und Freundschaft verbleibe ich

Ihr ganz ergebenster
C. G. J. Jacobi

Berlin
den 2[illegible] Februar
1845

Fig. III.1B. A letter from Jacobi to Kummer in favour of Eisenstein
Archiv der Berlin-Brandenburgischen Akademie der Wissenschaften, Nachlaß Dirichlet
(Courtesy of ABBAW)

Kummer did propose to the Philosophical Faculty of Breslau University the award of a doctorate *honoris causa* to Eisenstein, and this was done in 1845.

bemüht gewesen sein. Zur Berliner Universität habe ich keine Stellung; Dirichlet ist nicht in der Facultät und es fragt sich, wann er dazu kommen wird, die dazu erforderliche Rede auszuarbeiten; von den andern kann niemand diese Arbeiten würdigen und verstehn.

With this doctorate, Eisentein became ostensibly a part of the network comprising Humboldt, Gauss, Dirichlet, Jacobi,[75] and Kummer. There is no room here to describe in every detail how Humboldt continuously acted in his favour, applying to the King, to the *Kultusminister*, to the *Finanzminister*, to the Academy of Sciences, and how he used repeatedly Dirichlet's, Jacobi's and above all Gauss's positive statements about Eisenstein. One more example will suffice: in April 1846, Gauss wrote to Humboldt that he "considers [Eisenstein's] gift as one that Nature bestows on only a few men in each century";[76] on April 17, Humboldt communicated this judgment to Eisenstein himself, but also to the minister Eichhorn; and on June 7, he sent Gauss's letter itself to Eichhorn, see [Humboldt & Gauss 1977], p. 93, [Biermann 1992], pp. 132–134. The success of the procedure, a renewed subvention for Eisenstein, was followed by another round of letters, with thanks and congratulations.

But it still remained to provide Eisenstein (who secured his *Habilitation* in 1847) with a professorship. When Jacobi was about to accept an offer from Vienna in 1850, Humboldt saw the opportunity to write once more to the Minister, Ladenberg at the time:

> His Excellency will gracefully excuse me, if I again write to you with a request in a matter which has occupied me without interruption over the last 4 years. For it concerns the living conditions of a rare and great talent, which is not merely budding, but is already established and productive. The works of the *Privat-Docent Dr. Eisenstein* have found the most vivid recognition with the most famous mathematicians of our time; with Gauss, who has edited a selection of these works, with Dirichlet, Cauchy and Poinsot in Paris. A new proof of his relentless activity is an investigation that has just appeared on one of the most difficult problems of higher analysis, "on the division of the lemniscate and its application to number theory." ... The painful loss that our university and academy are suffering by Jacobi's departure prompts me to plead for the request: to most gracefully announce to the *Privat-Docent*

[75] It is well-known that a public quarrel broke out between Jacobi and Eisenstein at the beginning of 1846, as Jacobi felt that Eisenstein failed to properly acknowledge his use of others' (in particular Jacobi's) ideas in his own work, [Biermann 1959b]. However, Jacobi's open criticism of Eisenstein's "carelessness" in scientific matters (*Leichtsinn* in Jacobi's words) did not mask out his recognition of Eisenstein's talent: *Der Dr. Eisenstein*, wrote Jacobi to the Minister, *hat vor einigen Jahren die mathematische Welt durch eine Reihe sehr schnell und in großer Menge aufeinanderfolgender Arbeiten in Verwunderung gesetzt und die Aufmerksamkeit auf sich gezogen. Es zeigte sich bei näherer Kenntnißnahme, daß diese Arbeiten von sehr verschiedenem Werth waren [Gauss's own judgment]. Einige waren bei einem sehr hohen Tone voll schülerhafter Überlegungen; bei anderen zeigte es sich, daß ihre Grundideen aus mündlichen Mittheilungen andrer oder ungedruckten Collegienheften entlehnt waren. ... Aber einige dieser Arbeiten waren so ausgezeichnet und trugen in solchem Grade das Gepräge eines großen und originellen Talentes, daß jeder unserer ersten Mathematiker mit Freude seinen Namen unter dieselben gesetzt haben würde*, [Biermann 1959b], pp. 111– 112; [*Kultusministerium*], Vf Litt E Nr 6, pp. 117–118.

[76] Gauss to Humboldt, April 14, 1846, [Humboldt & Gauss 1977], p. 93: *seine Begabung wie eine solche betrachte, welche die Natur in jedem Jahrhundert nur wenigen ertheilt.*

> *Dr. Eisenstein* that he will receive as of Easter a fixed salary of five to six hundred *Thaler* by way of appointment to extraordinary professor.[77]

But Jacobi, as we have seen, remained in Prussia, partly thanks to Humboldt, [Pieper 2005]. At the end of March, he himself suggested to Ladenberg to offer Eisenstein a position in Halle or Bonn,[78] and the request was repeated jointly by Dirichlet, Jacobi, and Humboldt at the beginning of August, again in vain. Dirichlet and Jacobi, this time with Encke, also proposed Eisenstein to a membership at the Academy of Sciences in December 1850. At this occasion, they reported on his work in some detail:

> For a number of years, *Herr Dr. Eisenstein* has gained the recognition of mathematicians by many important publications in which new aspects of the most difficult problems have been extricated. In particular, several new proofs of the cubic and biquadratic reciprocity laws that he has given – laws that Gauss had called a *mysterium maxime reconditum* – belong to the most beautiful enrichments of this subtle part of mathematics, due to their astuteness and the specificity of their principles. Another investigation of Herr Eisenstein concerns a subject that was first initiated by Gauss. It has been known since Fermat, and Euler, of whom this proof is one of the fundamental discoveries, first demonstrated that a prime number which leaves the residue 1 when divided by 4 can always be decomposed into two squares in a unique way. However, the link of the roots of those squares with the prime number to be decomposed remained obscure until Gauss made the remarkable discovery that these roots are the residues that result from the division of certain binomial coefficients by the prime number. This beautiful theorem was extended shortly afterwards and simultaneously by Cauchy and one of the undersigned to infinitely many quadratic expressions. But these new results only concerned the representation of prime numbers that are contained in arithmetic progressions starting with 1. An interesting remark obtained inductively by Stern prompted Herr Eisenstein to prove the first analogous theorems for prime numbers contained in different arithmetic progressions, thus opening a new field of research. Herr Eisenstein who had based

[77] Humboldt to Ladenberg, February 20, 1850, [Humboldt 1985], pp. 131–132: *Ew. Excellenz werden gewogentlichst verzeihen, wenn ich noch einmal mich bittend an Sie wende in einer Angelegenheit, die mich seit 4 Jahren ununterbrochen beschäftigt, weil sie die Lebensbedingnisse eines seltenen, großen, nicht etwa aufkeimenden, sondern erprobten und producirenden Talentes betrifft. Die Arbeiten des Privat-Docenten Dr. Eisenstein haben bei den berühmtesten Mathematikern unserer Zeit, bei Gauß, der einen Theil derselben mit glänzendem Lobe herausgegeben, bei Dirichlet, Cauchy und Poinsot in Paris, die lebhafteste Anerkennung gefunden. Ein neuer Beweis seiner unermüdeten Thätigkeit ist eine eben erschienene Untersuchung über eine der schwierigsten Aufgaben der höheren Analysis, "über die Lemniscatentheilung und ihre Anwendung auf die Zahlentheorie" [See [Eisenstein 1975], vol. 2, pp. 536–619] ... Der schmerzliche Verlust, den unsere Akademie und die Universität durch die Abberufung von Jacobi erleidet, veranlaßt mich ... die ... Bitte vorzutragen: dem Privat-Docenten Dr. Eisenstein zu Ostern ein festes Gehalt von fünf- bis sechshundert Thalern mit dem Charakter als außerordentlicher Professor gnädigst zu verheißen.*

[78] See [*Kultusministerium*], Vf Litt J Nr 7, Bl. 129–130.

> one of his proofs of the biquadratic reciprocity law on the algebraic division of the lemniscate later succeeded in deriving also the reciprocity laws for the 8th powers from the same source. All these works, which the class [of the Berlin Academy] has accepted for publication in the *Monatsberichte*, allot to Herr Eisenstein a place of honour among the most distinguished mathematicians.[79]

Jacobi died a few weeks after this episode, on February 18, 1851. Two days later, Humboldt wrote to Johannes Schulze that, "in the middle of the deep grief which I feel upon Jacobi's death … all my attention is directed to Eisenstein," [Humboldt 1985], pp. 143–144. At least, Dirichlet, Encke, and Ludwig Hagen renewed a proposal to the Academy and in March 1852, Eisenstein was chosen as ordinary member of the Berlin Academy of Sciences. At age 29, he was the youngest member. In his inaugural lecture, on July 1, he said:

> I have been attracted early on by the beauties of a field which differs from others not only by its subject matter but distinguishes itself from all others by the peculiarity

[79] [Biermann 1960c], p. 19 and [Biermann 1990], pp. 210–211: *H[err] Dr. Eisenstein hat sich seit einer Reihe von Jahren die Anerkennung der Mathematiker durch bedeutende und zahlreiche Arbeiten erworben, in denen den schwierigsten Fragen der Wissenschaft neue Gesichtspunkte abgewonnen sind. Es gehören namentlich mehrere der von ihm gegebenen neuen Beweise der kubischen und biquadratischen Reziprozitätsgesetze, deren Begründung Gauß als ein mysterium maxime reconditum bezeichnet, durch ihren Scharfsinn und die Eigentümlichkeit ihrer Prinzipien zu den schönsten Bereicherungen dieses subtilen Teiles der Mathematik. Eine andere Untersuchung des H[errn] Eisenstein betrifft einen von Gauß zuerst angeregten Gegenstand. Seit Fermat ist es bekannt und Euler, zu dessen Fundamentalentdeckungen dieser Beweis gehört, hat zuerst dargetan, daß eine Primzahl, welche bei der Division durch 4 die Einheit zum Rest läßt, immer in zwei Quadrate, und zwar nur auf eine Weise, zerlegbar ist. Verborgen blieb jedoch der Zusammenhang der Wurzeln dieser Quadrate mit der zu zerlegenden Primzahl, bis Gauß die merkwürdige Entdeckung machte, daß diese Wurzeln die Reste sind, welche sich bei der Division gewisser Binomialkoeffizienten durch die Primzahl ergeben. Dieser schöne Satz wurde bald nachher gleichzeitig durch Cauchy und einen der Mitunterzeichner auf unendlich viele quadratische Ausdrücke ausgedehnt, aber diese neuen Resultate bezogen sich ausschließlich auf die Darstellung von Primzahlen, die in arithmetischen Reihen enthalten sind, welche mit der Einheit beginnen. Eine interessante, von Stern auf dem Wege der Induktion gemachte Bemerkung hat H[errn] Eisenstein Veranlassung gegeben, die ersten analogen Sätze für Primzahlen zu beweisen, welche in anderen arithmetischen Reihen enthalten sind, und so diesen Untersuchungen ein neues Feld zu eröffnen. Herr Eisenstein, der einen seiner Beweise für die biquadratische Reziprozität auf die algebraische Teilung der Lemniskate gegründet hatte, ist es später gelungen, aus derselben Quelle auch die bisher noch unbekannten Reziprozitätsgesetze für die 8ten Potenzen abzuleiten. Alle diese Arbeiten, welche die Klasse in die Monatsberichte aufgenommen hat, weisen H[errn] Eisenstein einen ehrenvollen Platz unter den ausgezeichneten Mathematikern an.* Although Eisenstein obtained an absolute majority of votes, there were only two positions available. They were given to the physiologist Emil du Bois-Reymond and to the zoologist Wilhelm Peters, who had obtained even more votes. On the other hand, Gauss successfully proposed both Kummer and Eisenstein as corresponding members of the Göttingen Society of Sciences in August 1851.

> and variety of its methods. Here it is not sufficient to unfold the consequences of a single idea in a long series of developments, but almost every step requires the mastering of new difficulties, the application of new principles. The theory of numbers … has taken such a flight in a short period of time with Gauss and his successors that it now does not lack depth nor breadth in comparison to any other mathematical discipline, and it has inspired many of them. A school has formed that counts among its followers the most outstanding mathematical talents, and in which I also proudly count myself, even if only as one of its least acolytes.[80]

But Eisenstein died only a few months later, on October 11, 1852.

7. A Diplomat for Science

Analyzing the development of mathematics during the XIX$^{\text{th}}$ century, Felix Klein wrote that Humboldt

> enjoyed an extraordinary position in Berlin society which gave him a great deal of influence through his link to the court and his manifold connections.[81]

One might also say that Gauss enjoyed "an extraordinary scientific position," in particular among circles of number theorists through the influence of his *Disquisitiones Arithmeticae*, the Bible of the domain. The good relations between Gauss and Humboldt eased the paths of Dirichlet, Jacobi, Kummer, and Eisenstein.

The discovery of these talents did not follow the same pattern. Humboldt heard about Gauss from French mathematicians, while in Paris, and likewise for Dirichlet. Humboldt then informed Gauss to whom Dirichlet himself sent one of his memoirs. Gauss recognized Jacobi's mathematical competence from a number-theoretical letter that Jacobi sent to him; and it was through Gauss and Legendre that Humboldt's attention was drawn to Jacobi's talent, while Dirichlet made the latter's acquaintance first through his articles and then personally. Kummer's talent was discovered by Jacobi, to whom Kummer had sent some papers, and who informed Humboldt. Dirichlet and Kummer, as well as Gauss and Kummer, again learned of each other through their work. Eisenstein's talent was detected by Dirichlet, and then he, or

[80] [Eisenstein 1975], vol. 2, pp. 762–763: *Schon früh wurde ich von den Schönheiten eines Gebietes angezogen, welches sich nicht allein von andern durch seinen Gegenstand unterscheidet, sondern sich vor allen durch die Eigenthümlichkeit und Mannigfaltigkeit seiner Methoden auszeichnet, indem es hier nicht genügt, die Folgen eines einzigen Gedankens in einer langen Reihe von Entwicklungen darzulegen, sondern fast jeder Schritt die Überwindung neuer Schwierigkeiten, die Anwendung neuer Prinzipien erfordert. Die Zahlentheorie … hat durch Gauß und einige seiner Nachfolger in kurzer Zeit einen solchen Aufschwung genommen, daß sie nunmehr an Tiefe und Umfang keiner andern mathematischen Disciplin nachsteht, auf viele derselben befruchtend eingewirkt hat; es hat sich eine Schule gebildet, welche die hervorragendsten mathematischen Talente zu ihren Anhängern zählt, der auch ich mich, wenn auch als einer ihrer geringsten Jünger mit Stolz zurechne.*

[81] [Klein 1926–1927], vol. 1, p. 17: … *in Berlin eine außerordentliche gesellschaftliche Stellung [genoß], die ihm durch seine Beziehung zum Hofe und seine vielseitigen Verbindungen einen großen Einfluß verschaffte.*

Crelle, wrote to Humboldt; Eisenstein himself sent his articles to the Berlin Academy, as well as to Gauss, and finally used Humboldt's recommendation to meet Gauss personally in Göttigen.

But through the discovery of these talents, a perpetually increasing circle of number theorists developed around Gauss and Humboldt and remained in close contact. They progressively constructed a network of relations, of friendships, of links, a communication network which was used sometimes to exchange mathematical knowledge, sometimes also to support newly-discovered young mathematicians. At times, as we have seen, also Leopold Crelle, the editor of the *Journal für die reine und angewandte Mathematik*, Christian Schumacher, the editor of the *Astronomische Nachrichten*, Franz Encke, the Secretary of the mathematical (resp. mathematical-physical) class of the Berlin Academy of Sciences, Wilhelm Bessel, the Director of the Köngisberg Observatory, and others, were involved in this network. We have seen how Humboldt and his colleagues operated their philanthropic activities in the interest of mathematics, using each other's judgments and arguments to secure financial means and positions for the newcomers.

As far as positions were concerned, Humboldt had mainly in view the Prussian universities. His declared objective on his return to Berlin was to act in favour of the development of mathematics and the natural sciences in Prussia, and first of all in Berlin. He also succeeded in avoiding several potential departures to non-Prussian universities by improving the financial situation of the scientist in question. He wrote recommendation letters to Gauss, to the King, to the ministers, but also gratifying and encouraging letters to young mathematicians with advice on efficient behaviour to adopt with respect to the King or to the ministers.

His networking activities turned out to be particularly efficient with respect to number theory. Thanking the Berlin Academy of Sciences for their congratulations on the occasion of the fiftieth anniversary of his doctorate, in 1849, Gauss recalled how few mathematicians in Germany had been interested in number theory twenty years after the publication of the *Disquisitiones Arithmeticae*. But then he added:

> How totally different is the situation today when higher arithmetic counts so many devotees, authorities, and – as I may add with sincere joy – friends of mine, especially among you, who develop it successfully further.[82]

Among the successors of Gauss who have most contributed to this recognition of number theory, indeed, Humboldt's protegees, Dirichlet, Jacobi, Kummer, und Eisenstein, occupy the first rank.

[82] *Bericht über die zur Bekanntmachung geeigneten Verhandlungen der Königlichen Preußischen Akademie der Wissenschaften zu Berlin. Aus dem Jahre 1849*, 276: *Wie ganz anders verhält es sich damit gegenwärtig, wo die Höhere Arithmetik so viele Verehrer, Kenner und, wie ich mit aufrichtiger Freude hinzusetzen kann, mir befreundete glückliche Fortbildner, vorzugsweise in Ihrer Mitte, zählt.*

References

BEGEHR, Heinrich G.W., KOCH, Helmut, KRAMER, Jürg, SCHAPPACHER, Norbert, THIELE, Ernst-Jochen (eds.). 1998. *Mathematics in Berlin*. Berlin, Basel, Boston: Birkhäuser.

BIERMANN, Kurt-R. 1959a. *Johann Peter Gustav Lejeune Dirichlet. Dokumente für sein Leben und Wirken*. Abhandlungen der Deutschen Akademie der Wissenschaften zu Berlin, Klasse für Mathematik, Physik und Technik 2. Berlin: Akademie-Verlag.

———. 1959b. Über die Förderung deutscher Mathematiker durch Alexander von Humboldt. In [Humboldt 1959], pp. 83–159.

———. 1959c. Crelles Verhältnis zu Gotthold Eisenstein. *Monatsberichte der Deutschen Akademie der Wissenschaften zu Berlin* 1, 67–72.

———. 1959d. P. G. Lejeune Dirichlet 1859–1959. *Monatsberichte der Deutschen Akademie der Wissenschaften zu Berlin* 1, 320–323.

———. 1960b. Dirichletiana. *Monatsberichte der Deutschen Akademie der Wissenschaften zu Berlin* 2, 386–389.

———. 1960c. *Vorschläge zur Wahl von Mathematikern in die Berliner Akademie [der Wissenschaften]. Ein Beitrag zur Gelehrten- und Mathematikgeschichte des 19. Jahrhunderts*. Abhandlungen der Deutschen Akademie der Wissenschaften zu Berlin. Klasse für Mathematik, Physik und Technik 3. Berlin: Akademie-Verlag.

———. 1961. Einige neue Ergebnisse der Eisenstein-Forschung. *NTM. Zeitschrift für Geschichte der Naturwissenschaften, Technik und Medizin* 1, 2, 1–12.

———. 1964. Gotthold Eisenstein. Die wichtigsten Daten seines Lebens und Wirkens. *Journal für die reine und angewandte Mathematik* 214/215, 19–30. Repr. in [Eisenstein 1975], vol. 2, pp. 919–929.

———. 1968. Alexander von Humboldts wissenschaftsorganisatorisches Programm bei der Übersiedlung nach Berlin. *Monatsberichte der Deutschen Akademie der Wissenschaften zu Berlin* 10, 142–147. Partial repr.: *Journal für die reine und angewandte Mathematik* 250 (1971), 1–2. Also in [Biermann 1990], pp. 169–171.

———. 1969. Die Beziehungen Alexander von Humboldts zu französischen Mathematikern. *Monatsberichte der Deutschen Akademie der Wissenschaften zu Berlin* 11, 458–463. German ext. version of: Les relations entre les mathématiciens français et Al. de Humboldt. *Actes du XII^e Congrès International d'Histoire des Sciences 1968*, vol. 11, p. 17–21, 1971.

———. 1970. Alexander von Humboldt. Ausgewählte Aspekte seines Lebens und Wirkens. *NTM. Schriftenreihe für Geschichte der Naturwissenschaften, Technik und Medizin* 7, 2, 51–67. Repr. in [Biermann 1990], pp. 15–26.

———. 1981. Alexander von Humboldts Einflußnahme auf die Entwicklung der Mathematik in Berlin. In *Die Entwicklung Berlins als Wissenschaftszentrum (1870-1930). Beiträge einer Kolloquienreihe Teil I*, pp. 93-112. Institut für Theorie, Geschichte und Organisation der Wissenschaft der Akademie der Wissenschaften der DDR 24. Berlin: Institut für Theorie, Geschichte und Organisation der Wissenschaft der Akademie der Wissenschaften der DDR.

———. 1981a. Humboldt, Friedrich Wilhelm Heinrich Alexander von. In *Dictionary of Scientific Biography*, ed. Ch. C. Gillispie, vol. 6, pp. 549–555.

———. 1981b. Eisenstein, Ferdinand Gotthold Max. In: *Dictionary of Scientific Biography*, ed. Ch. C. Gillispie, vol. 4, pp. 340–343.

———. 1981c. Kummer, Ernst Eduard. In: *Dictionary of Scientific Biography*, ed. Ch. C. Gillispie, vol. 7, pp. 521–524.

———. 1983. *Alexander von Humboldt*. Biographien hervorragender Naturwissenschaftler, Techniker und Mediziner 47. 3e ed. Leipzig: Teubner.

———. 1985 (ed.). *Alexander von Humboldt. Vier Jahrzehnte Wissenschaftsförderung. Briefe an das preußische Kultusministerium 1818-1859.* Beiträge zur Alexander-von-Humboldt-Forschung 14. Berlin: Akademie-Verlag.

———. 1988. *Die Mathematik und ihre Dozenten an der Berliner Universität 1810–1933. Stationen auf dem Wege eines mathematischen Zentrums von Weltgeltung*. Berlin: Akademie-Verlag. 1st ed., 1973.

———. 1990. *Miscellanea Humboldtiana*, Zusammenstellung und Redaktion: U. Moheit. Beiträge zur Alexander-von-Humboldt-Forschung 15. Berlin: Akademie-Verlag.

———. 1991. *Beglückende Ermunterung durch die akademische Gemeinschaft*. Beiträge zur Alexander-von-Humboldt-Forschung 17. Berlin: Akademie-Verlag.

———. 1992. *"Ja, man muß sich an die Jugend halten!". Alexander von Humboldt als Förderer der forschenden Jugend.* Schernfeld: SH-Verlag.

Bruhns, Karl. 1872. *Alexander von Humboldt. Eine wissenschaftliche Biographie*. 3 vols. Leipzig: Brockhaus. Repr. Osnabrück: Zeller, 1969.

Dirichlet, Johann Peter Gustav Lejeune-. 1852. Gedächtnisrede auf Carl Gustav Jacob Jacobi. *Abhandlungen der Königlich Preußischen Akademie der Wissenschaften*, 1–27. Repr. in [Dirichlet 1889–1897], pp. 227–252 and [Reichardt 1988], pp. 8–32.

———. 1889–1897. *Werke*, ed. L. Kronecker and L. Fuchs. 2 vols. Berlin: Reimer. Repr. in 1 vol., New York: Chelsea, 1969.

———. NL. *Nachlass*. Archiv der Berlin-Brandenburgischen Akademie der Wissenschaften (ABBAW). Berlin.

Dunken, Gerhard. 1958. Alexander von Humboldt und der Plan der Gründung einer höheren Lehranstalt in Berlin. *Wissenschaftliche Zeitschrift der Humboldt-Universität zu Berlin, math.-nat. Reihe* 8 (1958–1959), 1, 131–134.

Edwards, Harold M. 1998. Kummer and Kronecker. In [Begehr, Koch, Kramer, Schappacher, Thiele 1998], pp. 61–70.

Eisenstein, Gotthold. 1847. *Mathematische Abhandlungen, besonders aus dem Gebiete der höheren Arithmetik und der elliptischen Funktionen. Mit einer Vorrede von C. F. Gauß.* 2e ed. with an introduction by K.-R. Bierman. Hildesheim: Olms, 1967.

———. 1975. *Mathematische Werke*. 2 vols. New York: Chelsea. 2nd ed. 1989.

Encke, Johann Franz. NL. *Nachlass*. Archiv der Berlin-Brandenburgischen Akademie der Wissenschaften (ABBAW). Berlin.

Gauss, Carl Friedrich. 1863–1933. *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. 12 vols. Göttingen: Universitäts-Druckerei (vols. I–VI); Leipzig: Teubner (vols. VII–X.1); Berlin: Julius Springer (vols. X.2–XII). Repr. Hildesheim, New York: Olms, 1981.

Gauss & Bessel. 1880. *Briefwechsel zwischen Gauß und Bessel*, ed. A. Auwers. Leipzig: W. Engelmann. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 1. Hildesheim: G. Olms, 1975.

Gauss & Gerling. 1927. *Briefwechsel zwischen Carl Friedrich Gauß und Christian Ludwig Gerling*, ed. C. Schaefer. Berlin: Elsner. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 3. Hildesheim: G. Olms, 1975.

Gauss & Olbers. 1900–1909. *Briefwechsel zwischen Olbers und Gauß*, ed. C. Schilling and I. Kramer. *Wilhelm Olbers, sein Leben und seine Werke*, ed. C. Schilling, vol. 2. Berlin: J. Springer. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 4. 2 vols. Hildesheim: G. Olms, 1976.

Gauss & Schumacher. 1860–1865. *Briefwechsel zwischen C. F. Gauß und H. C. Schumacher*, ed. Chr. A. F. Peters. 6 vols. Altona: Esch. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 5. 3 vols. Hildesheim: Olms, 1975.

Harnack, Adolf. 1900. *Geschichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin*. 3 vols. Berlin: Reichsdruckerei.

Hensel, Kurt. 1910. Gedächtnisrede auf Ernst Eduard Kummer. In *Festschrift zur Feier des 100. Geburtstages Eduard Kummers*, pp. 1–37. Leipzig, Berlin: Teubner. Rep. in [Kummer 1975], vol. 1, pp. 33–69; [Reichardt 1988], pp. 75–111.

Hofmann, Joseph E. 1959. Alexander von Humboldt in seiner Stellung zur reinen Mathematik und ihrer Geschichte. In [Humboldt 1959], pp. 239–287.

Humboldt. 1959. *Alexander von Humboldt. Gedenkschrift zur 100. Wiederkehr seines Todestages*, ed. Alexander-von-Humboldt-Kommission der Deutschen Akademie der Wissenschaften zu Berlin. Berlin: Akademie-Verlag.

———. 1985. *Vier Jahrzehnte Wissenschaftsförderung. Briefe an das preußische Kultusministerium 1818–1859* ed. K.-R. Biermann. Beiträge zur Alexander-von-Humboldt-Forschung 14. Berlin: Akademie-Verlag.

Humboldt & Dirichlet. 1982. *Briefwechsel zwischen Alexander von Humboldt und Peter Gustav Lejeune Dirichlet*, ed. K.-R. Biermann. Beiträge zur Alexander-von-Humboldt-Forschung 7. Berlin: Akademie-Verlag.

Humboldt & Gauss. 1977. *Briefwechsel zwischen Alexander von Humboldt und Carl Friedrich Gauß. Zum 200. Geburtstag von C. F. Gauß im Auftrage des Gauß-Komitees bei der Akademie der Wissenschaften der DDR*, ed. K.-R. Biermann. Beiträge zur Alexander-von-Humboldt-Forschung 4. Berlin: Akademie-Verlag.

Humboldt & Jacobi. 1987. *Briefwechsel zwischen Alexander von Humboldt und C. G. Jacob Jacobi*, ed. H. Pieper. Beiträge zur Alexander-von-Humboldt-Forschung 11. Berlin: Akademie-Verlag.

Humboldt & Schumacher. 1979. *Briefwechsel zwischen Alexander von Humboldt und Heinrich Christian Schumacher*, ed. K.-R. Biermann. Beiträge zur Alexander-von-Humboldt-Forschung 6. Berlin: Akademie-Verlag.

Jacobi, Carl Gustav Jacob. 1881–1891. *Gesammelte Werke*. ed. C. W. Borchardt, K. Weierstraß, and E. Lottner. 7 vols. + Supplement. Berlin: Reimer.

Jacobi & Jacobi. 1907. *Briefwechsel zwischen C. G. J. Jacobi und M. H. Jacobi*, ed. W. Ahrens. Leipzig: Teubner.

JACOBI & LEGENDRE. 1875/1998. Correspondance entre Jacob Jacobi et Adrien-Marie Legendre. Ed. C. Borchardt. *Journal für die reine und angewandte Mathematik* 80, 205–279. Repr. in [Jacobi 1881–1891], vol. 1, pp. 385–461. Reed. with German transl.: *Korrespondenz A.-M. Legendre – C. G. J. Jacobi. Correspondance mathématique entre Legendre et Jacobi*, ed. H. Pieper. Teubner-Archiv zur Mathematik 19. Stuttgart, Leipzig: Teubner.

KLEIN, Felix. 1926–1927. *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert*. Berlin: Springer.

KOCH, Helmut. 1981. J. P. G. Lejeune Dirichlet zu seinem 175. Geburtstag. *Mitteilungen der Mathematischen Gesellschaft der DDR* 2/4, 153–164.

———. 1998. Gustav Peter Lejeune Dirichlet. In [Begehr, Koch, Kramer, Schappacher, Thiele 1998], pp. 33–39.

KOENIGSBERGER, Leo. 1904. *Carl Gustav Jacob Jacobi. Festschrift zur Feier der hundertsten Wiederkehr seines Geburtstages*. Leipzig: Teubner.

KNOBLOCH, Eberhard, PIEPER, Herbert, PULTE, Helmut. 1995. "… das Wesen der reinen Mathematik verherrlichen". Reine Mathematik und mathematische Naturphilosophie bei C. G. J. Jacobi. *Mathematische Semesterberichte* 42, 99–132.

Kultusministerium. Archives. Geheimes Staatsarchiv – Stiftung Preußischer Kulturbesitz. Hauptabteilung 1. Repositur 76.

KUMMER, Ernst E. 1860. Gedächtnisrede auf Gustav Peter Lejeune Dirichlet. *Abhandlung der Königlich Preußischen Akademie der Wissenschaften*, 1–36. Repr. in [Dirichlet 1889–1897], vol. 2, pp. 311–344; [Kummer 1975], vol. 2, pp. 721–756; [Reichardt 1988], pp. 36–71.

———. 1975. *Collected papers*, ed. A. Weil. 2 vols. Berlin, Heidelberg, New York: Springer.

MICHLING, Horst. 1997. *Carl Friedrich Gauß. Episoden aus dem Leben des Princeps Mathematicorum*. 3^{e} ed. Göttingen: Verlag Göttinger Tageblatt. 4^{e} ed., 2005.

ORE, Oystein. 1981. Dirichlet, Gustav Peter Lejeune. In *Dictionary of Scientific Biography*, ed. Ch. C. Gillispie, vol. 4, pp. 123–127.

PIEPER, Herbert. 1988. Urteile C. G. J. Jacobis über den Mathematiker E. E. Kummer. *NTM. Schriftenreihe für Geschichte der Naturwissenschaft, Technik und Medizin* 25, 23–36.

———. 1991. *Heureka. Ich hab's gefunden*. 2nd ed. Berlin, Frankfurt, Thun: Hari Deutsch.

———. 1995. Carl Gustav Jacob Jacobi (1804–1851). In *Die Albertus-Universität zu Königsberg und ihre Professoren*, ed. D. Rauschning, D. v. Nerée, pp. 473–488. Jahrbuch der Albertus-Universität zu Königsberg/Pr. XXIX. Berlin: Duncker, Humblot.

———. 1998. Carl Gustav Jacob Jacobi. In [Begehr, Koch, Kramer, Schappacher, Thiele 1998], pp. 41–48.

———. 2004. *Netzwerk des Wissens und Diplomatie des Wohltuns. Berliner Mathematik, gefördert von A. v. Humboldt und C. F. Gauß*. Leipzig: Edition am Gutenbergplatz.

———. 2005. Alexander von Humboldt und die Berufung Jacob Jacobis an die Wiener Universität. *NTM. Internationale Zeitschrift für Geschichte und Ethik der Naturwissenschaften, Technik und Medizin* Neue ser. 13, 137–155.

REICHARDT, Hans (ed.). 1963. *Bericht von der Dirichlet-Tagung*. Schriftenreihe der Institute für Mathematik bei der Deutschen Akademie der Wissenschaften zu Berlin 13. Berlin: Akademie-Verlag.

——— (ed.). 1988. *Nachrufe auf Berliner Mathematiker des 19. Jahrhunderts. C. G. J. Jacobi, P. G. L. Dirichlet, E. E. Kummer, L. Kronecker, K. Weierstraß. Mit Fotos, Dokumenten und Archivalien*. Teubner-Archiv zur Mathematik 10. Leipzig: Teubner.

SCHAPPACHER, Norbert. 1998. Gotthold Eisenstein. In [Begehr, Koch, Kramer, Schappacher, Thiele 1998], pp. 55–60.

SCHUBRING, Gert. 1981a. On education as a mediating element between development and application: the plan for the Berlin Polytechnical Institute (1817–1850). In *Epistemological and Social Problems of the Sciences in the Early Nineteenth Century*, ed. H. N. Jahnke, M. Otte, pp. 269–284. Dordrecht, Boston, London: Reidel.

———. 1981b. Mathematics and teacher training: Plans for a polytechnic in Berlin. *Historical Studies in the Physical Sciences* 12, 161–194.

———. 1982. Pläne für ein Polytechnisches Institut in Berlin. In *Philosophie und Wissenschaft in Preußen*, ed. F. Rapp, H.-W. Schütt, pp. 201–224. TUB-Dokumentation Kongresse und Tagungen 14. Berlin: TUB-Dokumentation.

———. 1984. Die Promotion von P. G. Lejeune Dirichlet. Biographische Mitteilungen zum Werdegang Dirichlets. *NTM. Schriftenreihe für Geschichte der Naturwissenschaft, Technik und Medizin* 21, 45–65.

SCRIBA, Christoph. 1981. Jacobi, Carl Gustav Jacob. In *Dictionary of Scientific Biography*, ed. Ch. C. Gillispie, vol. 7, pp. 50–55.

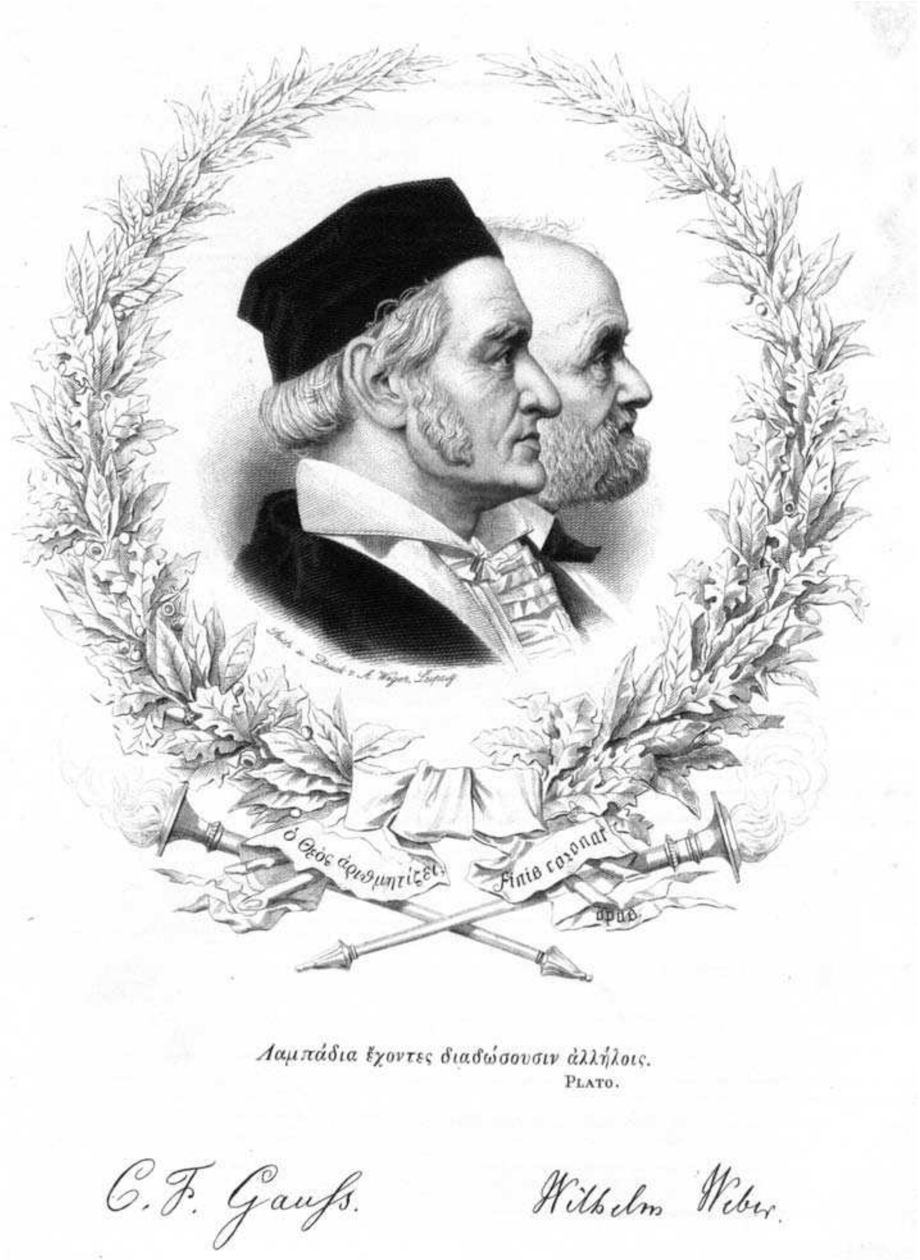

Stich u. Druck v. A. Weger, Leipzig
ὁ Θεὸς ἀριθμητίζει.
Finis coronat
opus.
Λαμπάδια ἔχοντες διαδώσουσιν ἀλλήλοις.
PLATO.
C. F. Gauss.
Wilhelm Weber.

Fig. III.2A. “God arithmetizes”
Etching of C.F. Gauss and W. Weber by A. Weger
(Scan from [Zöllner 1878], p. v, by courtesy of NSUB Göttingen)

III.2

Ὁ Θεὸς Ἀριθμητίζει: The Rise of Pure Mathematics as Arithmetic with Gauss

José Ferreirós

The beautiful picture facing this page, which displays Carl Gauss and his colleague physicist Wilhelm Weber, is noteworthy not just for the quality and accuracy of the portraits, but also because of the mottos it includes. It was composed upon the inspiration of Friedrich Zöllner (1834–1882), an astrophysicist, professor at Berlin, and close follower of Weber.[1] Among the mottos, one originates with Gauss himself: ὁ θεὸς ἀριθμητίζει, God does arithmetic, or more literally "God arithmetizes" – presumably meaning that in his thoughts God is always dealing with numbers and number-relations. This motto is an adaptation of a sentence attributed to Plato: ὁ θεὸς ἀεὶ γεωμέτρει, "God geometrizes eternally."[2] Although this sentence is not found in Plato's dialogues, nevertheless they offer declarations in the same spirit (see for instance the dialogue *The Republic*). Interestingly, the very same sentence, in Greek, is quoted by Kepler in his first work, *Mysterium cosmographicum* (1596), a book that Gauss must have been familiar with. Plato's words can be found in the crucial chapter where Kepler describes the main guidelines of his peculiarly platonic reconstruction of the architecture of the universe, based on a clever combination of the regular solids.[3]

Several witnesses attest to the fact that the motto stems directly from Gauss, among them his friend the Göttingen professor Wolfgang Sartorius von Waltershausen, and the physician who treated him, Dr. Wilhelm Baum. Thus, Dr. Baum

[1] See [Zöllner 1878]. The portrait of Gauss was based on the well-known oil painting by Jensen and on the medal prepared for the 1877 centenary by the Göttingen Academie der Wissenschaften. Weber was portrayed on the basis of a photograph taken in 1877. The drawing is by August Weger. See [Zöllner 1878], p. v.

[2] See [Plutarch], book VIII, quest. 2, where Plutarch indicates that the phrase cannot be found in extant writings of Plato.

[3] See [Kepler 1858], p. 124.

wrote to Alexander von Humboldt immediately after Gauss's death:

> The last days of his life were often very painful owing to the aggravated complaint of dropsy, which the hypertrophy of his heart produced – but still he always maintained his freedom and greatness of spirit, the strongest conviction of his personal permanence, the firmest hope in the still deeper intelligent insight into the number-relationships, which God places in matter and which he would perhaps be able to recognize in the intensive magnitudes, for he used to say: ὁ θεὸς ἀριθμητίζει.[4]

In fact, Gauss employed those words when talking about questions that lay beyond the reach of human knowledge, at least in its present stage. Waltershausen explains it as follows:

> By science he understood only that rigorous logical edifice, closed in itself, whose foundations rest on some truths generally acknowledged by the human mind, truths which, once admitted, open for us an immense field of most intricate researches, linked to one another by an iron chain of thoughts. Therefore, as we have already mentioned, he placed arithmetic at the top, and, in connection with questions that we cannot ascertain scientifically, he loved to employ the words: ὁ θεὸς ἀριθμητίζει, with which he acknowledged the logic that goes through the whole cosmos, also for those domains in which our mind is not allowed to penetrate.[5]

The Gaussian motto implies that there is a theological explanation for the impressive applicability and effectiveness of mathematics: God's creation bears the mark of His thought, which we are able to grasp because we are of His lineage. But this point is perhaps less interesting than the way in which his adaptation of Plato's words reflects changing perceptions of mathematical knowledge. The above motto and related statements document the end of the thousand year long domination of geometry in Western images of mathematics, and the corresponding rise of arithmetic as the paradigmatic mathematical discipline. As Hilbert wrote at the close of the century,[6] mathematics in the XIX$^{\text{th}}$ century had developed "*under the sign of number*," a topic that was discussed by Klein, Poincaré and others under the name of "arithmetization."[7]

[4] Quoted from the end of [Dunnington 1927]. I should mention that M. Kline has wrongly attributed the motto "God ever arithmetizes" to Jacobi; see [Kline 1972], vol. 3, p. 1026. While the attribution is wrong factually, it seems however quite right in spirit (see below).

[5] See [Waltershausen 1856], p. 97: *Unter Wissenschaft verstand er allein jenes streng in sich abgeschlossene logische Gebäude, dessen Fundamente auf gewissen vom menschlichen Geist allgemein anerkannten Wahrheiten beruhe, die ein Mal zugegeben ein unabsehbares Feld der verwickeltsten durch eine eiserne Gedankenkette mit einander zusammenhängenden Forschungen gestatte. Er stellte daher wie schon bemerkt die Arithmetik an die Spitze und pflegte in Bezug auf Fragen die für uns wissenschaftlich nicht zu ergründen sind die Worte zu gebrauchen:* ὁ θεὸς ἀριθμητίζει, *womit er die durchs ganze Weltall gehende Logik auch für solche Gebiete anerkannte, in welche einzudringen unserm Geiste nicht verstattet ist.*

[6] See [Hilbert 1897], p. 66.

[7] See also B. Petri and N. Schappacher's chap. V.2 below.

The purpose of this chapter is to discuss the complex of ideas and viewpoints related to the Gaussian conception of arithmetic and its role in mathematics: the new demarcation between pure and applied mathematics; aspects of the modern transformation of mathematics such as arithmetization and the conceptual approach; the role of conceptual developments, new cultural values, and epistemological views in the process. It will be argued that already in the case of Gauss, philosophical motives played a role in the rise of arithmetic as a paradigm, and that the intellectual atmosphere of Neohumanism promoted such approaches. It is obvious from this short summary that the picture I am about to draw is a multifaceted one. In my opinion it is essential to provide such an analysis in order to account for the emergence of modern mathematics.

1. Pure Mathematics: Arithmetic versus Geometry

In order to understand what is behind Gauss's motto, it is worthwhile to pause over the following sentences that the mathematician wrote to Heinrich Wilhelm Matthias Olbers in April 1817:

> I come more and more to the conviction, that the necessity of our [Euclidean] geometry cannot be proven, at least not *by human* understanding nor *for* human understanding. Perhaps in another life we come to different insights into the essence of space, that are now impossible for us to reach. Until then, we should not put geometry on the same rank with arithmetic, which stands purely *a priori*, but say with mechanics.[8]

Three aspects of this quote deserve to be emphasized. First, and as will become clearer soon, Gauss uses a rather philosophical language to express his views. Second, although the passage is usually quoted in connection with the foundations of geometry, it also presents us with a very characteristic view on the foundations of arithmetic. This branch of pure mathematics "stands purely *a priori*," it consists of a priori knowledge. The language is Kantian, although the viewpoint might also be understood in the sense of Leibniz (see § 5).

A letter to Friedrich Wilhelm Bessel written in April 1830 is even more striking:

> According to my most intimate conviction, the theory of space has a completely different position with regards to our knowledge *a priori*, than the pure theory of magnitudes. Our knowledge of the former lacks completely *that* absolute conviction of its necessity (and therefore of its absolute truth) which is characteristic of the latter. We must humbly acknowledge that, whereas number is *just* a product of our minds, space also has a reality outside our minds, whose laws we cannot prescribe *a priori.*[9]

[8] See [Gauss 1900], p. 177: *Ich komme immer mehr zu der Überzeugung, dass die Nothwendigkeit unserer Geometrie nicht bewiesen werden kann, wenigstens nicht* vom menschlichen *Verstande noch* für *den menschlichen Verstand. Vielleicht kommen wir in einem andern Leben zu andern Einsichten in das Wesen des Raumes, die uns jetzt unerreichbar sind. Bis dahin müsste man die Geometrie nicht mit der Arithmetik, die rein* a priori *steht, sondern etwa mit der Mechanik in gleichen Rang setzen.*

[9] See [Gauss 1900], p. 201, or [Gauss & Bessel 1880], p. 497: *Nach meiner innigsten Überzeugung hat die Raumlehre in unserm Wissen a priori eine ganz andere Stellung*

Here again, a clear distinction between geometric and arithmetic knowledge is drawn by characterizing the latter as "knowledge *a priori*," consisting of necessary, certain, absolute truths. Concepts and terminology seem to be taken from Kant, who emphasized that true science consists of necessary, certain, absolute truths, not just of empirical knowledge (see § 5).

The third aspect is that Gauss draws a neat distinction between what might be called, using XVIII$^{\text{th}}$ century language, pure and mixed mathematics. Mixed mathematics is that part of the discipline which deals with knowledge having (at least partly) empirical origins; specifically Gauss indicates that geometry and mechanics belong here. Pure mathematics is that part of mathematical knowledge which stands completely *a priori*. On the basis of further passages in the correspondence and writings of Gauss (see the previous quotation and below), this must be taken to include not only arithmetic, but also what he calls the "pure theory of magnitudes" (*reine Grössenlehre*), i.e., the theory of the full complex number system in all its different aspects, which we may presently identify as arithmetical, algebraic, topological, and analytical. Here again, the basic apriorist standpoint might be consistent with the philosophy of either Leibniz or Kant, but not with most other philosophers of the XVII$^{\text{th}}$ and XVIII$^{\text{th}}$ centuries.

The conception of pure mathematics, its identification with (general) arithmetic, and even the thesis that it "stands purely *a priori*," can be found in later German authors as central to XIX$^{\text{th}}$ century mathematical developments as Karl Weierstrass, Richard Dedekind. The deep change in the image of mathematics relates obviously to systematic work on number theory, to work in geometry leading to non-Euclidean systems, and to foundational work in the field of analysis (the so-called rigorization or arithmetization). The case of Gauss invites an exploration of the emergence of this approach to mathematical knowledge, which, historically, was typical of XIX$^{\text{th}}$ century German mathematicians.

As chapter V.2 in this book will help to make clear, the historical issue of arithmetization is rather complex. Versions of arithmetization ranged from the radical one advocated by Kronecker in the 1880s, which amounted to a constructivist revision of pure mathematics, to the no less radically abstract (set-theoretical and logicistic) approach of Dedekind.[10] Compared with these, Weierstrass's standpoint would seem to deserve being qualified as intermediate or, perhaps, even semi-constructivistic.[11]

The leader of the extremely influential Berlin school was convinced that "the main difficulties in higher analysis arise precisely from a hasty and not sufficiently detailed exposition of the basic notions and the arithmetical operations."[12] His

wie die reine Grössenlehre; es geht unserer Kenntniss von jener durchaus diejenige *vollständige Überzeugung von ihrer Nothwendigkeit (also auch von ihrer absoluten Wahrheit) ab, die der letztern eigen ist; wir müssen in Demuth zugeben, dass, wenn die Zahl* bloss *unseres Geistes Product ist, der Raum auch ausser unserm Geiste eine Realität hat, der wir a priori ihre Gesetze nicht vollständig vorschreiben können.*

[10] See [Dedekind 1872], [Dedekind 1888].

[11] For further details on this point see [Ferreirós 1999], 34–38.

[12] Quoted by Kopfermann from an 1874 lecture course in [Behnke, Kopfermann 1966],

remedy was to devote about one fourth of his introductory lectures (on the theory of analytic functions) to the number system and arithmetical operations. He frequently emphasized that his approach to the foundations of analysis was essentially based on the idea of starting from algebraic truths, which in turn meant to start from the number concept and the basic arithmetical operations, and to avoid geometry and "transcendental" means.[13] This difference in viewpoint he marked by talking of *arithmetisch* as opposed to *geometrisch*. For instance, in his lecture course of the summer term 1874, he is reported to have said:

> Furthermore we shall give a purely arithmetical definition of complex magnitudes. The geometrical representation of the complex magnitudes is regarded by many mathematicians not as an explanation, but only as a sensorial representation, while the arithmetical representation is a real explanation of the complex magnitudes. In analysis we need a purely arithmetical foundation, which was already given by Gauss. Although the geometrical representation of the complex magnitudes constitutes an essential means for investigating them, we cannot employ it, for analysis must be kept clean of geometry.[14]

As we shall see, this was essentially Gauss's own standpoint on the topic.[15] Weierstrass was later credited with having completed the rigorization of analysis by basing it upon arithmetic; see [Klein 1895], [Poincaré 1900].

Arithmetization became dominant during the age of highest national and international impact of the Berlin school, namely the 1870s and 1880s. But it had begun as a trend much earlier, perhaps in the 1830s, since related ideas can be found at that time in the work of two very different Berlin professors, Gustav Lejeune-Dirichlet and the much less known Martin Ohm (1792–1872). Dirichlet is reported to have frequently stated that all theorems of algebra and analysis could be formulated directly as theorems about the natural numbers; the arithmetizing viewpoint is already

p. 78: *Die Hauptschwierigkeiten der höheren Analysis haben nämlich ihren Grund gerade in einer unscharfen und nicht hinreichend umfassenden Darstellung der arithmetischen Grundbegriffe und Operationen.*

[13] See his letter to du Bois-Reymond of December 21, 1873 in [Weierstrass 1923], pp. 203f, and his letter to Schwarz dated October 3, 1875 in [Dugac 1973], p. 144.

[14] I thank Reinhard Bölling for his comments on this matter, and for pointing me to this text. The Göttingen version of the Hettner notes have been photocopied and distributed to various libraries in Germany; the quote has been checked against the photocopy in the library of the *Fachbereich Mathematik*, TU Darmstadt; p. 5–6: *Wir werden ferner eine rein arithmetische Definition der complexen Grössen geben. Die geometrische Darstellung der complexen Grössen wird von vielen Mathematikern nicht als eine Erklärung, sondern nur als eine Versinnlichung betrachtet, während die arithmetische Darstellung die complexen Grössen wirklich erklärt. Wir bedürfen jedoch für die Analysis eine rein arithmetische Begründung, die schon Gauss gegeben hat. Obgleich die geometrische Repräsentation der complexen Grössen ein wesentliches Hülfsmittel zur Untersuchung derselben ist, können wir sie hier nicht anwenden, da die Analysis von der Geometrie rein erhalten werden muss.*

[15] For a detailed comparison between Gauss's and Kronecker's points of view, see J. Boniface's chap. V.1 below [Editors' note].

behind his crucial contribution to analysis (Fourier series) in 1829.[16]

Ohm, brother of the famous physicist, became *ausserordentlicher Professor* at Berlin in 1824, having just published an influential treatise in which he attempted to systematize pure mathematics on the sole basis of the natural numbers. In 1819 he wrote that it had been a bad mistake on the part of mathematicians to think that the subject matter of the calculus was *magnitudes*, when in fact "it has to do solely and exclusively with the so-called *absolute integers*," i.e., with the natural numbers;[17] this circumstance was to be blamed, in his view, for the lack of sound foundations in then current expositions of arithmetic, algebra and analysis.

While this is obviously not the place to enter into a detailed discussion of arithmetization, it is necessary for us to indicate some aspects of this trend, particularly traits that can be related in one way or another to the work of Gauss. It must be noted that until late in the XIX$^{\text{th}}$ century there was no use of the word "arithmetization" (introduced in [Klein 1895]), nor of the verb "to arithmetize" (coined in [Kronecker 1887]). What became ever more common, early on, was to use the name "arithmetic" in a very general sense, stretching it to the point of identifying all of pure mathematics as arithmetic.[18] The model for this linguistic usage seems to be those letters by Gauss that we quoted at the very beginning, although as early as 1822 Ohm also used the term *Zahlenlehre*, i.e., arithmetic, or literally "theory of numbers," to mean pure mathematics, including algebra and analysis.[19]

There are three features in this historical trend that deserve special notice here. First, the identification of pure mathematics with arithmetic seems to have been a German tendency. It was developed most seriously by German-speaking authors, and more precisely by mathematicians who lived and worked in northern Germany (Göttingen and the Prussian universities). Not just that this foundational conception promoted a certain vision of pure mathematics: emphasis on *pure* mathematics was itself characteristic of German mathematicians.[20] This first feature, striking as it may seem at first sight, will be substantiated in what follows, and we shall locate historical factors that help to explain it.

Secondly, it is obvious that, in order to be consistent and convincing, the conception of pure mathematics as arithmetic depended on the existence of a sound and rigorous foundation for the number system. It is well known that this root of

[16] On mathematics in Berlin, see [Biermann 1973]. Our source for Dirichlet's opinion is [Dedekind 1888], p. 338.

[17] Ohm's work is carefully analyzed in [Bekemeier 1987] and [Jahnke 1987]. The quotation is taken from [Bekemeier 1987], p. 38: … *man sich gänzlich hinsichtlich des Gegenstandes des Kalkuls täuschte, und mit* Grössen *(Zahlgrössen) zu arbeiten vermeinte, während man es einzig und allein nur mit sogenannten* absoluten ganzen Zahlen *zu thun hat.*

[18] This terminology can be found in works as varied as [Dedekind 1872], [Dedekind 1888], p. 335, [Pasch 1882], p. 164, [Kronecker 1887], p. 253, and [Schröder 1890], 441.

[19] See [Bekemeier 1987], p. 102, and elsewhere, for instance p. 40.

[20] This must be embedded within the larger picture of the German tendency to emphasize pure science; see § 3. Among previous studies of the rise of pure mathematics, I would recommend [Bos, Mehrtens, Schneider 1981] and [Goldstein 1989].

mathematical knowledge, the theory of natural numbers, was only axiomatized informally in the 1880s (with the work of Dedekind and Peano). But efforts to present the natural number system, and its extensions, in a detailed and rigorous exposition began much earlier. German authors who were involved in the attempt include Martin Ohm as early as 1822, Hermann Grassmann in 1861, Weierstrass in his lectures from the 1860s, Dedekind in unpublished work and lectures after 1858 (published in 1872), and Georg Cantor in lectures from 1870 (published in 1872). Moreover, one should not forget that the earliest and most influential attempt to rigorize and systematize arithmetic is the *Disquisitiones Arithmeticae*, though of course this time we are talking about the *higher* arithmetic.

A third aspect of arithmetization must be emphasized. As we know from the work of Dedekind, Weierstrass and Cantor, the proposal of arithmetical foundations for pure mathematics is part and parcel of what has come to be called the "conceptual approach" in XIX$^{\text{th}}$ century mathematics. But this topic deserves more detailed treatment.

2. Arithmetization and the Conceptual Approach

Simplifying somewhat, the main motivation for the arithmetization of mathematics was the need to rigorize the field of analysis, responding both to advances in research and to new didactical pressures (due to the professionalization of mathematicians within higher education). This led to the abandonment of geometrical intuition as a source in analysis,[21] so that intuitive geometrical notions such as the continuity of functions were studied and made explicit by means of abstract formulations. This happened in the definition due to Cauchy and Bolzano, who explained continuity in terms of arithmetical inequalities. But, in order to appreciate the importance of Gauss's work properly, it is worthwhile to consider that rigorization of calculus could in principle have followed an alternative route.

The infinitesimal calculus did not by necessity have to give rise to analysis, that is, a general theory of continuous magnitudes, their relations and operations (in the style of Cauchy). It could also have been developed on the basis of a rigorous theory of formal expressions, in the tradition of Lagrange. This has become particularly clear through historical studies of the work of Martin Ohm, the above-mentioned Berlin professor, who was very influential among students and *Gymnasium* teachers.[22] Even before 1820, Ohm was convinced that mathematics lacked a sound scientific foundation, and thought he had been chosen by destiny to provide it.[23] Starting in 1822, he published his *Versuch eines vollkommen consequenten Systems der Mathematik*, i.e., an attempt to develop pure mathematics, and especially the calculus, in a completely logical way, taking as the only absolute basis the natural numbers. He regarded the

[21] However, this tendency was already present in attempts to establish algebraic foundations for analysis such as Lagrange's.

[22] Although he would be ridiculed by his colleagues Steiner and Kummer for not sufficiently embodying the Humboldtian ideal of the unity of teaching and research (see §§ 3 and 4).

[23] See the report by the Berlin professor Ideler in [Bekemeier 1987], p. 53.

natural numbers with their characteristic properties as given to us human beings.[24]

Ohm devised a systematic development of mathematical knowledge, progressing from the natural numbers to more general number domains in response to the need to ensure general applicability of inverse arithmetical operations. (This key principle is found later in the writings of both Weierstrass and Dedekind.) He defined the generalized operations in a rigorous way, by requesting the permanence of formal laws (a similar principle can be found in the British school of symbolic algebra, and later on in Hermann Hankel). It became clear to Ohm that previous mathematicians had been working with formal expressions in a careless way, and that it was necessary to articulate the connections between "forms" and quantitative interpretations consistently. But his proposals diverge from later approaches in that he found ways to make rigorous the XVIII$^{\text{th}}$ century style of calculating with "forms without a content."[25] The introduction of a clear distinction between general forms and quantitative expressions, together with sound criteria for their interrelation, made it possible to operate rigorously with contentless forms.

However, with Gauss, Cauchy, Dirichlet and other authors, the tendency to eliminate contentless forms altogether won the day. Underlying this approach was the idea that the subject matter of mathematics is not formal expressions – these being just a means to denote the objects of mathematical knowledge, to represent relations and operations among them, and to calculate results. The subject matter was not the formulas, but independent objects. Calculation was to proceed in such a way that the formal transformations mirrored admissible interrelations among and operations upon those objects. It became customary to speak of a new conceptual approach, for, as Dirichlet said in his obituary of Jacobi, by 1850 there was in analysis an ever more prominent tendency "to put thoughts in the place of calculations." Minkowski described the gist of the conceptual approach, this "other Dirichlet principle,"[26] as the art of bending problems with a minimum of blind calculations and a maximum of insightful thoughts. Incidentally, it must be emphasized that this tendency would receive a new, more abstract, and decisive impulse with Riemann's work.

By the time of Gauss, the content of pure mathematics, its subject matter, came to be identified with magnitudes and the relations and operations upon them. Later on, however, mathematicians preferred to avoid the word "magnitude," which had been used in confusing ways, and settled for numbers and number systems as their objects.[27] This had also been the standpoint of Martin Ohm, whose ideas (though in need of refinement in some key points) enjoyed wide diffusion because of the success of his textbooks among *Gymnasium* teachers.[28] The main proponents of

[24] See [Bekemeier 1987], pp. 101–104, 173 (… *die Zahlen und ihre Verbindungen Gegenstände unsrer inneren Anschauung sind*), 290.

[25] These were Kummer's words in an 1842 review which is extensively quoted in [Bekemeier 1987], pp. 196–208.

[26] See [Minkowski 1905], p. 163.

[27] This step and its rationale are particularly clear in Dedekind's work, see [Ferreirós 1996], 39–40.

[28] See [Bekemeier 1987].

arithmetization believed that the natural numbers were the very keystone of the whole edifice. All remaining mathematical objects, traditionally introduced by reference to magnitudes and relations between magnitudes (proportions), were now assumed to be definable by purely logical processes on the sole basis of the theory of natural numbers. This is the foundational viewpoint that Weierstrass, Dedekind, and Cantor articulated in detail.

What, if any, was the role played by Gauss and the *Disquisitiones Arithmeticae* in this whole development? It seems to me that the treatise had a more important role than has previously been realized. As regards the objects and methods introduced by Gauss, it is indeed natural to say that his approach to number theory was more conceptual than Legendre's. We find here a contrast that mirrors the one between the views of Lagrange and Cauchy on the foundations of analysis, and this is not just a retrospective evaluation: the point is elaborated upon at the very beginning, in the preface of the D.A. Legendre relied heavily on methods then classified as belonging to algebraic analysis, and he dealt at length with Diophantine analysis. Gauss, by contrast, takes care to explicitly distinguish number theory, as he conceives it, from algebraic and Diophantine analysis.[29]

Dedekind pointed out in 1895 that the key idea of the conceptual approach is already present in "a beautiful passage" of D.A., art. 76, dealing with Wilson's theorem. There Gauss commented on the fact that neither Wilson nor Waring was able to prove the theorem:

> And Waring confessed that the proof seemed the more difficult, since one cannot imagine any *notation* to express a prime number. – In our opinion, however, such truths should be extracted from notions rather than from notations.[30]

Dedekind commented that these last words, "if they are taken in the most general sense," express "a great scientific thought, the decision for the inner in contrast to the outer."[31] He meant that mathematical theories should be based upon concepts expressing the "characteristic inner properties" of the objects under study, while "outer forms of representation" should always arise from the general theory, not the other way around. As a key example of this way of proceeding he liked to mention Riemannian function theory, and his own theory of ideals was designed to comply with that methodological principle. This methodology, in turn, was for Dedekind a decisive argument against Kronecker's approach to the theory of algebraic integers, based on forms.[32]

Riemann and Dedekind gave the conceptual approach a particularly abstract turn,

[29] On this issue, see chap. I.1, § 2 [Editors' note].

[30] See D.A., art. 76: *... et cel. Waring fatetur demonstrationem eo difficiliorum videri, quod nulla* notatio *fingi possit, quae numerum primum exprimat. – At nostro quidem iudicio huiusmodi veritates ex notionibus potius quam es notationibus hauriri debebant.*

[31] See [Dedekind 1895], 54–55: *In diesen letzten Worten liegt, wenn sie im allgemeinsten Sinne genommen werden, der Ausspruch eines großen wissenschaftlichen Gedankens, die Entscheidung für das Innerliche im Gegensatz zu dem Äußerlichen.* Wilson's theorem says that, for any prime p, the product of all $n < p$ is congruent to -1 modulo p.

[32] See his remarks presented in [Edwards, Neumann, Purkert 1982].

which links clearly with some characteristic traits of contemporary mathematics. It is thus interesting to note that the latter looked back to the D.A. in search of the origins of this conceptual approach, later represented forcefully in that great follower of Gauss, Dirichlet. Although it is not easy to find general methodological pronouncements in the writings of Gauss, he expressed his standpoint more clearly in a letter to Schumacher, late in life:

> It is the character of the mathematics of modern times (in contrast to Antiquity) that with our symbolic language and terminology we possess a lever, by which the most complex arguments are reduced to a certain mechanism. Thereby the science has won infinitely in richness, but in beauty and solidity how the trade is usually practiced, it has lost just as much. How frequently that lever is applied in a merely mechanical way, although the authorization to do so implies in most cases certain tacit assumptions. It is my request that, by every use of the calculus, by any application of concepts, one should always remain aware of the original conditions, and never consider the products of the mechanism as a property beyond that explicit authorization.[33]

It is certainly noteworthy that the emergent conceptual approach was closely linked with mathematicians of the Gaussian, Göttingen tradition, and in particular with number theorists.

Was there any particular reason why Gauss opted for that orientation? One might reply – just good mathematical reasons; it was the outcome of sound, deep mathematical thinking. It is certainly obvious that, had the conceptual orientation not been fruitful (leading to incisive methods, promoting interesting problems and results), it would have been abandoned by the mathematical community. On the other hand, it is true that the conceptual approach can speed up theoretical developments immensely, and at times makes it possible to establish results unattainable by calculations. Such virtues, however, could scarcely be foreseeable by the time Gauss, or even Dirichlet, opted for this orientation. Only questions of method, systematization, and proper understanding of mathematical theories could have played a role in their options, and these are characteristically philosophical questions.

It thus seems clear that we must look for specific factors in the intellectual atmosphere surrounding Gauss, which may help us understand his conception of mathematics and its methodology. Relevant factors can indeed be found, and as we

[33] Gauss to Schumacher, September 1, 1850 (discussing a paper by Prehn on divergent series), see [Gauss 1917], pp. 434–435: *Es ist der Character der Mathematik der neueren Zeit (im Gegensatz gegen das Alterthum), dass durch unsere Zeichensprache und Namengebungen wir einen Hebel besitzen, wodurch die verwickelsten Argumentationen auf einen gewissen Mechanismus reducirt werden. An Reichtum hat dadurch die Wissenschaft unendlich gewonnen, an Schönheit und Solidität aber wie das Geschäft gewöhnlich betrieben wird, eben so sehr verloren. Wie oft wird jener Hebel eben nur mechanisch angewandt, obgleich die Befugniss dazu in den meisten Fällen gewisse stillschweigende Voraussetzungen implicirt. Ich fordere, man soll bei allem Gebrauch des Calculs, bei allen Begriffsverwendungen sich immer der ursprünglichen Bedingungen bewusst bleiben, und alle Producte des Mechanismus niemals über die klare Befugniss hinaus als Eigenthum betrachten.*

shall see they are particularly helpful when it comes to understanding why Gauss's proposals were received in Germany with more enthusiasm than elsewhere. The reception of the D.A. was of course a complex matter,[34] but it still seems true that the acceptance of Gauss's conception of number theory was above all a German affair. This can be explained by pointing out that some key background motives were strongly promoted within the setting of the reformed German universities. For the rest of this chapter, we shall concentrate on such broader factors, particularly philosophical motives and the impact of Neohumanism.

3. Gauss the Neohumanist

Neohumanism is the immediate cultural background for the Gaussian motto that I have chosen for the title. Only his love of philology and neohumanist interest in Ancient culture can explain why he chose to express his conception of mathematics in Greek, by reformulating what Plutarch attributed to Plato.

The characteristic trait of Neohumanism was a preoccupation with integral education (*Bildung*) of the individual – in mind (intellectual education), body (physical exercise, music and the arts), and soul (education of the temperament, Christian behaviour). That goal was to be reached, above all, by sticking to the classical models handed down to us by the great Greek and Roman authors. Thus, philological and historical knowledge was at the very centre of neohumanist education, but so too were philosophy and mathematics. The point relative to the classical studies (*Altertumswissenschaften*) and the emergence of seminars in Christian Gottlob Heyne's Göttingen and Friedrich August Wolf's Halle, is too well-known for us to develop it further.[35]

The role of philosophy, considered to be the highest peak of education, is natural when one takes into account the Platonic origins of Humanism. Suffice it to say that the age of Neohumanism is also the Golden Age of German philosophy. But it is important, in this connection, to remind the reader that Neohumanism should not be equated with the philosophy of Absolute Idealism (Fichte, Schelling, Hegel). Certainly the German idealists were under the influence of Neohumanism, but there was no dearth of neohumanists who disagreed with that speculative philosophical orientation.[36] As to the role of mathematics, it was also secured by Platonic educational ideals, and based on the generalized assumption that it constitutes the best possible training for our intellectual, logical abilities. This explains why mathematics had a much clearer status than the natural sciences in the early decades of the reformed German universities.[37]

One further aspect of Neohumanism is essential here. Education, *Bildung*, was always meant to promote the "higher" aspects of human activity, and there was a

[34] On the early reception, see chap. I.1 above.

[35] See, e.g., [McClelland 1980]. Detailed analyses of the links between Neohumanism and mathematics can be found in [Pyenson 1983] and [Jahnke 1990].

[36] Gauss himself, for one, or the philologist Wolf, who admired Kant but not the idealists, or philosophers like Herbart.

[37] On this topic, see [Jungnickel, McCormmach 1986].

resistance to serving pragmatic or utilitarian goals. In this respect, Neohumanism was a reaction against the Enlightenment, and the German model of *Kultur* and *Bildung* was conceived to stand in opposition to the French one of *civilisation*. This links immediately with crucial traits of the reformed, Humboldtian university – the ideals of science for its own sake, of a university environment aimed at living the sciences, and of the unity of teaching and research.

The cultural impact of German Neohumanism will help us explain some of the characteristic traits of arithmetization. If Gauss shared the neohumanist ideals, it becomes easier to understand his conception of mathematics, particularly the division he established between pure mathematics and the rest. But, can we make the case for a neohumanist Gauss? Superficially, it might seem that Gauss the astronomer, the geodesist, the man interested in physics and technology, can hardly represent the neohumanist model. However, many aspects of neohumanist culture are present in Gauss's work, in his writings and letters, and in the role he represented within the scientific and learned community of his time. Let us consider some facts about his early life.

A particularly apt place to look is the inaugural lecture that Gauss gave in 1808, on the occasion of taking charge as Director of the Göttingen Astronomical Observatory. Toward the end of this lecture, we find Gauss citing Plato, Schiller, Ovid, and his beloved writer Jean Paul. The first two parts of the lecture had discussed the aims of the course, analyzed in reference to the kinds of listeners that Gauss expected, and had defined the general topic (theoretical astronomy, with some hints of the practical side) and its main parts. In the third part, Gauss formulated the question: what is the use of this science? It will be instructive to read Gauss's reflections about it. It seems difficult to find a text that may better embody the constellation of values characteristic of Neohumanism.

First comes an excursus, in which Gauss states that "it is no good sign of the spirit of the times" that this kind of question is formulated so frequently and given such weight. It shows a petty and narrow-hearted way of thinking, a disposition to evaluate constantly the reward of every effort, and to relate everything to our "physical well-being." It demonstrates "coolness and lack of sense for what is great and honors mankind," a clear indifference to great ideas. In this context, Gauss offers us a glimpse at his political tendencies, his horrified reaction to "the catastrophes that we have experienced" (the Revolution and the Empire in France, the Napoleonic invasion of the German states, the death at war of his protector the Duke of Brunswick):

> It is quite certain that precisely that [utilitarian] way of thinking stands in a very precise connection with the misfortune that has struck so many states in recent times.[38]

[38] See [Gauss 1808], pp. 191–192: *Es ist kein gutes Zeichen von dem Geiste der Zeit, wenn man eine solche Frage oft und immer wieder aufwerfen hört. … documentiert zugleich eine kleinliche, engherzige und träge Denkungsart, einen Kaltsinn und eine Gefühllosigkeit gegen das Grosse und den Menschen Ehrende. … es ist wohl völlig gewiss, dass gerade diese Denkart mit dem Unglück, was in den letzten Zeiten so viele Staaten betroffen hat, in einem sehr genauen Zusammenhange steht … ich meine, dass*

There are sciences, says Gauss (and number theory comes to mind), that could never arise under the sign of such a way of thinking. Astronomy is not one of these, because it is clearly useful to human society, but our young astronomer-mathematician is convinced "that the true, authentic warmth for science will not be brought forward by *such* considerations." The "happy great spirits" that created and developed astronomy and the "remaining more beautiful parts" of mathematics, were not driven by the prospect of future benefits.

> They searched the truth for its own sake and found in the very success of their efforts their reward and their happiness. I cannot avoid at this point reminding you of Archimedes, who was admired by his contemporaries mainly just because of his artful machines, because of the apparently magical workings they had, but who placed so little value on all this, compared with his magnificent discoveries in the field of pure mathematics - which in themselves usually had no visible benefits in the common sense of the term, at least then - that he did not write down for us anything about the former, while he developed the latter with affection in his immortal works. You must all know the beautiful poem by Schiller. Let us consider also the sublime astronomy from this beautiful standpoint above all.[39]

Schiller's poem "Archimedes and the apprentice" was quite popular among German mathematicians in the XIX$^{\text{th}}$ century. There, the sage replies to the apprentice seeking initiation into the "divine art," that she [the art] was divine before she served the state: "If you want fruits, those a mortal can also beget, / He who woos the goddess, seek in her not the maid." Gauss seems to have been the first important mathematician to refer to this poem, Jacobi and Kronecker, among others, did so later.

Gauss proceeds to recite some pentameters by Ovid, and concludes. The worthy answers to the question of utility, are the higher and peculiar satisfaction which the sciences afford, the "beneficial retirement from the sometimes unpleasant external world through quiet contemplation that excites no frenzy," the greatness of the matter under study, which leaves far behind things that seem important for us in daily life.

solche Charakterzüge ... einen starken Ausschlag bei den Katastrophen, die wir erlebt haben, gegeben haben können.

[39] See [Gauss 1808], pp. 192: *Allein ich behaupte, dass die wahre, ächte Wärme für die Wissenschaft nicht durch* solche *Betrachtungen hervorgebracht wird. Die glücklichen grossen Geister, die die Astronomie eben so wie die andern schönern Theile der Mathematik geschaffen und erweitert haben, wurden gewiss nicht durch die Aussicht des künftigen Nutzens angefeuert: sie suchten die Wahrheit um ihrer selbst willen und fanden in dem Gelingen ihrer Anstregungen allein schon ihren Lohn und ihr Glück. Ich kann nicht umhin, Sie hier an Archimedes zu erinnern, den seine Zeitgenossen am meisten nur wegen seiner künstlichen Maschinen, wegen der zauberhaft scheinenden Wirkungen derselben bewunderten, der aber auf alles dieses in Vergleichung mit seinen herrlichen Entdeckungen im Felde der reinen Mathematik, die an und für sich nach dem gewöhnlichen Sprachgebrauch wenigstens damals meistens gar keinen sichtbaren Nutzen hatten, einen so geringen Werth legte, dass er uns über jene nichts aufzeichnete, während er diese in seinen unsterblichen Werken mit Liebe entwickelt hat. Sie kennen gewiss alle das schöne Gedicht von Schiller. Lassen Sie uns auch die erhabene Astronomie am liebsten aus diesem schönern Gesichtspunkte betrachten.*

And why should we not acknowledge, he adds, also the tranquility of finding each time, in the wonderful ordering of the cosmos, the traces of an eternal wisdom.[40] Finally, an idea borrowed from the then-fashionable German writer Jean Paul:[41] the stars are there for some higher reason, not just to serve as pacemakers and indicators for pepper fleets on their way back (from India), and the muses possess a higher sense than merely serving as maids to our needs.

It is clear that we listeners are not hearing the discourse of a typical man of the Enlightenment, a free-thinker. It is clear, too, that the very peculiar historical situation of 1808, the Napoleonic invasion, has left clear marks on the talk, as it did generally on German social, cultural and political life. But we should not create a wrong impression: Gauss shared the neohumanist values, but he also was a scientist, and one who knew well how to value the empirical and practical side of science. The last five pages of his inaugural lecture are devoted to explaining the practical services that astronomy has done to mankind, by liberating us from superstition, making possible the measurement of time, affording knowledge of the figure and size of the Earth, and enabling men to navigate long distances.

In 1808 there were still no pure mathematicians in Europe. As a truly transitional figure, Gauss was never a professional mathematician in the sense of later generations, but an astronomer. He devoted himself primarily to such topics as astronomy and geodesy, traditional within the broader framework of early-modern mathematics. But, if Gauss was forced to devote most of his time to the "less beautiful and elevated" parts of mathematics, we have every reason to think that he conceived of himself as a modern Archimedes.[42] Even in the realm of practical tasks, he found ways to reformulate the problems at hand and transform them into questions of pure mathematics. And he kept proclaiming the higher value of the pure theory of magnitudes, especially of number theory, complaining that he lacked the time necessary for devoting himself to this topic. Gauss is famously reported to have said that mathematics is the queen of the sciences and higher arithmetic the very queen of mathematics.[43] In the preface to the crown's jewel, the D.A., he speaks of the "sanctuary of this divine

[40] [Gauss 1808], p. 194: *das wohlthätige Abziehen von der manchmal nicht erfreulichen Aussenwelt durch stille, keine Leidenschaften aufregende Contemplation, ... und, warum sollen wir es nicht bekennen, die Beruhigung, in der wunderbaren Anordnung des Weltbaus immer die Spuren einer ewigen Weisheit wiederzufinden.*

[41] See Jean Paul, *Hesperus, 13. Hundsposttag.*

[42] Here it is less a question of the real Archimedes, than of the sage as portrayed by Plutarch and Schiller. Obviously Gauss borrowed heavily on Plutarch's widely-read description in his *Parallel Lives* (Life of Marcellus), but this was written 300 years after Archimedes lived, and with clear philosophical intentions. We have little evidence about the actual views of Archimedes, and some of the evidence we have (e.g., the *Method*) suggests that he may not have agreed with Platonism.

[43] See [Waltershausen 1856], p. 79. The quote continues: "Mathematics then often condescends to render a service to astronomy and other natural sciences, but in all relations mathematics is entitled to the first rank." (*Diese [die Mathematik] lasse sich dann öfter herab der Astronomie und andern Naturwissenschaften einen Dienst zu erweisen, doch gebühre ihr unter allen Verhältnissen der erste Rang).*

science,"another noteworthy exercise of neohumanist rhetoric.

Let us now consider some aspects of the early life and education of Gauss, during the years preceding publication of his D.A. While studying at the *Collegium Carolinum* in Braunschweig, 1792 to 1795, he received at least two important influences, the most crucial from Eberhard August Wilhelm von Zimmermann (1743–1815), his professor of mathematics and promoter *vis-à-vis* the Duke of Brunswick and Lüneburg; the other from Johann Joachim Eschenburg (1743–1820), professor of literature and philosophy, and a friend of the great Enlightenment philosopher Lessing. In 1796, while publishing an announcement of the first important mathematical result by Gauss, the construction of the regular 17-gon, Zimmermann wrote:

> It is worth being noticed, that Mr. Gauss is now in his XVIII^th^ year, and that here in Braunschweig he has devoted himself with just as much success to philosophy and classical literature, as to higher mathematics.[44]

This statement could be merely rhetorical and would then be of little value, were it not that many passages in Gauss's writings and letters attest, in their very terminology and the problems that they address, this early acquaintance with philosophy (we have seen two examples at the very beginning). In a letter to the neo-Kantian philosopher Jacob Friedrich Fries, he states that he has always had a great passion for philosophical speculation, although he has not found satisfaction in the writings of some philosophers (particularly the famous emergent figures of the post-Kantian period, Hegel, Schelling, etc.). The famous biologist Matthias Jacob Schleiden, father of the cell theory, who studied in Göttingen 1831 to 1834, attests that the *princeps mathematicorum* had studied the works of Kant in detail. Schleiden, himself a follower of Kant and Fries, also tells a story which shows the respect that Gauss had for Fries's work *Die mathematische Naturphilosophie* (Heidelberg, 1822).[45]

As regards philology and classical literature, suffice it to mention the well-known facts that Gauss had a great ability for languages, and that he considered studying philology when he matriculated at Göttingen. The university of Göttingen was by the late XVIII$^{\text{th}}$ century the most advanced one in the German states, one that from its beginnings in 1737 was much more in line with the Enlightenment and the new trends of Western culture than perhaps any other European university. During his period here, from 1795 to 1798, Gauss was fond of the lectures by Christian Gottlob Heyne (1729–1812) and by the naturalist Georg Christoph Lichtenberg (1742–1799). Both place us right in the middle of the neohumanist atmosphere. The importance of

[44] Quoted after [Wussing 1974], p. 19: *Es verdient angemerkt zu werden, dass H. Gauss jetzt in seinem XVIII*$^{\text{ten}}$ *Jahre steht, und sich hier in Braunschweig mit eben so glücklichem Erfolg der Philosophie und der classischen Literatur als der höheren Mathematik gewidmet hat.*

[45] For the letter to Fries, May 11, 1841, see [Gauss 1929], p. 204: *Ich habe von jeher grosse Vorliebe für philosophische Speculation gehabt.* For Schleiden's comments, see [Gauss 1917], p. 206, and [Gauss 1927], p. 63. On Hegel et al., see e.g., the letter to Schumacher, November 1, 1844, reproduced in [Gauss 1927], pp. 62–63. This last letter is noteworthy because it includes a passing criticism of Kant's distinction between analytical and synthetic truths, seemingly pointing in the direction of XX$^{\text{th}}$ century work.

Heyne as a philologist, historian, and founder of an influential seminar, has already been mentioned. As regards Lichtenberg, he was a very well respected experimental physicist, but also a successful writer whose aphorisms embody the ideals of the Enlightenment. In one of his short stories, a godlike figure charges a *savant* with the task of analyzing the chemical composition of a spherical body. After having listed its chemical composition, the *savant* realizes that the body was in fact the Earth, which he had destroyed in the process. The moral is that the analytical powers of the human mind may become dangerous when overplayed, and that only a more philosophical orientation can offer us a true understanding of reality and existence.

Gauss was a widely read man, and in the style of his times he liked to collect favourite quotations and mottos. One of them was the following, from Shakespeare's *King Lear*: “Thou, nature, art my goddess; / To thy laws my services are bound.”[46] This again brings to mind the figure of Gauss the astronomer, his actual profession, more than the pure mathematician. But, most importantly, we could cite similar thoughts stemming from the pens of early romantic writers like Goethe, Novalis, or Schiller. The very topic of ὁ θεὸς ἀριθμητίζει is already present in a poem by Novalis, whose second line might seem fitting for Gauss: “The life of the gods is mathematics. All divine messengers should be mathematicians.”[47]

Also the topic of science for its own sake is very much present in Gauss. A letter to Dirichlet of November 1838 emphasizes how much he values those who practice science in the Greek spirit, devoting themselves to pure contemplation, and how much he despises those who enter into petty disputes and competition.[48] Already in 1811, at the beginning of the famous letter to Bessel containing Cauchy's theorem on complex integration, he writes: “here it is not a question of practical utility, I take analysis to be an autonomous science” (we will return to this passage in § 5). These words are prototypical of Neohumanism and of the German intellectual atmosphere.

4. Neohumanism in the Prussian Universities

If we consider who were the most important German number theorists one or two generations after Gauss, we find the names of Carl Gustav Jacob Jacobi, Johann Peter Gustav Lejeune-Dirichlet, Ernst Eduard Kummer, Gotthold Eisenstein, Leopold Kronecker. They taught at the universities of Königsberg, Berlin, and Breslau – all of them Prussian universities.[49] Likewise, considering the most important early exponents of arithmetization, we are led to two Berlin professors, Ohm and Dirichlet. It would seem that there is some hidden connection between Prussia, or more generally the northern German states, and the new trends in pure mathematics.

[46] Quoted in [Wussing 1974], p. 88.

[47] [Novalis 1978], p. 791: *Das Leben der Götter ist Mathematik. Alle göttlichen Gesandten müssen Mathematiker seyn.* On Novalis and mathematics, see [Jahnke 1990], but one should beware that in his thought one finds extreme romantic tendencies which are obviously foreign to Gauss.

[48] This letter is photographically reproduced in [Scharlau, Opolka 1980], following p. 120, and it is translated as an appendix to the English version of this book.

[49] One might also consider secondary figures like Moritz Stern who taught at Göttingen (not part of Prussia at the time, but in northern Germany).

The connection seems to consist of the strong presence of neohumanist ideals in the reformed universities of northern Germany. Even if the usual idea that neohumanism and romantic ideals reigned supreme at the time is, itself, a piece of romantic *Zeitgeist* historiography,[50] it is no less true that they had a strong impact upon university professors, including mathematicians. Studies on the reform of the German university system in the early XIX$^{\text{th}}$ century have always emphasized the important role of Wilhelm von Humboldt, the philologist, during the short period of time (February 1809 through July 1810) in which he drew and developed plans for the establishment of Berlin University. Considering the role played by his brother naturalist Alexander von Humboldt in the promotion of the above-mentioned mathematicians,[51] the point becomes even stronger, for Alexander's figure is again characteristic of Neohumanism.

Neohumanism was a cultural movement embodying a peculiar constellation of values that, as we could vividly appreciate in Gauss's inaugural lecture, shaped or tinted approaches to the various sciences in XIX$^{\text{th}}$ century Germany. To understand how this could come to happen, it is important to consider two points. By 1800, the scientific disciplines were not yet professionalized, a process that would take place precisely during the subsequent decades. Not being professionals yet, representatives of the sciences were much more liable to be influenced by broader cultural influences. Besides, value systems are much more effective and durable when they are embodied in institutional arrangements. As a result of the university reform, mathematics and the sciences were housed in the renewed faculty of philosophy, sharing rooms with the philosophers, philologists, and historians.

Up to then, mathematicians had mostly been practitioners or academicians. University professors of mathematics had taught topics that would be classified today as belonging to secondary-school level. Only that branch of mixed mathematics, astronomy, had become professionalized in a strong sense. Taking all of this into account, it is no wonder that Gauss should become a professional astronomer, nor that he disliked teaching the very elementary mathematical lectures at the university. The situation changed very quickly during the decades following 1810, and in the process mathematicians had to adapt to the milieu of the Philosophical Faculty. In Berlin and northern Germany, this meant that they had to prove their subject worthy of being studied at the university level. To comply with neohumanist and university-level expectations, mathematics had to be "elevated to the dignity of a well-ordered philosophical science,"[52] turning it into a true system of pure science. The best way to do it was, of course, to orient their investigations toward pure mathematical topics, and to rework the basis of their discipline with the aim of systematizing it.

The reader should consider how well this fits both the rise of Gaussian number theory in Germany, and the new foundational trend of arithmetization. Consider also how the above fits with the following passage, in which Felix Klein describes the

[50] See, e.g., [McClelland 1980].

[51] See H. Pieper's chap. III.1 above.

[52] I adapt here the words that F.A. Wolf employed to describe his new conception of philology as a discipline. See the quotation in [Paulsen 1897], p. 209, or in [Ferreirós 1999], p. 5.

first important research school in German mathematics, the Königsberg school of Jacobi and Franz Ernst Neumann:

> If we now ask about the spirit that characterizes this whole development, we can in short say: it is a scientifically-oriented Neohumanism, whose aim is the inexorably strict cultivation of pure science, and in search of that aim establishes a specialized higher culture, with a splendour never seen before, through a concentrated effort of all its powers.[53]

It is well known that the institution of the seminar, adapted by Jacobi and Neumann to mathematics and physics, was first introduced by neohumanist philologists and historians. The statements of Gauss that we reviewed in the previous section agree perfectly with such famous neohumanist lore as Jacobi's frequently quoted sentence, contradicting Fourier's enlightened view that mathematics is of value because of its applications, and charging that mathematics and pure number theory are valuable "for the honour of the human spirit."[54] Most important for us is that we are not talking about eccentricities of isolated figures, but about a general cultural movement that became an important element in the self-perception of the German bourgeoisie, most particularly of university professors.

Of course, the very example of Gauss and the *Disquisitiones Arithmeticae* shows that the resulting movement, and the changes in scientific disciplines, was not just a mechanical reaction to new institutional arrangements. The idea of reforming Prussian universities emerged after the Prussian defeat at Jena in 1806, while the D.A. was published in 1801. But the neohumanist trend antedates the reform and links back to the German Enlightenment, as the pioneering cases of the philologists Heyne and Wolf mentioned above, or even of Kant himself, make clear.

The influence of Neohumanism stimulated the orientation of Gauss's work in the direction of pure mathematics. The very good reception of his ideas, methods, and aims in northern Germany (not an immediate one, certainly, but a powerful reception and further development from about 1825) would be difficult to explain, were it not for the catalyzing role played by contextual factors, most particularly by the neohumanist atmosphere.

Cultural environments may change rapidly, though, and the neohumanist ideals began to fade, or at least to be mixed up with other cultural influences (e.g., positivism), after the middle of the century. But by then the reorientation had become institutionalized in the research tendencies of the German community of professional

[53] See [Klein 1926], vol. 1, p. 114: *Fragen wir nun nach dem Geist, der diese ganze Entwicklung trägt, so können wir kurz sagen: es ist der naturwissenschaftlich gerichtete Neuhumanismus, der in der unerbittlich strengen Pflege der reinen Wissenschaft sein Ziel sieht und durch einseitige Anspannung aller Kräfte auf dies Ziel hin eine spezialfachliche Hochkultur von zuvor nicht gekannter Blüte erreicht.*

[54] See [Jacobi 1881], p. 454–455, letter from Jacobi to Legendre, July 2, 1830 : *mais un philosophe comme lui [Fourier] aurait dû savoir que le but unique de la science, c'est l'honneur de l'esprit humain, et que sous ce titre, une question de nombres vaut autant qu'une question du système du monde.* On the changing professional status of number theory, see [Goldstein 1989].

mathematicians, having thus gained a momentum that sustained its autonomous development.

5. Gauss and the "Metaphysics" of Mathematics

Neohumanism fomented interrelations among the different disciplines, and particularly between the scientific disciplines and philosophy. The resulting intellectual orientations and institutional arrangements seem to offer the best explanation for the otherwise surprising fact that German scientists in the XIX$^{\text{th}}$ and early XX$^{\text{th}}$ centuries show a rather high degree of commitment to philosophical questions and argument. Not only were the sciences part of the Faculty of Philosophy, but the curricular freedom of the German university system (*Lernfreiheit*) allowed students to choose the lectures they attended at will, from the whole spectrum of topics covered in the Faculty.

The "metaphysics" (philosophical foundations) of mathematics seems to have been a topic that the *princeps mathematicorum* enjoyed discussing. Sartorius von Waltershausen wrote:

> It was especially noteworthy, and extremely instructive, to observe Gauss expose the foundations on which mathematics is based, and delimit it sharply against metaphysics.[55]

The reader may be struck by the apparent contradiction between Sartorius and Gauss himself as to the concept of "metaphysics," but it seems to be mainly a matter of words. Gauss employed what was a common way of expression around 1800 (there was frequent talk, for example about the "metaphysics of the calculus"), to mean what we might nowadays call the philosophical foundations of mathematical knowledge. Sartorius seems to be speaking the language of early positivism around 1850, distinguishing the philosophy of mathematics from metaphysical speculation.

In accordance with Sartorius's recollections, the topic appears several times in the correspondence of Gauss, but there are very few extant writings touching upon it. Two of them deal with questions in the metaphysics of mathematics, but they were left unpublished.[56] The most important piece, perhaps the only important one, since it was the only one published during his lifetime, is the famous *Selbstanzeige* [Gauss 1831] of the *Theoria residuorum biquadraticorum, commentatio secunda*. This is the frequently cited paper in which Gauss defends the complex numbers and their right of citizenship in the *polis* of mathematics.

Gauss's reflections on the foundations of mathematics are, in some ways, similar to those of Riemann.[57] His point of departure was the traditional, and in his lifetime

[55] See [Waltershausen 1856], p. 81, or [Gauss 1900], 267: *Es war besonders merkwürdig und überaus lehrreich, von Gauss die Fundamente, auf denen die Mathematik basirt ist, blosgelegt und sie gegen die Metaphysik scharf abgegrenzt zu erblicken.*

[56] See [Gauss 1917], pp. 396–397, a document of 1825, and [Gaus 1929], pp. 57–61, around 1800. We shall rely on the earlier document below.

[57] See [Scholz 1982] and [Scholz 1992], [Laugwitz 1996], [Ferreirós 1996], and [Ferreirós 1999], chap. 2. I have offered a more detailed analysis in the introduction to the Spanish edition of *Riemanniana Selecta* [Ferreirós 2000], pp. LXXIV–CXVII.

still customary, definition of mathematics as a science of magnitudes (*Grössenlehre*). But, like Riemann and other authors (and, as usual, preceding all of them), Gauss presented a novel conception of magnitudes, turning them into more abstract objects. Thereby he came to conceive of mathematics as a theory of *relational structures*. I shall allow myself the use of this modern term "structure," but it is of course not my aim to modernize Gauss or to present his ideas in the light of current foundational views. Rather, the phrase seems to offer an apt description of his own views, provided that we understand the term "structure" in a primitive, intensional sense, and refrain from assigning to it the usual extensional interpretation of set theory.

Gauss thought that the subject matter of mathematics was not certain particular objects, but rather relations between objects, and interrelations among those relations. In his opinion, mathematics is "in the most general sense, the science of relations"; or, as he put it in the 1831 *Selbstanzeige*:

> The mathematician abstracts entirely from the quality of the objects and the content of their relations; he just occupies himself with counting and comparing their relations to each other.[58]

In 1825, he exemplified this with the lattice of points corresponding to the Gaussian integers in the complex plane. Those points are objects, but it is the *transitions (Übergänge)* from one to another which represent relations, and thus the magnitudes studied by the mathematician. The conception of mathematics as a science of relational structures forms the keystone of Gauss's defence of the complex numbers.

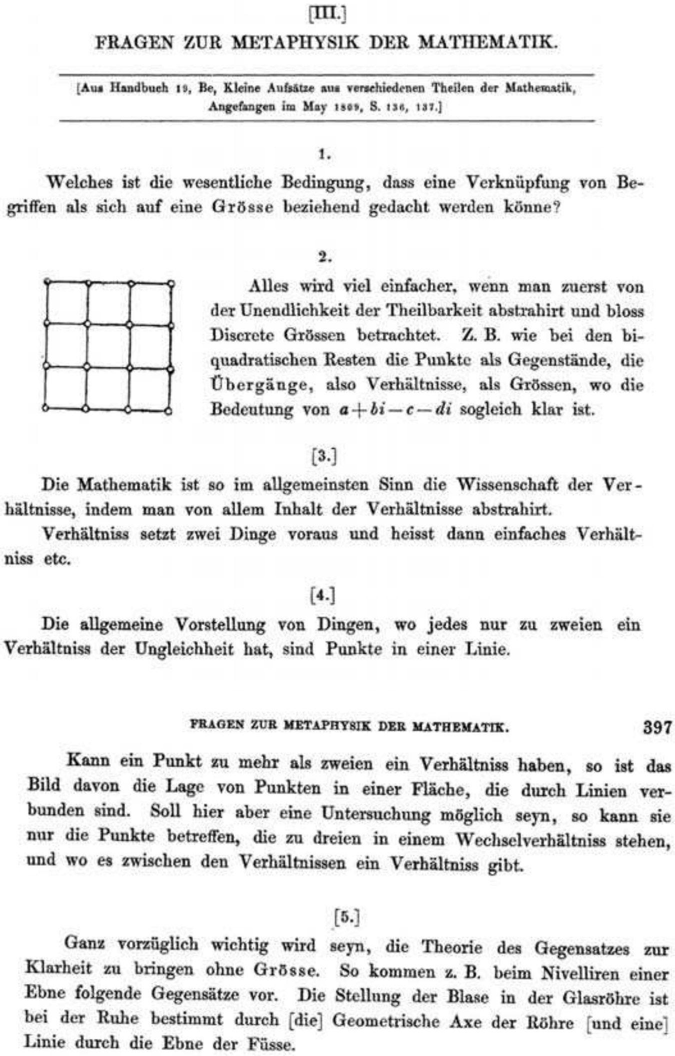
Full acceptance of the complex numbers had been a key motive in his work from the late 1790s. His first attempt at a proof of the "Fundamental Theorem of Algebra," contained in his 1799 dissertation, emerged from the consideration of polynomials as complex functions;[59] but knowing that the complex numbers were still regarded with mistrust by almost all mathematicians, Gauss omitted carefully from the text of his dissertation any reference to his motivating, heuristic ideas. For the time being, he would only express his actual thoughts in letters to close friends; in the above-mentioned letter of 1811 to Bessel, Gauss wrote:

> To somebody who wishes to introduce a new function in analysis, I would ask above all … whether he accepts my basic principle, that within the realm of magnitudes one must regard the imaginary $a + b\sqrt{-1} = a + bi$ as enjoying the same rights as the real [magnitudes]. … Here it is not a question of practical utility – I take analysis to be an autonomous science, which by relegating those fictitious magnitudes would lose enormously in beauty and roundedness, and at every instant would be forced to add quite cumbersome restrictions to truths that otherwise would be generally valid.[60]

[58] See [Gauss 1831], p. 176: *Der Mathematiker abstrahirt gänzlich von der Beschaffenheit der Gegenstände und dem Inhalt ihrer Relationen; er hat es bloss mit der Abzählung und der Vergleichung der Relationen unter sich zu thun.* Already in 1825, Gauss wrote [Gauss 1917], p. 396: *Die Mathematik ist so im allgemeinsten Sinne die Wissenschaft der Verhältnisse, indem man von allem Inhalt der Verhältnisse abstrahirt.*

[59] This he emphasized in [Gauss 1831], and later in [Gauss 1849].

[60] See [Gauss 1917], p. 90, letter Gauss to Bessel, December 18, 1811: *Zuvörderst würde*



[III.]

FRAGEN ZUR METAPHYSIK DER MATHEMATIK.

[Aus Handbuch 19, Be, Kleine Aufsätze aus verschiedenen Theilen der Mathematik, Angefangen im May 1809, S. 136, 137.]

1.

Welches ist die wesentliche Bedingung, dass eine Verknüpfung von Begriffen als sich auf eine Grösse beziehend gedacht werden könne?

2.

Alles wird viel einfacher, wenn man zuerst von der Unendlichkeit der Theilbarkeit abstrahirt und bloss Discrete Grössen betrachtet. Z. B. wie bei den biquadratischen Resten die Punkte als Gegenstände, die Übergänge, also Verhältnisse, als Grössen, wo die Bedeutung von $a+bi-c-di$ sogleich klar ist.

[3.]

Die Mathematik ist so im allgemeinsten Sinn die Wissenschaft der Verhältnisse, indem man von allem Inhalt der Verhältnisse abstrahirt.

Verhältniss setzt zwei Dinge voraus und heisst dann einfaches Verhältniss etc.

[4.]

Die allgemeine Vorstellung von Dingen, wo jedes nur zu zweien ein Verhältniss der Ungleichheit hat, sind Punkte in einer Linie.

FRAGEN ZUR METAPHYSIK DER MATHEMATIK. 397

Kann ein Punkt zu mehr als zweien ein Verhältniss haben, so ist das Bild davon die Lage von Punkten in einer Fläche, die durch Linien verbunden sind. Soll hier aber eine Untersuchung möglich seyn, so kann sie nur die Punkte betreffen, die zu dreien in einem Wechselverhältniss stehen, und wo es zwischen den Verhältnissen ein Verhältniss gibt.

[5.]

Ganz vorzüglich wichtig wird seyn, die Theorie des Gegensatzes zur Klarheit zu bringen ohne Grösse. So kommen z. B. beim Nivelliren einer Ebne folgende Gegensätze vor. Die Stellung der Blase in der Glasröhre ist bei der Ruhe bestimmt durch [die] Geometrische Axe der Röhre [und eine] Linie durch die Ebne der Füsse.

Fig. III.2B. Gauss's remarks on metaphysics in mathematics. From Gauss, *Werke* X.1, pp. 396–397.

ich jemand, der eine neue Function in die Analyse einführen will fragen … ob er meinem Grundsatze beitrete, dass man in dem Reiche der Grössen die imaginären als gleiche Rechte mit den reellen geniessend ansehen müsse. … Es ist hier nicht von praktischem Nutzen die Rede, sondern die Analyse ist mir eine selbständige Wissenschaft, die durch Zurücksetzung jener fingirten Grössen ausserordentlich an Schönheit und Rundung velieren und alle Augenblick Wahrheiten, die sonst allgemein gelten, höchst lästige Beschränkungen beizufügen genöthigt sein würde.

It is noteworthy that he went so far as to call this principle of "equal rights" for real and imaginary magnitudes his *Grundsatz*, his fundamental principle in analysis.

At last, in 1831, and motivated by number theory – namely, by the need to expand the field of number theory to the Gaussian integers $a+bi$ (with a, b rational integers), and even to other domains of algebraic integers – Gauss presented the well-known geometrical interpretation of complex numbers as points in the Gaussian plane. This, however, was only an *intuitive* illustration, to which he added a more abstract philosophical argument for their full acceptability as mathematical objects.

In the early XIX$^{\text{th}}$ century, the thesis of the *intuitiveness (Anschaulichkeit)* of mathematical knowledge was well-known to German scientists and mathematicians, being the key tenet of Kant's philosophy of mathematics. Mathematical truths are not merely conceptual truths, as Leibniz pretended, but truths involving in an essential way the "construction of concepts in intuition" (*Anschauung*). One could even say that the *Anschaulichkeit* thesis was somewhat commonplace, or at least so did Gauss treat it. It is for this reason that he took care to indicate that, by introducing the complex numbers, one does not "distance oneself from intuitiveness." On the contrary, "the arithmetic of the complex numbers can be given a most intuitive representation" in terms of the Gaussian plane.[61] But the main point in his argument was more general and abstract.

Gauss claimed that the mathematical study of the complex (resp., the negative) numbers is justified, as soon as there exist physical situations that give occasion to their employment. That is to say, it suffices to show that some physical situations present us with relational structures that can only be represented by means of the complex (resp., the negative) numbers. For this to be the case, Gauss claims, one cannot be dealing with simple substances, but rather must be handling relations between substances or objects. When the relations can be inverted, the need for negative numbers emerges. When the objects and their relations cannot be ordered into a single series, but give rise to a "series of series" or, as Gauss also put it, a "manifold of two dimensions," one must introduce a "lateral unit" i, and with it the complex numbers.[62] When the objects and their relations give rise to a "manifold of two dimensions," one must introduce complex numbers. In this sense, they are no less real or justifiable than the rational or the "real" numbers.

As we saw at the beginning, Gauss regarded arithmetic as "knowledge *a priori*," contrasting it with geometry and mechanics. Numbers are "*just* a product of our minds," and we can "prescribe [their] laws *a priori*"; space has "a reality outside our minds," and its laws must be determined (partly at least) by experiment, just like the laws of mechanics. Apriority is not limited to the arithmetic of natural

[61] See [Gauss 1831], p. 174: *dass die Untersuchung dadurch ... sich von der* Anschaulichkeit *ganz entferne. Nichts würde ungegründeter sein, als eine solche Meinung. Im Gegentheil ist die Arithmetik der complexen Zahlen der anschaulichsten Versinnlichung fähig.* The correspondence between August Ferdinand Möbius and the philosopher Ernst Friedrich Apelt exemplifies the wide diffusion of the *Anschaulichkeit thesis*; see [Lewis 1977].

[62] Cf. [Gauss 1831], p. 176.

numbers, it characterizes the whole "pure theory of magnitudes."[63] Our knowledge of the full number system, from the natural to the complex numbers, is characterized by "absolute conviction of its necessity (and therefore of its absolute truth)."

We remarked, too, that this philosophical conception of mathematics seems to be precisely in the tradition of Leibniz and Kant. That seems appropriate, given the outstanding role that Leibnizian philosophy played in Germany during the XVIII$^{\text{th}}$ century,[64] and the comparable role of Kantian philosophy since about 1785. The reflections of Gauss thus seem to be located in a playground delimited by Leibniz's rationalism and Kant's criticism. To clarify the limits of this philosophical playground, I shall comment briefly on the philosophy of arithmetic defended by these two authors.

For Leibniz, arithmetic consists of *verités de raison*, i.e., *a priori, analytical* truths based merely on definitions and logic. Thus, from $2 = 1 + 1$ (def.) and $4 = 1 + 1 + 1 + 1$ (def.), and by the logical principle of substitution, one can reduce $2 + 2 = 4$ to an elementary identity of the form $A = A$. The opposite of this *a priori* truth is the impossibility $A \neq A$ which is ruled out by the principle of contradiction.[65] Such necessary truths are contrasted with the *verités de fait*, empirical truths, which are merely contingent (their opposite is possible).

Kant was strongly influenced by Leibniz in his early pre-critical period, and always retained the basic idea that mathematical truths are necessary and *a priori*. However, in his view neither arithmetic nor geometry is merely analytical, none of them reduces to logic plus definitions – they are synthetic, based on intuition (*Anschauung*), more precisely on the "pure intuitions" of space and time. He claimed that, in order to show that the sum $7 + 5$ is precisely 12, one has to go beyond the concept of sum and rely on intuitions, e.g., of fingers or perhaps dots.[66] Mathematical truths derive their validity from the "construction" of mathematical concepts in intuition. This came to be known as the *Anschaulichkeit* thesis, i.e., the view that mathematics is characterized by "intuitiveness."

There is evidence suggesting that Gauss was not a Leibnizian but a Kantian (though not completely orthodox) in the foundations of mathematics. In a review of 1816, he discussed a book by a certain Johann Christoph Schwab, who aimed to prove philosophically the truth of Euclid's postulates. Gauss first criticized the faulty

[63] In the light of other writings, we can interpret this to mean the theory of real and complex numbers; by the end of his life Gauss seems to have also included the theory of n-dimensional manifolds (of constant, non-negative curvature). In this paragraph I am simply extracting points from the 1830 letter to Bessel; all quotations come from it (see above).

[64] Above all in the somewhat simplistic version due to the philosopher Christian Wolff (who is not to be confused with the philologist Friedrich August Wolf mentioned before).

[65] See [Leibniz 1704], book IV, chap. VII; also the Monadologie [Leibniz 1714], prop. 33.

[66] See [Kant 1787], e.g., B 3–4, B 14–16, and all of part I; also [Kant 1783], part I: "How is pure mathematics possible?" The example $7+5 = 12$ is not very convincing, particularly after Leibniz; besides, the sum $3512 + 478$ is certainly not done in intuition; one can make a better case for Kant's views using the principle of mathematical induction as an example, as Poincaré did in [Poincaré 1902].

attempt to prove the parallel axiom, and then he commented on another main goal of the work: to show that Kant's philosophy of geometry is wrong, that the axioms of geometry are "not founded on the senses and *intuition* but on the *intellect*."[67] From the description it is clear that Schwab adopted a Leibnizian view of geometry: everything should be based on definitions and logical principles. But Kant has not denied, said Gauss, that geometers are constantly using logical principles to present and enchain the truths, from postulates to theorems. The point is that those principles do not suffice for founding the postulates themselves, and nobody who is familiar with the essence of geometry will deny

> that for themselves [the logical means] are not enough to obtain anything, and will only bloom sterile flowers, if the fructifying, living intuition of the object does not act everywhere.[68]

This viewpoint is strongly reminiscent of (and clarifies) a manuscript *Zur Metaphysik der Mathematik* written around 1800. Here we learn that the subject matter of mathematics is magnitudes, but only insofar as they bear relations to each other:

> Mathematics really teaches general truths concerning the relations between magnitudes, and its aim is to *describe* magnitudes that bear known relations *to known magnitudes* or *to which known magnitudes* bear known relations, i.e., to make possible a representation of them.[69]

Now, one can obtain a representation of a magnitude in two ways: (1) by "immediate intuition (an immediate representation)," or (2) by comparison with magnitudes given in the first way. In the case of geometry one represents the sought magnitudes directly, by "geometrical representation or construction."[70] As one can see (1), intuition has a key role to play.

Both of these documents are very Kantian in terminology and ideas. They show that, at least up to 1816, Gauss shared many of Kant's views on the philosophy of mathematics. According to the 1800 manuscript, geometry is for Gauss just a part of the science of "the relations among magnitudes," mathematics; it deals with magnitudes directly according to their geometrical relations, just as arithmetic –

[67] See [Gauss 1900], pp. 170–172; here p. 172: *non sensu et* intuitione *sed* intellectu *fundata.*

[68] See [Gauss 1900], p. 172: *Dass von diesen logischen Hülfsmitteln zur Einkleidung und Verkettung der Wahrheiten in der Geometrie fort und fort Gebrauch gemacht werde, hat wohl* Kant *nicht läugnen wollen: aber dass dieselben für sich nichts zu leisten vermögen, und nur taube Blüten treiben, wenn nicht die befruchtende lebendige Anschauung des Gegenstandes selbst überall waltet, kann wohl niemand verkennen, der mit dem Wesen der Geometrie vertraut ist.*

[69] See [Gauss 1929], p. 57: *Die Mathematik lehrt nun eigentlich allgemeine Wahrheiten, welche die Relationen der Grössen betreffen, und der Zweck davon ist, Grössen, die* zu bekannten Grössen *oder* zu denen bekannte Grössen *bekannte Beziehungen haben,* darzustellen*, d.h. eine Vorstellung davon möglich zu machen.*

[70] See [Gauss 1927], p. 57: *durch unmittelbare Anschauung (eine unmittelbare Vorstellung) ... geometrische Darstellung oder Construction.* The arithmetical *Darstellung* by means of numbers is more abstract and general.

which is more general and indirect – treats their arithmetical relations. The role of "immediate intuition (an immediate representation)" has been clearly affirmed before distinguishing the two branches of mathematics, so it applies also in the case of arithmetic.

Seemingly we could conclude that, when Gauss stated that arithmetic "stands purely *a priori*," he intended this in a Kantian sense, not a Leibnizian one. But there is still the possibility that his later reflections, going in the direction of a more abstract and conceptual (or relational) approach, may have led him to reject the idea that arithmetical knowledge depends on an intuitive element. This would bring his position closer to Leibniz, without however committing him to the view that pure mathematics is analytical in the simplest sense of this term. In my opinion, the most plausible reconstruction is that Gauss was much closer to Kantian views of arithmetic in 1800 than 25 years later.

In order to be "purely *a priori*," arithmetic should be based on *pure*, not empirical intuition. That is an orthodox Kantian view. But Gauss was not orthodox, for he regarded geometry as based (partly at least) on empirical intuition.[71] This of course was a way of accommodating his non-Euclidean discoveries in the Kantian framework: the parallel axiom was to be decided by experiment, not *a priori*. That Gauss preserved the Kantian framework is suggested by the fact that, from this time, he no longer regarded geometry as pure mathematics. Eventually, Gauss even developed an argument that, in his view, offered a decisive refutation of Kant's "phantastic idea" (*Einbildung*) that space is merely the form of our intuition.[72] This is a crucial modification of the Kantian scheme, for it brings us back to a more common-sense worldview, which warrants that our geometrical models of the world can be interpreted realistically – contrary to Kant, they *do* represent aspects of the real world.

By assimilating geometry with mechanics, Gauss introduced an unorthodox revision of Kantianism. The difference is certainly important,[73] but Gauss incorporated these novelties into a general framework that seems to be clearly Kantian. That is, the difference is not so strong as to conclude that he rejected Kantian epistemology – those can be regarded as corrections *from within* Kantianism (in the case of mechanics, already Kant admitted that it has an empirical component, although he believed that some of its key laws are *a priori*).[74] He seems to have thought

[71] This must be taken into account in order to interpret correctly the views he expressed in the 1816 review; see above and compare with the 1817 letter to Olbers quoted in § 1.

[72] This argument was briefly sketched in print; see [Gauss 1831], p. 177. It elaborates upon Kant's argument of "incongruous counterparts" (left and right hand). See also Gauss's letter to Schumacher, February 8, 1846 in [Gauss 1900], p. 247.

[73] The difference would have deep consequences for other parts of the Kantian system, but it seems clear that Gauss never considered these. Despite his love of philosophy, he was not a professional philosopher and he limited his reflections to issues touching the theory of knowledge, and thereby mathematics and science.

[74] The corrections are actually lighter than some proposed by neo-Kantians around 1900; see [Cassirer 1907]. And one may remark that (at least in philosophy) a good disciple must be critical towards his master's ideas.

that geometry has an *a priori* component too, because space is a magnitude, a 3-dimensional manifold, and the "pure theory of magnitudes" is *a priori*. The *a priori* properties of space would probably include topological properties (e.g., continuity or completeness, three-dimensionality), and perhaps some of the metric properties of Lobachevskii-Bolyai geometry.

Gauss's reconception of the traditional *Grössenlehre* was in no way conservative, but led to novel views, since analysis and comparison of relations required the development of innovative theories. In particular, in 1849 he stressed the need to develop a branch or "higher domain of the abstract theory of magnitudes," dealing with "combinations among magnitudes linked by continuity," where metrical relations would not be taken into account.[75] This is what his student Johann Benedikt Listing would call *Topologie*, and what his most brilliant student, Riemann, called *analysis situs*, borrowing a phrase of Leibniz. Such were the considerations involving the interrelations and knots among curves that motivated Gauss in his proofs of the "Fundamental Theorem of Algebra" and more generally in function theory.

Once again, Gauss appears as a truly transitional figure. One cannot deny the modernity of the new domains whose study he opened up, the novel thoughts and viewpoints he introduced, and the deep methods he employed (deep in the sense that later they could be applied to much more general problems). The same applies to his understanding of mathematics as such, of its subject matter and its methods: we find Gauss advancing quite clearly toward structural and abstract conceptions.[76]

6. Arithmetic and the Foundations of Mathematics

In order to gain a deeper understanding of Gauss's role within the emergence of arithmetization, we shall now discuss the role played by arithmetic in his understanding of the "metaphysics" of mathematics. We need further clarification of the precise role of the natural numbers in Gauss's "pure theory of magnitudes." The issue becomes problematic due to ambiguous usage of the term "arithmetic," an ambiguity that was still very much present in the work of Hilbert early in the XX$^{\text{th}}$ century. By "arithmetic," German authors sometimes meant the theory of natural numbers, sometimes the theory of real or even complex numbers. Indeed, with arithmetization in the late XIX$^{\text{th}}$ century, it was not uncommon to expand the meaning of "arithmetic" to include all of pure mathematics. In particular, algebra and real and complex analysis were regarded as parts of general arithmetic.

Extant foundational pronouncements by Gauss usually take us into the realm of the complex numbers, so central to many of his deeper mathematical contributions.

[75] See [Gauss 1849], p. 79: *einem höhern vom Räumlichen unabhängigen Gebiete der allgemeinen abstracten Grössenlehre … dessen Gegenstand die nach der Stetigkeit zusammenhängenden Grössencombinationen sind.* The idea is implicit in Gauss's work on function theory, and it is elaborated in manuscripts dealing with *geometria situs* in [Gauss 1900].

[76] The point is reinforced by a letter to Grassmann in which Gauss suggests that there is much in common in their foundational conceptions; see [Gauss 1927], pp. 436–437. The obvious common point is their abstractness, particularly the idea to distinguish an abstract theory of magnitudes from the theory of spatial magnitudes; see, e.g., [Gauss 1849].

To the best of my knowledge, none of his foundational passages deals concretely with the real numbers. This is entirely consistent with his basic principle (*Grundsatz*) of assigning equal rights to the real and the complex numbers; see the letter to Bessel from 1811 quoted in § 5.

Gauss seems to have thought of a rigorous, systematic development of the theory of magnitudes in the following terms. One would begin with utmost generality, introducing quite generally relations, magnitudes and operations, and developing the theory of the universal properties of all magnitudes. Such results would not belong to arithmetic, but to the pure theory of magnitudes; they apply to the natural numbers because they are a particular case, namely the theory of discrete magnitudes.[77]

In the preface to the D.A., Gauss calls the pure theory of magnitudes "analysis," and contrasts it with "arithmetic understood as the theory of the integers."[78] Here, "arithmetic" refers only to the system of the natural numbers, the study of their operations and properties. Gauss then distinguishes "elementary" arithmetic (*Arithmetica elementaris*) which focuses on the basic operations and computational technique, from "higher arithmetic" (*Arithmetica sublimior*), i.e., the general study of the "proper," particular properties of the integers (our number theory).[79]

By contrast, in the 1800 manuscript he distinguishes two parts of the arithmetical sciences, depending whether the concept of the infinite is assumed or not. These parts are called "common or lower" mathematics and "higher" mathematics, the calculus of the infinite.[80] Here the notion of arithmetic is used in an expanded sense, to include analysis, while in the D.A. its meaning is much narrower.

Thirty years later, Gauss called for an expansion of the field of "higher arithmetic," i.e., number theory, to include the Gaussian and other algebraic integers. The immediate motivation was the need to rely on such number domains in the study of higher residues and higher reciprocity laws:

> Accordingly, one soon realizes that in this rich domain of higher arithmetic one can only penetrate through completely new roads ... that to that end a specific expansion of the whole field of higher arithmetic is an essential necessity.[81]

[77] This statement would need qualification after 1825, since then and in [Gauss 1831], Gauss suggests that the restriction to discrete magnitudes takes us from the full domain of the complex numbers to that of the Gaussian integers. That is, he then went one step further in his emphasis on the rights of the complex numbers.

[78] See D.A., *praefatio*: *Nimirum quemadmodum ad* Analyseos *ditionem referuntur omnes quae circa quantitatem affectiones generales institui possunt disquisitiones: ita numeri integri (fractique quatenus per integros determinantur) obiectum proprium* Arithmeticae *constituunt.*

[79] D.A., *praefatio*: *omnes autem disquisitiones generales de numerorum integrorum affectionibus propriis* Arithmeticae sublimiori ... *vindicare.*

[80] See [Gauss 1929], p. 58.

[81] See [Gauss 1831], p. 171: *Man erkennt demnach bald, dass man in dieses reiche Gebiet der höhern Arithmetik nur auf ganz neuen Wegen eindringen kann ... dass dazu eine eigenthümliche Erweiterung des ganzen Feldes der höhern Arithmetik wesentlich erforderlich ist.*

But even here, it seems clear that Gauss placed severe restrictions as to the subject matter and methods of number theory, namely that one studies discrete domains (from our standpoint, rings of integers) by characteristically number-theoretical means. The introduction of continuous domains and topological considerations takes us into a different, more general part of mathematics, which we might call the pure theory of magnitudes (*Grössenlehre*) or, following the D.A., "analysis."

It thus seems that, by sticking to the old terminology of *Arithmetik* and *Grössenlehre* (respectively analysis), Gauss usually avoided the ambiguity of later usage. His conception of arithmetic was preferentially linked with number-theoretical methods and subject matter. As we have seen, however, in one of his early writings one finds the tendency to identify pure mathematics with arithmetic, in an expanded sense of the word. This is the tendency that won the day in Germany, late in the XIX$^{\text{th}}$ century, due to the influence of authors such as Weierstrass and Dedekind.

In his foundational fragments on *Metaphysik der Mathematik*, Gauss used the concept of relation as the basic notion. Numbers are defined more or less in the classical way, in reference to particular kinds of relations between magnitudes (reminiscent of the usual definition of the reals as proportions) or relations between relations (a sophisticated refinement of the classical procedure). In strong contrast to Weierstrass and Dedekind, who were following Ohm, there seems to be no attempt to build up the full number system from the natural numbers alone.

In this light, it seems that Gauss never promoted arithmetization in the sense of a program for the reduction of pure mathematics to the theory of natural numbers (in a sense however, only Kronecker – and Ohm earlier – worked along strictly reductionistic lines).[82] On the other hand, he did promote arithmetization, in the sense of an *identification of pure mathematics with a most general theory of the (complex) number system.* The evidence suggests that Gauss conceived of algebra and analysis as parts of the general study of the complex numbers, their operations, relations, and properties. Weierstrass and Dedekind followed him in this.

That constitutes an essential part of what arithmetization meant later in the century. To that, Weierstrass and Dedekind added the notion that pure mathematics can be developed on the sole basis of the arithmetic of natural numbers by purely logical means; a thought that seems to be inspired by Ohm, not by Gauss.[83] With this, there emerged the problem of giving an adequate foundation for the elementary arithmetic of natural numbers. In the 1860s and 1870s, Hermann Grassmann, Hermann Hankel and Ernst Schroeder tried their hands at the problem, but they still remained far from a satisfactory system. Much closer was Weierstrass in his introductory university lectures, and above all Dedekind with his booklet *Was sind und was sollen die*

[82] In [Dedekind 1888], p. 338, strong reductionistic views are explicitly rejected, and Dedekind recalls that Dirichlet had also been far from such views. From our standpoint, what Weierstrass did was to reduce pure mathematics to sets and natural numbers; [Dedekind 1888] went further and reduced everything to sets and mappings; see [Ferreirós 1999], chap. VII.

[83] Interestingly, on this point Riemann followed Gauss and seems to have been far from Ohm's influence.

Zahlen? Here he approached the theory of natural numbers in such a way that, with one stroke, a sufficient and quite general basis was gained for "the purely logical development of the science of numbers": "arithmetic (algebra, analysis)."[84] But with Richard Dedekind, Georg Cantor, Gottlob Frege, and Giuseppe Peano, the course of history takes us into a different field, that of contemporary set theory, logic, and foundational studies.

7. Conclusion

The *Disquisitiones Arithmeticae* turned number theory, or the "higher arithmetic," into a true system, a rigorous and well-ordered science dealing essentially with the theory of congruences and forms. Gauss did not just pose new problems and present superb new thoughts. He reconstructed number theory, he introduced new language embodying a novel conceptual understanding of the subject, and he developed the corresponding new methods. This step itself bore seeds for a deep transformation of XIX$^{\text{th}}$ century images of the mathematical field. Further impulses came with the birth of modern analysis – the reform of the infinitesimal calculus, its further development, and the introduction of rigorous foundations – and with the growing awareness of weaknesses in the foundations of geometry, particularly after the emergence of non-Euclidean systems. Important as this last factor may have been, in that it contributed greatly to tilting the foundational balance towards arithmetic, without the first two factors (and not just the second) the program of arithmetization (§ 1) would never have been seriously undertaken.

Not all of the characteristic traits of arithmetization seem to be present in Gauss (§ 6), but his contribution to the rise of pure mathematics advancing "*under the sign of number*" is undeniable. Indeed, the sentence ὁ θεὸς ἀριθμητίζει symbolizes this arithmetization of the image of mathematics, but also the rise of a disciplinary divide between pure and "mixed" mathematics in the XIX$^{\text{th}}$ century. The work of Gauss and his correspondence (well-known after about 1860) lent the whole support of his immense reputation to that process. Euclidean geometry was degraded to the status of a semi-empirical science, joining mechanics, while the "arithmetical sciences" from number theory through complex analysis became the model of truly mathematical, *a priori* knowledge.

However, as we have seen, the reasons why those mathematical investigations produced a decisive turn in the conception of mathematics can only be fully analyzed when we take into account two other threads - the philosophical views and the cultural values which we have found present in Gauss's reflections. The intellectual dominance of Neohumanism in the conception of the German professoriate of itself had a noticeable impact upon scientific work, not directly on its results, but indirectly by reorienting it. Gauss's inaugural lecture at Göttingen (§ 3) is a perfect example of what the associated values amounted to, and how they stimulated a characteristic emphasis on pure science. The impact of this orientation became particularly strong

[84] See [Dedekind 1888], p. 335. He discovered that the arithmetic of **N** can itself be reduced to the "logic" of classes and mappings, and thereby arrived at a logicistic standpoint, simultaneously with, and independently of Frege.

as Neohumanism was embodied in the Prussian reformed universities (§ 4), a highly successful model for higher education during the whole of the XIXth century and beyond. Professionalization of mathematicians within the institutional context of philosophy faculties forced their adaptation to the cultural values they embodied.

Gauss's reflections on philosophical foundations, the "metaphysics of mathematics" as he used to say (§ 5), were also instrumental in bringing about the shift we have analyzed. Kantian philosophy laid great emphasis on pure mathematics as a quintessential example of true human knowledge. The *a priori* truths of pure mathematics were precisely the kind of topic that could be regarded as most appropriate for its inclusion in the curriculum of neohumanist Faculties of Philosophy. Gauss embraced the Kantian epistemology of mathematics to an important extent: he shared its belief in the existence of *a priori* knowledge, and its evaluation that such knowledge ranks higher than empirical knowledge. This, combined with the above two threads, produced his characteristic new image of mathematical knowledge.

It is of course difficult, perhaps impossible, to evaluate the precise contribution that each of those motives made to the emergence of a new style of mathematics. But it is clear that they fit perfectly the kind of conceptual approach (§ 2) that was an essential part of pure mathematics in XIXth century Germany. Kantian epistemology promoted conceptual approaches, not formal ones. Gauss regarded relations and magnitudes as the referents of mathematical knowledge and mathematical symbolism (§ 5), and this conditioned his preference for the conceptual against the formal – "the inner in contrast to the outer," as Dedekind said. One can hardly avoid the conclusion that the Gaussian understanding of mathematics as a science of relational structures was related to his methodological preferences. All of this, in turn, has obvious connections with the methodology of modern XXth century mathematics.

The history of reformulations of Plato's sentence did not end with the Gaussian motto. It had a sequel, again intimately involved with arithmetic, number theory, arithmetization, and cultural changes. Dedekind modified it once more in his 1888 booklet *Was sind und was sollen die Zahlen?*, writing: ἀεὶ ὁ ἄνθρωπος ἀριθμητίζει. He seemed to mean that it is not God who arithmetizes, but only *man* – implying that mathematics is a human product, a creation of the human mind, and that it does not deal with the laws of God, but rather with the laws of thought.[85]

Acknowledgements

I am grateful to the participants in the Gauss Tagung at Oberwolfach for their reactions and suggestions. My work was partially supported by the Ministerio de Ciencia y Tecnología, Spain, grant BFF2000-0097-C02-02.

References

Bekemeier, Bernd. 1987. *Martin Ohm (1792-1872): Universitätsmathematik und Schulmathematik in der neuhumanistischen Bildungsreform.* Göttingen: Vandenhoeck & Ruprecht.

[85] This motto was again intimately related to changes in foundational and epistemological views, including Dedekind's logicism. See [Ferreirós 1999], pp. 215–217 and chap. VII.

Behnke, Heinrich, Kopfermann, Klaus (eds.). 1966. *Festschrift zur Gedächtnisfeier für Karl Weierstrass 1815–1965*. Köln: Westdeutscher Verlag.

Biermann, Kurt-R. 1973. *Die Mathematik und ihre Dozenten an der Berliner Universität 1810–1920*. Berlin: Akademie-Verlag.

Bos, Henk, Mehrtens, Herbert, Schneider, Ivo (eds.). 1981. *Social History of Nineteenth Century Mathematics*. Basel, Boston: Birkhäuser.

Bühler, Walter Kaufmann-. 1982. *Gauss: A Biographical Study*. Berlin: Springer.

Cassirer, Ernst. 1907. Kant und die moderne Mathematik. *Kant-Studien* 12, 1–49.

Dedekind, Richard. 1930–1932. *Gesammelte mathematische Werke*, ed. R. Fricke, E. Noether, O. Ore. 3 vols. Braunschweig: Vieweg.

———. 1872. *Stetigkeit und irrationale Zahlen*. Braunschweig: Vieweg. Repr. in [Dedekind 1930–1932], vol. 3, pp. 315–334. Engl transl. in [Ewald 1996], pp. 765–779.

———. 1888. *Was sind und was sollen die Zahlen?* Braunschweig, Vieweg. Repr. in [Dedekind 1930–1932], vol. 3, pp. 335–390. Engl transl. in [Ewald 1996], pp. 787–833.

———. 1895. Über die Begründung der Idealtheorie. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 106–113. Repr. in [Dedekind 1930–1932], vol. 2, pp. 50–58.

Dugac, Pierre. 1973. Eléments d'analyse de Karl Weierstrass. *Archive for History of Exact Sciences* 10, 41–176.

Dunnington, Guy Waldo. 1927. The Sesquicentennial of the Birth of Gauss. *The Scientific Monthly* XXIV, 402–414.

Edwards, Harold M., Neumann, Olaf, Purkert, Walter. 1982. Dedekinds «Bunte Bemerkungen» zu Kroneckers «Grundzüge». *Archive for History of Exact Sciences* 27, 49–85.

Ewald, William Bragg. 1996. *From Kant to Hilbert*, vol. 2. Oxford: Oxford University Press.

Ferreirós, José. 1996. Traditional Logic and the Early History of Sets, 1854–1908. *Archive for History of Exact Sciences* 50, 5–71.

———. 1999. *Labyrinth of Thought. A History of Set Theory and its Role in Modern Mathematics*. Basel, Boston: Birkhäuser.

———. 2000. *Riemanniana Selecta*. Madrid: Consejo Superior de Investigaciones Científicas.

Gauss, Carl Friedrich. 1808. *Astronomische Antrittsvorlesung*. In [Gauss 1929], pp. 177–198.

———. 1831. Selbstanzeige der Theoria residuorum biquadraticorum, commentatio secunda. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen*. Repr. in [Gauss 1863], pp. 169–178. English transl. in [Ewald 1996], vol. 1, 306–313.

———. 1849. Beiträge zur Theorie der algebraischen Gleichungen. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen*. Repr. in [Gauss 1866], pp. 71–102.

———. 1863. *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universitäts-Druckerei. 2$^{\text{nd}}$ ed., Göttingen, 1876. Repr. Hildesheim, New York: Olms, 1981.

———. 1866. *Werke*, vol. III, *Analysis*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universitäts-Druckerei. Repr. Hildesheim, New York: Olms, 1981.

———. 1900. *Werke*, vol. VIII, *Arithmetik und Algebra: Nachträge zu Band 1–3*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Leipzig: Teubner. Repr. Hildesheim, New York: Olms, 1981.

———. 1917. *Werke*, vol. X-1, *Nachträge zur reinen Mathematik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Leipzig: Teubner. Repr. Hildesheim, New York: Olms, 1981.

———. 1929. *Werke*, vol. XII, *Varia. Atlas des Erdmagnetismus*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Berlin: Julius Springer. Repr. Hildesheim, New York: Olms, 1981.

Gauss & Bessel. 1880. *Briefwechsel zwischen Gauß und Bessel*, ed. A. Auwers. Leipzig: Engelmann. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 1. Hildesheim: G. Olms, 1975.

Goldstein, Catherine. 1989. Le métier des nombres aux XVII^{e} et XIX^{e} siècles. In *Éléments d'Histoire des Sciences*, ed. M. Serres, pp. 274–295. Paris: Bordas. Engl. transl. in *A History of scientific thought*, ed. M. Serres, pp. 160-190. Oxford, Cambridge (MA): Blackwell, 1995.

Hilbert, David. 1897. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4 ("1894–1895"), 177–546 + Vorwort 1–xviii. Repr. in *Gesammelte Abhandlungen*, vol. 1, pp. 63–363. Berlin: Springer, 1932. 2^{e} ed., 1970. Engl. transl. I. Adamson: *The Theory of Algebraic Number Fields*, introd. F. Lemmermeyer, N. Schappacher. New York: Springer, 1998.

Jacobi, Carl Gustav Jacob. 1881. *Gesammelte Werke*, vol. 1, ed. C.W. Borchardt. Berlin: Reimer.

Jahnke, Hans Niels. 1987. Motive und Probleme der Arithmetisierung der Mathematik in der ersten Hälfte des 19. Jahrhunderts. Cauchys Analysis in der Sicht des Mathematikers Martin Ohm. *Archive for History of Exact Sciences* 37, 101–182.

———. 1990. *Mathematik und Bildung in der Humboldtschen Reform*. Göttingen: Vandenhoeck & Ruprecht.

Jungnickel, Christa, McCormmach, Russell. 1986. *Intellectual Mastery of Nature. Theoretical physics from Ohm to Einstein*, vol. 1. Chicago: University of Chicago Press.

Kant, Immanuel. 1783. *Prolegomena zu einer jeden künftigen Metaphysik*. Riga: Hartknoch. Numerous reprs.

———. 1787. *Kritik der reinen Vernunft*. 2nd ed. (quoted as "B"). Riga, Hartknoch. Engl. transl. London, Macmillan, 1933.

Kepler, Johannes. 1858. *Opera omnia*, vol. I, ed. Ch. Frisch. Frankfurt, Erlangen: Heyder & Zimmer.

Klein, Felix. 1895. Über Arithmetisierung der Mathematik. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen, Geschäftliche Mitteilungen*, 82–91. Repr. in *Gesammelte mathematische Abhandlungen*, vol. 2, pp. 232–240. Berlin: Springer, 1922. Engl. transl. in *Bulletin of the AMS* 2, 241–249, repr. in [Ewald 1996], pp. 965–971.

———. 1926. *Vorlesungen über die Entwicklung der Mathematik im 19. Jahrhundert*, vol. 1. Berlin: Springer. Repr., 1979.

Kline, Morris. 1972. *Mathematical Thought from Ancient to Modern Times*. Oxford: Oxford University Press.

Kronecker, Leopold. 1887. Über den Zahlbegriff. *Journal für die reine und angewandte Mathematik* 101, 337–355. Repr. in *Werke*, ed. K. Hensel, vol. 3(1), pp. 249–274. Leipzig: Teubner, 1895–1930; reimp., vol. 3 (first part), New-York: Chelsea, 1968. Engl. transl. in [Ewald 1996], pp. 947–955.

Laugwitz, Detlef. 1996. *Bernhard Riemann, 1826-1866: Wendepunkte in der Auffassung der Mathematik*, Basel, Boston: Birkhäuser.

Leibniz, Gottfried Wilhelm. 1704. *Nouveaux essais sur l'entendement humain*. In *Oeuvres philosophiques latines et françoises de feu Mr de Leibnitz*, ed. R.E. Raspe. Amsterdam, Leipzig: Schreuder, 1765.

———. 1714. *Monadologie*. In *Die philosophischen Schriften*, vol. 6, ed. C.J. Gerhardt, pp. 607-23. Hildesheim: Olms, 1960.

Lewis, Albert C. 1977. Hermann Grassmann's 1844 *Ausdehnungslehre* and Schleiermacher's *Dialektik*. *Annals of Science* 34, 103–162.

McClelland, Charles E. 1980. *State, Society, and University in Germany, 1700–1914*. Cambridge: Cambridge University Press.

Minkowski, Hermann. 1905. Peter Gustav Lejeune-Dirichlet und seine Bedeutung für die heutige Mathematik. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 14, 149–163.

Novalis. 1799–1800. Fragmente und Studien. In *Werke, Tagebücher und Briefe Friedrich von Hardenbergs*, vol. 2, *Das philosophisch-theoretische Werk*, ed. H.-J. Mähl. München, Wien: Carl Hanser Verlag, 1978.

Ohm, Martin. 1822. *Versuch eines vollkommen consequenten Systems der Mathematik. Lehrbuch der Arithmetik, Algebra und Analysis*. 2 vols. Berlin: T.H. Riemann. Repr. with a 3$^{\text{rd}}$ vol., 1828–1829; 1853–1855.

Pasch, Moritz. 1882. *Vorlesungen über neuere Geometrie*. Berlin: Springer.

Paulsen, Friedrich. 1897. *Geschichte des gelehrten Unterrichts auf den deutschen Schulen und Universitäten*, vol. 2. Leipzig: Teubner.

Poincaré, Henri. 1900. Le rôle de l'intuition et la logique dans les mathématiques. *Compte rendu du deuxième Congrès international des mathematiciens*, p. 115–130. Paris, Gauthier-Villars 1902. Repr. with modifications in *La valeur de la science*, chap. 1. Paris: Flammarion 1905. English transl. in [Ewald 1996], 1012-1020.

———. 1902. *La science et l'hypothèse*. Paris: Flammarion.

Plutarch of Chaeronea. *Quaestiones Convivales.* In *Moralia IX*, Table-Talk, Books 7–9. Loeb Classical Library. Cambridge, MA: Harvard University Press, 1961.

Pyenson, Lewis. 1983. *Neohumanism and the Persistence of Pure Mathematics in Wilhelmian Germany*. Philadelphia: American Philosophical Society.

Scharlau, Winfried, Opolka, Hans. 1980. *Von Fermat bis Minkowski. Eine Vorlesung über Zahlentheorie und ihre Entwicklung*. Berlin, New York: Springer. Engl. transl. Berlin: Springer, 1985.

Scholz, Erhard. 1982. Herbart's influence on Bernhard Riemann. *Historia Mathematica* 9, 413–440.

———. 1992. Riemann's vision of a new approach to geometry. In *1830-1930: A Century of Geometry*, ed. L. Boi, D. Flament, J.-M. Salanskis, pp. 22–34. Berlin: Springer.

SCHRÖDER, Ernst. 1890. *Vorlesungen über die Algebra der Logik*, vol. 1. Leipzig: Teubner. Repr. New York: Chelsea, 1966.

WALTERSHAUSEN, Wolfgang SARTORIUS VON. 1856. *Gauss zum Gedächtniss*. Leipzig: S. Hirzel.

WEIERSTRASS, Karl Theodor Wilhelm. 1923. Briefe an Paul du Bois-Reymond. *Acta Mathematica* 39, 199–225.

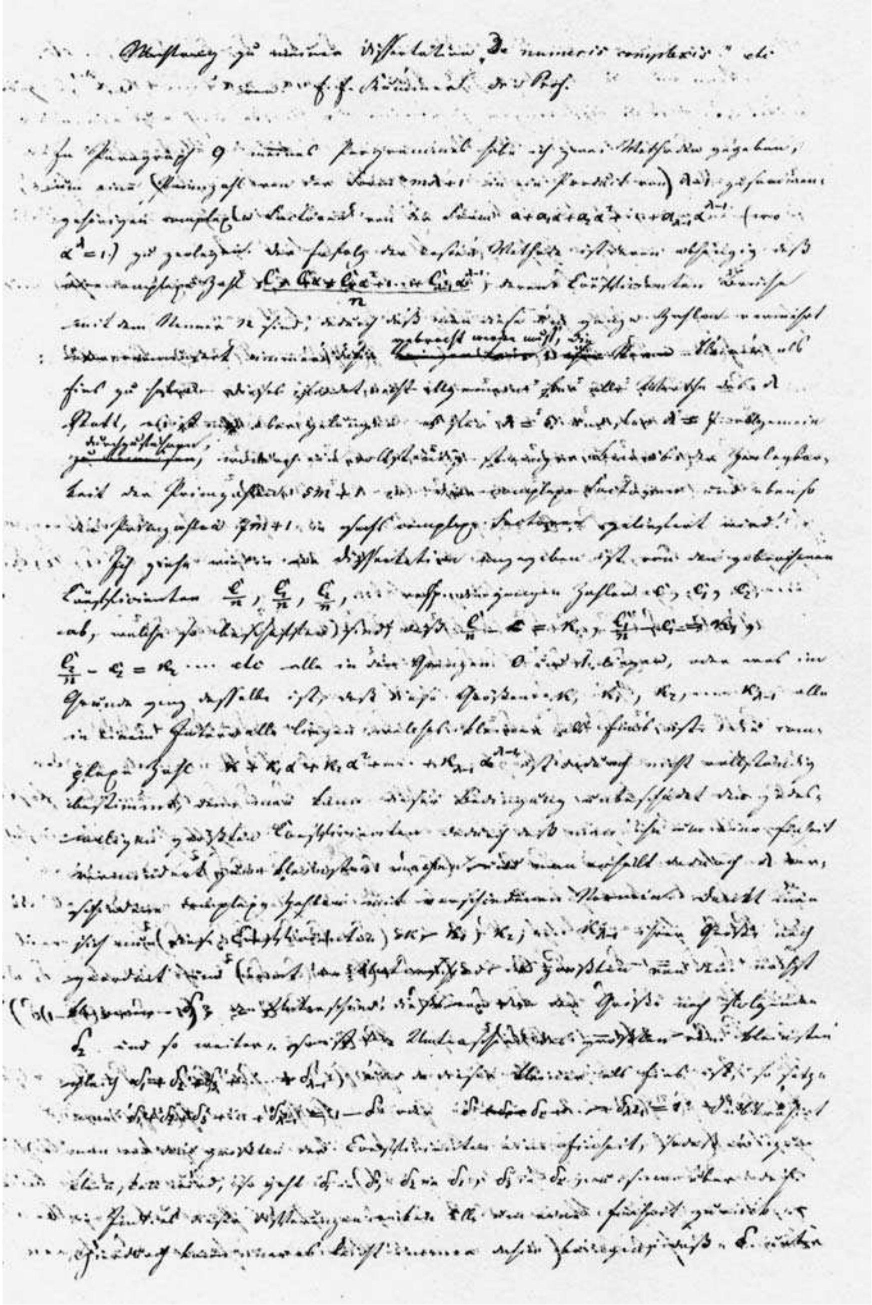
WUSSING, Hans. 1974. *Carl Friedrich Gauss*. Leipzig: Teubner. 4th ed., 1982.

ZÖLLNER, Johann Karl Friedrich. 1878. *Wissenschaftliche Abhandlungen*, vol. 2, part I. Leipzig: L. Staackmann.

Part IV

Complex Numbers and Complex Functions in Arithmetic

> *Die Einführung complexer ganzer Zahlen ... ist nach Jacobis Meinung ... nicht aus dem Gebiete der Arithmetik allein erwachsen, sondern uner Mitwirkung der Theorie der elliptischen Funktionen, namentlich der lemniskatischen, für die eine complexe Multiplikation mit Zahlen von der Form $a + b\sqrt{-1}$ und die entsprechende Division Statt hat, welche Gauss für sich schon über ein Vierteljahrhundert eher gekannt hat, als sie durch die Arbeiten von Abel und Jacobi ein Allgemeingut der Wissenschaft geworden ist.*
>
> Ernst Eduard Kummer
> Berlin Academy, February 18, 1858



Nachtrag zu meiner Dissertation „De numeris complexis" etc

Fig. IV.1A. The first page of Kummer's *Nachtrag zur Dissertation "De numeris"*
(Courtesy of Institute Mittag-Leffler)

IV.1

From Reciprocity Laws to Ideal Numbers: An (Un)Known Manuscript by E.E. Kummer

REINHARD BÖLLING

By inventing his "ideal complex numbers" in 1845, Ernst Eduard Kummer took the decisive step towards overcoming the problem that, in the rings of cyclotomic integers he was studying, unique factorization did not hold in general. This "giant step," as André Weil called it,[1] has marked the development of number theory like few other events. But Kummer had been convinced of the validity of unique factorization at least until April 1844.[2] The error was then recognized. Kummer's contribution to the volume compiled by Breslau University in honour of the tercentenary of Königsberg University was published that same year.[3] There he expressed his regret that this *propositio fundamentalis* does not continue to hold. This was also the reason why the main result of the manuscript dated April 20, 1844 which he had submitted to the Berlin Academy was wrong. It stated that all prime numbers p of the form $m\lambda + 1$ (where λ is an odd prime, and m a positive integer) is a norm of an integer of the field generated by the λ^{th} roots of unity, or in other words that

$$p = N\big(f(\alpha)\big) = f(\alpha)f(\alpha^2)\cdots f(\alpha^{\lambda-1}). \tag{*}$$

Here, α denotes a primitive λ^{th} root of 1, $f(\alpha)$ an integral linear combination of powers of α (whose exponents may be assumed to be $\leq \lambda - 2$), i.e., an element of the ring $\mathbf{Z}[\alpha]$ of integers in the field $\mathbf{Q}(\alpha)$ generated by the λ^{th} roots of unity, and N denotes the norm from $\mathbf{Q}(\alpha)$ to $\mathbf{Q}$. Kummer retracted his paper between June 17 and July 10, 1844.[4]

[1] [Kummer 1975], p. 5.

[2] [Bölling 1997].

[3] [Kummer 1844c].

[4] [Bölling 1997], p. 146.

What could be saved of his theorem after this failure? In the paper alluded to, [Kummer 1844c], Kummer mentions a few results which are of course more modest than the original claim. For every prime number λ such that $5 \leq \lambda \leq 23$, he has checked for all $p \leq 1000$ of the form $m\lambda + 1$ whether or not they are norms as above, i.e., decompose in $\mathbf{Z}[\alpha]$ into a product of $\lambda - 1$ conjugate factors. It turned out that this was true for all λ except for $\lambda = 23$. Among the eight primes of the form $p = 23m + 1 < 1000$ there are precisely five which are not norms in the above sense, the smallest one being $p = 47$. Kummer does not go beyond recording the numerical evidence. For none of the smaller primes $\lambda < 23$ does he prove the decomposition of primes $p \equiv 1 \pmod{\lambda}$ into $\lambda - 1$ factors in general.

It is here that a hitherto unknown manuscript of Kummer's comes into play which the author chanced upon during his archival studies on Weierstrass and Kovalevskaia at the Mittag-Leffler Institute at Djursholm, Sweden, in 1992. It shows that Kummer managed to find such proofs immediately after his paper in the Königsberg tercentenary volume.

1. … *einige Resultate meines Fleißes …*[5]

On October 2, 1844, Kummer wrote to Leopold Kronecker:

> And furthermore I have searched, and found, these days a veritably rigorous proof of the fact that every prime number $p = 5m + 1$ may be cast in the form $p = f(\alpha)f(\alpha^2)f(\alpha^3)f(\alpha^4)$. [6]

He mentions a few details of this proof; it contains the distinction of six cases according to the relative sizes of the coefficients of the elements in question. Then, he adds:

> The proof I found … is not elegant, yet it is a rigorous proof, and if I manage to continue in this way, I think already the proof for the case $\lambda = 7$ will retroactively improve the one for $\lambda = 5$. For in going further one will be obliged to hold onto the essentials, neglecting the more accidental circumstances.[7]

And this is exactly what happened next. Only two weeks later, on October 16, 1844, Kummer wrote to Kronecker:

> I have been working fairly hard towards the end of the holidays, and share with you a few results of my hard work since you are also working in the realm of complex numbers; you will find them in the addendum to my programme. After you have

[5] "… a few results of my hard work," see the quote below, [Kummer 1844a], pp. 61–62.

[6] [Kummer 1844a], p. 58: *Ferner habe ich in diesen Tagen einen wahrhaftigen strengen Beweis dafür gesucht und gefunden, daß jede Primzahl* $p = 5m + 1$ *in die Form* $p = f(\alpha)f(\alpha^2)f(\alpha^3)f(\alpha^4)$ *gesetzt werden kann.*

[7] [Kummer 1844a], pp. 60–61: *Elegant ist der gefundene Beweis … nicht, indessen es ist doch ein strenger Beweis, und wenn es mir gelingen sollte auf diesem Wege weiterzugehen, so glaube ich wird schon der Beweis für den Fall* $\lambda = 7$ *auf den für* $\lambda = 5$ *günstig zurückwirken, denn beim weitergehen wird man genöthigt sein das mehr Zufällige außer Acht zu lassen und das Wesentliche festzuhalten.*

> read it, may I ask you to hand it over to Jacobi, with my due regards, to whom this addendum as well as the programme itself is dedicated. You will see from it that the proof of the decomposability of the prime numbers $5m + 1$ into 4 complex factors could indeed be nicely simplified, and that the case $\lambda = 7$ can be dealt with according to entirely the same principles. … This type of proof cannot be stretched any further, but I do not doubt that it will be possible to find similar easy proofs also for $\lambda = 11, 13, 17, 19$. [8]

It turns out that the manuscript found in Djursholm is precisely the addendum mentioned in the preceding letter – in that sense it was a "known manuscript." From the letters quoted it follows that it has been written between October 2 and 16, 1844. The original is undated; we reproduce it in the appendix.

2. The Manuscript's Content

The goal of Kummer's addendum is to prove for $\lambda = 5$ and $\lambda = 7$ the theorem which he had wrongly announced for all odd primes λ in his paper of April 20, 1844. In order to achieve this, he shows that for every $\xi \in \mathbf{Q}(\alpha)$ there exists $\rho \in \mathbf{Z}[\alpha]$ such that $N(\xi - \rho) < 1$. In other words, he shows that $\mathbf{Z}[\alpha]$ is a Euclidean ring in the two cases considered. This is all he does in the manuscript.

Let us add that the sources we have do not contain any information about analogous proofs for the other four primes envisaged by Kummer. Using his invention of "ideal complex numbers," Kummer would very soon obtain the proof of the decomposition (*) in an altogether different way, via the class number – see below. At least at this point, the question whether the corresponding rings were Euclidean was then probably abandoned.

Kummer's proof is based on an application of the arithmetic-geometric mean inequality

$$N\big(f(\alpha)\big) \le \Big(\frac{2}{\lambda - 1}\sum_{i=1}^{\frac{\lambda-1}{2}} f(\alpha^i) f(\alpha^{\lambda-i})\Big)^{\frac{\lambda-1}{2}}.$$

[8] [Kummer 1844a], p. 61–62: *Ich bin zu Ende der Ferien noch ziemlich fleißig gewesen und theile Ihnen als meinem Mitarbeiter im Reiche der complexen Zahlen einige Resultate meines Fleißes mit, welche Sie in dem beiliegenden Nachtrage zu meinem Programme finden. Nachdem Sie denselben durchgelesen haben bitte ich Sie ihn mit den gehörigen Empfehlungen von mir, an Jacobi zu übergeben, welchem dieser Nachtrag ebenso wie das Programm selbst gewidmet ist. Sie werden aus demselben ersehen, daß der Beweis der Zerfällbarkeit in 4 compl[exe] Factoren der Primzahlen* $5m + 1$ *in der That noch schöner Vereinfachungen fähig war, und daß der Fall* $\lambda = 7$ *sich ganz nach denselben Principien abmachen läßt.… Weiter auszudehnen geht diese Art des Beweises nicht, ich zweifle aber nicht daran, daß auch für* $\lambda = 11, 13, 17, 19$ *sich ähnliche einfache Beweise werden finden lassen.*

To bound the right hand side, he uses[9]

$$2\sum_{i=1}^{\frac{\lambda-1}{2}} f(\alpha^i)f(\alpha^{\lambda-i}) = \sum_{0\le i<j\le\lambda-1} (k_i-k_j)^2 \qquad \Big(\text{where } f(\alpha)=\sum_{i=0}^{\lambda-1} k_i\alpha^i\Big).$$

To establish $N\big(f(\alpha)\big) < 1$ it therefore suffices to show

$$\sum_{0\le i<j\le\lambda-1} (k_i-k_j)^2 < \lambda - 1. \tag{**}$$

In order to get there, Kummer determines, for each $\sum_{i=0}^{\lambda-1} u_i\alpha^i$ (with $u_i \in \mathbf{Q}$), numbers $k_i \in \mathbf{Q}$ for $0 \le i \le \lambda-1$, such that:

(K1) $u_i - k_i \in \mathbf{Z}$ for all i.

(K2) For every pair (k_a, k_b) such that $k_a < k_b$, one has $|k_a - k_b| \le \delta$, where $\delta = 1 - \max_{i,j}(k_i - k_j)$.

This yields the proof of (**). In the case $\lambda = 5$, Kummer's estimates yield the bound 3.17 for the sum of squares in (**) – see footnote 53 below –, which secures (**) and finishes the proof in this case. For $\lambda = 7$, the sum (**) is considered as a function of δ, whose maxima in the intervals $\big[\frac{1}{r+1}, \frac{1}{r}\big]$, for $r = 1, \dots, 6$ are determined. It follows (p. 4 of the manuscript) that

$$\sum_{0\le i<j\le 6} (k_i-k_j)^2 \le 2\cdot\frac{63}{25} = 5.04$$

which proves the inequality (**).

3. Lenstra's Reconstruction

Hendrik W. Lenstra[10] has made an interesting attempt to reconstruct Kummer's proof for the case $\lambda = 5$ from the indications contained in the two letters to Kronecker mentioned above, basing himself in particular on the detailed description of his earlier proof of the case $\lambda = 5$ in the first letter. Just as in Kummer, the essential point is to bound the sum occurring in (**). In Lenstra's reconstruction, however, this is done differently; for every $\sum_{i=0}^{\lambda-1} u_i\alpha^i$ (with $u_i \in \mathbf{Q}$), Lenstra determines numbers $k_i \in \mathbf{Q}$ for $0 \le i \le \lambda-1$, such that:

[9] Note that here and throughout his later work Kummer (like Gauss in sec. 7 of the *Disquisitiones Arithmeticae*) does not assume that $k_{\lambda-1} = 0$. This sacrifices the uniquenesss of the representation in the interest of symmetry in the k_i, and leaves the possiblity of a later calibration of the coefficients.

[10] [Lenstra 1979], p. 13–14.

(L1) $u_i - k_i \in \mathbf{Z}$ for all i.

(L2) There are two different indices a, b such that $|k_a - k_b| \leq \frac{1}{\lambda}$.

(L3) For all other indices i one has $|k_i - m| \leq \frac{1}{2}$, where m is the arithmetic-geometric mean of k_a and k_b.

For the comparison with Kummer we note that (K2) entails $\delta \geq \frac{1}{\lambda}$, so that all k_i are contained in an interval of length $\leq \frac{\lambda-1}{\lambda}$. This implies condition (L2), and condition (L3) can then be met for the other k_i after possible changes by 1 or -1. However, this may have the effect of destroying Kummer's condition (K2).[11] Kummer's procedure thus differs at this point from Lenstra's reconstruction by limiting the distances between the k_i more severely. It turns out that in this way Kummer does produce sharper bounds.

For all $x \in \mathbf{R}$, one has[12]

$$\sum_{0 \leq i < j \leq \lambda-1} (k_i - k_j)^2 = \lambda \sum_{i=0}^{\lambda-1} (k_i - x)^2 - \Bigl(\sum_{i=0}^{\lambda-1} (k_i - x)\Bigr)^2 .$$

Putting $x = m$ yields the estimate

$$\sum_{0 \leq i < j \leq \lambda-1} (k_i - k_j)^2 \leq \lambda\Bigl(\frac{1}{(2\lambda)^2} + \frac{1}{(2\lambda)^2} + (\lambda - 2)\frac{1}{4}\Bigr).$$

If $\lambda = 5$, the right hand side gives 3.85 which still suffices to prove (**), but is already weaker than Kummer's bound. For $\lambda = 7$, Lenstra only obtains $8 + \frac{23}{28}$ which does not suffice to prove (**). But Lenstra wrote: "Nevertheless it is believable that Kummer did prove [the inequality (**)]"[13] – which is indeed the case, as we now know.

4. Decomposing Primes

In order to explain how Kummer obtained the decomposition of the primes $p \equiv 1 \pmod{\lambda}$ from the fact that certain rings of cyclotomic integers are Euclidean, let us first look at the situation from today's vantage point. We know that Euclidean rings are factorial, their irreducible and prime elements coincide, and these rings $\mathbf{Z}[\alpha]$ are even PIDs. Furthermore, we know how prime numbers $p \in \mathbf{Z}$, $p \neq \lambda$, split in $\mathbf{Z}[\alpha]$: if p modulo λ has order f, then p splits into $\frac{\lambda-1}{f}$ different prime ideals of degree f, all conjugates of one another. The $p \equiv 1 \pmod{\lambda}$ considered by

[11] Such is always the case when one has only strict inequalities $|k_a - k_b| < \delta$ in (K2) to start with. See footnote 48 below.

[12] For $x = 0$, this identity can be found already in a posthumous note of Gauss. He called the left hand side *Generalmensur*, which he obtained by summing the *Partialmensuren* $\frac{1}{2}\sum_{i=0}^{\lambda-1}(k_i - k_{i+j})^2$ for $1 \leq j \leq \lambda - 1$. The same quantities also occur in Kummer's manuscript where they are called P, Q, R. See [Gauss 1863b], p. 395.

[13] [Lenstra 1979], p. 14.

Kummer are therefore products of $\lambda - 1$ prime ideals. These ideals being principal and conjugates of each one of them, p is the norm of a cyclotomic integer.

But this is not how Kummer got there in 1844; in his manuscript he leaves it at a reference to [Kummer 1844c]. Let us reconstruct here what his argument seems to have been.

Kummer uses the following statement:

Claim 1. Let p be as above and let $\xi \in \mathbf{Z}$. Every non-unit common factor in $\mathbf{Z}[\alpha]$ of $(\xi - \alpha)$ and p has norm p.

Thus, once such a common factor has been found, Kummer has attained his goal: p will be the product of $\lambda - 1$ conjugate cyclotomic integers. Kummer gives a justification for claim 1 already in his defective manuscript of April 1844. In my opinion it makes tacit use of unique factorization in $\mathbf{Z}[\alpha]$ and is therefore not valid in general.[14] In [Kummer 1844c], however, Kummer argues as follows:

> Let $f(\alpha)$ be this common factor of the numbers p and $\xi - \alpha$. Then $f(\alpha^2)$ will be a common factor of the numbers p and $\xi - \alpha^2$, and so forth. Therefore all the conjugate complex numbers $f(\alpha)$, $f(\alpha^2)$, ..., $f(\alpha^{\lambda-1})$ will be factors of the number p. And they will all be distinct because $\xi - \alpha$, $\xi - \alpha^2$, etc. cannot have common factors except those of norm 1 or λ, namely $\alpha - \alpha^2$, $\alpha - \alpha^3$, etc. From this it will follow that any prime number $p = m\lambda + 1$ is a product of $\lambda - 1$ conjugate complex factors.[15]

This deduction would be legitimate if Kummer was using that $f(\alpha)$ is a prime element; but there is neither an allusion to nor a proof of this fact. All that Kummer has shown in a preceding paragraph is that elements of $\mathbf{Z}[\alpha]$ with prime norm have to be irreducible. But Kummer actually had all he needed at his disposal to show that they are also prime elements. The argument goes like this.

Claim 2. Notation being as above, every non-unit common factor $f(\alpha)$ of p and $(\xi - \alpha)$ is a prime element of $\mathbf{Z}[\alpha]$.

Proof. A proof can be given in the style of [Kummer 1844c]. Assume $f(\alpha)$ divides a product $\varphi(\alpha)\psi(\alpha)$ of two cyclotomic integers. Then $\alpha \equiv \xi \pmod{f(\alpha)}$ implies $0 \equiv \varphi(\alpha)\psi(\alpha) \equiv \varphi(\xi)\psi(\xi) \pmod{f(\alpha)}$. Hence $f(\alpha)$ divides the greatest common divisor of the rational integers p and $\varphi(\xi)\psi(\xi)$. Since $f(\alpha)$ is not a unit, p has to divide $\varphi(\xi)\psi(\xi)$, and therefore, say, $\varphi(\xi)$. It follows that $\varphi(\alpha) \equiv \varphi(\xi) \equiv 0 \pmod{f(\alpha)}$, i.e., $f(\alpha)$ divides $\varphi(\alpha)$.

Note that, from today's point of view, the hypotheses tell us that the residue ring modulo $f(\alpha)$ has p elements, and is therefore a field.

At any rate, even without the information that $f(\alpha)$ is prime, claim 1 can be derived within the framework of [Kummer 1844c] as follows.

[14] [Bölling 1997], pp. 148–149.

[15] [Kummer 1844c], p. 202: *Sit $f(\alpha)$ hic factor communis numerorum p et $\xi - \alpha$, $f(\alpha^2)$ erit factor communis numerorum p et $\xi - \alpha^2$, et ita porro; omnes igitur numeri complexi conjuncti $f(\alpha)$, $f(\alpha^2)$, ..., $f(\alpha^{\lambda-1})$, factores essent numeri p, omnesque inter se diversi, quia $\xi - \alpha$, $\xi - \alpha^2$, etc., non possunt factores communes habere nisi eos quorum norma sit 1 vel λ, scilicet $\alpha - \alpha^2$, $\alpha - \alpha^3$, etc. Inde sequeretur ut quilibet numerus primus* $p = m\lambda + 1$ *esset productum* $\lambda - 1$ *factorum complexorum conjunctorum.*

Proof. Since $f(\alpha)$ is a non-unit divisor of p, one has that $N\big(f(\alpha)\big) = p^n$ for some $n \geq 1$. Assume we had $n > 1$. Write $p = f(\alpha)F(\alpha)$ with a suitable $F(\alpha) \in \mathbf{Z}[\alpha]$. We obtain

$$f(\alpha^2)\cdots f(\alpha^{\lambda-1}) = f(\alpha)^{n-1}F(\alpha)^n,$$

and hence

$$f(\xi^2)\cdots f(\xi^{\lambda-1}) \equiv f(\xi)^{n-1}F(\xi)^n \pmod{p}.$$

Since $f(\xi) \equiv 0 \ \big(\mathrm{mod}\ f(\alpha)\big)$, the rational integer $f(\xi)$ is in fact divisible by p, so that at least one of the factors $f(\xi^r)$, for $2 \leq r \leq \lambda-1$ has to be divisible by p. Since $f(\xi^r) \equiv f(\alpha^r) \ \big(\mathrm{mod}\ f(\alpha)\big)$, we conclude that $f(\alpha^r) \equiv 0 \ \big(\mathrm{mod}\ f(\alpha)\big)$. In [Kummer 1844c], Kummer does indeed arrive at such a congruence, and immediately deduces from it the identity $f(\alpha^r) = f(\alpha)$ which he had shown to imply a contradiction in the preceding paragraph. Such a contradiction is just as readily deduced from the Kummer quotation above; for otherwise $f(\alpha)$ would be a common divisor of $\xi - \alpha$ and $\xi - \alpha^r$, hence also of $\alpha - \alpha^r$, which is absurd in view of $N(\alpha - \alpha^r) = \lambda$.

Note that, from today's point of view, claim 1 follows from the fact that the order of the residue ring modulo $f(\alpha)$ equals the (absolute value of) the norm of $f(\alpha)$.

We have seen why common divisors of p and $\xi - \alpha$ are relevant to what Kummer wanted to do. In order to find them, Kummer in [Kummer 1844c] employed the norm algorithm. If it works, i.e., if for every $\xi \in \mathbf{Q}(\alpha)$, there exists $\rho \in \mathbf{Z}[\alpha]$ such that $N(\xi - \rho) < 1$, then it produces such a common divisor. In Kummer's words:

> If indeed this norm is smaller than 1, which usually can always be achieved, then we have $N\big(\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha)\big) < 1$, and therefore $N\big(\varphi(\alpha) - f(\alpha)\psi(\alpha)\big) < N\big(f(\alpha)\big)$. Putting $\varphi(\alpha) - f(\alpha)\psi(\alpha) = R(\alpha)$, it is obvious that the greatest common divisor of the numbers $\varphi(\alpha)$ and $f(\alpha)$ is the same as that of $f(\alpha)$ and $R(\alpha)$. Hence the search for the common divisor reduces to finding the common divisor of the other two numbers whose norms are smaller. Thus by repeating this method, if that adverse case which we have recalled above never arises, we finally arrive at two numbers of which one divides the other and therefore this divisor is the common factor we were after. If its norm is 1, those numbers we started from are relatively prime.[16]

Kummer thus imitates the well-known Euclidean algorithm in his situation. He uses the expression "greatest common divisor" without comment. This is reasonable under the current hypothesis, but not in general. But applying this algorithm to our numbers p and $\xi - \alpha$ considered above, one still has to rule out the possibility that the g.c.d. found is a unit. On this Kummer writes:

[16] [Kummer 1844c], p. 204: *Si vero, quod fere semper evenire solet, talis norma unitate minor fit, habemus* $N\big(\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha)\big) < 1$, *ideoque* $N\big(\varphi(\alpha) - f(\alpha)\psi(\alpha)\big) < Nf(\alpha)$. *Posito* $\varphi(\alpha) - f(\alpha)\psi(\alpha) = R(\alpha)$, *patet factorem maximum communem numerorum* $\varphi(\alpha)$ *et* $f(\alpha)$ *eumdem esse numerorum* $f(\alpha)$ *et* $R(\alpha)$; *unde indagatio factoris communis eo reducta est, ut aliorum duorum numerorum, quorum normæ minores sunt, factor communis quærendus sit. Itaque, hac methodo repetita, nisi forte casus ille adversus evenit, quem supra commemoravimus, tandem ad duos numeros pervenimus, quorum alter factor alterius, ideoque hic ipse factor communis est quem quærimus; cujus norma si unitas est, numeri illi sunt inter se primi.*

> Furthermore, if complex numbers of smaller norm are found by the indicated method, it is plain that all their norms are divisible by p because there is no way in which we could get to norm 1; therefore the common factor will always be found to be a non-unit.[17]

Here is a way to see this: If a rational integer ξ behaves like a λ^{th} root of 1 modulo p, i.e., if we have

$$1+\xi+\xi^2+\cdots+\xi^{\lambda-1}\equiv 0 \pmod{p},$$

then one has, for every polynomial $h(x)$ with integral coefficients having α as root, $h(\xi)\equiv 0 \pmod{p}$. (Note that such ξ exist because λ divides $p-1$.) For each step in Kummer's algorithm, we therefore find:

$$R_{i-1}(\xi)\equiv R_i(\xi)\psi_i(\xi)+R_{i+1}(\xi) \pmod{p}.$$

Now, if the two numbers we start with, $\varphi(\alpha)$ and $f(\alpha)$, satisfy $\varphi(\xi)\equiv f(\xi)\equiv 0 \pmod{p}$ – as is the case for our pair p and $(\xi-\alpha)$ – then all $R_i(\xi)$ will be divisible by p, in particular the last one. Its norm will then also be divisible by p,[18] and the g.c.d. cannot be a unit.

This is Kummer's method to get from the norm algorithm to the decomposition of primes $p\equiv 1 \pmod{\lambda}$ into $\lambda-1$ factors.

5. Background

It is time to discuss why Kummer was interested in these decompositions in the first place. From the point of view of algebraic number theory, the following reasoning suggests itself: If every prime number $p\equiv 1 \pmod{\lambda}$ splits in $\mathbf{Z}[\alpha]$ into $\lambda-1$ factors, then every prime ideal of degree 1 in $\mathbf{Z}[\alpha]$ is principal. Since each ideal class contains a prime ideal of degree one, the class number will be 1, and the ring $\mathbf{Z}[\alpha]$ factorial. It is conceivable that Kummer, after realizing the error in his manuscript of April 1844, was looking for examples of rings $\mathbf{Z}[\alpha]$ which are factorial, so that the conclusions of that paper remained valid at least in these cases. However, there is no indication that Kummer was aware of this connection in October 1844 when he was writing the manuscript we are concerned with.

There is, however, another reason which prompted Kummer's investigations.[19] From an 1827 letter of Carl Gustav Jacob Jacobi to Gauss[20] we learn that Jacobi had deduced, as an arithmetic application of his results on cyclotomy, that every prime

[17] [Kummer 1844c], p. 204: *[P]orro si per methodum traditam numeri complexi normarum minorum quaeruntur, patet eorum omnium normas per p divisibiles esse, quam ob rem nullo modo ad normam unitatem pervenire possumus; semper igitur factor communis ab unitate diversus inveniretur.*

[18] See [Kummer 1844c], p. 200.

[19] For the history of Kummer's invention of ideal complex numbers, see [Neumann 1981]; cf. [Haubrich 1992].

[20] Jacobi to Gauss, February 8, 1827, see [Jacobi 1881–1891], vol. 7, pp. 393–400. Cf. [Jacobi 1837].

number $p \equiv 1 \pmod{\lambda}$ could be written, in $\lambda - 2$ different ways, as a product of two factors in $\mathbf{Z}[\alpha]$ like this:

$$p = \psi_k(\alpha)\psi_k(\alpha^{-1}), \qquad\qquad k = 1, \ldots, \lambda - 2.$$

This he interpreted as evidence for the fact that these factors in $\mathbf{Z}[\alpha]$ had to be themselves products of "true complex prime numbers" in such a way that the various decompositions resulted simply from regrouping those underlying factors.[21] No definition of the term "complex prime number" is given. Jacobi presumably thought that $\psi_k(\alpha)$ and $\psi_k(\alpha^{-1})$ are somehow still decomposable in $\mathbf{Z}[\alpha]$, and uses the expression in the sense of "truly indecomposable numbers" in $\mathbf{Z}[\alpha]$.

Kummer also mentions "true complex prime numbers" in his manuscript of April 1844 (see the Kummer quotation displayed below). Nor was Kummer the only one. Gauss himself, exploring further his theory of sec. 7 of the *Disquisitiones Arithmeticae*, had found such decompositions, but they were published only after Gauss's death by Dedekind.[22] Also Augustin-Louis Cauchy, independently of Gauss and Jacobi, published such decompositions for the first time in 1829, pointing out that Jacobi had obtained "results of the same kind."[23] Cauchy continued to publish abundantly on this matter.[24]

As for Jacobi, he started to look for these hypothetical prime numbers and declared in 1839 that in the case $\lambda = 5$ he had succeeded in splitting each his two factors again in two so that every prime number of the form $5m + 1$ could be split into four factors.[25] Jacobi did not explain how he had proved these facts.

Kummer, in his manuscript of April 1844 which he would eventually retract, refers explicitly to Jacobi's results and writes

> This is the basis of my further investigations by which I have found the true complex prime numbers.[26]

Thus Kummer takes Jacobi's search for the true complex primes further. But this search was not a goal in itself: The arithmetic of the third and fourth roots of unity had yielded simple proofs of the reciprocity laws for the corresponding power residues. It is therefore natural to assume that, from the very start, Kummer had in mind the application of cyclotomic arithmetic to finding and proving higher

[21] [Jacobi 1839], p. 317.

[22] See [Gauss 1863a].

[23] [Cauchy 1829], p. 107, where he mentions Jacobi's "résultats du même genre."

[24] [Cauchy 1840].

[25] At that time he had already found analogous results for primes of the form $8m + 1$ and $12m + 1$. These cases have in common that the fields of 5th, 8th, and 12th roots of unity each have degree 4 over the rationals. H. Pieper has pointed out that there is a manuscript of Jacobi's in the Archives of the Berlin-Brandenburg Academy of Sciences entitled "Zerlegung der Primzahlen von der Form $8n + 1$ in 4 complexe Faktoren" – see [Neumann 1981], p. 191. [Editors' note: see also chap. I.1, § 4 above.]

[26] [Kummer 1844b], p. 389: *Hierauf nun gründen sich meine weiteren Untersuchungen, durch welche ich die wahren complexen Primzahlen … ermittelt habe.*

reciprocity laws.[27] If the modern reader may be surprised by a manuscript which covers just two special cases: the case of the 5th roots of 1 already treated by Jacobi, and the 7th roots of 1, it should be remembered that, at the beginning of the 1840s, every value of $\lambda > 3$ stood above all for a new, hitherto undiscovered or unproven reciprocity law.

6. Further Development

Soon after his first two communications about his newly invented "ideal complex numbers,"[28] Kummer published a few numerical examples in his paper dated September 1846.[29] For each prime number λ below 50 he exhibits a positive integer n such that the n^{th} power of every "ideal complex number" of $\mathbf{Z}[\alpha]$ is an "actual complex number," i.e., the n^{th} power of every ideal is principal. The exponent of the ideal class number then has to divide n. For all $\lambda \leq 19$, Kummer finds $n = 1$,[30] so the corresponding rings $\mathbf{Z}[\alpha]$ are principal and factorial. In this way, Kummer could deduce the decomposability of all $p \equiv 1 \pmod{\lambda}$ into $\lambda - 1$ factors in $\mathbf{Z}[\alpha]$. The method of the manuscript published here would probably have been difficult to extend to these cases, as is shown by the further development.

Since Kummer's manuscript remained unpublished, it is not surprising that proofs of its results were published by other authors which we will now mention briefly. In 1847, Cauchy could prove a few rings $\mathbf{Z}[\alpha]$ to be norm-Euclidean, among them the special cases $\lambda = 5$ and $\lambda = 7$. But his presentation is quite short and partly incomprehensible, partly wrong, so that the overall correctness of his proof is difficult to judge. It is thought to be probably incorrect; but at least for the case $\lambda = 5$, one can extract a correct proof from his paper.[31] Cauchy's immediate motivation for studying cyclotomic integers was related to his efforts to prove Fermat's Last Theorem. The factoriality of the rings $\mathbf{Z}[\alpha]$ seems to have been an essential point for him in this context; there is no evidence that he was aware of such rings which are not factorial, before he learned about Kummer's result for $\lambda = 23$.[32] But let us add that Cauchy had first embarked on cyclotomic studies much earlier, trying to generalize the quadratic reciprocity law to higher power residues.[33]

After the posthumous publication of Gauss's above-mentioned, undated notes on Fermat's Last Theorem, Uspenskij published a proof in 1906 that $\mathbf{Z}[\alpha]$ is norm-

[27] Cf. [Edwards 1977] and [Neumann 1981].

[28] The letter to Kronecker dated October 18, 1845, [Kummer 1844a], pp. 64–68, contains his definition of "ideal prime factors" of cyclotomic integers together with their basic properties, and his communication to the Berlin Academy dated March 26, 1846: [Kummer 1846], contains for the first time the term *ideale complexe Zahl*.

[29] [Kummer 1847a].

[30] [Kummer 1847a], p. 367.

[31] [Cauchy 1847]. Cf. [Lenstra 1979], p. 10.

[32] And he learnt of it late, through the reprint in Liouville's *Journal*: see Liouville's remark to a letter of Kummer's dated April 28, 1847, in [Kummer 1847b].

[33] See [Cauchy 1829] and [Cauchy 1840].

Euclidean for $\lambda = 5$, probably without knowing Cauchy's work.[34] Ernst Schering had already indicated in his commentary on Gauss's notes how one could settle this case in analogy with the case $\lambda = 3$ which Gauss had treated in greater detail.[35] One may view Uspenskij's proof as an elaboration of Schering's indications. At any rate, Schering undoubtedly had a proof.

Charles Hermite proved for $\lambda = 5$, resp. $\lambda = 7$, that prime numbers $p \equiv 1 \pmod{\lambda}$ are products of four, resp. six, conjugate cyclotomic factors, but by a method entirely different from Kummer's. This can be seen from a letter of Hermite to Jacobi from the summer of 1847 which also contains a hint of how to proceed for $\lambda = 11$.[36] Hermite's investigation had been triggered by Jacobi's 1835 paper on fourfold periodic functions of two complex variables.[37] Jacobi showed that the periods of a complex function which admits at least 3 $\mathbf{Z}$-linearly independent periods which span $\mathbf{C}$ over $\mathbf{R}$ are dense in $\mathbf{C}$ – a conclusion he found absurd. Hermite, however, related the questions of approximation of complex numbers arising in this context to the reduction of quadratic forms in several variables with real coefficients. He then deduced the above-mentioned results from his theorems on the minima of such forms (for integer values of the variables).

More than one century after Kummer's result about the prime numbers $\lambda \leq 19$, Uchida proved in 1971 that class number one cannot occur for any other value of λ.[38] Before, it had been known that the class number of $\mathbf{Z}[\alpha]$ tends to infinity with λ. In 1976, Masley and Montgomery gave a complete list of all rings of m^{th} roots of 1 of class number one, thus in particular reproving Uchida's result.[39]

Regarding Kummer's 1844 manuscript, the question arises for which $\lambda \geq 11$ the ring $\mathbf{Z}[\alpha]$ is norm-Euclidean. In 1975, Lenstra published a paper proving this fact for all primes $\lambda \leq 11$, counting Kummer's case $\lambda = 7$ among the "apparently new" ones.[40] (Who could have guessed at the time that Kummer had not spoken his last word yet?) Later McKenzie in his thesis checked with the help of a computer that $\mathbf{Z}[\alpha]$ for $\lambda = 13$ is also norm-Euclidean.[41] The cases $\lambda = 17, 19$ do not seem to have been settled to date.

[34] [Uspenskij 1906].

[35] [Gauss 1863b]. Here, Gauss's *(der) Determinant* coincides with our norm.

[36] [Hermite 1850], pp. 268, 277. [Editors' note: on this development, see C. Goldstein and N. Schappacher's chap. I.1, § 4 and C. Goldstein's chap. VI.1.]

[37] [Jacobi 1835].

[38] [Uchida 1971]. In [Masley, Montgomery 1976], this is referred to as a conjecture of Kummer's; I am not aware of any documental evidence for this attribution.

[39] [Masley, Montgomery 1976].

[40] [Lenstra 1975]. The result for $\lambda \leq 11$ follows from Lenstra's inequality quoted in footnote 51 below.

[41] [McKenzie 1988], cf. [McKenzie 1995]. We heartily thank F. Lemmermeyer for these references.

7. Appendix: Kummer's Manuscript

We now give the faithful transcription of the undated manuscript written by Kummer between October 2 and 16, 1844, conserved at the Institute Mittag-Leffler, Djursholm, Sweden.[42]

Nachtrag zu meiner Dissertation "De numeris"[43] etc von E. E. Kummer Dr. u[nd] Prof.

In Paragraph 9 meines Programmes[44] habe ich zwei Methoden gegeben, um eine Primzahl von der Form $m\lambda + 1$ in ein Product von $\lambda - 1$ zusammengehörigen complexen Factoren von der Form $a + a_1\alpha + a_2\alpha^2 + \cdots + a_{\lambda-1}\alpha^{\lambda-1}$ (wo $\alpha^\lambda = 1$) zu zerlegen. Der Erfolg der ersten Methode ist davon abhängig daß eine complexe Zahl $\frac{C+C_1\alpha+C_2\alpha^2+\cdots+C_{\lambda-1}\alpha^{\lambda-1}}{n}$, deren Coefficienten Brüche mit dem Nenner n sind, dadurch daß man diese um ganze Zahlen vermehrt oder vermindert immer dahin gebracht werden muß, die Norm kleiner als Eins zu haben.[45] Dieses findet nicht allgemein für alle Werthe der λ Statt, es ist mir aber gelungen es für $\lambda = 5$ und für $\lambda = 7$ allgemein durchzuführen, wodurch ein vollständig strenger Beweis der Zerlegbarkeit der Primzahlen $5m + 1$ in vier complexe Factoren und ebenso der Primzahlen $7m + 1$ in sechs complexe Factoren geliefert wird.

Ich ziehe wie in der Dissertation angegeben ist[46] von den gebrochenen Coefficienten $\frac{C}{n}, \frac{C_1}{n}, \frac{C_2}{n}, \ldots$ resp. die ganzen Zahlen $c, c_1, c_2, \ldots$ ab, welche so beschaffen sind, daß $\frac{C}{n} - c = k$, $\frac{C_1}{n} - c_1 = k_1$, $\frac{C_2}{n} - c_2 = k_2, \ldots$ etc alle in den Grenzen 0 und 1 liegen, oder was im Grunde ganz dasselbe ist, daß diese Größen $k, k_1, k_2, \ldots, k_{\lambda-1}$ alle in einem Intervalle liegen welches kleiner als Eins ist.[47] Die complexe Zahl $k + k_1\alpha + k_2\alpha^2 + \cdots + k_{\lambda-1}\alpha^{\lambda-1}$ ist dadurch nicht vollständig bestimmt, denn man kann dieser Bedingung unbeschadet den jedesmaligen größten Coefficienten dadurch daß man ihn um eine Einheit vermindert zum kleinsten machen, und man erhält dadurch λ verschiedene complexe Zahlen mit verschiedenen Normen. Denkt man sich nun diese Coefficienten $k, k_1, k_2, \ldots, k_{\lambda-1}$ ihrer Größe nach geordnet und nennt den Unterschied des größten von dem nächst kleineren δ_1, den Unterschied von dem der Größe nach folgenden δ_2 und so weiter, so ist der Unterschied des größten

[42] The only changes applied to the text in this transcription are a few tacit and unproblematic corrections of punctuation. The text is reproduced with kind permission of the Institute Mittag-Leffler.

[43] [Kummer 1844c], a paper which he alludes to as his "dissertation" both in [Kummer 1844a], p. 58, and in [Kummer 1847b]. The word should be taken literally; dissertation meaning argument, investigation.

[44] [Kummer 1844c]. In [Kummer 1846], p. 323, Kummer calls this his *Breslauer Programm.*

[45] Every quotient $\frac{\varphi(\alpha)}{f(\alpha)} \in \mathbf{Q}(\alpha)$ can be written in the form given by Kummer, with $n = N\big(f(\alpha)\big) = f(\alpha)f(\alpha^2)\cdots f(\alpha^{\lambda-1})$. We are looking for a complex number $\psi(\alpha)$ such that $N\big(\frac{\varphi(\alpha)}{f(\alpha)} - \psi(\alpha)\big) < 1$ – see [Kummer 1844c], p. 203.

[46] [Kummer 1884c], pp. 203-204.

[47] Since $1 + \alpha + \cdots + \alpha^{\lambda-1} = 0$, the complex number does not change if any constant is added to all the $k, k_1, k_2, \ldots$ at once.

vom kleinsten gleich $\delta_1 + \delta_2 + \delta_3 + \cdots + \delta_{\lambda-1}$, und da dieser kleiner als Eins ist, so setze man $\delta_1 + \delta_2 + \delta_3 + \cdots + \delta_{\lambda-1} = 1 - \delta$ oder $\delta + \delta_1 + \delta_2 + \delta_3 + \cdots + \delta_{\lambda-1} = 1$. Subtrahirt man von dem größten der Coefficienten eine Einheit, sodaß er zum kleinsten wird, so geht δ_1 in δ, δ_2 in δ_1, δ_3 in δ_2, u.s.w. über d.h. die Indices dieser Differenzen rücken alle um eine Einheit zurück. Hierdurch kann man es leicht im-
1|2 mer dahin bringen, daß δ unter | allen diesen Differenzen die größte wird, $\delta > \delta_1$, $\delta > \delta_2, \delta > \delta_3, \ldots$ etc.[48]

Wenn nun die complexe Zahl $f(\alpha) = k + k_1\alpha + k_2\alpha^2 + \cdots + k_{\lambda-1}\alpha^{\lambda-1}$ so zubereitet ist, daß die Differenzen je zweier der Größe nach auf einander folgenden Coefficienten alle kleiner sind als der Unterschied der Summe aller (oder des Unterschiedes des größten vom kleinsten) von Eins, so werden wir jetzt für die beiden Fälle $\lambda = 5$ und $\lambda = 7$ zeigen, daß die Norm dieser complexen Zahl $f(\alpha)$ kleiner als Eins ist.

Sei also $\lambda = 5$, $f(\alpha) = k + k_1\alpha + k_2\alpha^2 + k_3\alpha^3 + k_4\alpha^4$. Wird nun $f(\alpha)$ mit ihrer reciproken[49] Zahl $f(\alpha^{-1})$ multiplicirt, so erhält man

$$f(\alpha)f(\alpha^4) = -P(\alpha + \alpha^4) - Q(\alpha^2 + \alpha^3)$$

ebenso

$$f(\alpha^2)f(\alpha^3) = -P(\alpha^2 + \alpha^3) - Q(\alpha + \alpha^4)\ ^{50};$$

wo

$$\begin{aligned} P &= k^2 + k_1^2 + k_2^2 + k_3^2 + k_4^2 - kk_1 - k_1k_2 - k_2k_3 - k_3k_4 - k_4k \\ Q &= k^2 + k_1^2 + k_2^2 + k_3^2 + k_4^2 - kk_2 - k_1k_3 - k_2k_4 - k_3k - k_4k_1 \end{aligned}$$

oder

$$\begin{aligned} 2P &= (k - k_1)^2 + (k_1 - k_2)^2 + (k_2 - k_3)^2 + (k_3 - k_4)^2 + (k_4 - k)^2 \\ 2Q &= (k - k_2)^2 + (k_1 - k_3)^2 + (k_2 - k_4)^2 + (k_3 - k)^2 + (k_4 - k_1)^2. \end{aligned}$$

Es wird hieraus $2P + 2Q$ gleich der Summe der Quadrate der Differenzen je zweier Coefficienten k, k_1, k_2, k_4, k_4, also wenn $\delta, \delta_1, \delta_2, \delta_3, \delta_4$ die oben angegebenen Bedeutungen haben

$$\begin{aligned} 2P + 2Q &= \delta_1^2 + \delta_2^2 + \delta_3^2 + \delta_4^2 + (\delta_1 + \delta_2)^2 + (\delta_2 + \delta_3)^2 + (\delta_3 + \delta_4)^2 + \\ &\quad (\delta_1 + \delta_2 + \delta_3)^2 + (\delta_2 + \delta_3 + \delta_4)^2 + (\delta_1 + \delta_2 + \delta_3 + \delta_4)^2 \end{aligned}$$

[48] Kummer fails to consider the case where there is more than one biggest coefficient. In general, only $\delta \geq \delta_1$, $\delta \geq \delta_2$, $\delta \geq \delta_3, \ldots$ can be achieved. At any rate, the coefficients $k, k_1, k_2, \ldots, k_{\lambda-1}$ lie in an interval of length strictly smaller than 1, which is all that is really used in the argument. Note that Kummer uses exclusively the signs $<$ and $>$ in this manuscript, never $\leq$ or $\geq$. The same is true for his discussion of the case $\lambda = 5$ in the above quoted letter of October 10, 1844 to Kronecker. However, it is not possible to read Kummer's $<$ or $>$ as meaning $\leq$ resp. $\geq$ throughout.

[49] That is, complex conjugate.

[50] In the original, one reads $-P(\alpha^2 + \alpha^4)$.

und wenn die Quadrate entwickelt werden

$$P+Q = 2\delta_1^2 + 3\delta_2^2 + 3\delta_3^2 + 2\delta_4^2 + 3\delta_1\delta_2 + 2\delta_1\delta_3 + \delta_1\delta_4 + 4\delta_2\delta_3 + 2\delta_2\delta_4 + 3\delta_3\delta_4.$$

Der Nerv des Beweises liegt nun darin, daß $P+Q$ niemals größer als 2 werden kann, wenn die Differenzen δ_1, δ_2, δ_3, δ_4 den oben festgestellten Bedingungen unterworfen sind.[51] Dieß geht hier sehr einfach daraus hervor daß $P+Q < (\sqrt{2}\delta_1 + \sqrt{3}\delta_2 + \sqrt{3}\delta_3 + \sqrt{2}\delta_4)^2$, denn dieses Quadrat entwickelt hat alle einzelnen Glieder gleich oder größer als die des $P+Q$[;] hieraus folgt $P+Q < 2\big(\delta_1 + \sqrt{\tfrac{3}{2}}\delta_2 + \sqrt{\tfrac{3}{2}}\delta_3 + \delta_4\big)^2$ und weil $\delta_1+\delta_2+\delta_3+\delta_4 = 1-\delta$, $P+Q < 2\Big(1-\delta+2\big(\sqrt{\tfrac{3}{2}}-1\big)(\delta_2+\delta_3)\Big)^2$. Es sind aber δ_2 u[nd] δ_3 beide kleiner als δ also $\delta_2+\delta_3 < 2\delta$,[52] daher $P+Q < 2\big(1-\delta+2(\sqrt{\tfrac{3}{2}}-1)\delta\big)^2$ also $P+Q < 2\big(1-(3-\sqrt{6})\delta\big)^2$ also $P+Q < 2$.[53] Nun ist nach den obigen Gleichungen $f(\alpha)f(\alpha^4) + f(\alpha^2)f(\alpha^3) = P+Q$, also $f(\alpha)f(\alpha^4) + f(\alpha^2)f(\alpha^3) < 2$. Die Größen $f(\alpha)f(\alpha^4)$ und $f(\alpha^2)f(\alpha^3)$ sind positiv, (weil ein imaginärer Ausdruck mit seinem reciproken multiplicirt die Summe zweier Quadrate giebt) und da die Summe dieser beiden positiven Größen kleiner als 2 ist, so muß das Product derselben kleiner als Eins sein (denn wenn die Summe 2|3 mehrerer Factoren | gegeben ist, so haben sie das größte Product wenn sie alle gleich sind). Dieses Product ist aber die Norm von $f(\alpha)$, es ist also $Nf(\alpha) < 1$ was zu beweisen war.

Dieselbe Methode mit einigen Modificationen wird nun mit gleichem Erfolge auf den Fall $\lambda = 7$ angewendet. Es sei also

$$f(\alpha) = k + k_1\alpha + k_2\alpha^2 + k_3\alpha^3 + k_4\alpha^4 + k_5\alpha^5 + k_6\alpha^6 \qquad (\alpha^7 = 1).$$

Hier wird

$$\begin{aligned}
f(\alpha)f(\alpha^6) &= -P(\alpha+\alpha^6) - Q(\alpha^2+\alpha^5) - R(\alpha^3+\alpha^4)\\
f(\alpha^2)f(\alpha^5) &= -P(\alpha^2+\alpha^5) - Q(\alpha^4+\alpha^3) - R(\alpha+\alpha^6)\\
f(\alpha^3)f(\alpha^4) &= -P(\alpha^3+\alpha^4) - Q(\alpha+\alpha^6) - R(\alpha^2+\alpha^5)
\end{aligned}$$

wo

$$\begin{aligned}
2P &= (k-k_1)^2 + (k_1-k_2)^2 + (k_2-k_3)^2 + (k_3-k_4)^2 + (k_4-k_5)^2 +\\
&\quad (k_5-k_6)^2 + (k_6-k)^2\\
2Q &= (k-k_2)^2 + (k_1-k_3)^2 + (k_2-k_4)^2 + (k_3-k_5)^2 + (k_4-k_6)^2 +\\
&\quad (k_5-k)^2 + (k_6-k_1)^2\\
2R &= (k-k_3)^2 + (k_1-k_4)^2 + (k_2-k_5)^2 + (k_3-k_6)^2 + (k_4-k)^2 +\\
&\quad (k_5-k_1)^2 + (k_6-k_2)^2.
\end{aligned}$$

[51] This estimate is not optimal. Lenstra was able to show that, for every element $\sum_{i=0}^{\lambda-1} a_i\alpha^i \in \mathbf{Q}(\alpha)$, there exists $\sum_{i=0}^{\lambda-1} k_i\alpha^i \in \mathbf{Q}(\alpha)$ such that $a_i - k_i \in \mathbf{Z}$ for all i and such that $\sum_{0\le i<j\le\lambda-1}(k_i-k_j)^2 \le \frac{\lambda^2-1}{12}$. For arbitrary odd primes λ, this bound is best possible, and the last inequality may not be strict – see [Lenstra 1975]. The best possible bound for $P+Q$ is therefore 1.

[52] In the four preceding inequalities, "$<$" has to be replaced by "$\le$".

[53] Taking into account $\delta \ge 0.2$, it follows (writing $k_0 = k$) that $\sum_{0\le i<j\le 4}(k_i-k_j)^2 = 2P+2Q < 4\big(1-(3-\sqrt{6})\frac{1}{5}\big)^2 < 3.17$.

Es ist also $2P + 2Q + 2R$ gleich der Summe der Quadrate der Differenzen je zweier Coefficienten der complexen Zahl $f(\alpha)$ also durch $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6$ ausgedrückt

$$\begin{aligned} 2P + 2Q + 2R \quad = \quad & \delta_1^2 + \delta_2^2 + \delta_3^2 + \delta_4^2 + \delta_5^2 + \delta_6^2 + (\delta_1 + \delta_2)^2 + \\ & (\delta_2 + \delta_3)^2 + (\delta_3 + \delta_4)^2 + (\delta_4 + \delta_5)^2 + (\delta_5 + \delta_6)^2 + \\ & (\delta_1 + \delta_2 + \delta_3)^2 + (\delta_2 + \delta_3 + \delta_4)^2 + (\delta_3 + \delta_4 + \delta_5)^2 + \\ & (\delta_4 + \delta_5 + \delta_6)^2 + (\delta_1 + \delta_2 + \delta_3 + \delta_4)^2 + \\ & (\delta_2 + \delta_3 + \delta_4 + \delta_5)^2 + (\delta_3 + \delta_4 + \delta_5 + \delta_6)^2 + \\ & (\delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5)^2 + (\delta_2 + \delta_3 + \delta_4 + \delta_5 + \delta_6)^2 + \\ & (\delta_1 + \delta_2 + \delta_3 + \delta_4 + \delta_5 + \delta_6)^2 \end{aligned}$$

und wenn die Quadrate entwickelt werden:

$$\begin{aligned} 2P + 2Q + 2R \quad = \quad & 3\delta_1^2 + 5\delta_2^2 + 6\delta_3^2 + 6\delta_4^2 + 5\delta_5^2 + 3\delta_6^2 + 5\delta_1\delta_2 + 4\delta_1\delta_3 + \\ & 3\delta_1\delta_4 + 2\delta_1\delta_5 + \delta_1\delta_6 + 8\delta_2\delta_3 + 6\delta_2\delta_4 + 4\delta_2\delta_5 + 2\delta_2\delta_6 + \\ & 9\delta_3\delta_4 + 6\delta_3\delta_5 + 3\delta_3\delta_6 + 8\delta_4\delta_5 + 4\delta_4\delta_6 + 5\delta_5\delta_6. \end{aligned}$$

Es ist nun hier zu beweisen, daß $P + Q + R$ unter den beschränkenden Bedingungen welchen die Differenzen $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6$ unterworfen sind stets kleiner als Drei ist.[54] Dieß läßt sich nicht ganz so einfach zeigen wie oben das entsprechende Resultat für den Fall $\lambda = 5$. Ich führe hier den Beweis dadurch, daß ich den größten Werth ermittele welchen $P + Q + R$ haben kann indem die Variabeln $\delta_1, \delta_2, \delta_3, \delta_4, \delta_5, \delta_6$ in ihren gehörigen Grenzen als Veränderliche angesehen werden. Hierzu wird eine besondere Betrachtung von 6 verschiedenen Fällen erforderlich, jenachdem δ in einer der Grenzen $\frac{1}{7}$ und $\frac{1}{6}$, $\frac{1}{6}$ und $\frac{1}{5}$, $\frac{1}{5}$ und $\frac{1}{4}$, $\frac{1}{4}$ und $\frac{1}{3}$, $\frac{1}{3}$ und $\frac{1}{2}$, $\frac{1}{2}$ und 1 liegt.[55] Wird der Kürze wegen $P + Q + R$ einfach durch Ψ bezeichnet, so ist:

1., Wenn δ in den Grenzen $\frac{1}{7}$ und $\frac{1}{6}$ liegt, so erhält man den größten Werth des Ψ für $\delta_1 = 1 - 6\delta$, $\delta_2 = \delta$, $\delta_3 = \delta$, $\delta_4 = \delta$, $\delta_5 = \delta$, $\delta_6 = \delta$, nämlich $\Psi = 3 - 21\delta + 98\delta^2$; der größte Werth in diesem Intervalle findet also für $\delta = \frac{1}{6}$ statt, für welchen $\Psi = \frac{20}{9}$ wird.[56]

3|4 |

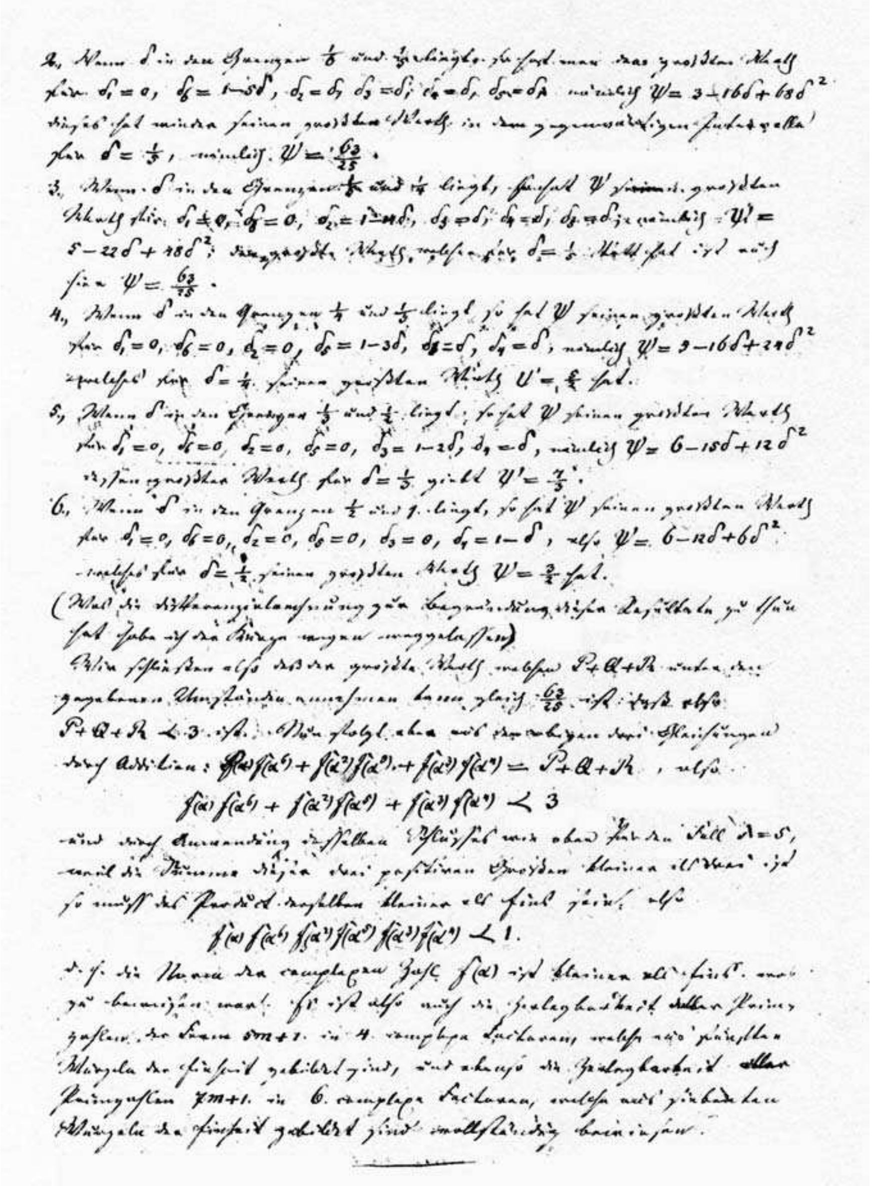
2., Wenn δ in den Grenzen $\frac{1}{6}$ und $\frac{1}{5}$ liegt, so hat man den größten Werth für $\delta_1 = 0$, $\delta_6 = 1 - 5\delta$, $\delta_2 = \delta$, $\delta_3 = \delta$, $\delta_4 = \delta$, $\delta_5 = \delta$, nämlich $\Psi = 3 - 16\delta + 68\delta^2$ [;] dieses hat wieder seinen größten Werth in dem gegenwärtigen Intervalle für $\delta = \frac{1}{5}$, nämlich $\Psi = \frac{63}{25}$.

3., Wenn δ in den Grenzen $\frac{1}{5}$ und $\frac{1}{4}$ liegt, so hat Ψ seinen größten Werth für $\delta_1 = 0$, $\delta_6 = 0$, $\delta_2 = 1 - 4\delta$, $\delta_3 = \delta$, $\delta_4 = \delta$, $\delta_5 = \delta$, nämlich $\Psi = 5 - 22\delta + 48\delta^2$; der größte Werth, welcher für $\delta = \frac{1}{5}$ Statt hat ist auch hier $\Psi = \frac{63}{25}$.

[54] The best possible estimate for $P + Q + R$ is 2 – see footnote 51 above.

[55] This exhausts all possible cases because $1 = \delta + \sum_{i=1}^{6} \delta_i \le 7\delta$.

[56] This may be surprising in view of footnote 54 above. However, Kummer's $\sum_{i=0}^{6} k_i\alpha^i$may still be modified by cyclotomic integers. So, even though it is true that the maximum value of Ψ in the interval in question is produced by an element whose coefficients k_i, in increasing order, are (without loss of generality – see footnote 47): 0, $\frac{1}{6}$, $\frac{2}{6}$, $\frac{3}{6}$, $\frac{4}{6}$, $\frac{5}{6}$, $\frac{5}{6}$, adding 1 to the two smallest coefficients yields $\Psi = \frac{31}{18}$, with the same δ. Analogous remarks apply to the following cases; except for the last one, Kummer's maximum value of Ψ is always > 2.



2, Wenn δ in den Grenzen $\frac{1}{6}$ und $\frac{1}{5}$ liegt, so hat man den größten Werth für $\delta_1 = 0$, $\delta_6 = 1-5\delta$, $\delta_2 = \delta$, $\delta_3 = \delta$, $\delta_4 = \delta$, $\delta_5 = \delta$, nämlich $\Psi = 3 - 16\delta + 68\delta^2$ dieses hat wieder seinen größten Werth in den gegenwärtigen Intervallen für $\delta = \frac{1}{5}$, nämlich $\Psi = \frac{63}{25}$.

3, Wenn δ in den Grenzen $\frac{1}{5}$ und $\frac{1}{4}$ liegt, so hat Ψ seinen größten Werth für $\delta_1 = 0$, $\delta_6 = 0$, $\delta_2 = 1-4\delta$, $\delta_3 = \delta$, $\delta_4 = \delta$, $\delta_5 = \delta$; nämlich $\Psi = 5 - 22\delta + 48\delta^2$; dessen größter Werth, welcher für $\delta = \frac{1}{5}$ Statt hat ist auch hier $\Psi = \frac{63}{25}$.

4, Wenn δ in den Grenzen $\frac{1}{4}$ und $\frac{1}{3}$ liegt so hat Ψ seinen größten Werth für $\delta_1 = 0$, $\delta_6 = 0$, $\delta_2 = 0$, $\delta_5 = 1-3\delta$, $\delta_3 = \delta$, $\delta_4 = \delta$, nämlich $\Psi = 5 - 16\delta + 24\delta^2$ welches für $\delta = \frac{1}{4}$ seinen größten Werth $\Psi = \frac{5}{2}$ hat.

5, Wenn δ in den Grenzen $\frac{1}{3}$ und $\frac{1}{2}$ liegt, so hat Ψ seinen größten Werth für $\delta_1 = 0$, $\delta_6 = 0$, $\delta_2 = 0$, $\delta_5 = 0$, $\delta_3 = 1-2\delta$, $\delta_4 = \delta$, nämlich $\Psi = 6 - 15\delta + 12\delta^2$ dessen größten Werth für $\delta = \frac{1}{3}$ giebt $\Psi = \frac{7}{3}$.

6, Wenn δ in den Grenzen $\frac{1}{2}$ und 1 liegt, so hat Ψ seinen größten Werth für $\delta_1 = 0$, $\delta_6 = 0$, $\delta_2 = 0$, $\delta_5 = 0$, $\delta_3 = 0$, $\delta_4 = 1-\delta$, also $\Psi = 6 - 12\delta + 6\delta^2$ welches für $\delta = \frac{1}{2}$ seinen größten Werth $\Psi = \frac{3}{2}$ hat.

(Was die Detailuntersuchung zur Begründung dieser Resultate zu thun hat habe ich der Kürze wegen weggelassen)

Wir schließen also daß der größte Werth welchen $P+Q+R$ unter den gegebenen Umständen annehmen kann gleich $\frac{63}{25}$ ist: daß also $P+Q+R < 3$ ist. Nun folgt aber aus den obigen drei Gleichungen durch Addition: $f(\alpha)f(\alpha^6) + f(\alpha^2)f(\alpha^5) + f(\alpha^3)f(\alpha^4) = P+Q+R$, also

$$f(\alpha)f(\alpha^6) + f(\alpha^2)f(\alpha^5) + f(\alpha^3)f(\alpha^4) < 3$$

und durch Anwendung desselben Schlusses wie oben für den Fall $\lambda = 5$, weil die Summe dieser drei positiven Größen kleiner als drei ist so muß das Product derselben kleiner als Eins sein, also

$$f(\alpha)f(\alpha^6)f(\alpha^2)f(\alpha^5)f(\alpha^3)f(\alpha^4) < 1.$$

d. h. die Norm der complexen Zahl $f(\alpha)$ ist kleiner als Eins, was zu beweisen war. Es ist also auch die Zerlegbarkeit aller Primzahlen der Form $5m+1$ in 4 complexe Factoren, welche aus fünften Wurzeln der Einheit gebildet sind, und ebenso die Zerlegbarkeit aller Primzahlen $7m+1$ in 6 complexe Factoren, welche aus siebenten Wurzeln der Einheit gebildet sind vollständig bewiesen.

Fig. IV.1B. The last page of Kummer's *Nachtrag zur Dissertation "De numeris"*
(Courtesy of the Institute Mittag-Leffler)

4., Wenn δ in den Grenzen $\frac{1}{4}$ und $\frac{1}{3}$ liegt, so hat Ψ seinen größten Werth für $\delta_1 = 0$, $\delta_6 = 0$, $\delta_2 = 0$, $\delta_5 = 1 - 3\delta$, $\delta_3 = \delta$, $\delta_4 = \delta$; nämlich $\Psi = 5 - 16\delta + 24\delta^2$ welches für $\delta = \frac{1}{4}$ seinen größten Werth $\Psi = \frac{5}{2}$ hat.
5., Wenn δ in den Grenzen $\frac{1}{3}$ und $\frac{1}{2}$ liegt, so hat Ψ seinen größten Werth für $\delta_1 = 0$, $\delta_6 = 0$, $\delta_2 = 0$, $\delta_5 = 0$, $\delta_3 = 1 - 2\delta$, $\delta_4 = \delta$, nämlich $\Psi = 6 - 15\delta + 12\delta^2$ dessen größter Werth für $\delta = \frac{1}{3}$ giebt $\Psi = \frac{7}{3}$.
6., Wenn δ in den Grenzen $\frac{1}{2}$ und 1 liegt, so hat Ψ seinen größten Werth für $\delta_1 = 0$, $\delta_6 = 0$, $\delta_2 = 0$, $\delta_5 = 0$, $\delta_3 = 0$, $\delta_4 = 1 - \delta$, also $\Psi = 6 - 12\delta + 6\delta^2$, welches für $\delta = \frac{1}{2}$ seinen größten Werth $\Psi = \frac{3}{2}$ hat.
(Was die Differenzialrechnung zur Begründung dieser Resultate zu thun hat habe ich der Kürze wegen weggelassen)

Wir schließen also daß der größte Werth welchen $P+Q+R$ unter den gegebenen Umständen annehmen kann gleich $\frac{63}{25}$ ist, daß also $P + Q + R < 3$ ist. Nun folgt aber aus den obigen drei Gleichungen durch Addition: $f(\alpha)f(\alpha^6) + f(\alpha^2)f(\alpha^5) + f(\alpha^3)f(\alpha^4) = P + Q + R$, also

$$f(\alpha)f(\alpha^6) + f(\alpha^2)f(\alpha^5) + f(\alpha^3)f(\alpha^4) < 3$$

und durch Anwendung desselben Schlusses wie oben für den Fall $\lambda = 5$, weil die Summe dieser drei positiven Größen kleiner als Drei ist so muß das Product derselben kleiner als Eins sein also

$$f(\alpha)f(\alpha^6)f(\alpha^2)f(\alpha^5)f(\alpha^3)f(\alpha^4) < 1.$$

d.h. die Norm der complexen Zahl $f(\alpha)$ ist kleiner als Eins, was zu beweisen war. Es ist also auch die Zerlegbarkeit aller Primzahlen der Form $5m + 1$ in 4 complexe Factoren, welche aus fünften Wurzeln der Einheit gebildet sind, und ebenso die Zerlegbarkeit aller Primzahlen $7m + 1$ in 6 complexe Factoren, welche aus siebenten Wurzeln der Einheit gebildet sind vollständig bewiesen.

References

BÖLLING, Reinhard. 1997. Kummer vor der Erfindung der "idealen complexen Zahlen": Das Jahr 1844. *Acta historica Leopoldina* 27, 145–157.

CAUCHY, Augustin-Louis. 1829. Mémoire sur la théorie des nombres. *Bulletin des sciences mathématiques, astronomiques, physiques et chimiques* [*Bulletin de Férussac*] 12, 205–221. Repr. in *Œuvres complètes*, 2nd ser., vol. 2, pp. 88-107. Paris: Gauthier-Villars, 1958.

———. 1840. Mémoire sur la théorie des nombres (dated May 31, 1830). *Mémoires de l'Académie des Sciences* 17, 249–768. Repr. in *Œuvres complètes*, 1st ser., vol. 3, pp. 5–449. Paris: Gauthier-Villars, 1911.

———. 1847. Mémoire sur de nouvelles formules relatives à la théorie des polynômes radicaux, et sur le dernier théorème de Fermat (suite). *Comptes rendus hebdomadaires des séances de l'Académie des sciences* 24 (29 mars 1847), 516–528. Repr. in *Œuvres complètes*, 1st ser., vol. 10, pp. 254–268. Paris: Gauthier-Villars, 1897.

EDWARDS, Harold M. 1977. Postscript to "The Background of Kummer's Proof …." *Archive for History of Exact Sciences* 17, 381–394.

GAUSS, Carl Friedrich. 1863a. Disquisitionum circa aequationes puras ulterior evolutio. In *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, vol. II, *Höhere Arithmetik*, pp. 243–265. Göttingen: Universitäts-Druckerei. German transl. in [Maser 1889], pp. 632–652.

———. 1863b. Zur Theorie der complexen Zahlen. In *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. vol. II, *Höhere Arithmetik*, pp. 387–397. Göttingen: Universitäts-Druckerei.

HAUBRICH, Ralf. 1992. *Zur Entstehung der algebraischen Zahlentheorie Richard Dedekinds*. Dissertation, Georg-August-Universität Göttingen. Göttingen.

HERMITE, Charles. 1850. Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres. *Journal für die reine und angewandte Mathematik* 40, 261–278. Repr. in *Œuvres*, ed. E. Picard, vol. 1, pp. 100–163. Paris: Gauthier-Villars, 1905.

JACOBI, Carl Gustav Jacob. 1835. De functionibus duarum variabilium quadrupliciter periodicis, quibus theoria transcendentium Abelianorum innititur. *Journal für die reine und angewandte Mathematik* 13, 55–78. Repr. in *Gesammelte Werke*, vol. 2, pp. 23–50. German transl. by A. Witting with comm. by H. Weber: *Über die vierfach periodischen Functionen zweier Variabeln, auf die sich die Theorie der Abel'schen Transcendenten stützt*. Ostwald's Klassiker der exakten Wissenschaften 64. Leipzig: Verlag von Wilhelm Engelmann, 1895.

———. 1837. Über die Kreistheilung und ihre Anwendung auf die Zahlentheorie. *Monatsbericht der Academie der Wissenschaften zu Berlin*, October 1837, 127–136. Repr. in *Journal für die reine und angewandte Mathematik* 30 (1846), 166–182. Repr. in *Gesammelte Werke*, vol. 6, pp. 254–274. French transl. in *Nouvelles Annales de Mathématiques* 15 (1856), 337–352.

———. 1839. Über die complexen Primzahlen, welche in der Theorie der Reste der 5-ten, 8-ten und 12-ten Potenzen zu betrachten sind. *Monatsberichte der Academie der Wissenschaften zu Berlin*, May 1839, 86–91. Repr. in *Journal für die reine und angewandte Mathematik* 19 (1839), 314–318. Repr. in *Gesammelte Werke*, vol. 6, pp. 275–280. French transl. in *Journal de mathématiques pures et appliquées* 8 (1843), 268–272.

———. 1881–1891. *Gesammelte Werke*, ed. C. W. Borchardt, K. Weierstraß, E. Lottner. 7 vols. + Supplement. Berlin: Reimer.

Kummer, Ernst Eduard. 1844a. Kummers Briefe an Leopold Kronecker. In: *Festschrift zur Feier des 100. Geburtstages Eduard Kummers mit Briefen an seine Mutter und an Leopold Kronecker*, ed. Vorstand der Berliner Mathematischen Gesellschaft, pp. 46–102. Leipzig, Berlin: Teubner, 1910. Repr. in [Kummer 1975], pp. 76–132. (In the present paper only letters dating from 1844 are quoted.)

———. 1844b. Ueber die complexen Primfactoren der Zahlen, und deren Anwendung in der Kreistheilung. Manuscript in: Archiv der Berlin-Brandenburgischen Akademie der Wissenschaften, Historische Abteilung, Abschnitt II: Akten der Preussischen Akademie der Wissenschaften 1812 bis 1945. Verhandlungen der physikalisch-mathematischen Klasse 1842–1844. Sign.: II–IV, 46, Bl. 235–238 (with accompanying letter, Bl. 234). Publ. in [Edwards 1977], 388–393.

———. 1844c. De numeris complexis, qui radicibus unitatis et numeris integris realibus constant. In *Academiae Albertinae Regiomontanae secularia tertia celebranti gratulatur Academia Vratislaviensis*, pp. 1–28. Breslau: Typis Universitatis. Repr. *Journal de mathématiques pures et appliquées* 12 (1847), 185–212. Repr. in [Kummer 1975], pp. 165–192.

———. 1846. Zur Theorie der complexen Zahlen. *Monatsberichte der Königlichen Akademie der Wissenschaften zu Berlin*, March 1846, 87–96. Repr. *Journal für die reine und angewandte Mathematik* 35 (1847), 319–326. Repr. in [Kummer 1975], pp. 203–210.

———. 1847a. Über die Zerlegung der aus Wurzeln der Einheit gebildeten complexen Zahlen in ihre Primfactoren. *Journal für die reine und angewandte Mathematik* 35, 327–367. Repr. in [Kummer 1975], pp. 211–251.

———. 1847b. Extrait d'une lettre de M. Kummer à M. Liouville. *Journal de mathématiques pures et appliquées* 12, 136. Repr. in [Kummer 1975], p. 298.

———. 1975. *Collected Papers*, ed. A. Weil, vol. 1, *Contributions to Number Theory*. Berlin, Heidelberg etc.: Springer.

Lenstra, Hendrik W., Jr. 1975. Euclid's algorithm in cyclotomic fields. *Journal of the London Mathematical Society* 2-10, 457–465.

———. 1979. Euclidean number fields 1. *The Mathematical Intelligencer* 2-1, 6–15.

McKenzie, Robert George. 1988. *The Ring of Cyclotomic Integers of Modulus Thirteen Is Norm-Euclidean*. Ph.D. thesis, Michigan State University. East Lansing.

———. 1995. The Euclidean algorithm in algebraic number fields. *Expositiones Mathematicae* 13, 385–416.

Maser, Hermann. 1889. *Carl Friedrich Gauss' Untersuchungen über höhere Arithmetik*. Berlin: Julius Springer.

MASLEY, J. Myron, MONTGOMERY, Hugh L. 1976. Cyclotomic fields with unique factorization. *Journal für die reine und angewandte Mathematik* 286/287, 248–256.

NEUMANN, Olaf. 1981. Über die Anstöße zu Kummers Schöpfung der "idealen complexen Zahlen." In *Mathematical Perspectives. Essays on Mathematics and Its Historical Development. Papers in honor of Kurt-Reinhard Biermann on the occasion of his 60th birthday*, ed. J.W. Dauben, pp. 179–199. New York, London: Harcourt Brace Jovanovich.

UCHIDA, Kôji. 1971. Class numbers of imaginary abelian number fields, III. *Tôhoku Mathematical Journal* 23, 573–580.

USPENSKIJ, Jakov Viktorovič. 1906. Zametka o celych čislach, zavisjaščich ot kornja 5-oj stepeni iz edinicy. (Remark on the integers which depend on the 5th roots of unity.) *Matematičeskij sbornik* 26 (1906/08), 1–17. French transl. of secs. II, III in [Uspenskij 1909].

——— [= OUSPENSKY, J.]. 1909. Note sur les nombres entiers dépendant d'une racine cinquième de l'unité. *Mathematische Annalen* 66, 109–112.

IV.2

Elliptic Functions and Arithmetic

CHRISTIAN HOUZEL

There are several places where Gauss's works hint at possible links between number theory and elliptic functions. Here are a few of them:

1. The introduction to sec. 7 of the *Disquisitiones Arithmeticae* provides us with a first example. There Gauss says that the principles he is about to explain for the divison of the circle "may be applied equally successfully to many other transcendental functions, for instance to those which depend on the integral $\int \frac{dx}{\sqrt{(1-x^4)}}$."[1] Gauss had elaborated the theory of this integral from 1797. It gives the length of an arc of the lemniscate, so the theory amounts to the study of the equation of the division of the lemniscate. Gauss defined the lemniscatic sine, $x = \sin \text{lemn}\, u$, by the relation $u = \int\limits_0^x \frac{dt}{\sqrt{(1-t^4)}}$. It is a periodic function with period 2ϖ, where $\varpi = 2\int_0^1 \frac{dx}{\sqrt{(1-x^4)}}$. The lemniscatic cosine is defined by $\cos \text{lemn}\, u = \sin \text{lemn}\, (\frac{\varpi}{2} - u)$. The lemniscatic sine and cosine are related by Fagnano's relation

$$\sin \text{lemn}^2\, u + \cos \text{lemn}^2\, u + \sin \text{lemn}^2\, u \cdot \cos \text{lemn}^2\, u = 1.$$

In view of $\frac{dx}{\sqrt{1-(ix)^4}} = i\frac{dx}{\sqrt{1-x^4}}$, Gauss defined $\sin \text{lemn}(iu) = i\, \sin \text{lemn}\, u$,

[1] D.A., art. 335: *Ceterum principia theoriae, quam exponere aggredimur, multio latius patent, quam hic extenduntur. Namque non solum ad functiones circulares, sed pari successu ad multas alias functiones transcendentes applicari possunt, e.g. ad eas quae ab integrali* $\int \frac{dx}{\sqrt{(1-x^4)}}$ *pendent.*

and then $\sin\operatorname{lemn} z$ for all $z = u + iv$ by Euler's addition theorem

$$\sin\operatorname{lemn}(u+v) = \frac{\sin\operatorname{lemn} u \cos\operatorname{lemn} v + \sin\operatorname{lemn} v \cos\operatorname{lemn} u}{1 - \sin\operatorname{lemn}(u)\sin\operatorname{lemn}(v)\cos\operatorname{lemn}(u)\cos\operatorname{lemn}(v)}.$$

Then the relation $\sin\operatorname{lemn}(u + 2m\varpi) = \sin\operatorname{lemn} u$ holds not only for an integer m, but for all $m = a + bi$, where a, b are integers. This marks the birth of the ring of Gaussian integers, which today is denoted by $\mathbf{Z}[i]$. For every Gaussian integer m, $\sin\operatorname{lemn}(mu)$ is a rational function of $\sin\operatorname{lemn} u$ and $\cos\operatorname{lemn} u$. This was later called the property of *complex multiplication* of the elliptic integral $\displaystyle\int \frac{dx}{\sqrt{(1-x^4)}}$. It is the reason for the analogy with the theory of the division of the circle.

2. In the last entry of Gauss's *Notizenjournal* or mathematical diary (July 9, 1814), we read:

> A most important observation made by induction which connects the theory of biquadratic residues most elegantly with the lemniscatic functions. Suppose that, if $a + bi$ is a prime number, $a - 1 + bi$ divisible by $2 + 2i$, then the number of all solutions of the congruence $1 = xx + yy + xxyy \pmod{a + bi}$ including $x = \infty$, $y = \pm i$; $x = \pm i$, $y = \infty$, equals $(a-1)^2 + bb$.[2]

Thus, from the modern point of view, Gauss had evaluated the number of points of an elliptic curve over the finite field $\mathbf{Z}[i]/(a+bi)$ to be the norm of $a + bi - 1$. The equation of this elliptic curve is precisely Fagnano's relation between the lemniscatic sine and cosine. Gauss's observation was finally proven by Gustav Herglotz, in [Herglotz 1921].

3. In Gauss's *Nachlass* we find the remarkable identity[3]

$$1 + \sum_{n=1}^{\infty} x^{n^2}\left(\alpha^n + \alpha^{-n}\right) = \prod_{n=1}^{\infty}\left(1 - x^{2n}\right)\prod_{n=0}^{\infty}\left(1 + \alpha x^{2n+1}\right)\left(1 + \frac{x^{2n+1}}{\alpha}\right). \tag{1}$$

If $\alpha = e^{\frac{i\pi u}{\omega}}$ and $x = e^{\frac{-\pi\omega'}{\omega}}$, where ω and ω' are complex numbers such that $\operatorname{Re}\frac{\omega'}{\omega}$ is greater than 0, then both sides represent an entire function of u (in fact, a theta function – see § 4 below) which gives the numerator of an elliptic function with periods ω and $i\omega'$; the left-hand side of (1) is the Fourier series expansion of this entire function. Gauss published a particular case of this identity in [Gauss 1808]. This is the paper where he determined the sign of the Gauss sums (as they are called today) introduced in art. 356 of the D.A. – cf. S.J. Patterson's chap. VIII.2 below.

[2] [Gauss 1796–1814], last entry: *Observatio per inductionem facta gravissima theoriam residuorum biquadraticorum cum functionibus lemniscaticis elegantissime nectens. Puta, si $a + bi$ est numerus primus, $a - 1 + bi$ per $2 + 2i$ divisibilis, multitudo omnium solutionum congruentiae* $1 = xx + yy + xxyy \pmod{a + bi}$ *inclusis $x = \infty$, $y = \pm i$, $x = \pm i$, $y = \infty$ fit* $= (a-1)^2 + bb$.

[3] See [Gauss 1866], p. 464, "Viertes Theorem."

Knowing that sign, Gauss obtained a new proof of the quadratic reciprocity law, his fourth proof.

4. Finally, number theory is used for studying elliptic modular functions. Gauss determined the fundamental domain of the group which we write today $\Gamma(2) = \ker\big(\mathrm{SL}(2,\mathbf{Z}) \to \mathrm{SL}(2,\mathbf{Z}/2\mathbf{Z})\big)$, operating on the right complex half plane $\{\mathrm{Re}\, t > 0\}$ via

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} t = \frac{\alpha t - \beta i}{\delta + \gamma i t}.$$

Here $t = \dfrac{\varpi'}{\varpi}$ is, up to a factor i, the ratio of the periods $(i\varpi', \varpi)$. Gauss remarked that, when t is so transformed, the quadratic form $|x - ity|^2 = x^2 + 2\,\mathrm{Im}\, t \cdot xy + |t|^2 y^2$ is transformed by the linear substitution $\begin{pmatrix} \delta & -\beta \\ -\gamma & \alpha \end{pmatrix}$. Then his theory of reduced quadratic forms (D.A., art. 171) allowed him to find a reduced value for t, i.e., one for which one has both $-1 < \mathrm{Im}\, t \leq 1$ and $-1 \leq \mathrm{Im}\, \frac{1}{t} < 1$.

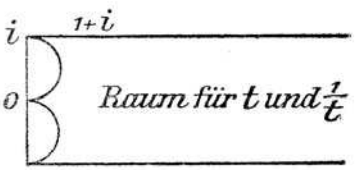


Fig. IV.2A. Gauss's drawing of a modular fundamental domain: the "space for t and $\frac{1}{t}$."
From *Werke*, vol. VIII, p. 105.

1. Niels Henrik Abel and Complex Multiplication

Gauss never published his work on elliptic functions. Abel rediscovered the theory in 1827, [Abel 1827–1828]. In this seminal article, Abel shifted attention from the elliptic integral to its inverse function. His theory deals with the function φ characterized by the equivalence

$$\varphi(\alpha) = x \qquad \Longleftrightarrow \qquad \alpha = \int_0^x \frac{dx}{\sqrt{(1 - c^2x^2)(1 + e^2x^2)}}.$$

The special case of the lemniscatic integral corresponds to the choice of parameters $c = e = 1$. Abel called the functions φ *elliptic functions* – much to Legendre's chagrin, who used this name for the corresponding integrals, and did not like to see his terminology replaced. In the same paper, Abel also studied the algebraic equation giving the non-zero values of $\varphi^2\Big(\dfrac{\Omega}{n}\Big)$, where Ω is a half-period of the elliptic function φ and n is a positive integer. For n an odd prime, this equation is of degree $\frac{n^2-1}{2}$, and Abel proved that it may be decomposed into $n+1$ equations of degree $\frac{n-1}{2}$ by means of an equation of degree $n+1$.[4] Each of the equations of degree $\frac{n-1}{2}$ is cyclic, as Abel saw by using Gauss's method from the seventh section of the D.A. He wrote their roots in the form $x_m = \varphi^2(\alpha^m \varepsilon)$, where ε is a suitable half-period divided by n and α is a primitive root mod. n, so one has $x_{m+n} = x_m$. The equation of degree $n+1$ is not solvable in general, except in special cases, like the lemniscatic case for $n \equiv 1 \pmod 4$, or, more generally, in the cases where $\varphi(\dfrac{\varpi i}{n})$ is a rational function of $\varphi(\frac{\omega}{n})$ and of the known quantities. Here ω and ϖi are the fundamental half-periods; in the lemniscatic case, one has $\varpi = \omega$.

The tool to prove this result is complex multiplication: for any δ, one has $\varphi(m+\mu i)\delta = xT(x^4)$, where $x = \varphi\delta$, T is a rational function, and m, μ are integers such that $m+\mu$ is supposed to be odd. As $n \equiv 1 \pmod 4$, there exist α and β such that $n = \alpha^2 + \beta^2$, and there exist integers q, r such that $2q\alpha - nr = 1$ because 2α and n are coprime. Therefore

$$\frac{1}{n} = q\frac{2\alpha}{n} - r = q\Big(\frac{1}{\alpha+\beta i} + \frac{1}{\alpha-\beta i}\Big) - r$$

and

$$\varphi\Big(\frac{\Omega}{n}\Big) = \pm\varphi\Big(\frac{q\Omega}{\alpha+\beta i} + \frac{q\Omega}{\alpha-\beta i}\Big).$$

One sees that it is sufficient to divide by $\alpha \pm \beta i$ and the corresponding equation is again a cyclic one, by Gauss's method.

At the end of his *Recherches*, [Abel 1827–1828], n$^{\mathrm{o}}$ 50, Abel states the general problem of complex multiplication: to find the moduli μ and irrational numbers a such that the equation

$$\frac{dy}{\sqrt{(1-y^2)(1+\mu y^2)}} = a\frac{dx}{\sqrt{(1-x^2)(1+\mu x^2)}} \tag{2a}$$

has a general algebraic solution. He finds that a has to be of the form $m + \sqrt{-n}$ for rational numbers $m, n, n \geq 0$, and that μ is an algebraic number if $n \neq 0$. He doubted at first that the equation giving μ for a given n was algebraically solvable. But in a subsequent paper [Abel 1828], he stated this as a theorem. Abel particularly considered the case where $a = \sqrt{-n}$ for an odd prime n, which implies $\frac{\omega}{\varpi} = \sqrt{n}$. For instance, the case $n = 3$ corresponds to $\mu = (2+\sqrt{3})^2$, and $n = 5$ to $\mu = \Big(2 + \sqrt{5} + 2\sqrt{2+\sqrt{5}}\Big)^2$.

By 1828, Abel was already in direct competition, as far as the theory of elliptic integrals and functions was concerned, with Carl Gustav Jacob Jacobi, who would

[4] Indeed, the roots correspond to the elements of $(\mathbf{F}_n^2 \setminus \{0\})/\{\pm 1\}$, $\mathbf{F}_n$ being the field with n elements, and one groups together the points on each of the $n+1$ straight lines in the plane $\mathbf{F}_n^2$.

publish his own formalism and notation of elliptic functions in the famous *Fundamenta nova* [Jacobi 1829]. Jacobi's particular emphasis was on the general theory of transformations of one elliptic integral into another. Complex multiplication, as seen in (2a), is a special type of transformation relating an integral to itself.

Jacobi's interest in complex multiplication can also be seen in a note [Jacobi 1881] which was published only after his death. There he observed that if p is a prime number, the number of transformations of order p of elliptic functions leaving the modulus k invariant and with a multiplier involving the irrationality $\sqrt{-n}$ is equal to the number of essentially distinct representations of p by the quadratic form $x^2 + ny^2$. To a representation $p = a^2 + nb^2$ corresponds a transformation with multiplier $\frac{1}{a+ib\sqrt{n}}$.

2. Leopold Kronecker

Kronecker was beyond doubt the most important mathematician who developed the theory of complex multiplication in the XIX$^{\text{th}}$ century. At the end of his note [Kronecker 1853], having essentially stated what is known today as the Kronecker-Weber Theorem,[5] Kronecker announced the corresponding result for the abelian equations with coefficients in $\mathbf{Z}[i]$, the division equations of the lemniscate playing the role of the cyclotomic equations for the case of rational coefficients. In [Kronecker 1857], he announced a proof of Abel's statement about the solvability of the equation giving the singular moduli.[6] This note was the point of departure for Kronecker's work on complex multiplication. Using Jacobi's notation, with the elliptic function $x = \sin \operatorname{am} u$ defined by

$$u = \int_0^x \frac{dt}{(1-t^2)(1-\kappa^2 t^2)},$$

he considers the algebraic equation with integer coefficients giving the moduli κ^2 for which there is a complex multiplication by $\sqrt{-n}$. The degree of this equation is six times the number of classes of binary quadratic forms with discriminant $-n$. This comes from the fact that complex multiplication is a particular case of transformations; the transformations of order p operate on the ratio ω of the two fundamental periods by a homography $\omega \mapsto \dfrac{c + d\omega}{a + b\omega}$ with integer coefficients a, b, c, d such that $ad - bc = p$. If ω is invariant by such a homography, then there is complex multiplication. This condition amounts to $a\omega + b\omega^2 = c + d\omega$, so ω is a quadratic complex number. Conversely, if ω is quadratic, then there is complex multiplication: for instance, starting from a properly primitive quadratic form (A, B, C) (in Gauss's notation from the D.A.) with negative discriminant $-n = B^2 - AC$, let us consider a root ω of the quadratic equation $A + 2B\omega + C\omega^2 = 0$. One has

[5] As Kronecker put it, the roots of all abelian equations with rational integer coefficients can be expressed as rational functions in suitable roots of unity.

[6] I.e., those for which there is complex multiplication by $\sqrt{-n}$ for a given n.

$\omega = \dfrac{-yA + (x - yb)\omega}{x + yB + yC\omega}$, for all integers x, y, and the discriminant of this homography leaving ω invariant is equal to $p = x^2 + ny^2$. So a transformation of order p is a complex multiplication by the number $x + y\sqrt{-n}$, and this proves the result announced by Jacobi.

To a number q represented by another quadratic form of discriminant $-n$, not by the principal one $x^2 + ny^2$, there is associated a transformation which changes the modulus κ to a new one λ, and $\sin^2\mathrm{am}(\mu u, \lambda)$ is rationally expressed in terms of $\sin^2\mathrm{am}(u, \kappa)$ and κ. This new modulus also admits complex multiplication by $\sqrt{-n}$, and μ is congruent mod q to a well-defined value of $\sqrt{-n}$. Kronecker interprets μ as a concrete representation of the corresponding ideal factor of q in Ernst Kummer's sense.[7]

Passing from ω to the modulus κ^2, one sees that the group $\mathrm{SL}(2, \mathbf{Z})$ operating on ω yields six values of κ^2, for the subgroup fixing κ^2 is $\Gamma(2) = \ker\big(\mathrm{SL}(2, \mathbf{Z}) \to \mathrm{SL}(2, \mathbf{Z}/2\mathbf{Z})\big)$ which is of index 6; each class of binary quadratic forms contains six subclasses with respect to $\Gamma(2)$ and the different moduli κ^2 correspond to these subclasses.

The equation is decomposed into factors with integer coefficients corresponding to the orders of quadratic forms (D.A., art. 226). The factor associated to the properly primitive order is decomposed in 6 factors of the same degree after adjunction of $\sqrt{n}$. Finally, each of these partial equations is abelian and thus in particular solvable by radicals.

Kronecker gave a hint at the proof of these results in a later paper, [Kronecker 1877]. If $D = b^2 - ac$ is a negative discriminant, he considered the equation $F(x) = 0$ of the division of the periods by a. Its roots are of the form $\pm\varphi\Big(\dfrac{\Omega}{a}\Big)$. If φ admits complex multiplication by $\sqrt{D}$, then $\varphi^2\Big((b+\sqrt{D})\dfrac{\Omega}{a}\Big)$ is rational with respect to $\varphi^2\Big(\dfrac{\Omega}{a}\Big)$. So these quantities are the roots of an equation $\Phi(x) = 0$ deduced from F by a rational computation. One finds that $\Phi(x) = x^{a-1}(c_1 + c_2 x + \cdots + c_a x^{a-1})^a$ and that c_1 is a new modulus with complex multiplication, rationally expressed in κ^2. This is how Kronecker proved that all these moduli are rational functions of one of them, with mutually permuting rational functions, i.e., one has an abelian equation.

Kronecker also conjectured the converse of the theorem thus proved. This is his famous *Jugendtraum*, formulated for instance at the end of [Kronecker 1877]. Speaking of abelian equations with coefficients in an imaginary quadratic field, he says:

> it is to be conjectured that the totality of such equations is exhausted by those which arise from the theory of elliptic functions.[8]

[7] Cf. the quote on p. 49 above; chap. I.1, note 166 [Editors' note].

[8] [Kronecker 1877], § XI: *und es ist zu vermuthen, dass die Gesammtheit solcher Gleichungen durch jene, die aus der Theorie der elliptischen Functionen hervorgehen, erschöpft wird.*

The problem thus formulated was later studied by Heinrich Weber,[9] Rudolf Fueter in [Fueter 1914], and then Teiji Takagi, in [Takagi 1920] in the general framework of class field theory.[10]

At the end of [Kronecker 1857] and in a subsequent paper [Kronecker 1860], Kronecker deduced from the study of the equation of singular moduli certain remarkable induction formulae for class numbers. For example, for each integer n, one has $\sum_{D>0} hH(D) = 2\varphi(n)$, where h is the number of representations of n by the quadratic form $x^2 + Dy^2$, $H(D)$ is the number of properly primitive classes of binary quadratic forms of discriminant $-D$, and $\varphi(n)$ is the sum of those divisors of n which are greater than $\sqrt{n}$. The first member is the degree of the equation $f(x) = 0$ for the singular moduli. The second member is obtained by considering the order of magnitude of $f(x)$ as $x \to \infty$, using the analytic expression for the modulus given by Jacobi. Another way to express this is to sum over all x such that $n - x^2 = Dy^2$. The left-hand side then becomes

$$F(n) + 2F(n - 1^2) + 2F(n - 2^2) + \cdots,$$

where $F(m)$ denotes the number of odd classes of binary quadratic forms of discriminant $-m$. As Kronecker gave no proof, only hints, Charles Hermite, Charles Joubert and Henry J. S. Smith worked to give a complete demonstration.

In his paper [Kronecker 1862], the author gave another decomposition of the equation for the singular moduli, according to genera — a notion introduced by Gauss in the D.A., art. 227. Let N be the number of properly primitive classes of discriminant $-n$. Then the equation of degree $6N$ corresponding to the properly primitive order decomposes into 3 equations of degree $2N$. One of them has for a root the modulus $k = \kappa^2$ corresponding to $q = e^{-\pi\sqrt{n}}$. If $p_1, \ldots, p_\nu$ are the prime numbers dividing n, this equation decomposes into 2^ν factors of equal degree after the adjunction of the $\sqrt{p_i}$ for $i = 1, \ldots, \nu$. If $n \equiv 3 \pmod 4$, the degree of each factor is equal to the number of classes in a given genus. If $n \equiv 1 \pmod 4$, one obtains an equation of that degree for $k(1-k)$, instead of k.

Kronecker computed several examples of singular moduli for $n = 6, 10, 15, 39, 63, 5, 13, 21, 37, 49, 105$. For instance, $n = 6$ gives $k = (1+\sqrt{2})^2(1+\sqrt{2}+\sqrt{6})^2$, and n = 10 yields $k = (1+\sqrt{2})^4(3+\sqrt{10})^2$. Finally, Kronecker explained that the partial equations are irreducible.

3. Eisenstein and the Reciprocity Laws of Degree 4 and 3

We saw that Gauss introduced the "Gaussian integers" $\mathbf{Z}[i]$ in connection with the complex multiplication of lemniscatic functions, and he used them to state the biquadratic reciprocity law in [Gauss 1828–1832]. Eisenstein gave a proof of this law using the complex multiplication of lemniscatic functions in [Eisenstein 1845]. He

[9] See [Weber 1891] and [Weber 1897–1898].

[10] Hermite explained a method for computing the equation of singular moduli from the classification of binary quadratic forms in a series of notes in the *Comptes rendus*, [Hermite 1859]. He interpreted the equation as the discriminant of the modular equation.

considered an odd prime number m of $\mathbf{Z}[i]$ and the residues mod. m of the integers $a + bi$ which are not divisible by m. The number of distinct residues is $p - 1$ where $p = N(m)$ is the norm of m, and they are equally distributed among 4 types r, ir, $-r$, $-ir$, where r varies over a system of representatives of the classes modulo m up to units ± 1, $\pm i$ of $\mathbf{Z}[i]$. If n is a Gaussian integer not divisible by m, then for each r there exists an r' and a $k = 0, 1, 2$, or 3, such that $nr \equiv i^k r' \pmod{m}$. Since $\sin\operatorname{lemn}(i^k u) = i^k \sin\operatorname{lemn} u$, one has

$$\sin\operatorname{lemn}\Big(nr\frac{\omega}{m}\Big) = i^k \sin\operatorname{lemn}\Big(r'\frac{\omega}{m}\Big), \tag{2}$$

with a period ω. Therefore $nr \equiv r'\dfrac{\sin\operatorname{lemn}(nr(\omega/m))}{\sin\operatorname{lemn}(r'(\omega/m))} \pmod{m}$. Multiplying the $\frac{p-1}{4}$ congruences thus obtained as r varies, Eisenstein obtains

$$n^{\frac{p-1}{4}} \equiv \prod_r \frac{\sin\operatorname{lemn}(nr\frac{\omega}{m})}{\sin\operatorname{lemn}(r'\frac{\omega}{m})} \pmod{m}, \tag{3}$$

where the right-hand side is a unit because of (2). If n is also an odd prime, $q = N(n)$ its norm, and if ρ varies over a system of representatives modulo n up to units, one finds

$$m^{\frac{q-1}{4}} \equiv \prod_\rho \frac{\sin\operatorname{lemn}(m\rho\frac{\omega}{n})}{\sin\operatorname{lemn}(\rho'\frac{\omega}{n})} \pmod{n}.$$

But one knows that $\dfrac{\sin\operatorname{lemn}(mv)}{\sin\operatorname{lemn} v}$ is a rational function of order $p - 1$ of $\sin\operatorname{lemn} v$. If $m \equiv 1(\operatorname{mod} 2 + 2i)$, i.e., if m is primary in Dirichlet's sense, then this function has the form

$$\frac{\prod\limits_\alpha (x^4 - \alpha^4)}{\prod\limits_\alpha (1 - \alpha^4 x^4)}, \quad \text{where} \quad x = \sin\operatorname{lemn} v \quad \text{and} \quad \alpha = \sin\operatorname{lemn}\Big(\frac{r\omega}{m}\Big).$$

In the same way, when n is primary, we have

$$\frac{\sin\operatorname{lemn}(nv)}{\sin\operatorname{lemn} v} = \frac{\prod\limits_\beta (x^4 - \beta^4)}{\prod\limits_\beta (1 - \beta^4 x^4)}, \quad \text{where} \quad \beta = \sin\operatorname{lemn}\Big(\frac{\rho\omega}{n}\Big).$$

Consequently,

$$n^{\frac{p-1}{4}} \equiv \prod_{\alpha,\beta} \frac{\alpha^4 - \beta^4}{1 - \alpha^4\beta^4} \pmod{m} \quad \text{and} \quad m^{\frac{q-1}{4}} \equiv \prod_{\alpha,\beta} \frac{\beta^4 - \alpha^4}{1 - \alpha^4\beta^4} \pmod{n}.$$

Gauss had defined the biquadratic residue symbol $\left[\frac{n}{m}\right]_4$ as the unit congruent to $n^{\frac{p-1}{4}}$ modulo m. So we see that $\left[\frac{n}{m}\right]_4 = \prod\limits_{\alpha,\beta} \dfrac{\alpha^4 - \beta^4}{1 - \alpha^4\beta^4}$, and $\left[\frac{n}{m}\right]_4 = \prod\limits_{\alpha,\beta} \dfrac{\beta^4 - \alpha^4}{1 - \alpha^4\beta^4}$.

Since the right-hand sides only differ by the sign $(-1)^{\frac{p-1}{4}\frac{q-1}{4}}$, the biquadratic reciprocity law announced by Gauss follows:

$$\left[\frac{n}{m}\right]_4\left[\frac{m}{n}\right]_4 = (-1)^{\frac{p-1}{4}\frac{q-1}{4}}.$$

Eisenstein also gave another proof of the law of biquadratic reciprocity in [Eisenstein 1845]. Writing φ for the lemniscatic sine, he proved that, for any primary odd complex number m,

$$\varphi(mt) = \varphi(t)\,\frac{m\mathcal{F} + \varphi^{p-1}(t)}{1 - m\mathcal{G}}, \tag{4}$$

where $\mathcal{F}$ and $\mathcal{G}$ are polynomials in $\varphi^4(t)$ with integer coefficients. He explicitly computed $\mathcal{F}$ and $\mathcal{G}$ for the cases $m = -1 + 2i, 3 + 2i, 1 + 4i$. The roots of the numerator in (4) are the numbers $\varphi^4(\frac{r\omega}{m})$, and their product equals $(-1)^{\frac{p-1}{4}}m$. Now by (3), $\left[\frac{n}{m}\right]_4 = \prod_r \frac{\varphi(nt)}{\varphi(t)}$ with $t = \frac{r\omega}{m}$ and (4) gives polynomials P, Q with integer coefficients such that $P(0) = 1$, $Q(0) = 0$, and

$$\left[\frac{n}{m}\right]_4 P(n) = \prod_r \varphi^{q-1}\Big(\frac{r\omega}{m}\Big) + Q(n).$$

Taken modulo n, this gives

$$\left[\frac{n}{m}\right]_4 \equiv (-1)^{\frac{p-1}{4}\frac{q-1}{4}} m^{\frac{q-1}{4}} \equiv (-1)^{\frac{p-1}{4}\frac{q-1}{4}}\left[\frac{m}{n}\right]_4.$$

A third proof invented by Eisenstein also applies to the cubic reciprocity law. It was published in [Eisenstein 1847]. Let $\beta = i$, $\vartheta = 4$ for the biquadratic case, and $\beta = r = \frac{-1+\sqrt{-3}}{2}$, $\vartheta = 6$ for cubic reciprocity, so that β is a generator and ϑ is the order of the group of units of the corresponding quadratic field. Eisenstein uses the function $F(x) = \prod_n \prod_m \Big(1 - \dfrac{tx}{m + n\beta}\Big)$, where t is an even integer.[11] Let k, ℓ be complex prime numbers,[12] and p, q their respective norms. Assume that p and q are congruent to 1 mod ϑ and write $p' = \dfrac{p-1}{\vartheta}$, $q' = \dfrac{q-1}{\vartheta}$, and take t prime to pq. Let $\{\sigma\}$, resp. $\{\tau\}$, be systems of representatives of the classes modulo k, resp. ℓ, up to units. For each σ, there exists a σ_1 and a unit $\mathfrak{e}$ such that $\ell\sigma = \mathfrak{e}\sigma_1 \pmod{k}$. Thus $F(\frac{\ell\sigma}{k}) = e^{\mathfrak{w}t^2} F(\frac{\mathfrak{e}\sigma_1}{k}) = \mathfrak{e}e^{\mathfrak{w}t^2} F(\frac{\sigma_1}{k})$, where $\mathfrak{w}$ denotes a number independent of t. Multiplying these identities for all σ, one gets first $\ell^{p'}\prod\sigma \equiv \prod\mathfrak{e}\prod\sigma \pmod{k}$,

[11] This is equivalent to studying Jacobi's function H which will be discussed in the following section.

[12] On this notion at the time, see R. Bölling's chap. IV.1, § 5 [Editors' note].

so $\ell^{p'} \equiv \prod \mathfrak{e}$ (mod k). Then $\prod\limits_{\sigma} F(\frac{\ell\sigma}{k}) = \prod\limits_{\sigma} \mathfrak{e} \cdot e^{\mathfrak{w}t^2} \prod\limits_{\sigma} F(\frac{\sigma}{k})$ whence $\prod\limits_{\sigma} \mathfrak{e} = e^{-\mathfrak{w}t^2} \prod\limits_{\sigma} \frac{F(\frac{\ell\sigma}{k})}{F(\frac{\sigma}{k})}$. But $\dfrac{F(\ell x)}{F(x)} = \rho' c^{q-1} e^{\mathfrak{w}t^2} \prod\limits_{\lambda'} F(x + \frac{\lambda'}{\ell})$, where c is a constant and ρ' is a unit defined in the following way: if $\beta = i$ and $\ell = a + bi$, then $\rho' = i^{b^2+b+a-1}$; if $\beta = r$ and $\ell = a + br$, then $\rho' = (-1)^{\frac{a+b}{2}} r^{-b}$. This implies

$$\ell^{p'} \equiv e^{\mathfrak{w}t^2} \rho'^{p'} c^{\vartheta p'q'} \prod_{\mathfrak{e},\sigma,\tau} F\Big(\frac{\sigma}{k} + \frac{\mathfrak{e}\tau}{\ell}\Big) \quad (\text{mod } k)$$

and likewise

$$k^{q'} \equiv e^{\mathfrak{w}t^2} \rho^{q'} c^{\vartheta p'q'} \prod_{\mathfrak{e},\sigma,\tau} F\Big(\frac{\mathfrak{e}\sigma}{k} + \frac{\tau}{\ell}\Big) \quad (\text{mod } \ell),$$

from which one finally derives for the biquadratic, resp. cubic residue symbol of ℓ modulo k, i.e., for the unit $\left(\frac{\ell}{k}\right)$ which is congruent to $\ell^{p'}$ modulo k:

$$\frac{\left(\frac{\ell}{k}\right)}{\left(\frac{k}{\ell}\right)} = \frac{\rho'^{p'}}{\rho^{q'}} (-1)^{p'q'} e^{\mathfrak{w}t^2}. \tag{5}$$

Here Eisenstein uses a lemma according to which if $A = Be^{\mathfrak{w}t^2}$, where t is a variable integer and A, B, $\mathfrak{w}$ do not depend on t , then $A = B$ and $\mathfrak{w}t^2$ is a multiple of $2\pi i$. One may suppose that t varies through the multiples of a finite set of prime numbers and that it is not divisible by the elements of another set of prime numbers other than 2 and 3. When t is not to be divisible by 3, the conclusion is that $\frac{A}{B}$ is a cube root of 1. Then (5) implies

$$\rho'^{p'} \left(\frac{k}{\ell}\right) = \rho^{q'} (-1)^{p'q'} \left(\frac{\ell}{k}\right), \tag{6}$$

provided neither p nor q is divisible by 3. If p or q is divisible by 3, $\beta = i$, and k or ℓ equals 3, so that p or q is equal to 9, then the ratio of the two sides of (6) is a cubic root of 1. Since both sides are quartic roots of 1, this ratio is equal to 1. So (6) is still true. In the case where k and ℓ are primary, one has $\rho = \rho' = 1$ and we get the reciprocity law. (Note that each number in $\mathbf{Z}[\beta]$ is the product of a primary number by a unit.)

We should add that Jacobi claimed he knew this method of establishing reciprocity laws for the degrees 3 and 4 before Eisenstein.[13]

[13] See chap. I.1, footnote 158 [Editors' note].

4. Fourier Series and q-Calculus

As indicated in the introduction, another theme arose from the Fourier series of numerators of elliptic functions. In the *Fundamenta nova*, [Jacobi 1829], Jacobi introduced, for each modulus k, entire functions H and Θ, such that[14] $\sin\operatorname{am} u = \dfrac{1}{\sqrt{k}}\dfrac{\mathsf{H}(u)}{\Theta(u)}$. Jacobi sets

$$K = \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}}$$

and

$$K' = \int_0^{\frac{\pi}{2}} \frac{d\theta}{\sqrt{1-k'^2\sin^2\theta}},$$

where $k'^2 = 1-k^2$. Then the periods of the function $\sin\operatorname{am} u$ are $4K$ and $2iK'$. If $q = e^{-\pi K'/K}$, one has [Jacobi 1829], § 63, p. 231:

$$\Theta\Big(\frac{2Kx}{\pi}\Big) = 1 - 2q\cos 2x + 2q^4\cos 4x - 2q^9\cos 6x + 2q^{16}\cos 8x - \cdots,$$
$$\mathsf{H}\Big(\frac{2Kx}{\pi}\Big) = 2\sqrt[4]{q}\sin x - 2\sqrt[4]{q^9}\sin 3x + 2\sqrt[4]{q^{25}}\sin 5x - 2\sqrt[4]{q^{49}}\sin 7x + \cdots.$$

These formulae are equivalent to Gauss's identity (1) quoted in the introduction. Jacobi deduced from the first one that $\sqrt{\frac{2K}{\pi}} = \Theta(K) = 1+2q+2q^4+\cdots = \sum_{-\infty}^{+\infty} q^{n^2}$. On the other hand, he had established in [Jacobi 1829], § 40, formula (4.) that

$$\frac{2K}{\pi} = 1 + \frac{4q}{1-q} + \frac{4q^3}{1-q^3} + \frac{4q^5}{1-q^5} + \cdots = 1 + 4\sum_{m,n,\ell} \psi(n) q^{2^\ell m^2 n},$$

where $\ell = 0, 1, 2, 3, \ldots$; m, n are odd, and every factor of m, resp. of n, is $\equiv -1$, resp. $\equiv +1$, modulo 4; and $\psi(n)$ denotes the number of factors of n.

Another elliptic identity obtained by Jacobi which is useful here are the following two expressions for $\Big(\dfrac{2K}{\pi}\Big)^2$:[15]

$$1+\frac{8q}{1-q}+\frac{16q^2}{1+q^2}+\frac{24q^3}{1-q^3}+\cdots = 1+8\sum_{p\text{ odd}} \varphi(p)(q^p+3q^{2p}+3q^{4p}+3q^{8p}+\cdots)$$

where $\varphi(p)$ is Jacobi's notation for the sum of the divisors of p. It follows that

$$\Big(\sum q^{n^2}\Big)^2 = 1 + 4\sum_{m,n,\ell} \psi(n) q^{2^\ell m^2 n}$$

[14] Recall from the beginning of §2 above Jacobi's function $\sin\operatorname{am} u$ for the modulus k. Its definition may also be written: $\sin\operatorname{am} u = \varphi \Leftrightarrow u = \int_0^{\varphi} \frac{d\theta}{\sqrt{1-k^2\sin^2\theta}}$.

[15] See [Jacobi 1829], § 40, formulae (8.) and (34.).

and

$$\Big(\sum q^{n^2}\Big)^4 = 1 + 8 \sum_{p \text{ odd}} \varphi(p) q^p + 24 \sum_{p \text{ odd}} \sum_{\nu \geq 1} \varphi(p) q^{2^\nu p}.$$

This gives the number $r_s(t)$ of decompositions of an integer t as a sum of s squares, for $s = 2$ or $s = 4$: $r_2(t) = 0$ unless $t = 2^\ell m^2 n$ with m, resp. n, being congruent to -1, resp. $+1$, modulo 4, and $r_2(2^\ell m^2 n) = 4\,\psi(n)$. Further, $r_4(p) = 8\,\varphi(p)$, if p is odd, whereas $r_4(2^\nu p) = 24\,\varphi(p)$. In particular, $r_4(t)$ is never 0, i.e., every integer n is a sum of 4 squares. Proving the four squares theorem in this way provided an answer to Euler's wish expressed in a letter to Goldbach of May 4, 1748. Jacobi communicated these results to Legendre in a letter of September 9, 1828.

In §42 of his *Fundamenta nova*, Jacobi proved new formulae, giving $r_8(t)$ and $r_6(t)$, respectively:

$$\Big(\frac{2K}{\pi}\Big)^4 = 1 + 16 \sum \frac{n^3 q^n}{(1 + (-1)^{n+1}) q^n} \quad \text{and} \quad \Big(\frac{2K}{\pi}\Big)^3 = 1 + 16 \sum \frac{n^3 q^n}{1 + q^{2n}}.$$

Jacobi returned to these methods in the long paper [Jacobi 1848]. Starting from the fundamental identity (1) (with the notation q, z instead of x, α), he replaced the variable z by some powers of q and obtained a series of identities between infinite products of factors of the type $1 - q^a$, and power series in q. Multiplying two such identities, Jacobi obtained a double series equal to an infinite product. Some infinite products coincide, yielding identities between double series. For instance,

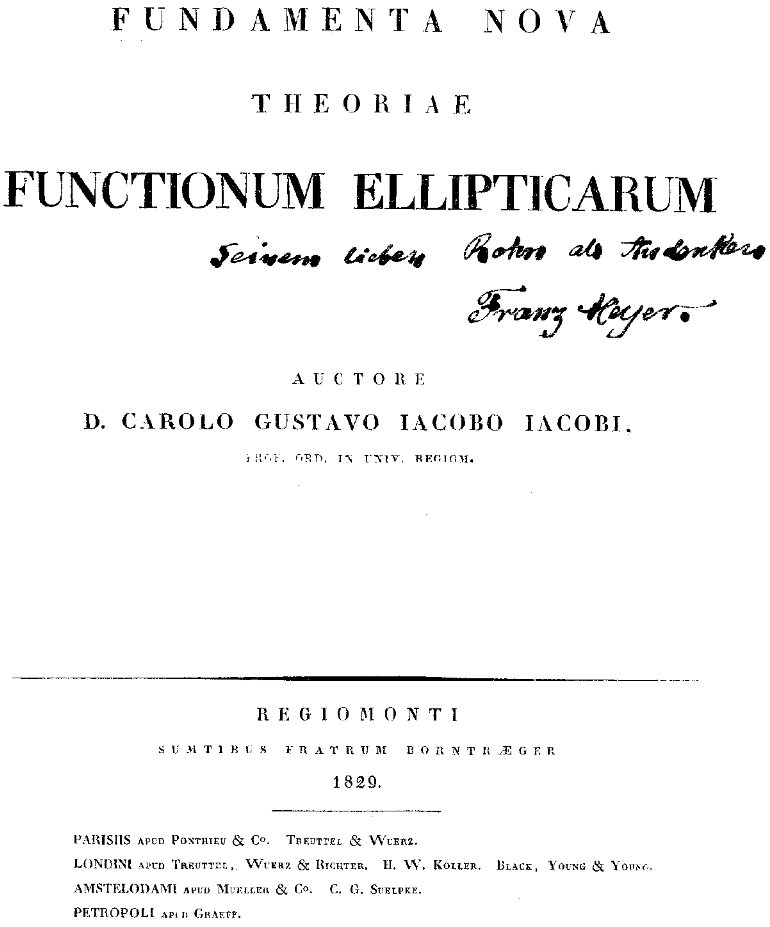
$$\sum_{j,k} (-1)^k q^{m(j^2+k^2)+n(j+k)} = \sum_{j,k} (-1)^{j+k} q^{2m(j^2+k^2)+2nj}.$$

As an application, Jacobi considered the number μ (resp. ν) of solutions of $P = (4m + 1)^2 + 16n^2$ with $m + n$ even (resp. odd), and the number μ' (resp. ν') of solutions of $P = (4m' + 1)^2 + 8n'^2$ with n' even (resp. odd), for P a given integer. He also proved that $\mu - \nu = \mu' - \nu'$. This result corresponds to a theorem of Gauss characterizing the prime numbers $p \equiv 1 \pmod 8$ modulo which 2 is a biquadratic residue. The characterization is in terms of the representations of p by the quadratic forms $aa + 2bb$ or $aa + bb$.

Kronecker also used this type of series in his paper [Kronecker 1860]. He considered, for instance, the function $E(n) = 2F(n) - G(n)$, where F (resp. G) is related to the number of odd classes (resp. all the classes) of binary quadratic forms of determinant $-n$. From the class relations, he deduced that $E(n) + 2E(n-1) + 2E(n-4) + 2E(n-9) + \cdots = \frac{2}{3}\Big(2 + (-1)^n\Big) X(n)$, where $X(n)$ is the sum of the odd divisors of n. Then one has

$$12 \sum E(n) q^n = \frac{1}{\Theta(K)} + \frac{8}{\Theta(K)} \sum \frac{q^{n+1}}{(1 \mp q^{n+1})^2},$$

where $\mp = (-1)^{n+1}$. This is equal to $\Theta(K)^3$, so one obtains a formula relating $r_3(t)$ to the number of classes of discriminant $-n$ as in D.A., art. 291. Kronecker came back to this method in [Kronecker 1875].



FUNDAMENTA NOVA

THEORIAE

FUNCTIONUM ELLIPTICARUM

Seinem lieben Sohne als Andenken
Franz Meyer.

AUCTORE

D. CAROLO GUSTAVO IACOBO IACOBI,

PROF. ORD. IN UNIV. REGIOM.

REGIOMONTI
SUMTIBUS FRATRUM BORNTRÆGER
1829.

PARISIIS apud Ponthieu & C^o. Treuttel & Wuerz.
LONDINI apud Treuttel, Wuerz & Richter. H. W. Koller. Black, Young & Young.
AMSTELODAMI apud Mueller & C^o. C. G. Suelpke.
PETROPOLI apud Graeff.

Fig. IV.2B. Title-page of Carl Gustav Jacob Jacobi's 1829 *Fundamenta nova theoriae functionum ellipticarum* (Private copy)

Hermite proved Kronecker's class relations using the Fourier series of certain products of theta functions, without any recourse to complex multiplication. He published his method in two notes in the *Comptes rendus de l'Académie des sciences de Paris*, [Hermite 1861] and [Hermite 1862]. For instance,[16]

$$\frac{K}{2\pi}\sqrt{\frac{2kK}{\pi}}\,\frac{\mathrm{H}^2(z)\Theta_1(z)}{\Theta^2(z)} = \\ A\Theta_1(z) - q\sqrt[4]{q^{-1}}\cos 2x - q^4\left(\sqrt[4]{q^{-1}} + 3\sqrt[4]{q^{-9}}\right)\cos 3x - \cdots$$

where $z = \frac{2Kx}{\pi}$, and

$$A = \frac{1}{2\pi}\int_0^K \frac{\mathrm{H}^2(z)\Theta_1(z)}{\Theta^2(z)}dz = \sum_{n,a}\frac{\sqrt{q^{2n+1}}}{1-q^{2n+1}}q^{\frac{(2n+1)^2}{4}-a^2} = \sum_N F(N)q^{\frac{N}{4}}.$$

Then Hermite interprets the coefficient $F(N)$ as the number of reduced binary quadratic forms of discriminant $-N$. Indeed, $N = (2n+1)(2n+4b+3) - 4a^2$ is the negative of the discriminant of the quadratic form $(2n+1, 2a, 2n+4b+3)$ or $(2n+1, 2n\mp 2a, 4n+4b+4\mp 4a)$, according as a is strictly smaller or strictly bigger than $\frac{2n+1}{4}$. Letting $x = 0$ in the Fourier series, Hermite finds $\sum_N q^{\frac{N}{4}}\frac{\sum d' - \sum d}{2}$, where the inner summations are extended to the divisors d', d of N such that $d < \sqrt{N} < d'$. Since the left-hand side of the formula is 0, Hermite obtained $\Theta_1(0)\sum F(N)q^{\frac{n}{4}} = \frac{1}{2}\sum \Psi(N)q^{\frac{n}{4}}$, with the notation $\Psi(N) = \frac{\sum d' - \sum d}{2}$. Thus $F(N) + 2F(N-2^2) + 2F(N-4^2) + \cdots = \frac{1}{2}\Psi(N)$.

By an analogous method, Hermite was able to obtain formulae for $r_3(n)$ and $r_5(n)$; see [Hermite 1887].

5. Gauss Sums and Theta Functions

We know that Gauss was conscious of the link between his fundamental relation (1) and the so-called Gauss sums. Augustin Louis Cauchy rediscovered this link [Cauchy 1840], starting from a particular case of an identity already known to Gauss:

$$\sum_{n=-\infty}^{n=+\infty} e^{-\alpha(n+\omega)^2} = \sqrt{\frac{\pi}{\alpha}}\,e^{-\alpha\omega^2}\sum_{n=-\infty}^{n=+\infty} e^{-\frac{\pi^2}{\alpha}(n+\frac{\alpha i\omega}{\pi})^2}.$$

Cauchy obtained it by the Poisson summation formula. He deduced from it the formula

$$\left(\sqrt{\log\frac{1}{x}}\right)\frac{\sum_{n=-\infty}^{n=+\infty} x^{n^2\pi}}{\sum_{n=-\infty}^{n=+\infty} y^{n^2\pi}} = 1, \tag{7}$$

[16] Here, $\Theta_1(x) = 2\sqrt[4]{q}\sin x - 2\sqrt[4]{q^9}\sin 3x + 2\sqrt[4]{q^{25}}\sin 5x - \cdots$.

if x and y are such that $\log x \cdot \log y = 1$, $|x|, |y| < 1$, and $\sqrt{z}$ denotes the determination of the square root with argument in the interval $]-\frac{\pi}{2}, \frac{\pi}{2}]$. Cauchy considered the case in which $-\log x = w^2 + \frac{\lambda i}{\mu}$ with λ, μ rational numbers, and w a real number tending to 0. He proved that the limit of $|\mu w| \sum_{n=-\infty}^{n=+\infty} x^{n^2\pi}$ is equal to the Gauss sum $\frac{1}{2}\sum_{k=0}^{2\mu-1} e^{-k^2\frac{\lambda\pi i}{\mu}} = G(\frac{\lambda i}{\mu})$. In the same way, $G(\frac{\mu}{\lambda i})$ is the limit of $|\mu w| \sum_{n=-\infty}^{n=+\infty} y^{n^2\pi}$, and relation (7) yields $\sqrt{\frac{\lambda i}{\mu}} G(\frac{\lambda i}{\mu}) = G(\frac{\mu}{\lambda i})$ by passing to the limit. Consequently

$$\sqrt{\rho}\,\frac{G(\rho)}{G(\frac{1}{\rho})} = 1 \tag{8}$$

for any purely imaginary rational number ρ. Now Gauss had proved that, for $\mu \equiv 1 \pmod 4$, the quotient $G\Big(\frac{2\lambda i}{\mu}\Big)/\sqrt{\mu}$ is equal to the Jacobi symbol $\Big(\frac{\lambda}{\mu}\Big)$, and we see that the quadratic reciprocity law is a consequence of identity (8). Indeed, (8) yields $G\Big(\frac{2r\lambda i}{\mu}\Big) = \Big(\frac{r}{\mu}\Big)G\Big(\frac{2\lambda i}{\mu}\Big)$ and $G\Big(\frac{2i}{\mu}\Big) = \sqrt{\frac{\mu}{2i}}\,G\Big(\frac{2\mu}{2i}\Big) = \sqrt{\mu}$.

Kronecker established the converse of Cauchy's result in [Kronecker 1880]. From identity (8) he deduces (7) and then the formula for the transformation of theta functions:

$$\vartheta\Big(\frac{\zeta}{\gamma\tau+\delta}, \frac{\alpha\tau+\beta}{\gamma\tau+\delta}\Big) = C\,\Big(\sqrt{\gamma\tau+\delta}\Big)^{\frac{\gamma\zeta^2}{\gamma\tau+\delta}\pi i}\,\vartheta(\zeta,\tau)$$

where $\vartheta(\zeta,\tau) = \sum_{\nu=-\infty}^{+\infty} e^{\frac{\pi i}{4}(\nu^2\tau+4\nu\tau-2\nu)}$, and $\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix} \in \mathrm{SL}(2,\mathbf{Z})$. The constant C equals $G\Big(\frac{\beta i}{\delta}\Big)$, resp. $G\Big(\frac{\alpha i}{\gamma}\Big)$, if $\beta+\delta$ is odd, resp. even. In the proof, Kronecker interchanged an infinite summation and a limit without the slightest justification. He also showed that, when one only knows the absolute value of $G(\rho)$, one has $\rho\Big(\frac{G(\rho)}{G(\frac{1}{\rho})}\Big)^2 = 1$ and it is possible to deduce from this that

$$\log\frac{1}{x}\,\Big(\frac{\sum x^{n^2\pi}}{\sum y^{n^2\pi}}\Big) = 1.$$

The square root is therefore ±1, and the sign is determined by examining the behaviour of this square root when x tends to 0. This is one way to determine the sign of the Gauss sum $G(\rho)$, and to prove the quadratic reciprocity law.

In the same paper, Kronecker also gave a new proof of the identity (1) of Gauss-Jacobi.

6. Kronecker's Limit Formula and the Pell-Fermat Equation

In [Kronecker 1863], Kronecker took the limit values of

$$\sum_{m>0,(m,2P)=1} \left(\frac{P}{m}\right) \frac{1}{m^{1+\rho}} \quad \text{and} \quad \sum_{n>0,(n,2Q)=1} \left(\frac{-Q}{n}\right) \frac{1}{n^{1+\rho}}$$

given by Dirichlet, where P and Q are squarefree and $P > 1$. Multiplying both formulae yields formula (9):

$$\lim_{\rho\to 0} \sum \left(\frac{P}{m}\right) \frac{1}{m^{1+\rho}} \sum \left(\frac{-Q}{n}\right) \frac{1}{n^{1+\rho}} = \frac{\pi}{4\sqrt{D}} H(-D)H(P)\log(T + U\sqrt{P}),$$

where $D = PQ$, $H(m)$ denotes the class number of properly primitive binary quadratic forms of discriminant m (with the convention that $H(-1) = \frac{1}{2}$), and (T, U) is a minimal solution of the Pell-Fermat equation $T^2 - PU^2 = 1$. If D is squarefree and $\equiv 1 (\text{mod } 4)$, then

$$\sum_m \sum_n \frac{\left(\frac{P}{m}\right)\left(\frac{-Q}{n}\right)}{(mn)^{1+\rho}} = \left(1 - \frac{\left(\frac{2}{R}\right)}{2^{2+\rho}}\right) \sum_{(a,b,c)} \left[\frac{a}{R}\right] \sum_{(x,y)} \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\rho}} \tag{10}$$

where x, y vary over non-zero integers, $R = P$ if $P \equiv 1$ (mod 4) and $R = Q$ if $P \equiv 3$ (mod 4). Here (a, b, c) is a variable, properly primitive quadratic form of discriminant $-D$, and $\left[\frac{a}{R}\right] = \left(\frac{a'}{R}\right)$ (Legendre symbol) with (a', b', c') a form equivalent to (a, b, c) such that a' is prime to R. Kronecker proved formulae of this type in [Kronecker 1864] and in part I, from 1885, of [Kronecker 1883–1890].

In order to compute (T, U) from (9), one is reduced to computing the limit of the right-hand side of (10). Kronecker showed that

$$\begin{aligned}\lim_{\rho\to 0} \sum_{x,y} \frac{e^{2\pi i(\alpha x+\tau y)}}{(ax^2 + 2bxy + cy^2)^{1+\rho}} &= \frac{2\sigma^2\pi^2}{a} + \frac{\pi}{3\sqrt{D}} \log \frac{1}{4\pi^2} \vartheta'(0, w_1)\vartheta'(0, w_2) \\ &\quad - \frac{\pi}{\sqrt{D}} \log \vartheta(\tau + \sigma w_1, w_1)\vartheta(\tau + \sigma w_2, w_2).\end{aligned}$$

Here we have used the notation $\vartheta(z, w) = -i \sum_{n=-\infty}^{n=+\infty} (-1)^n e^{(n+\frac{1}{2})^2 w\pi i + (2n+1)z\pi i}$ with $w_1 = \dfrac{-b + i\sqrt{D}}{a}$ and $w_2 = \dfrac{b + i\sqrt{D}}{a}$. Kronecker obtains from this the formula (11):

$$\begin{aligned}\lim_{\rho\to 0} \left(\sum_{x,y} \frac{1}{(ax^2 + 2bxy + cy^2)^{1+\rho}} - \sum_{x,y} \frac{1}{(a'x^2 + 2b'x + c'y^2)^{1+\rho}}\right) \\ = \frac{2\pi}{3\sqrt{D}} \log \frac{a\sqrt{a}\vartheta'(0, w_1')\vartheta(0, w_2')}{a'\sqrt{a'}\vartheta'(0, w_1)\vartheta(0, w_2)}\end{aligned}$$

which gives

$$H(-Q)H(P)\log(T+U\sqrt{P})=\frac{2}{3}\Bigl(2-\Bigl(\frac{2}{R}\Bigr)\Bigr)\sum_{(a,b,c)}\Bigl[\frac{a}{R}\Bigr]\log\frac{a\sqrt{a}}{\vartheta'(0,w_1)\vartheta(0,w_2)},$$

with an approximate value $\Bigl(2-\Bigl(\frac{2}{R}\Bigr)\Bigr)\sum_a\Bigl[\frac{a}{R}\Bigr]\Bigl(\frac{\pi\sqrt{D}}{3a}+\log a\Bigr)$. Kronecker published the proofs of these limit formulae in the first seven installments of [Kronecker 1883–1890]. He used the function

$$\Lambda(\sigma,\tau,w_1,w_2)=(4\pi^2)^{\frac{1}{3}}e^{\tau^2(w_1+w_2)\pi i}\frac{\vartheta(\sigma+\tau w_1,w_1)\vartheta(\sigma-\tau w_2,w_2)}{(\vartheta'(0,w_1)\vartheta'(0,w_2))^{\frac{1}{3}}}$$

and first proved that

$$\log\Lambda(\sigma,\tau,w_1,w_2)=\frac{-1}{2\pi}\lim_{h\to\infty}\lim_{k\to\infty}\sum_{m=-h}^{+h}\sum_{n=-k}^{+k}\frac{e^{2(m\sigma+n\tau)\pi i}}{a_0m^2+b_0mn+c_0n^2},$$

where $(m,n)\neq(0,0)$, $a_0i=\dfrac{w_1w_2}{w_1+w_2}$, $b_0i=\dfrac{w_1-w_2}{w_1+w_2}$, $c_0i=\dfrac{-1}{w_1+w_2}$, and σ, τ are chosen so that the real parts of $(\tau w_1+\sigma)i$, $w_1-(\tau w_1+\sigma)i$, $(\tau w_2-\sigma)i$, $w_2-(\tau w_2-\sigma)i$ are negative. From this formula, Kronecker deduced

$$\begin{aligned}\log\Lambda(\sigma,\tau,w_1,w_2)&=\frac{-1}{2\pi}\lim_{\rho\to 0}\sum_{m,n=-\infty}^{+\infty}\frac{e^{2(m\sigma+n\tau)\pi i}}{(a_0m^2+b_0mn+c_0n^2)^{1+\rho}}\\&=\frac{-\sqrt{\Delta}}{2\pi}\lim_{\rho\to 0}\sum_{m,n=-\infty}^{+\infty}\frac{e^{2(m\sigma+n\tau)\pi i}}{(a_0m^2+b_0mn+c_0n^2)^{1+\rho}}\end{aligned}$$

where $(m,n)\neq(0,0)$, $a=a_0\sqrt{\Delta}$, $b=b_0\sqrt{\Delta}$, $c=c_0\sqrt{\Delta}$, so that $4ac-b^2=\Delta>0$, and $w_1=\dfrac{-b+i\sqrt{\Delta}}{2c}$, $w_2=\dfrac{b+i\sqrt{\Delta}}{2c}$. From this he finally obtained[17] (11) and an elliptic formula for

$$\lim_{\rho\to 0}\Bigl(-\frac{1}{\rho}+\sum_{m,n}\frac{2\pi}{(a_0m^2+b_0mn+c_0n^2)^{1+\rho}}\Bigr).$$

Kronecker explicitly computed some numerical examples: for $P=D=5,13,37$, he finds that $T+U\sqrt{P}$ is approximately $\frac{1}{8}e^{\frac{1}{2}\pi\sqrt{D}}$ – the exact values being respectively $2+\sqrt{5}$, $18+5\sqrt{13}$, $882+145\sqrt{37}$. For $P=D=17,97$, the exact values are respectively $4+\sqrt{17}$ and $5604+569\sqrt{97}$, and Kronecker's approximations are $\dfrac{2}{9}e^{\frac{5}{18}\pi\sqrt{17}}$, $\dfrac{2}{49}e^{\frac{17}{42}\pi\sqrt{97}}$. For $D=85$, one may choose $(P,Q)=(85,1)$, $(17,5)$ or $(5,17)$. The corresponding values of $T+U\sqrt{P}$ are respectively $378+41\sqrt{85}$, $4+\sqrt{17}$, $2+\sqrt{5}$, and the approximate values are $\dfrac{1}{8}e^{\frac{3}{10}\pi\sqrt{85}}$, $\dfrac{1}{\sqrt{5}}e^{\frac{1}{10}\pi\sqrt{85}}$, $e^{\frac{1}{20}\pi\sqrt{85}}$.

[17] See parts XIII–XXI of [Kronecker 1883–1890].

7. Diophantine Equations

In 1835, Jacobi published a short note, [Jacobi 1835], in which he explained how to construct solutions of a Diophantine equations of the type $y^2 = f(x)$, for a polynomial f, using the addition theorem for elliptic integrals or Abel's theorem.

For instance, if f is a polynomial of degree 3 or 4 , the integral $\Pi(x) = \int_0^x \frac{dt}{\sqrt{f(t)}}$ is an elliptic integral of the first kind, and the addition theorem says that, for given $x_1, x_2, \ldots, x_n$ and $m_1, m_2, \ldots, m_n$ integers, $\sum_{i=1}^n m_i \Pi(x_i) = \Pi(x)$, where x and $\sqrt{f(x)}$ are rational functions of $x_1, x_2, \ldots, x_n$ and $\sqrt{f(x_1)}$,$\sqrt{f(x_2)}$,..., $\sqrt{f(x_n)}$. So if $(x_1, y_1), (x_2, y_2), \ldots, (x_n, y_n)$ are known solutions of the Diophantine equation $y^2 = f(x)$, then $(x, f(x))$ is a new one given by the addition theorem.

Jacobi expressed his conviction that Euler had already known this relation between elliptic integrals and Diophantine equations. Indeed, the computation made by Euler in [Euler 1780] to transform a Diophantine equation of the type $z^2 = f(x)$, f a polynomial of degree 4, into the canonical form $\Phi(x, y) = 0$, with Φ of degree 2 in x and y, and such that $\Phi(x, y) = \Phi(y, x)$, is exactly the same as the computation he made in 1757 in order to obtain the addition theorem for elliptic integrals. The idea is to determine $\Phi(x, y) = A(x)y^2 + 2B(x)y + C(x)$ in such a way that its discriminant $B^2 - AC$ equals $f(x)$. Then $\Phi(x, y) = 0$ gives $\frac{\partial \Phi}{\partial y}(x, y) = \pm 2\sqrt{f(x)}$, and $\frac{dx}{\sqrt{f(x)}} \pm \frac{dy}{\sqrt{f(y)}} = 0$. If a rational solution (x, y) of the equation $\Phi(x, y) = 0$ is known, then $y = \frac{-B(x) + z}{A(x)}$, with $z = \sqrt{f(x)}$, so z is rational and one has a second solution: $y_1 = \frac{-B(x) - z}{A(x)}$. Then, from (x, y_1), with $x = \frac{-B(y_1) + t}{A(y_1)}$ and $t = \sqrt{f(y_1)}$, one deduces $x_1 = \frac{-B(y_1) - t}{A(y_1)}$, etc.

But Euler did not make this process explicit. Nevertheless, ever since Leibniz, the change of variables which transforms $\frac{dx}{\sqrt{f(x)}}$, for a polynomial f of degree 2, into a rational differential form was explicitly referred to as the method used to solve the Diophantine equation $z^2 = f(x)$.

The geometric interpretation of these Diophantine problems as the search for rational points on algebraic curves of genus 0 or 1, already known to Newton, had to wait until later works, in particular [Sylvester 1879–1880], [Hilbert, Hurwitz 1890] and [Poincaré 1901].

8. Conclusion

We have tried to show the beginnings of the intervention of the theory of elliptic functions in arithmetic: complex multiplication, q-calculus, and the functional equation for the theta functions, Kronecker's limit formula, addition theorem and Diophantine analysis. The germs of most of these ideas were already present in Gauss's work. Gauss clearly saw the necessity to use methods not restricted to the consideration of natural numbers, in order to prove properties of natural numbers.

After Abel and Jacobi, the mathematicians who developed these theories in the first two thirds of the XIX$^{\text{th}}$ century were Eisenstein, Kronecker, and Hermite. We saw the particular importance of Kronecker's work which vindicates this author's insistence on formulae as the essence of mathematics.

At the end of the XIX$^{\text{th}}$ century, and throughout the XX$^{\text{th}}$ century, the theories mentioned have continually developed and this growth continues to this day. This is a testimony to the continuing presence of Gauss's work.

References

Abel, Niels Henrik. 1827–1828. Recherches sur les fonctions elliptiques. *Journal für die reine und angewandte Mathematik* 2, 101–181; 3, 160–190. Repr. in [Abel 1881], pp. 263–388.

———. 1828. Solution d'un problème général concernant la transformation des fonctions elliptiques, *Astronomische Nachrichten* 6, no 138. Repr. in [Abel 1881], pp. 403-428.

———. 1829. Addition au mémoire précédent. *Astronomische Nachrichten* 7, n$^{\text{o}}$ 147. Repr. in [Abel 1881], pp. 429-443.

———. 1881. *Œuvres complètes*, ed. L. Sylow, S. Lie, vol. I. Christiania: Grøndahl.

Cauchy, Augustin-Louis. 1840. Mémoire sur la théorie des nombres. *Mémoires de l'Académie des sciences de Paris* 17, Notes IX–XI, 589–665. Repr. in *Œuvres complètes*, 1$^{\text{st}}$ ser., vol. 3, pp. 293–359. Paris: Gauthier-Villars. 1882.

Eisenstein, Gotthold. 1845. Applications de l'algèbre à l'arithmétique transcendante. *Journal für die reine und angewandte Mathematik* 29, 174–184. Repr. in [Eisenstein 1975], pp. 291–298.

———. 1846. Beiträge zur Theorie der elliptischen Functionen I. Ableitung des biquadratischen Fundamentaltheorems aus der Theorie der Lemniscatenfunctionen, nebst Bemerkungen zu den Multiplications- und Transformationsformeln. *Journal für die reine und angewandte Mathematik* 30, 185–210. Repr. in [Eisenstein 1975], pp. 299–324.

———. 1847. Beiträge zur Theorie der elliptischen Functionen VI. Genaue Untersuchung der unendlichen Doppelproducte, aus welchen die elliptischen Functionen als Quotienten zusammengesetzt sind. *Journal für die reine und angewandte Mathematik* 35, 153–274. Repr. in [Eisenstein 1975], pp. 357–478.

———. 1975. *Mathematische Werke*, vol. 1. New York: Chelsea.

Euler, Leonhard. 1780. I: De insigni promotione analysi Diophanteae; II: De resolutione huius equationis $0 = a + bx + cy + dxx + exy + fyy + gxxy + hxyy + ixxyy$ per numeros rationales; III: Methodus nova et facilis formulas cubicas et biquadraticas ad quadratum reducendi. *Mémoires de l'académie des sciences de Saint-Pétersbourg* 11 (1830), 1–11; 58–68; 69–91. Repr. in *Opera Omnia*, ed. A. Speiser, L. G. du Pasquier, H. Brandt, E. Trost. Series prima, vol. 5. *Commentationes arithmetica*, ed. R. Fueter, vol. IV, pp. 82–93; pp. 146–156; pp. 157–181. Thur, Leipzig: Orell Füssli; Leipzig, Berlin: Teubner, 1944.

Euler & Goldbach. 1965. *Briefwechsel 1729–1764*, ed. A.P. Yuškevič, E. Winter, pp. 288–291. Berlin: Akademie-Verlag.

Fueter, Rudolf. 1914. Abelsche Gleichungen in quadratisch-imaginären Zahlkörpern. *Mathematische Annalen* 75, 177–255.

GAUSS, Carl Friedrich. 1796–1814. Mathematical Diary. Original manuscript in Latin: Handschriftenabteilung Niedersächsische Staats- und Universitätsbibliothek Göttingen, Cod. Ms. Gauss Math. 48 Cim. Ed. (Latin with German annotations): Abdruck des Tagebuchs (Notizenjournals), *Werke*, X.1, pp. 483–575. Leipzig: Teubner, 1917. French annotated transl. by P. Eymard, J.-P. Lafon: Le journal mathématique de Gauss. *Revue d'histoire des sciences et de leurs applications* 9 (1956), 21–51. English commented transl. J. Gray: A commentary on Gauss's mathematical diary, 1796-1814, with an English translation. *Expositiones Mathematicae* 2 (1984), 97–130. Repr. in [Dunnington 2004], pp. 409-505. German transl. E. Schuhmann, with a historical introduction by K.-R. Biermann, and annotations by H. Wußing und O. Neumann: *Mathematisches Tagebuch 1796–1814*. 5th ed. Ostwalds Klassiker der exakten Wissenschaften 256. Leipzig: Akademische Verlagsgesellschaft Geest & Portig; Frankfurt am Main, Thun: Harri Deutsch, 2005.

———. 1808. Summatio quarundam serierum singularium. *Commentationes societatis regiae scientiarum Gottingensis recentiores* 1 (1811). Repr. in [Gauss 1863], pp. 11–45.

———. 1828–1832. Theoria residuorum biquadraticorum. *Commentationes societatis regiae scientiarum Gottingensis recentiores* 6 (1828), 27–58; 7 (1832), 89–148. Repr. in [Gauss 1863], pp. 67-148.

———. 1863. *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universitäts-Druckerei.

———. 1866. *Werke*, vol. III, *Analysis*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universitäts-Druckerei.

———. 1917. *Werke*, vol. X.1, *Nachträge zur reinen Mathematik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Leipzig: Teubner.

HERGLOTZ, Gustav. 1921. Zur letzten Eintragung im Gauß'schen Tagebuch. *Berichte über die Verhandlungen der Sächsischen Akademie der Wissenschaften Math.-phys. Klasse* 73, 271–276. Repr. in *Gesammelte Schriften*, ed. H. Schwerdtfeger, pp. 415–420. Göttingen: Vandenhoeck 1979.

HERMITE, Charles. 1859. Sur la théorie des équations modulaires. *Comptes rendus de l'Académie des sciences de Paris* 48, 940–947, 1079–1084, 1095–1102; 49, 16–24, 110–118, 141–144. Repr. in [Hermite 1905–1917], vol. 2, pp. 38–82.

———. 1861. Lettre adressée à M. Liouville sur la théorie des fonctions elliptiques et ses applications à l'arithmétique. *Comptes rendus de l'Académie des sciences de Paris* 53, 214–228. Repr. in *Journal de mathématiques pures et appliquées* 2$^{\text{nd}}$ ser. 7 (1862), 25–40. Repr. in [Hermite 1905–1917], vol. 2, pp. 109–124.

———. 1862. Sur les théorèmes de M. Kronecker relatifs aux formes quadratiques. *Comptes rendus de l'Académie des sciences de Paris* 55, 11–85. Repr. in *Journal de mathématiques pures et appliquées* 2$^{\text{nd}}$ ser. 9 (1864), 145–159. Repr. in [Hermite 1905–1917], vol. 2, pp. 241–254.

———. 1886. Remarques sur les formes quadratiques de déterminant négatif. *Bulletin des sciences mathématiques*, 2$^{\text{nd}}$ ser. 10, 23–30. Repr. in [Hermite 1905–1917], vol. 4, pp. 215–222.

———. 1887. Remarques arithmétiques sur quelques formules de la théorie des fonctions elliptiques. *Journal für die reine und angewandte Mathematik* 100, 51–65. Repr. in [Hermite 1905–1917], vol. 4, pp. 223–238.

———. 1905–1917. *Œuvres*, ed. E. Picard. 4 vols. Paris: Gauthier-Villars.

Hilbert, David, Hurwitz, Adolf. 1890–1891. Über die diophantischen Gleichungen vom Geschlecht Null, *Acta Mathematica* 14, 217–224. Repr. in D. Hilbert, *Gesammelte Abhandlungen*, vol. 2. pp. 258–263. Berlin, Heidelberg: Springer 1933; repr., 1970. Repr. in A. Hurwitz, *Mathematische Werke*, vol. 2, pp. 116–121. Basel, Stuttgart: Birkhäuser, 1933; repr., 1963.

Jacobi, Carl Gustav Jakob. 1829. *Fundamenta nova theoriae functionum ellipticarum.* Königsberg: Borntraeger. Repr. in *Gesammelte Werke*, vol. 1, ed. C.W. Borchardt, pp. 49–138. Berlin: Reimer, 1881.

———. 1835. De usu theoriae integralium ellipticorum et integralium abelianorum in analysi diophantea. *Journal für die reine und angewandte Mathematik* 13, 353–355. Repr. in *Gesammelte Werke*, vol. 2, ed. K. Weierstrass, pp. 53-55. Berlin: Reimer, 1882.

———. 1848. Über unendliche Reihen, deren Exponenten zugleich in zwei verschiedenen quadratischen Formen enthalten sind. *Journal für die reine und angewandte Mathematik* 37, 61–94, 221–254. Repr. in *Gesammelte Werke*, vol. 2, ed. K. Weierstrass, pp. 219–288. Berlin: Reimer, 1882.

———. 1881. De multiplicatione functionum ellipticarum per quantitatem imaginariam pro certo quodam modulorum systemate. In *Gesammelte Werke*, ed. C.W. Borchardt, vol. 1, pp. 489–496. Berlin: Reimer.

Jacobi & Legendre. 1869. Correspondance mathématique entre Legendre et Jacobi, ed. C.W. Borchardt. *Journal für die reine und angewandte Mathematik* 80, 205–279. Repr. in C. Jacobi, *Gesammelte Werke*, vol. 1, ed. C.W. Borchardt, pp. 387–461. Berlin: Reimer 1881. Repr., German transl. and comment. in *Korrespondenz A.-M. Legendre – C.G.J. Jacobi*, ed. H. Pieper. Stuttgart, Leipzig: Teubner, 1998.

Joubert, Charles. 1860. *Sur la théorie des fonctions elliptiques et son application à la théorie des nombres*. Paris: Mallet-Bachelier.

Kronecker, Leopold. 1853. Über die algebraisch auflösbaren Gleichungen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 365-374. Repr. in [Kronecker 1895–1931], vol. 4, pp. 3–11.

———. 1857. Über die elliptischen Functionen, für welche complexe Multiplication stattfindet. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 455–460. Repr. in [Kronecker 1895–1931], vol. 4, pp. 179–183.

———. 1860. Über die Anzahl der verschiedenen Classen quadratischer Formen von negativer Derterminante. *Journal für die reine und angewandte Mathematik* 57, 248–255. Repr. in [Kronecker 1895–1931], vol. 4, pp. 185–195.

———. 1862. Über die complexe Multiplication der elliptischen Functionen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 363–372. Repr. in [Kronecker 1895–1931], vol. 4, pp. 207–217.

———. 1863. Über die Auflösung der Pellschen Gleichung mittels elliptischer Functionen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 44–50. Repr. in [Kronecker 1895–1931], vol. 4, pp. 219–225.

———. 1864. Über den Gebrauch der Dirichletschen Methoden in der Theorie der quadratischen Formen, *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 285–303. Repr. in [Kronecker 1895–1931], vol. 4, pp. 229–244.

———. 1875. Über quadratische Formen von negativer Determinante. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 223–236. Repr. in [Kronecker 1895–1931], vol. 4, pp. 247–259.

———. 1877. Über Abelsche Gleichungen, *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 845–851. Repr. in [Kronecker 1895–1931], vol. 4, pp. 63–71.

———. 1880. Über den vierten Gauss'schen Beweis des Reciprocitätsgesetzes für die quadratischen Reste. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 686–698, 854–860. Repr. in [Kronecker 1895–1931], vol. 4, pp. 277–294.

———. 1883–1890. Zur Theorie der elliptischen Functionen. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 1883: 497–506, 525–590; 1885: 761–784; 1886: 701–780; 1889: 53–63, 123–135, 199–220, 255–175, 309–317; 1890: 99–120, 123–130, 219–241, 307–318, 1025–1029. Repr. in [Kronecker 1895–1931], vol. 4, pp. 347–395; vol. 5, pp. 3–132.

———. 1895–1931. *Werke*, ed. K. Hensel. 5 vols. Leipzig: Teubner.

Poincaré, Henri. 1901. Sur les propriétés arithmétiques des courbes algébriques. *Journal de Mathématiques pures et appliquées* 5th ser. 7, 161–233. Repr. in *Œuvres*, vol. 5, ed. A. Châtelet. pp. 483–550. Paris: Gauthier-Villars, 1950.

Smith, Henry John Stephen. 1859–1865. Report on the Theory of Numbers. *Report of the British Association for the Advancement of Science* 1859, 228-267; 1860, 120–169; 1861, 292–340; 1862, 503–526; 1863, 768–786; 1865, 322–375. Repr. in *The Collected Mathematical Papers*, ed. J.W.L. Glaisher, vol. 1. Oxford: Clarendon Press, 1894.

Sylvester, James Joseph. 1858. Note on the algebraic theory of derivative points of curves of the third degree. *Philosophical Magazine* XVI, 116–119. Repr. in *The Collected Mathematical Papers*, ed. H. F. Baker, vol. 2, pp. 107–109. Cambridge: Cambridge University Press, 1908.

———. 1879–1880. On certain ternary cubic-form equations. *American Journal of Mathematics* 2 (1879), 280–285, 357–393; 3 (1880), 58–88, 179–189. Repr. in *The Collected Mathematical Papers*, ed. H. F. Baker, vol. 3, pp. 312–391. Cambridge: Cambridge University Press, 1909.

Takagi, Teiji. 1920. Über eine Theorie des relativ Abel'schen Zahlkörpers. *Journal of the College of Science, Tokyo Imperial University* 41, art. 9, 133 pp. Repr. in *Collected Papers*, ed. Sh. Iyanaga, K. Iwasawa, K. Kodaira, K. Yosida, pp. 73–167. Tokyo, Berlin, etc.: Springer, 1990.

Weber, Heinrich. 1891. *Elliptische Funktionen und algebraische Zahlen*. Braunschweig: Vieweg.

———. 1897–1898. Über Zahlengruppen in algebraischen Körpern. *Mathematische Annalen* 48 (1897), 433–473; 49 (1897), 83–100; 50 (1898), 1–26.

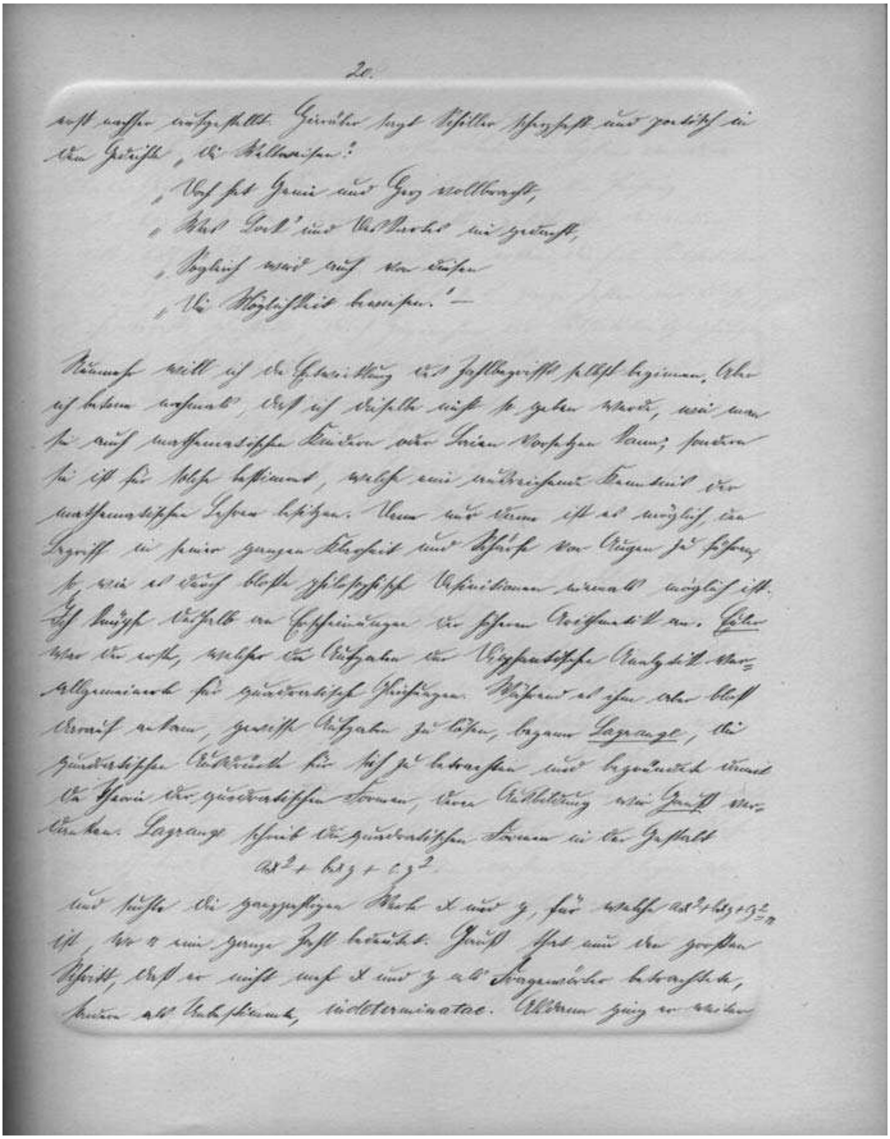
———. 1908. *Lehrbuch der Algebra*, vol. 3. Braunschweig: Vieweg.

Part V

Numbers as Model Objects of Mathematics

Es gibt Gleichungen, die keine Anzahl zur Lösung haben. … Von hier aus nimmt KRONECKER *den ihm eigenthümlichen Weg: … Es wird eine solche Gleichung, die allerdings eine unvollziehbare Aufgabe darstellt, aber darum durchaus nicht sinnlos ist, gleichwohl als sinnlos betrachtet und ihr damit, dass sie einer anderen Aufgabe, nämlich der in jener Congruenz involvirten … gleichwerthig gesetzt wird, ein Sinn allererst beigelegt.*

Benno Kerry, 1889



20.

erst nachher entgegengestellt. Darüber sagt Schiller scherzhaft und zugleich in dem Gedichte „Die Weltweisen":

„Doch hat Genie und Herz vollbracht,
„Was Lock' und Des Cartes nie gedacht,
„Sogleich wird auch von diesen
„Die Möglichkeit bewiesen." —

Nunmehr will ich die Entwicklung des Zahlbegriffs selbst beginnen. Aber ich bitte zu bemerken, daß ich dieselbe nicht so geben werde, wie man sie auch mathematischen Kindern oder Laien vortragen kann; sondern sie ist für solche bestimmt, welche ein umfassendes Verständniß der mathematischen Lehren besitzen. Nur und dann ist es möglich, den Begriff in seiner ganzen Klarheit und Schärfe vor Augen zu führen, so wie es durch bloße philosophische Definitionen niemals möglich ist. Ich knüpfe deshalb an Erscheinungen der höheren Arithmetik an. Euler war der erste, welcher die Aufgaben der Diophantischen Analysis verallgemeinerte für quadratische Gleichungen. Während es ihm aber bloß darauf ankam, gewisse Aufgaben zu lösen, begann Lagrange, die quadratischen Ausdrücke für sich zu betrachten und begründete damit die Theorie der quadratischen Formen, deren Ausbildung wir Gauß verdanken. Lagrange schrieb die quadratischen Formen in der Gestalt

$$ax^2 + bxy + cy^2$$

und suchte die ganzzahligen Werthe x und y, für welche $ax^2+bxy+cy^2 = n$ ist, wo n eine ganze Zahl bedeutet. Gauß that nun den großen Schritt, daß er nicht mehr x und y als Fragewörter betrachtete, sondern als Unbestimmte, indeterminatae. Alsdann ging er weiter

Fig. V.1A. Kronecker's last lecture course:
On the concept of number
(Courtesy of the Bibliothèque de l'IRMA, Strasbourg)

V.1

The Concept of Number from Gauss to Kronecker

JACQUELINE BONIFACE

Nineteenth-century mathematics developed "under the sign of number," in David Hilbert's words.[1] The starting point of this development, as stated by Hilbert in the preface of the so-called *Zahlbericht*, [Hilbert 1897], is that a fact in function theory is considered to be proved only if, ultimately, it could be expressed as relations between rational integers. Hilbert explained that Dedekind's and Weierstrass's definitions of arithmetical fundamental concepts, as well as Cantor's numerical sets, were realizations of this principle. Thus, the XIX$^{\text{th}}$ century witnessed a change in the hierarchical order of mathematical domain: geometry, considered since Euclid as a model of rigour and on which the emerging function theory was still founded in the XVIII$^{\text{th}}$ century, lost precedence to arithmetic. Such a change is attributed to the development of function theory in the XVIII$^{\text{th}}$ century and at the beginning of the XIX$^{\text{th}}$, as well as to the emergence of non-Euclidean geometries; both generated new demands that classical geometric proofs could no longer satisfy. Such proofs were beginning to appear as simple "confirmations" (*Gewissmachungen*), in Bernard Bolzano's words, and opposed to "justifications" (*Begründungen*):

> If one considers that the proofs of science should not merely be confirmations, but rather justifications, i.e., presentations of the objective reason for the truth concerned, then it is self-evident that the strictly scientific proof, or the objective reason, of a truth which holds equally for *all* quantities, whether in space or not, cannot possibly lie in a truth which holds merely for quantities which are in *space*.[2]

[1] See [Hilbert 1897], p. v, or [Hilbert 1932], p. 66: *Es kommt endlich hinzu, daß, wenn ich nicht irre, überhaupt die moderne Entwickelung der reinen Mathematik vornehmlich* unter dem Zeichen der Zahl *geschieht.*

[2] [Bolzano 1817], p. 7, transl. [Russ 1980], p. 160, and [Ewald 1996], vol. 1, p. 228: *Denn in der That, wer immer bedeutet, dass die Beweise in der Wissenschaft keineswegs blosse*

Frege expressed analogous requirement for proofs. They have not only to bring moral conviction (*eine bloß moralische Überzeugung*), but also to found truths, i.e. here, to establish the deductive chain leading from axioms or theorems to new truths.

> The proof has not only for an aim to set a proposition free of doubt, but also to get an insight into the relative dependence of truths.[3]

At the same time, the need became apparent to define more rigorously the basic concepts of the theory (those of function, of limit, of continuity, etc.). And it was towards arithmetic that mathematicians turned, persuaded they would find in it the rigour now disputed in geometry. But did arithmetic keep its leading place? Analysis, having gained some legitimacy through its arithmetization, could very well at the same time have incorporated arithmetic. For it is indeed an incorporation of arithmetic by analysis, or at least a subordination of arithmetic to the needs of analysis, which is found in the works of mathematicians such as Weierstrass and his followers, and which shaped the dominant tendency of the time. However, this subordinate role given to arithmetic was not accepted by all of Weierstrass's contemporaries. Kronecker in particular rejected it strongly and, if he participated in the trend of arithmetization, it was in an opposite direction to that of Weierstrass's school. The first aim of this article will be to highlight that the arithmetization of mathematics along the lines suggested by Weierstrass, proceeds through extension of the concept of number and thus of the domain of arithmetical objects. It will be shown, moreover, that this procedure is generally considered by mathematicians and philosophers alike, as paradigmatic of the development of modern mathematics. It will also appear that, through his concept of number and his position concerning imaginaries, Gauss can be considered as initiating this trend. Our second aim will be to present another direction in the arithmetization of mathematics, proposed by Kronecker, and to assess Gauss's contribution to the Kroneckerian solution. The fact that Gauss initiated the dominant trend did not prevent Kronecker from using some of Gauss's calculation methods to carry out his own undertaking:

> Because Gauss is a true scientific prophet, the concepts he finds in the depths of science go beyond the goal for which they have been established.[4]

Gewissmachungen, sondern vielmehr Begründungen d.h. Darstellungen jenes objectiven Grundes, den die zu beweisende Wahrheit hat, seyn sollen: dem leuchtet von selbst ein, dass der echt wissenschaftliche Beweis, oder der objective Grund einer Wahrheit, welche von allen Grössen gilt, gleich viel, ob sie im Raume sind, unmöglich in einer Wahrheit liegen könne, die bloss von Grössen, welche im Raume sind, gilt.

[3] [Frege 1884/1988], p. 14: *Der Beweis hat eben nicht nur den Zweck, die Wahrheit eines Satzes über jeden Zweifel zu erheben, sondern auch den, eine Einsicht in die Abhängigkeit der Wahrheiten von einander zu gewähren.*

[4] [Kronecker 1891], lesson 11, p. 57, in [Boniface, Schappacher 2001], p. 261: *Weil Gauss ein echter Prophet der Wissenschaft ist, deshalb reichen die Begriffe, die er aus der Tiefe der Wiessenschaft schöpft, weit hinaus über den Zweck, zu welchem sie aufgestellt wurden.*

1. The Arithmetization of Analysis: A Paradigm of the Development of Modern Mathematics

The expression "arithmetization of mathematics," introduced by Felix Klein, usually refers to the movement which took place in the second half of the XIX$^{\text{th}}$ century and aimed at giving to mathematics, and first of all to analysis, an arithmetical foundation.[5] The purpose was, as we indicated in the introduction, to define more rigorously the basic concepts of analysis, and in particular irrational numbers, only justified, until then, by geometrical considerations. Mainly German and French mathematicians took part in this trend, and Weierstrass is generally considered as their leader. One usually recalls from this trend, besides the definition of irrational numbers by Weierstrass, those given by Cantor by means of so-called "Cauchy sequences" and by Dedekind with the "cuts" named after him. But, for these mathematicians, the purpose was not only to define analytical concepts in terms of integers, but also to promote analysis as an autonomous branch of mathematics by extracting it from the field of geometry, and to give the status of number to irrational and complex magnitudes. This meant including these new numbers in an extension of rational numbers, itself already considered as an extension of the domain of integers.

Charles Méray, who was the first to publish a coherent theory of irrational numbers, defined, in the same spirit, mathematical analysis as the "general science of numbers."[6] It includes arithmetic and analysis strictly speaking (i.e., general theory of functions). Arithmetic deals with "special properties of integer (and fractional) numbers." Analysis stricly speaking includes algebra, which is the theory of rational and algebraic irrational functions, and infinitesimal analysis, which is "the science of general properties given to functions by their fundamental property: to be all and always representable by power series."[7] For Méray, mathematical analysis is the whole of pure mathematics, geometry being classified, beside mechanics and physics, within applied mathematics. Like Bolzano and Frege, Méray critized the use of geometrical concepts in the proofs of analytical propositions. He fought against the importance given to continuity, considered in classical treatises of analysis as "a sufficient reason of all analytical facts," [Méray 1894], preface, p. ix, n. 3. In so doing, he agreed with a lot of his contemporaries, but he disagreed with those who, according to him, considered functions as "pure beings of reason." Those mathematicians, he said, took interest in functions that are "discontinuous, without derivative, non-integrable, etc., functions, *one only meets in metaphysical dissertations*," [Méray 1894], preface, p. xiii. Instead of considering functions as "pure beings of reason," Méray considered them as "expressions of calculation," according to Lagrange's definition. He replaced the property of continuity by the property of being expressible as a power series.

[5] On this movement and its roots, see chap. III. 2 by J. Ferreirós and chap. V.2 by B. Petri and N. Schappacher [Editors' note].

[6] See [Méray 1892], p. 105; [Méray 1894], p. 1. On Méray, see [Boniface 2002], chap. 1.

[7] [Méray 1894], p. 2: ... *la science des propriétés générales que confère aux fonctions leur propriété fondamentale d'être en fait toutes et toujours représentables par des séries entières.*

> All analytical functions have the common property, which was guessed by Lagrange, *to be always expressible as a power series, in other words, by Taylor's formula, except in exceptional cases which can be determined* a priori. Substituting this general property for continuity, monogeneity, etc., I choose it as the unique basis for all reasonings.[8]

The characterization of functions by their analyticity, that is to say, by the possibility of expressing them as Taylor series, induced Méray to give a fundamental role to the notion of limit, which also led him to build a theory of irrational numbers, in order to legitimize this notion. In the usual way, Méray explained the origin of fractions and irrationals by the impossibility of accomplishing certain operations without them. In a less usual way, he considered the new numbers not as real objects, but only as useful *fictions*, which allow us to extend arithmetical operations and to bring a greater uniformity to analysis.

> The integral numbers of elementary arithmetic, on which all operations required by numerical applications are exclusively based, are also the only ones which occur in theoretical speculations. But the frequent impossibility of certain operations would disturb heavily the uniformity required by the mechanism of the analytical transformations; it would complicate statements by continual restrictions if the obstacle is not overcome by replacing the genuine numbers and operations by fictions, for which this impossibility never happens, and from which one comes back to reality without any effort, when it is necessary. Such is, in particular, the origin of fractions.[9]

Like Méray, Dedekind conceived the arithmetization of analysis as an extension of the domain of natural numbers through successive creations of other numbers. Unlike Méray, however, he considered those creations not as fictions, but as the consequences of a necessary widening of the number concept. Thus, he explained in his essay *Was sind und was sollen die Zahlen?*

> how the step-by-step extension of the concept of number is subsequently to be carried out – the creation of zero, of the negative, rational, irrational, complex numbers – always by a reduction to earlier concepts, and indeed without any introduction of foreign conceptions (such as, for example, that of measurable magnitudes).[10]

[8] [Méray 1894], preface, pp. xv–xvi: *Toutes les fonctions analytiques possèdent la propriété commune devinée par Lagrange* d'être toujours développables en séries entières, autrement dit par la formule de Taylor, sauf dans des cas exceptionnels dont la détermination se fait *a priori. Substituant cette propriété générale à la continuité, à la monogénéité, etc., je la choisis pour base unique de tous les raisonnements.*

[9] [Méray 1894], pp. 2–3: *Les nombres entiers de l'Arithmétique élémentaire, sur lesquels roulent exclusivement en définitive toutes les opérations exigées par les applications numériques, sont les seuls aussi qui interviennent au fond des spéculations théoriques. Mais l'impossibilité fréquente de certaines opérations troublerait gravement l'uniformité désirable dans le mécanisme des transformations analytiques; elle compliquerait les énoncés de restrictions continuelles si l'on ne tournait l'obstacle en substituant aux nombres et aux opérations véritables des fictions, pour lesquelles cette impossibilité ne se présente jamais, et d'où, quand il le faut, on revient à la réalité sans aucun effort. Telle est en particulier l'origine des fractions.*

[10] [Dedekind 1888], preface to the 1st ed., p. 338, transl., [Ewald 1996], vol. 2, p. 792:

This mode of development, linked to a widening of the number concept, is not solely limited to analysis but is also applicable to algebra. Thus, in his introduction to the *Zahlbericht*, Hilbert inscribed the trend of arithmetization of analysis in a wider movement which he presented as the conquest of all mathematics by arithmetic:

> Thus, we see how arithmetic, the "queen" of mathematical sciences, is conquering large parts of algebra and function theory, and how it takes the leading role in them.[11]

Dedekind also associated algebra and analysis in the arithmetization trend. Moreover, according to him, the widening of the concept of number, and hence the extension of the realm of numbers, were more important than the simple expression of analytic or algebraic concepts and statements in terms of integers. Even more, and we want to stress this point, he interpreted scientific progress in general, and in mathematics in particular, as generated by conceptual development, namely by the creation and introduction of new concepts. He wrote:

> It appears as something self-evident and not new that every theorem of algebra and higher analysis, no matter how remote, can be expressed as a theorem about natural numbers – a declaration I have heard repeatedly from the lips of Dirichlet. But I see nothing meritorious – and this was just as far from Dirichlet's thought – in actually performing this wearisome circumlocution and insisting on the use and recognition of none other than natural numbers. On the contrary, the greatest and most fruitful advances in mathematics and other sciences have invariably been made by the creation and introduction of new concepts, rendered necessary by the frequent recurrence of complex phenomena which could be mastered by the old notions only with difficulty.[12]

Philosophers have similarly described mathematical progress through an extension of its domain of objects. Gilles-Gaston Granger, for instance, considering the irreducible case of the cubic equation, a subject with which the XVI^th^-century geometers Scipione del Ferro and Cardano were confronted, explained that it is the

In welcher Art später die schrittweise Erweiterung des Zahlbegriffes, die Schöpfung der Null, der negativen, gebrochenen, irrationalen und komplexen Zahlen stets durch Zurückführung auf die früheren Begriffe herzustellen ist, und zwar ohne jede Einmischung fremdartiger Vorstellungen (wie z. B. der der meßbaren Größen).

[11] [Hilbert 1897], p. iv, or [Hilbert 1932], p. 65: *So sehen wir, wie die Arithmetik, die "Königin" der mathematischen Wissenschaft, weite algebraische und funktionentheoretische Gebiete erobert und in ihnen die Führerrolle übernimmt.*

[12] [Dedekind 1888], preface to the 1st ed., p. 338, transl., [Ewald 1996], vol. 2, p. 792: ... *erscheint es als etwas Selbstverständliches und durchaus nicht Neues, daß jeder auch noch so fern liegende Satz der Algebra und höheren Analysis sich als ein Satz über die natürlichen Zahlen aussprechen läßt, eine Behauptung, die ich auch wiederholt aus dem Munde von Dirichlet gehört habe. Aber ich erblicke keineswegs etwas Verdienstliches darin – und das lag auch Dirichlet gänzlich fern –, die mühselige Umschreibung wirklich vornehmen und keine anderen als die natürlichen Zahlen benutzen und anerkennen zu wollen. Im Gegenteil, die größten und fruchtbarsten Fortschritte in der Mathematik und anderen Wissenschaften sind vorzugsweise durch die Schöpfung und Einführung neuer Begriffe gemacht, nachdem die häufige Wiederkehr zusammengesetzer Erscheinungen, welche von den alten Begriffen nur mühselig beherrscht werden, dazu gedrängt hat.*

encounter, in the exercise of mathematics, of "impossible," of "imaginary" objects, obtained through "illegitimate practice of operations," which brings about the necessity of a renewal (most often of a widening) of concepts, and which leads to the production of new objects.[13] For Granger, moreover, conceptual progress is the paradigm of the development of mathematics, which he interprets as "a process giving birth to formal contents."[14] He specifies:

> Thus, it is the description and the careful interpretation of these chains of deductions and of these concepts' renewals which can give sense to the idea of a secretion of contents by forms, particularly recognizable in mathematical knowledge.[15]

Cassirer's analyses – see, for instance, [Cassirer 1923–1929] – entirely agree with Granger's: mathematical development is described as the result of a play between objects and operations, and the generalization of number testify in favour of its universality. The conceptual widening and the emergence of objects that came along had, however, not always been approved in the same way by philosophers. Léon Brunschvicg, for example, had interpreted this enlargment of mathematics as inevitably going down towards nominalism.

> Thus, the juxtaposition of natural numbers and artificial expressions constitutes only a temporary pause in the movement of arithmeticism. The latter has to reach the realism of the Pythagoreans, or to slide down to nominalism and scepticism. The alternative being presented in that way, what we had already said of the formation and evolution of arithmeticism leads us to forecast that nineteenth-century scientists had surely to choose the second road.[16]

After describing the arithmetization of analysis to its end, which he called "nominalist" or "conventionalist" because it reduced numbers to simple signs organized by conventional rules, he concluded with some regrets that mathematics was evolving towards pragmatism at the cost of truth.

> The cycle of evolution that arithmeticism could cover is now achieved. … At the same time as mathematics perfected the rigour of its methods and had at its disposal more

[13] However, the use of the words "imaginary," "impossible," may delay for a time (two centuries in the case discussed by Granger) this production of new objects.

[14] See [Granger 1994], p. 66: *Ainsi la présence de ce que nous nommons contenus formels se trouve-t-elle révélée en mathématiques par le mouvement même du progrès conceptuel* (So the presence of what we call formal contents is revealed in mathematics by the movement itself of the conceptual progress).

[15] [Granger 1994], p. 66: *C'est donc la description et l'interprétation soigneuse de ces enchaînements et de ces renouvellements des concepts qui peut donner sens à cette idée d'une sécrétion de contenus par les formes, particulièrement reconnaissable dans la connaissance mathématique.*

[16] [Brunschvicg 1912], p. 362: *La juxtaposition des nombres naturels et des expressions artificielles ne constitue donc qu'un arrêt provisoire dans le mouvement de l'arithmétisme. Il faudra qu'il remonte jusqu'au réalisme des Pythagoriciens, ou qu'il descende la pente du nominalisme et du scepticisme. Or l'alternative étant ainsi présentée, ce que nous avons déjà dit de la formation et de l'évolution de l'arithmétisme fait prévoir que les savants du XIX^{e} siècle devaient inévitablement prendre le second parti.*

> subtle and stronger weapons for the conquest of the physical universe, mathematical philosophy was incapable of accounting for the truth of science. It lost itself in the current of pragmatism, increased its force, transforming it into a "tidal wave."[17]

Thus, the development of mathematics, though it was appreciated differently by philosophers, was interpreted by most of them as a conceptual widening, linked with the emergence of new objects.

2. Gauss as the Pioneer of the Conceptual Trend

In Hilbert's understanding of the conquest of various mathematical areas by arithmetic, Gauss appeared as one of the main actors. Hilbert admitted that Gauss still had, in his *Disquisitiones Arithmeticae*, a narrow conception of arithmetic from which he expressly excluded complex numbers and thus the theory of cyclotomy (*Kreisteilung*).[18] However, as Hilbert pointed out, Gauss explained that the principles of this theory "are derived from higher Arithmetic." Moreover, Hilbert gave credit to Gauss for "bringing the first seed of the theory of number fields." He clearly indicated that Gauss's method consisted of an extension of arithmetic through the introduction of new numbers (the so-called "Gaussian integers"); classical arithmetical laws can be extended to these numbers.[19] This work placed Gauss at the origin of the "conceptual" trend that we described earlier. In order to make precise what was transmitted from Gauss to the mathematicians following this trend, it is important to clarify Gauss's conception of the foundations of mathematics.

Gauss rarely expressed his ideas on the foundations of mathematics. Some indications can be found in his letters and in a small note entitled: "Zur Metaphysik der Mathematik," which was found in the Nachlaß and published in volume 12 of Gauss's *Werke*, [Gauss 1929], pp. 57–61. The editor, Ludwig Schlesinger, dated it to the first years of the XIX$^{\text{th}}$ century, that is, to the time of the *Disquisitiones Arithmeticae*. The word *Metaphysik* was usually understood, at that time, as a reflection on the philosophical foundations or on the highest parts of the discipline.[20] It is indeed

[17] [Brunschvicg 1912], p. 367: *Le cycle d'évolution que l'arithmétisme pouvait parcourir est donc achevé. … En même temps que la mathématique perfectionnait la rigueur de ses méthodes, qu'elle disposait d'armes plus subtiles et plus fortes pour la conquête de l'univers physique, la philosophie mathématique apparaissait impuissante à rendre raison de la vérité que la science possède. Elle allait se perdre dans le courant pragmatique, elle en redoublait la force jusqu'à lui donner l'aspect d'un "raz de marée".*

[18] See the preface of the *Disquisitiones Arithmeticae* and [Hilbert 1897], pp. ii–iii, or [Hilbert 1932], p. 64.

[19] [Hilbert 1897], p. iii, or [Hilbert 1932], p. 64: *Das Verdienst, den ersten Keim für die Theorie der Zahlkörper gelegt zu haben, gebührt wiederum Gauß. Gauss erkannte die natürliche Quelle für die Gesetze der biquadratischen Reste in einer "Erweiterung des Feldes der Arithmetik", wie er sagt, nämlich in der Einführung der ganzen imaginären Zahlen von der Form* $a+bi$*; er stellte und löste das Problem, alle Sätze der gewöhnlichen Zahlentheorie … auf jene ganzen imaginären Zahlen zu übertragen.*

[20] Schlesinger comments at the end of the text, [Gauss 1929], p. 61, that *man wird also dem, was Gauss im Auge hat, wenn er von der "Metaphysik" der Mathematik oder*

with the foundations of mathematics that Gauss dealt with in this text, through the notion of magnitude. He wrote that

> mathematics has for its object all extensive magnitudes (whose parts can be thought); intensive ones (all non-extensive magnitudes) only insofar as they depend on the extensive.[21]

Number is given as an example of an extensive magnitude, together with space (or, according Gauss's definition, "the geometric magnitudes") and time. Any non-extensive magnitude is called an intensive one: Gauss gave speed, density, hardness, height and depth of tones, intensity of tones and of light, probability, etc., as examples of intensive magnitudes. He then specified that

> a magnitude in itself cannot yet be the object of a mathematical investigation: mathematics considers magnitudes only in their relations to one another.[22]

These relations are divided into two types: the relations that magnitudes have to each other in so far as they are magnitudes are called arithmetical relations; moreover, geometrical magnitudes may also have, besides arithmetical relations, a geometrical relation, "with respect to location."[23] Mathematics deals with *relations* between magnitudes, not with magnitudes themselves; consequently, arithmetic and geometry differ rather by the types of relation between their objects, than by these objects themselves.[24] The goal of mathematics, Gauss specified,

> is to represent the known relationships that magnitudes have with known ones or with those obtained from known ones ; that is, to make a representation of them possible.[25]

einzelner mathematischer Disziplinen handelt, am nächsten kommen, wenn man ihm das moderne Wort "Grundlagenforschung", wenn auch nicht immer im Sinne von Axiomatik, an die Seite stellt (one will come at the closest of what Gauss has in sight when he deals with "metaphysics" of mathematics or of individual mathematical disciplines, when one replaces it by the modern word "foundations," although not always in the sense of axiomatic).

[21] [Gauss, 1929], p. 57, transl. in [Ewald 1996], vol. 1, p. 293: *Gegenstand der Mathematik sind alle extensive Grössen (solche, bei denen sich Theile denken lassen); intensive Grössen (alle nicht extensive Grössen) nur insofern, als sir von extensiven abhangen.*

[22] [Gauss 1929], p. 57, transl. in [Ewald 1996], vol. 1, p. 294: *Eine Grösse für sich kann noch kein Gegenstand einer wissenschaftlichen Untersuchung werden: die Mathematik betrachtet die Grössen nur in Beziehung zuf einander.*

[23] For instance, the equality of two sides of a triangle is an arithmetical relation, the orthogonality is a geometrical relation [Editors' note].

[24] One must not rush to conclude, from the primacy that Gauss gave to the relations compared with the objects, that he already had a structuralist view of mathematics. Indeed, he did not consider the relations in themselves and only mentioned relations between magnitudes.

[25] [Gauss 1929], p. 57, transl. in [Ewald 1996], vol. 1, p. 294: ... *Grössen, die zu bekannten Grössen oder zu denen bekannten Grössen bekannte Beziehungen haben, darzustellen, d.h. eine Vorstellung davon möglich zu machen.*

This representation is made either by immediate intuition, or by comparison with a magnitude given in immediate intuition. In the first case the representation is said to be immediate, in the second one it is said to be mediate. Gauss added that

> the duty of the mathematician is accordingly either to actually represent the sought-for magnitude (geometrical representation or construction), or to indicate the way and manner in which from the representation of an immediately given magnitude, one can achieve the representation of the sought magnitude (arithmetical representation).[26]

The latter indicates, by means of a number, how many times a directly given magnitude, called the unit, is contained in the sought magnitude. Thus, Gauss concluded that "the proper object of arithmetic is number," [Gauss 1929], p. 59, transl. in [Ewald 1996], vol. 1, p. 295. This object, the number, presents itself as the relation between one magnitude and another one considered as a unit.[27]

Let us point out that the concept of infinity is not excluded by Gauss; within arithmetic he makes a difference between higher mathematics or "calculation with infinity" and lower or common mathematics, where the concept of infinity is not used.

> Since there can be a great difference among the arithmetical relations of quantities to one another, the parts of mathematical science are of very diverse nature. The most important circumstance is whether these relations presuppose the concept of infinity or not; in the former case, they belong to the realm of higher mathematics; in the latter, to common or lower mathematics.[28]

[26] [Gauss 1929], pp. 57–58, transl. in [Ewald 1996], vol. 1, p. 294: *Die Pflicht des Mathematikers ist demnach, die gesuchte Grösse entweder wirklich darzustellen (geometrische Darstellung oder Construction) oder die Art und Weise anzugeben, wie man von der Vorstellung einer unmittelbar gegebnen Grösse zu der Vorstellung der gesuchten Grösse gelange (arithmetische Darstellung).*

[27] Gauss's presentation of the number considered as a relation (a ratio) between magnitudes includes all rational and irrational numbers. This presentation seems better and at least more general than Weierstrass's one. Nevertheless Gauss's definition was a classical definition, already used by Newton; Hermann Hankel's 1876 *Theorie der complexen Zahlensysteme* follows the same lines, see p. 6: *die Zahl ist der begriffliche Ausdruck der gegenseitigen Beziehung zweier Objekte, soweit dieselbe quantitativen Messungen zugänglich ist.* This definition was later criticized by Frege in his *Grundlagen der Arithmetik* [Frege 1884]. Indeed Frege blamed this "geometrical" definition for not providing a definition of natural numbers (cardinal numbers), whereas, on the other hand, the definition of other numbers can be founded on natural numbers – this is precisely the arithmetization project. It is clear here that Weierstrass, who took part in this project, did not need to start with a wide definition of numbers.

[28] [Gauss 1929], p. 58, transl. in [Ewald 1996], pp. 294–295: *Da unter den arithmetischen Beziehungen der Grössen auf einander eine grosse Verschiedenheit statt finden kann, so sind auch die Theile der arithmetischen Wissenschaften von sehr verschiedener Natur. Am wichtigsten ist der Umstand, ob bei dieser Beziehung der Begriff des Unendlichen muss vorausgesetzt werden oder nicht; der erste Fall gehört in die Rechnung des Unendlichen oder die höhere Mathematik, der letztere in die gemeine oder niedere Mathematik.*

In the *Disquisitiones Arithmeticae*, however, higher mathematics is not connected with calculation with infinity, but defined as dealing with "the general research about affections characteristic of integers" (*Disquisitiones Arithmeticae*, preface).

In a standard way at that time, arithmetic operations are presented by Gauss in the text "Zur Metaphysik der Mathematik," not for numbers (e.g. natural integers), but more generally for magnitudes. Addition and subtraction originate from "the simplest relationship between magnitudes," that between the whole and its parts. Thus, adding boils down to "finding the whole from its parts" – the whole is then named "sum" or "aggregate" – and subtracting to "finding from the whole and one part, the other part." Multiplication and division are then defined from the relationship between the "simple" (*das Einfache*) and the "multiple" (*das Vielfache*). Multiplication consists in finding the multiple (named the product) from the two other terms named factors. Division consists in finding the number (*Zahl*) from the two first terms, the simple and the multiple; Gauss added that the roles of the simple and the number can be exchanged. It is from this same notion of aggregate, used by Gauss to designate a whole made of parts, that Weierstrass gave his own definition of integers, then of rational numbers and eventually of irrational numbers. We shall show that these definitions are in line with those of Gauss and, in particular, in line with his definition of addition as an aggregate or a sum of units, even if Gauss's view based on magnitudes is more general than Weierstrass's one and would appear too geometrical for the latter (see note 26).

Let us first notice that for Weierstrass the term "number," without further precision, generally designates a positive integer, the other numbers being called "mixed numbers," "complex numbers" or also "numerical magnitudes" (*Zahlgrösse*). A number (a positive integer) is defined by Weierstrass as an aggregate (i.e., a sum) of units, a definition emerging from Euclid but also from the Gaussian definition of addition. A (positive) rational number is defined as an aggregate of different units, a "principal" unit (making up the integral part) and its "exact parts" (of the form $1/n$ where n is an integer). For instance, the rational number 11/3 is made of 3 principal units and of the aggregate (1/3, 1/3) which can itself be written (1/3, 1/6, 1/6) or alternatively (1/6, 1/6, 1/6, 1/6). In order to reduce to one single number the infinitely many different ways to write this number, Weierstrass introduced a proper equality relation and showed that it was symmetric and transitive – he did not mention the term "equivalence relation" not yet in use: two numerical magnitudes are said to be equal if any constituent part (*Bestandteil*)[29] of one can be transformed into a constituent part of the other and reciprocally.[30]

The aggregates considered until now were supposed to contain only a finite

[29] Weierstrass defined a constituent part as following, [Weierstrass 1878], p. 11, [Dugac 1973], p. 101: *Nennen wir nun a' dann einen Bestandteil von a, wenn a' in a'' transformiert werden kann, so dass sämtliche Elemente von a'' ebenso oft in a vorkommen als in a'' und a ausserdem noch andere Elemente oder dieselben in grösserer Anzahl enthält, als a''.*

[30] [Weierstrass 1878], p. 12, [Dugac 1973], p. 101: *Wir nennen zwei Zahlengrössen a und b* gleich, *wenn ein* jeder *Bestandteil von a durch Transformation zu einem von b gemacht werden kann und umgekehrt jeder Bestandteil von b zu einem von a.*

number of elements, but subsequently Weierstrass considered those which contained infinitely many elements and discarded those whose value (i.e., the sum of the elements) was infinite, because they did not obey the elementary arithmetical laws. Then the question arose of knowing whether the aggregates made of infinitely many elements and which have a finite value (i.e., those for which the sum of the elements is bounded by a rational number), are new numbers. The number e defined by the aggregate $(1, 1/2, 1/6, \ldots, 1/n!, \ldots)$, shown by Hermite not to be rational, allowed Weierstrass to answer this question positively, i.e., to exhibit an aggregate not corresponding to a rational number. From his definition of equality, everything is in place to widen the domain of rational numbers to "numerical magnitudes" which are the aggregates made of infinitely many elements and having a finite value – it is enough to verify that the arithmetical operations apply to the new numbers. As is known, Cantor improved Weierstrass's construction of irrationals by replacing the notion of aggregates with that of "fundamental sequence" (today "Cauchy sequence"), then identifying such a sequence with the number he wanted to define. Thus, from Gauss to Cantor, through Weierstrass, successive extensions of the concept of number continued, complex and transfinite numbers being added to negative, rational and irrational ones. Three questions could then arise: that of the goal of the extension of arithmetic, that of its limitation and that of the legitimacy of these new numbers.

Above we started to consider the question of the goal of the extension of the number concept; we saw that it was essentially in order to give to analysis a foundation that geometry could no longer provide. Gauss specified indeed, in a famous letter to Bessel on December 18, 1811, that it was not only because of their practical usefulness, but also to ensure the scientific independence of analysis, that complex numbers had to be introduced and considered as enjoying the same rights as real numbers. He stated as his "fundamental proposition" (*Grundsatz*) that

> in the realm of magnitudes, the imaginary numbers $a + b\sqrt{-1} = a + bi$ have to be considered as having the same rights as the reals. The matter is not here the practical usefulness, but analysis is for me an independent science, which by rejecting these fictitious magnitudes would lose enormously in beauty and roundness.[31]

The limitation of the extension of the concept of number was, most often, and for Gauss in particular, motivated by the wish to preserve the laws of elementary arithmetic. This wish was then expressed under the form of Ohm's, Peacock's and Hankel's "principle of the permanence of formal laws." This principle, which was later violently critized by Kronecker, acted as a brake to the Gaussian invention. Gauss, for instance, did not consider complex expressions with more than two principal units as numbers, probably because they did not match with the rules of classical elementary calculation. In a note about the "mutations of space" (*Mutationen des*

[31] [Gauss & Bessel 1880], p. 156: ... *man in dem Reiche der Grössen die imaginären $a + b\sqrt{-1} = a + bi$ als gleiche Rechte mit den reellen geniessend ansehen müsse. Es ist hier nicht von praktischem Nutzen die Rede, sondern die Analyse ist mir eine selbstständige Wissenschaft, die durch Zurücksetzung jener fingirten Grössen ausserordentlich an Schönheit und Ründung verlieren.*

Raumes),[32] for instance, he observed that the product of two combinations (a, b, c, d) and (a, b, g, d) is not commutative:

> We generally designate the combination a, b, c, d by (a, b, c, d) and we write
>
> $$(a, b, c, d)(\alpha, \beta, \gamma, \delta) = (A, B, C, D).$$
>
> Therefore, $(a, b, c, d)(\alpha, \beta, \gamma, \delta)$ and $(\alpha, \beta, \gamma, \delta)(a, b, c, d)$ are not be confused.[33]

One knows that Hamilton would later develop the calculation of complex numbers with four principal units (quaternions), for which the commutativity of multiplication should be dropped. Cantor's transfinite arithmetic, too, did not satisfy some classical arithmetical laws, such as the commutativity of addition and of multiplication. But generally speaking, the mathematicians of the conceptual tendency tried to preserve these laws as much as possible. However, this will act either as a brake or, on the contrary, as a major spur for the development of the theory. Concerning the question of the legitimacy of the created numbers, Gauss invented a geometrical representation of complex numbers; he wrote in the letter to Bessel mentioned above:

> in the same way as one can represent the whole domain of real quantities using a infinite straight line, one can represent the complete domain of all quantities, the real and the imaginary ones, by an unbounded plane, where each point is determined by its abcissa a and its ordinate b and represents, so to say, the quantity $a + ib$.[34]

Therefore the representation of complex numbers by the points of a plane gave them a legitimacy and thus the same rights as real numbers. Gauss expressed this idea again in his 1831–1832 *Commentatio secunda* on biquadratic residues, in which he wanted to clarify what he called "the metaphysics of imaginary quantities." He explained that if one associates two complex quantities m and m' with two points M and M', the difference $m - m'$ will be nothing else but the position of the point M relatively to the point M'; also, the points corresponding to the complex quantities mm', m, m', 1 form a proportion. The images of the Gaussian integers – corresponding to $a + bi$, with a and b integers – constitute a system of equidistant points, placed on equidistant straight lines dividing the plane into an infinite number of identical squares.

As for Weierstrass, he did not resort to geometry in order to justify the existence of newly created numbers. However, it is necessary to qualify this assertion. Indeed,

[32] [Gauss 1900], pp. 357–362. The editor of the volume, Paul Stäckel, suggested 1819 as the date of composition.

[33] [Gauss 1900], pp. 359–360: *Wir bezeichnen allgemein die Combination a, b, c, d durch* (a, b, c, d) *und schreiben* $(a, b, c, d)(\alpha, \beta, \gamma, \delta) = (A, B, C, D)$. *Es ist also* $(a, b, c, d)(\alpha, \beta, \gamma, \delta)$ *nicht mit* $(\alpha, \beta, \gamma, \delta)(a, b, c, d)$ *zu verwechseln.*

[34] [Gauss & Bessel 1880], pp. 156–157: *So wie man sich das ganze Reich aller reellen Grössen durch eine unendliche gerade Linie denken kann, so kann man das ganze Reich aller Grössen, reeller und imaginärer Grössen, sich durch eine unendliche Ebene sinnlich machen, worin jeder Punct, durch Abscisse =a Ordinate= b bestimmt, die Grösse $a + bi$ gleichsam repräsentirt.*

the reasons why Weierstrass dealt with the existence of irrational numbers are not theoretical, but practical ones; what interested him when he was trying to define irrational numbers was not to establish a theory of real numbers, but to specify the notion of limit that he needed to found his theory of functions. Thus, he considered the question of the existence of these numbers only with respect to the existence of the limit of a sequence of rational numbers, to give a meaning to this limit when it is not rational. Indeed, one can talk about such a limit only if irrational numbers have been defined before. Weierstrass expressed this problem clearly:

> If we start from the existence of rational numerical magnitudes, there is no sense to define irrationals as limits of them, because we cannot know at first if there exist other magnitudes than the rational ones. It is only when we deal with extensive magnitudes that one can speak of the limit of a segment, but not if one takes the purely arithmetical point of view. However, numerical magnitudes as we defined them before include all rational numbers, but contain also other magnitudes. Let us consider for example the number *e* which is composed of the elements 1, $1/2$, $1/6$,..., $1/n!$,..., it is a well-defined sequence which defines a well-determined numerical magnitude; at the same time, Hermite could show that there exists no rational numerical magnitude which is equal to it according to the given definition. It follows that the domain of magnitudes is not exhausted by the rational numbers.[35]

Thus, at no time did Weierstrass wonder about the nature of this irrational limit. Is it as "real' as a rational limit, as Dedekind and Cantor will assert later? Or is it only fictitious, as Méray will insist? Resorting to geometry in order to legitimize the existence of irrational numbers is a trait absent from Weierstrass's work, but present in Gauss's, and also to be found in Cantor's. The latter stated as an axiom the existence of a one-to-one relation which exists between the domain of real numbers and the points on a straight line, and noticed that with this axiom one gained "also, afterwards, a certain objectivity[36] for numerical magnitudes."[37] One can see in this legitimization

[35] [Weierstrass 1886], p. 59, [Dugac 1973], p. 134–135: *Wenn wir von der Existenz rationalen Zahlgrößen ausgehen, so hat es keinen Sinn, die irrationalen als Grenzen derselben zu definieren, weil wir zunächst gar nicht wissen können, ob es außer den rationalen noch andere Zahlgrößen gebe. Nur wenn man es mit extensiven Größen zu tun hat, kann man von der Grenze einer Strecke sprechen, nicht aber, wenn man sich auf den rein arithmetischen Standpunkt stellt. Aber die Zahlgrößen, wie wir sie im Vorstehenden definiert haben, umfassen die rationalen Zahlen sämtlich, enthalten aber auch noch andere. Betrachten wir, z. B. die Zahl e, die zusammengesetzt ist aus den Elementen* 1, $\frac{1}{2}$, $\frac{1}{3}$, ..., $\frac{1}{n}$, ..., *so ist dies eine wohldefinierte Reihe, die eine ganze bestimmte Zahlgröße definiert, gleichwohl hat Hermite zu zeigen vermocht, daß es keine rationale Zahlgröße gibt, die ihr nach den aufgestellten Definitionen gleich ist, daraus geht hervor, daß das Größengebiet mit den rationalen Zahlen nicht erschöpft ist.*

[36] The term "objectivity" is to be understood here in the standard philosophical sense, i.e., as independent of the mind. For Cantor and most mathematicians at the time, this objectivity was to be found in the physical world; for Frege, however, it was to be found in pure logic.

[37] Let us notice that Cantor will also try to justify the existence of transfinite numbers: their ontological status is conferred, not by their geometrical representation, as in the case

by geometry of the objects of analysis the lasting prevalence of a conception in which existence is assimilated to being visible. The geometrical or physical substratum which represents the created numbers confers upon them, whose existence is at first only abstract, formal, an objectivity and thus a legitimacy, in providing them with the guarantee of a concrete referent. But this guarantee of objectivity must not be mistaken for a foundation. New numbers (negative, rational, irrational, complex numbers) are indeed founded on natural numbers and are independent from their representations by points. And positive integers are themselves founded, for Gauss for example, on the notion of relationship between magnitudes. Thus, Gauss could at the same time say that "number is a product of our mind alone"[38] and introduce spatial representation in order to prove the objectivity of number.[39] The place that Gauss gave to arithmetic compared with geometry can be likened to that which, more generally, Cantor gave to pure mathematics compared with reality. Indeed, Cantor distinguished between two sorts of realities for mathematical objects. The first one, that he named *intrasubjective* or *immanent* reality, was obtained when conditions of no contradiction and of coherence were achieved. The second reality, named *transsubjective* or *transcendent*, is assigned to a concept inasmuch as it represents an element or a relation of the physical world. These two types of reality are closely linked; a concept existing under the first condition, that is to say free of contradiction, has also necessarily a transcendent reality. But the mathematician does not have to deal with this transcendent reality, which gives mathematics its character of freedom.

On the other hand, the guarantee of objectivity that arithmetic finds in geometry does not imply a subordination of the former to the latter. For Gauss, arithmetic was the "queen" of mathematical disciplines; it is a pure discipline, whereas geometry cannot be established entirely a priori. Gauss expressed this idea in his letter to Bessel dated January 27, 1829:

> My conviction that we cannot establish geometry entirely a priori has, if possible, become even firmer.[40]

He went further on April 9, 1830:

> It is my deepest conviction that the theory of space has a completely different position in our *a priori* knowledge than does the pure theory of quantity. Our knowledge of the former utterly lacks the complete conviction of necessity (and also of absolute truth) that belongs to the latter; we must in humility grant that, if number is *merely*

of the finite numbers, but by their existence in "physical and spiritual nature," [Cantor 1883], § 8.

[38] See [Gauss & Bessel 1880], p. 497 and [Gauss 1900], p. 201: *[D]ie Zahl [ist] bloss unseres Geistes Product.* Cf. note 40.

[39] Cantor also expressed this independence of pure mathematics, of number theory, with respect to reality, see [Cantor 1883], *Anm. an* § 8, p. 182 in [Cantor 1932]: *Die Mathematik ist in ihrer Entwickelung völlig frei.*

[40] [Gauss & Bessel 1880], in [Gauss 1900], p. 200, transl. in [Ewald 1996], vol. 1, p. 301: *Meine Überzeugung, daß wir die Geometrie nicht vollständig a priori begründen können ist, wo möglich, noch fester geworden.*

> the product of our mind, space also possesses a reality outside our mind, and that we cannot entirely prescribe its laws *a priori*.[41]

Thus, arithmetic and geometry do not have the same position in *a priori* knowledge. But there is no frontier between the two disciplines whose transgression would be an intolerable fault. Gauss considered arithmetic and geometry as species of the same kind, mathematics being conceived as the science of magnitudes, or more precisely, as the study of relations between magnitudes. The frontier between arithmetic and geometry is therefore only weakly established; its transgression is often encouraged. Indeed, Gauss recalled that the Ancients presented arithmetical relations in a geometrical way (for instance the presentation of a square number by a plane square) and observed

> that the moderns so strongly prefer the arithmetical manner of representation to the geometric is not without a reason, especially since our method of counting (by tens) is so much easier than that of the ancients.[42]

Let us summarize what these observations and analyses allow us to understand about the philosophical position of Gauss concerning pure mathematics. For Gauss, well before Weierstrass, Dedekind and Cantor, mathematics was a "free creation of the human mind." The Gaussian theory of numbers developed, as we saw, through conceptual extension; geometrical intuition came in only *afterwards*, in order to justify the existence of the created numbers. This late intervention of intuition, as well as its empirical nature, sets Gauss's conception radically against Kant's. For the latter, mathematics proceeds synthetically, i.e., by the construction of concepts, unlike philosophy and logic, which proceed analytically, i.e., through concepts alone. To construct a concept, for Kant, "means to present a priori the intuition which corresponds to it."[43] For Kant, then, pure intuitions are at the basis of mathematics. On the contrary, for Gauss, pure mathematics was conceptual and the sensible intuitions to which he resorted in order to justify the existence of the numbers created by the mathematician were empirical. On the other hand, Gauss's opinion on Kant's doctrine about mathematics and on philosophers' mathematical competencies in general, clearly appeared in a letter of November 1, 1844, to his friend Schumacher:

[41] [Gauss & Bessel 1880], in [Gauss 1900], p. 201, transl. in [Ewald 1996], vol. 1, p. 301: *Nach meiner innigsten Überzeugung hat die Raumlehre in unserm Wissen a priori eine ganz andere Stellung, wie die reine Grössenlehre; es geht unserer Kenntniss von jener durchaus* diejenige *vollständige Überzeugung von ihrer Nothwendigkeit (also auch von ihrer absoluten Wahrheit) ab, die der letztern eigen ist; wir müssen in Demuth zugeben, dass, wenn die Zahl* bloss *unseres Geistes Product ist, der Raum auch ausser unserm Geiste eine Realität hat, der wir a priori ihre Gesetze nicht vollständig vorschreiben kann.*

[42] [Gauss 1929], p. 58, transl. in [Ewald 1996], vol. 1, p. 294: *Dass die Neuern der arithmetischen Darstellungsart so sehr den Vorzug vor der geometrischen geben, geschieht nicht ohne Grund, besonders da unsere Methode zu zählen (nach der Dekadik) so unendlich leichter ist, als die der Alten.*

[43] [Kant 1781], vol. III, p. 469: *Einen Begriff aber construiren, heißt die ihm correspondirende Anschauung a priori darstellen.*

> Just look around at the modern philosophers, at Schelling, Hegel, Nees von Essenbeck[44] and consorts – don't their definitions make your hair stand on end? Read in the history of ancient philosophy what the men of the day, Plato and others (I except Aristotle), gave as explanations. But even in Kant matters are often not much better; his distinction between analytic and synthetic propositions seems to me to be either a triviality or false.[45]

The refusal to place sensible intuition at the foundation of pure mathematics will be fully accepted and often even demanded, also by mathematicians such as Bolzano, Dedekind, and Cantor. Cantor, for example, clearly stated this refusal: contrary to what is believed "since the growth of modern empirism, sensualism and scepticism, as well as the Kantian criticism that grows out of them," "the source of knowledge and certainty" does not lie in the senses or in the so-called "pure forms of intuition of the world of appearances," but science in general, and mathematics in particular, is a free conceptual construction; it obtains its knowledge only "from concepts and ideas," by "inner induction and deduction."[46] According to Cantor, mathematics

> is only bound in the self-evident respect that its concepts must both be consistent with each other and also stand in exact relationships,ordered by definitions, to those concepts which have previously been introduced and are already at hand and established.[47]

3. The Kroneckerian Trend

Kronecker's ideas on the foundations of mathematics, and especially on the concept of number, were first published in his 1887 contribution to the doctorate jubilee of

[44] A natural philosopher and professor of vegetal physiology.

[45] [Gauss 1863–1929], vol. XII, pp. 62–63: *Sehen Sie sich doch nur bei den heutigen Philosophen um, bei Schelling, Hegel, Nees von Essenbeck und Consorten, stehen Ihnen nicht die Haare bei ihren Definitionen zu Berge? Lesen Sie in der Geschichte der alten Philosophie, was die damaligen Tagesmänner Plato und andere (Aristoteles will ich ausnehmen) für Erklärungen gegeben haben. Aber selbst mit Kant steht es oft nicht viel besser; seine Distinction zwischen analytischen und synthetischen Sätzen ist meines Erachtens eine solche, die entweder nur auf eine Trivialität hinausläuft oder falsch ist.*

[46] See [Cantor 1883], *Anm. [6] an* § 8, p. 207 in [Cantor 1932], transl. in [Ewald 1996], vol. 2, p. 918: *Erst seit dem neueren Empirismus, Sensualismus und Skeptizismus, sowie dem daraus hervorgegangenen Kantischen Kritizismus glaubt man die Quelle des Wissens und der Gewißheit in die Sinne oder doch in die sogenannten reinen Anschauungsformen der Vorstellungswelt verlegen und auf sie beschränken zu müssen; meiner Überzeugung nach liefern die Elemente durchaus keine sichere Erkenntnis, weil letztere nur durch Begriffe und Ideen erhalten werden kann, die von äußerer Erfahrung höchstens angeregt, der Hauptsache nach durch innere Induktion und Deduktion gebildet werden als etwas, was in uns gewissermaßen schon lag und nur geweckt und zum Bewußtsein gebracht wird.*

[47] [Cantor 1883], § 8, p. 182 in [Cantor 1932], transl. in [Ewald 1996], vol. 2, p. 896: *Die Mathematik ist in ihrer Entwickelung völlig frei und nur an die selbstredende Rücksicht gebunden, daß ihre Begriffe sowohl in sich widerspruchslos sind, als auch in festen durch Definitionen geordneten Beziehungen zu den vorher gebildeten, bereits vorhandenen und bewährten Begriffen stehen.*

Eduard Zeller (a historian of Greek philosophy), then, the same year but in a revised version, in the Crelle's *Journal*, under the title "Über den Zahlbegriff." Kronecker also gave a series of lectures on this subject during the 1891 Summer Semester, the last one he taught; this last course was entitled "on the concept of number in mathematics" (*Über den Begriff der Zahl in der Mathematik*). We shall in particular rely on this text in order to make the "Kroneckerian trend" more precise and to compare it with the "conceptual one" that we previously described. In the first lecture of the course, Kronecker explained that this subject, the concept of number, was dear to him; he had been thinking about it for a long time, but he had much hesitated to talk about it in a course, because he knew his ideas would be fiercely criticized. As we shall see in the following pages, Kronecker's ideas could not suit the conceptual tendency which was going to become the dominant one. As already hinted in the title of the course, Kronecker made explicit that it was indeed in mathematics, and not in another field, that he intended to found the concept of number. On the one hand, he criticized Hegel and Schelling who, according to him, had made "philosophy infringe on natural sciences and mathematics,"[48] and on the other hand, he also criticized Peirce and Peano, who thought they could extend mathematics beyond its frontiers, and dominate "all the spiritual realm" (*alles Geistige beherrschen*) (lesson 1). Kronecker strongly insisted on this first thesis: the necessity for each science not to overlap on the realm of another.

The second thesis expressed by Kronecker, even more important than the first one in order to understand his conception of the foundations of mathematics, stated that mathematics was a natural science, and therefore had to be treated as a natural science. Kronecker explained this thesis by asserting that the objects of mathematical science "are as real as those of its sister sciences," i.e., of the other natural sciences. "Each one speaking about mathematical 'discoveries' and not about mathematical 'inventions' feels it." For, he said, what is discovered can only be what really existed before, but what the human mind produces is called "invention." That is why, he continued, mathematicians "discover" results through methods that they had "invented" for that purpose.[49] Mathematics being nothing else than a natural science, the task of mathematicians is "to describe phenomena simply and completely," (*die Erscheinungen einfach und vollständig zu beschreiben*). Kronecker was here following the lesson of Kirchhoff, the physicist. He was not the only one to support this thesis. In France, Jules Molk, a former student of Kronecker, expressed the same conception very clearly in an 1885 article published in *Acta Mathematica*, "on the notion of divisibility and on the general theory of elimination":

[48] [Kronecker 1891], p. 4, in [Boniface, Schappacher 2001], p. 222: *Noch mehr als Hegel leistete Schelling in Übergriffen der Philosophie auf Naturwissenschaften und Mathematik.*

[49] [Kronecker 1891], lesson 4, p. 18, in [Boniface, Schappacher 2001], pp. 232–233: *Ihre Gegenstände sind ebenso wirklich wie diejenigen ihrer Schwesterwissenschaften. Daß dem so ist, fühlt ein jeder, der von mathematischen Entdeckungen, nicht aber von mathematischen Erfindungen spricht.*

> Arithmetic and algebra belong to a well defined domain; the positive integers, the systems of integers represented by integral functions with positive integer coefficients, are considered there as motion in kinematics and as matter in natural sciences.[50]

Charles Hermite, in the same spirit, asserted that "one must turn into a naturalist in order to observe arithmetical phenomena."[51] The expression of the same conception of mathematics is also found in Great Britain, with Cayley and Sylvester, for instance, who preferred the language of natural science to that of modern mathematics, see [Crilly 1986]. This conception of mathematics as a natural science must not be confused with an empirism in the style of John Stuart Mill, for whom number existed in reality and mathematical propositions were physical facts.[52] It led to the consideration of algebraic or analytic expressions as phenomena, these phenomena being not physical but mathematical ones, and to classify them into genera and species. This conception was probably the dominant one until the end of the XIX$^{\text{th}}$ century, with Dedekind's and Cantor's more conceptual points of view. Kronecker's particularity is that he supported the conception of mathematics as a natural science to its ultimate consequences. One of these consequences is the necessity of a rigorous separation between the various mathematical areas. Indeed, as an experimental science, mathematics must adapt the methods of each of its constitutive disciplines to the phenomena they deal with; it is therefore important, according to Kronecker, to establish strictly the domain of each. The special disciplines of mathematical science are: mechanics which operates with the concept of time, geometry which is looking for spatial relationships in which time is not involved, and pure mathematics in which neither time nor space are involved and that Kronecker designated as arithmetic (lesson 2 of [Kronecker 1891]). Kronecker particularly insisted on the necessity of a separation between pure mathematics or arithmetic ("general" arithmetic which also includes algebra and analysis) on the one hand, and geometry and mechanics on the other.[53]

His epistemological positions being clarified, Kronecker could then develop his definition of the concept of number. He began by specifying what mathematical definitions must be. They must not only be free of contradiction, but must also result from experience, and, what is even more essential, must include the criterion according to which one can decide, for each particular case, whether the presented

[50] [Molk 1885], p. 3: *L'arithmétique et l'algèbre ont un domaine bien défini; les nombres entiers positifs, les systèmes de nombres entiers représentés par des fonctions entières à coeffcients entiers positifs, y sont considérés comme le mouvement en cinématique et la matière des sciences naturelles.*

[51] *Il faut se transformer en naturaliste pour observer les phénomènes du monde arithmétique*, see C. Goldstein's chap. VI.1 below.

[52] J. S. Mill, *System of logic*, livre II, chap. VI, §2, quoted in [Frege 1884], pp. 9–10.

[53] Cf. [Kronecker 1891], lesson 3, p. 15, in [Boniface, Schappacher 2001], pp. 230–231: *Alles, was nicht zur Mechanik und Geometrie gehört und was ich also unter dem Namen der Arithmetik zusammenfassen möchte, müsste auch wirklich arithmetisiert werden. Von denjenigen, welche die verschiedenen Gebiete zusammen mengen, gilt das französische Sprichwort:* Qui trop embrasse mal étreint.

concept is subsumed under the definition or not. A definition which does not achieve this, Kronecker added, "can be advocated by philosophers or logicians, but for us mathematicians it is a mere nominal definition, and worthless."[54] The experience from which the concept of number results is that of counting; this experience, according to Kronecker, itself assumes ordinal numbers. Thus, for Kronecker, the ordinal numbers come before the cardinals. Among the mathematicians who have a conception close to his, Kronecker cited Lipschitz, Fine,[55] and Helmholtz. However Helmholtz started with counting, whereas Kronecker said he preferred to begin with ordinals. The sequence of ordinal numbers being given to us, it is therefore possible to number collections of objects by using these numbers and to define cardinal numbers.

In order to build this definition, Kronecker used four notions inherited from Gauss: those of equivalence, of class, of invariant, and of representative. He began by defining the relation of equivalence between any systems of magnitudes by stating that two systems (z) and (z') are equivalent "if I can deduce the system (z') from the system (z) in some univocally determined way."[56] Kronecker explained that "one can consider, for instance, a given computational procedure which allows one to establish the system (z') from the system (z)." Then he defined as invariants of equivalent systems the "functions of the elements which take the same value for the whole class of equivalent systems." The invariants will respectively be said to be arithmetical, algebraical or analytical, depending on the arithmetical, algebraical or analytical nature of the function. Kronecker noticed that, according to his definition of equivalence, the elements of any system of a class of equivalent systems can be taken as the characteristic invariant of the class.

> The elements are an invariant because I can reach them from every system, and they are a characteristic invariant because they represent a system which belongs to the determined class and not to any other.[57]

To define the cardinal number, Kronecker chose as equivalence relation a one-to-one relation. Then he has to choose a characteristic invariant, or as he also expressed it, a representative of the class of equivalent collections. As he showed before, any collection of the considered class is a characteristic invariant of this class and can therefore be chosen as a representative of the class:

[54] [Kronecker 1891], p. 28, in [Boniface, Schappacher 2001], p. 240: *Eine Definition, welche dies nicht leistet, mag von den Philosophen oder Logikern gepriesen werden, für uns Mathematiker ist sie eine bloße Wortdefinition und ohne jeden Wert.*

[55] Henry Burchard Fine, who was professor at Princeton and left his name to Fine Hall, at the Institute for Advanced Study, had followed lectures by Kronecker.

[56] [Kronecker 1891], lesson 5, p. 23, in [Boniface, Schappacher 2001], p. 236: *wenn ich imstande bin, auf irgend eine, aber eindeutig bestimmte Weise das System (z') aus dem System (z) abzuleiten.*

[57] [Kronecker 1891], lesson 5, p. 24, in [Boniface, Schappacher 2001], p. 237: *Die Elemente sind Invarianten, weil ich von jedem System zu diesem einen gelangen kann, und sie sind die charakteristischen Invariante, weil sie ein System repräsentieren, welches nur der einen bestimmten Klasse, aber keiner anderen zugehört.*

> Thus, for instance, "three fingers" is a characteristic invariant of the class formed with the collections of three objects.[58]

So as to simplify the problem, Kronecker suggested choosing as characteristic invariant the collection formed with a part of the sequence of ordinal numbers ordered from 1, and to choose as a representative of this collection the last ordinal number of the collection. Thus, "each ordinal number characterises a determined class of equivalent collections."[59]

We can compare Kronecker's definition of cardinal numbers to the one given by Frege in his 1884 *Grundlagen der Arithmetik*. Frege's definition is considered by Hilbert as the most complete definition of the time and will be taken up again, and modified, by Russell. The three definitions have in common that they are founded on an equivalence relation: equinumericity between concepts for Frege, one-to-one relation between collections for Kronecker and Russell. However, whereas for Frege and Russell the cardinal number is directly defined by the class of equivalent collections (Russell) or by the class of equivalent concepts (Frege), these definitions are much too abstract for Kronecker. To avoid this drawback and give the concept of cardinal number a more "real" foundation, Kronecker used the notion of invariant, or even, more significantly, that of representative. He came back to this last notion in lesson 6, in which he explained that this recourse is useful and frequent in all sciences. "Logic knows really only one mortal man, Cajus, while in law, Titus must always pay as the scapegoat." And Kronecker added:

> Thus it appears to each one, even without credentials, that Cajus in one case and Titus in the other both represent human kind generically.[60]

Resorting to a generic representative also has the considerable advantage of avoiding the logical difficulties related to infinite classes. One will find, for instance, with Hilbert's choice function, a similar recourse. Thus Kronecker reached a definition of cardinal number logically indisputable and perfectly in accordance with current usage, which was missing in Frege's and Russell's definitions.

4. From Gauss to Kronecker: Influences and Differences

Kronecker's reference to Gauss is constant: Gauss is quoted on several occasions in his 1887 article, [Kronecker 1887], and his last course began with a tribute to the *Disquisitiones Arithmeticae*, "the Book of all Books." The first point on which

[58] [Kronecker 1891], p. 26, in [Boniface, Schappacher 2001], p. 239: *So sind z. B. drei Finger zunächst die charakteristische Invariante der Klasse, welche nur aus Scharen von je 3 Objekten besteht.*

[59] [Kronecker 1891], p. 27, in [Boniface, Schappacher 2001], p. 239: *Jede Ordnungszahl charakterisiert also eine bestimmte Klasse von äquivalenten Scharen.*

[60] [Kronecker 1891], pp. 31–32, in [Boniface, Schappacher 2001], p. 243: *So kennt die Logik eigentlich nur einen Menschen, welcher sterblich ist, und zwar ist das der Cajus, während in der Rechtswissenschaft stets der Titus als Stündenbock herhalten muß. ... Hier leuchtet jedem auch ohne Beglaubigungsurkunde ein, daß in dem einen Falle der Cajus, in dem anderen der Titus die Menschheit* in genere *repräsentiert.*

Kronecker agrees with Gauss concerns the primacy of arithmetic among scientific subjects; Kronecker accepts as his own, in the article of 1887, the famous passage by Gauss, quoted by W. Sartorius von Waltershausen:

> Mathematics is the queen of the sciences and arithmetic is the queen of mathematics. From time to time it condescends to pay service to astronomy and other natural sciences, but it ranks first in all circumstances.[61]

This primacy of arithmetic goes hand in hand with its status of pure science, that is, science which is independent from reality. Kronecker refers also to Gauss on this point, and he expresses this idea in the same terms as the latter:

> The difference in principles between geometry and mechanics on the one hand and the remaining mathematical disciplines, here understood as "arithmetic" on the other hand, consists, according to Gauss, in the fact that the object of the latter, number, is *solely* the product of our mind, whereas space, as well as time, also has a *reality, outside* our mind, to which we cannot entirely prescribe its laws *a priori*.[62]

Kronecker's insistence on refering to Gauss does not go, however, without certain differences, even certain oppositions between the two mathematicians. Concerning the boundaries of arithmetic, for example, Kronecker differs from Gauss: while the latter considered "arithmetic" in a strict sense, i.e., as the theory of integers, Kronecker gathered under this term the set of pure mathematics (arithmetic, analysis and algebra). He highlighted this difference of point of view in his lessons on number theory, [Kronecker 1901]. He underlined that the limitation of the domain of arithmetic to the integers alone, stated by Gauss, was no longer accepted when the subject developed. He added that the frontier between the three subjects, arithmetic, algebra and analysis is not, in fact, always respected by Gauss himself: the whole seventh section of the *Disquisitiones Arithmeticae* deals with the theory of the circle division, which takes trigonometric magnitudes, as well as irrational numbers, into consideration.

[61] [Kronecker 1887/1968], vol. 3, p. 252: *Die Mathematik ist die Königin der Wissenschaften und die Arithmetik die Königin der Mathematik. Diese lasse sich dann öfter herab, der Astronomie und anderen Naturwissenschaften einen Dienst zu erweisen, doch gebühre ihr unter allen Verhältnissen der erste Rang.* Kronecker added in a footnote: "cf. 'Gauss zum Gedächtniss' from W. Sartorius v. Waltershausen, Leipzig 1856, p. 79. On page 97 of this text, *ho theos arithmetidsei* is mentioned as a motto of Gauss, which is confirmed by a letter, found in G. Lejeune-Dirichlet's Nachlass, from Gauss's doctor, Baum, to Humboldt." On this motto, see chap. III.2 by J. Ferreirós [Editors' note].

[62] [Kronecker 1887/1968], p. 253: *Der prinzipielle Unterschied zwischen der Geometrie und Mechanik einerseits und zwischen den übrigen hier unter der Bezeichnung "Arithmetik" zusammengefassten mathematischen Disciplinen andererseits besteht nach* Gauss *darin, daß der Gegenstand der letzteren, die Zahl,* bloss *unseres Geistes Product ist während der Raum ebenso wie die Zeit auch* ausser *unserem Geiste eine* Realität *hat, der wir a priori ihre Gesetze nicht vollständig vorschreiben können.* Kronecker refers here to Gauss's letter to Bessel of April 9, 1830, quoted above, [Gauss & Bessel 1880], in [Gauss 1900], p. 201, transl. in [Ewald 1996], vol. 1, p. 301.

The difference between Gauss's and Kronecker's conceptions about the frontier of arithmetic is in relation with their conception of number. The extension given to arithmetic by each of the two mathematicians is indeed in inverse proportion to the extension each one gives to the concept of number. We have seen that for Gauss the successive widenings of the concept of number were the most important feature of the development of pure mathematics. Thus, he originally limited arithmetic to the positive integers alone, but associated to this position a concept of number which includes the rational, irrational, and complex numbers, and which therefore concerns not only arithmetic, but also algebra and analysis. For Kronecker, on the contrary, the concept of number must be strictly limited to positive integers, while arithmetic is extended to algebra and to analysis. It is very important for Kronecker to keep the initial meanings of the concept of number and, more generally, of fundamental concepts, because by widening these concepts to adapt them to other scientific areas, their meanings risk being diluted.[63] Thus fundamental mathematical concepts have fixed meanings, determined by experience, and must not be changed. A generalization of the concept of number and, therefore, a development of mathematics through an extension of the domain of its objects are thus forbidden.

This philosophical difference between Gauss and Kronecker concerning the fundamental concepts also radically separates Kronecker from those contemporaries who participated in the arithmetization movement. Neverthless, Kronecker also claimed he wanted to *arithmetize* mathematics. Do they mean the "same" arithmetization? Otherwise, what difference is there between Kronecker's arithmetization project and, for example, Weierstrass's? In fact, Kronecker's project goes exactly in the opposite direction from Weierstrass's. The latter, as we saw above, wanted to define analytical concepts from arithmetical ones, and particularly from the concept of an integer, and so doing, to incorporate arithmetic into analysis. For Kronecker, what matters, on the contrary, is to bring analysis and algebra back into the domain of a general arithmetic (*allgemeine Arithmetik*), from which the non-arithmetical concepts of analysis, such as those of magnitude and of continuity, are excluded.[64]

[63] See [Kronecker 1891], lesson 3, p. 15, in [Boniface, Schappacher 2001], p. 231: *Wenn wir den Grössenbegriff z.B. ganz allgemein fassen, sodass er auch noch für Geometrie und Mechanik gilt, so muss er mehr und mehr verschwimmen. … Eindeutig kann man freilich den Begriff nicht fixieren, da es überhaupt keinen eindeutigen Begriff im mathematischen Sinne giebt, aber die Vieldeutigkeit muss so gering wie möglich sein. Ist dies nicht der Fall, so gleicht die Zahl einer abgegriffenen Münze, deren Prägung nicht mehr recht zu erkennen ist – oder ich kann den Besitz eines solchen Zahlbegriffs demjenigen des Geldes vergleichen in einem Staate, wo nicht mehr Gold- und Silberwährung alleine, sondern auch Papierwährung besteht.*

[64] [Kronecker 1891], lesson 2, p. 11, in [Boniface, Schappacher 2001], p. 227: *Dem Begriffe der Stetigkeit, welcher in der Geometrie oder der Mechanik in gewisser Weise vorhanden ist, steht die Diskontinuität der Zahlenreihe gegenüber. Diesen Gegensatz hat man auf alle mögliche Weise zu überbrücken versucht und die Stetigkeit in der Arithmetik auf irgend eine Weise hervorzaubern wollen. Mir fällt bei diesen vergeblichen Bemühungen immer das Wort aus der Hexenküche ein: "Ein vollkommener Widerspruch / Ist gleich geheimnisvoll für Weise und für Thoren."*

Thus it is the relationship between arithmetic and analysis, even the cancellation of the one for the benefit of the other, which was at stake in the conflict which opposed Kronecker and Weierstrass. This conflict originates in a difference of conception of number already clearly manifest between Gauss and Weierstrass. If, as we have just seen, concerning the concept of number, the inheritance was from Gauss to Weierstrass, rather than from Gauss to Kronecker, this is not the case for other concepts. Kronecker is certainly among those who knew best how to use operative concepts as well as Gauss's methods, by generalizing and applying them to another area. One can mention, for instance, the notions of equivalence, of class and of invariant, that Kronecker used in his definition of number (see above), and the notion of congruence, which will allow him to avoid introducing the concepts of negative number and of fractional number (see below). One of the Gaussian concepts that Kronecker also most particularly praised was that of composition:

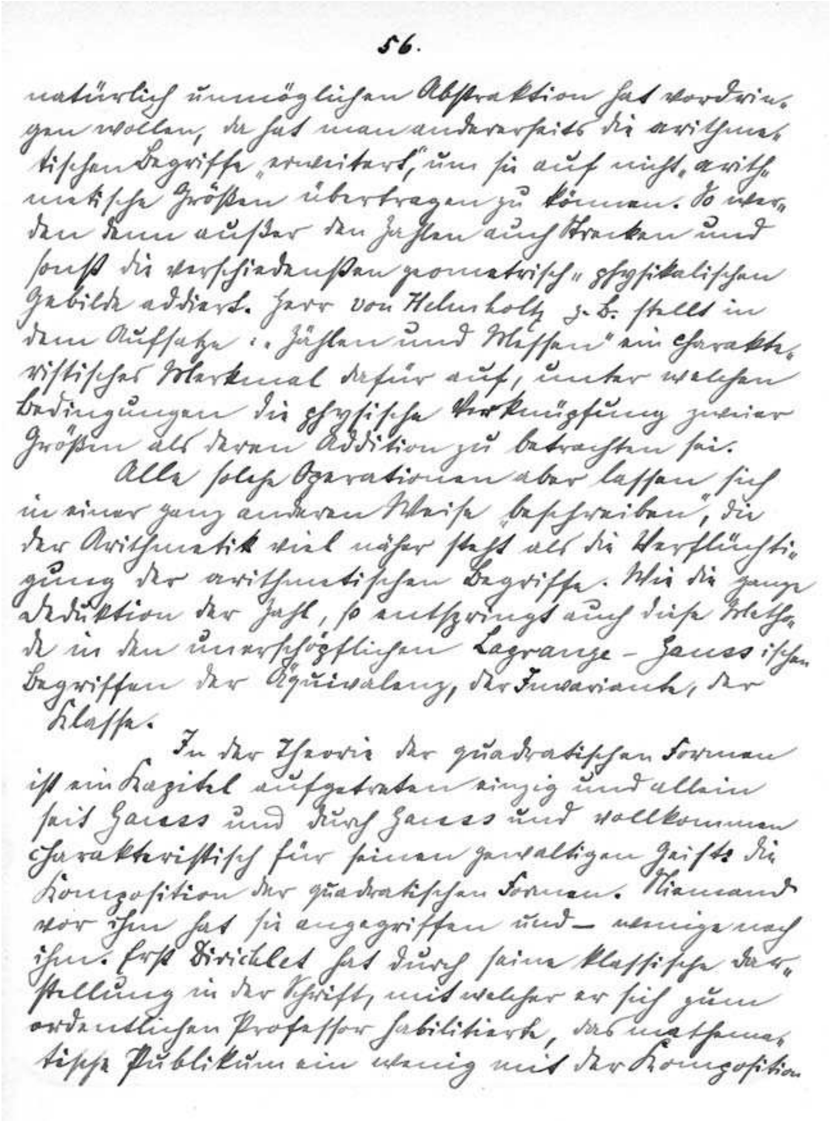
> All the new theory of complex numbers, as well as Kummer's ideal divisor theory, are nothing else but Gauss's composition.[65]

This concept has one avantage: it avoids the widening of the concept of addition refused by Kronecker. Composition, rigorously defined, applies legitimately to the number systems, whereas addition applies just to positive integers. Thus composition plays for addition the role of equivalence for equality: composition and equivalence generalize the elementary relations of addition and equality, and prevent from resorting to fictitious relations. Composition, equivalence, congruence, etc. are operative concepts: they do not create any new object, but they make certain operations possible and legitimate. Besides these concepts, Gauss made a very important contribution, acknowledged as such by Kronecker, which consisted in the consideration of letters not any more as "unknowns" but as "indeterminates." Here is what Kronecker precisely said about this:

> Euler was the first to generalize the problems of diophantine analysis to quadratic equations. But, as it was only important to him to solve certain problems, Lagrange was the first one to consider for themselves the quadratic expressions and thus he founded the theory of quadratic forms that Gauss developed. Lagrange wrote the quadratic forms under the form:
>
> $$ax^2 + bxy + cy^2$$
>
> and found the integer values x and y for which $ax^2 + bxy + cy^2 = n$, in which n is an integer. Gauss made then the great step forward, while considering x and y no longer as unknowns, but as indeterminates (indeterminatae).[66]

[65] [Kronecker 1891], lesson 11, p. 57, [Boniface, Schappacher 2001], p. 261: *Die ganze neue Theorie der komplexen Zahlen, auch Kummers berühmte Theorie der idealen Teiler ist nichts als Gaussische Komposition.*

[66] [Kronecker 1891], lesson 4, p. 20, [Boniface, Schappacher 2001], p. 234: *Euler war der erste, welcher die Aufgaben der diophantischen Analytik für quadratische Gleichungen verallgemeinerte. Während es ihm aber bloß darauf ankam, gewisse Aufgaben zu lösen, begann Lagrange, die quadratischen Ausdrücke für sich zu betrachten, und begründete*



56.

natürlich unmöglichen Abstraktion hat vordringen wollen, da hat man andererseits die arithmetischen Begriffe „erweitert", um sie auf nicht-arithmetische Größen übertragen zu können. So werden denn außer den Zahlen auch Strecken und sonst die verschiedensten geometrisch- physikalischen Gebilde addiert. Herr von Helmholtz z. B. stellt in dem Aufsatze: „Zählen und Messen" ein charakteristisches Merkmal dafür auf, unter welchen Bedingungen die physische Verknüpfung zweier Größen als deren Addition zu betrachten sei.

Alle solche Operationen aber lassen sich in einer ganz anderen Weise „beschreiben", die der Arithmetik viel näher steht als die Verflüchtigung der arithmetischen Begriffe. Wie die ganze Addition der Zahl, so entspringt auch diese Methode in den unerschöpflichen Lagrange-Gauss'ischen Begriffen der Äquivalenz, der Invarianten, der Klasse.

In der Theorie der quadratischen Formen ist ein Kapitel aufgetreten einzig und allein seit Gauss und durch Gauss und vollkommen charakteristisch für seinen gewaltigen Geist: die Komposition der quadratischen Formen. Niemand vor ihm hat sie angegriffen und – wenige nach ihm. Erst Dirichlet hat durch seine klassische Darstellung in der Schrift, mit welcher er sich zum ordentlichen Professor habilitierte, das mathematische Publikum ein wenig mit der Komposition

Fig. V.1B. Gauss's step forward in the theory of quadratic forms, in lesson 4 of Kronecker's 1891 course (Courtesy of the Bibliothèque de l'IRMA, Strasbourg)

damit die Theorie der quadratischen Formen, deren Ausbildung wir Gauss verdanken. Lagrange schrieb die quadratischen Formen in der Gestalt $ax^2 + bxy + cy^2$ und suchte die ganzzahligen Werte x und y, für welche $ax^2 + bxy + cy^2 = n$ ist, wo n eine ganze Zahl bedeutet. Gauss tat nun der großen Schritt, daß er nicht mehr x und y als Fragewörter betrachtete, sondern als Unbestimmte, indeterminatae.

It is known that the use of indeterminates is one of the most characteristic methods of the Kroneckerian style. To specify this method, also widely inspired from Cauchy, we shall see how the latter linked the use of indeterminates with a calculation of congruences (on the polynomial ring with one indeterminate and real coefficients) in order to avoid the use of $\sqrt{-1}$ sign. He explained his method in his memoir entitled "On the theory of algebraic equations substituted to the theory of imaginaries":

> In the theory of algebraic equivalences substituted to the theory of imaginaries, the letter i will cease to represent the $\sqrt{-1}$ symbolic sign that is completely rejected and that can be given up with no regret, since we do not know what this so-called sign means nor what meaning should be given to it. On the contrary, we shall represent the letter i by a real but undetermined quantity; and, by substituting the $\underline{\smile}$ sign to the $=$ sign, we transform what was called an imaginary equation into an algebraic equivalence, depending on the variable i and the divisor $i^2 + 1$. In fact, as this divisor remains the same in all formulas, it is thus possible to avoid writing it. It will be enough to admit, as we shall indeed do, that the $\underline{\smile}$ sign always indicates an algebraic equivalence with respect to the divisor $i^2 + 1$. This being admitted, one will go without effort from equations containing a real variable to equivalences which must replace the imaginary equations.[67]

Cauchy, as Kronecker suggested later, substituted an algebraic equivalence for an equality which would be illegitimate, "imaginary" as Cauchy said. Kronecker took up Cauchy's method precisely in order to *avoid* the concepts of negative number and of fractional number. Thus, to avoid the introduction of the concept of negative number, he replaces equality by a congruence and the "minus" sign by an indeterminate:

> The concept of negative number can be avoided by replacing, in the formulas, the -1 factor by an indeterminate x and the equality by Gauss's congruence sign modulo $(x + 1)$. Thus the equality: $7 - 9 = 3 - 5$ changes into the congruence $7 + 9x \equiv 3 + 5x \bmod x + 1$.[68]

[67] [Cauchy 1847/1938], 2nd part of the memoir, pp. 100–101: *Dans la théorie des équivalences algébriques substituée à la théorie des imaginaires, la lettre i cessera de représenter le signe symbolique* $\sqrt{-1}$ *que nous répudierons complètement, et que nous pouvons abandonner sans regret, puisqu'on ne saurait dire ce que signifie ce prétendu signe, ni quel sens on doit lui attribuer. Au contraire, nous représenterons par la lettre i une quantité réelle, mais indéterminée; et en substituant le signe* $\underline{\smile}$ *au signe =, nous transformons ce qu'on appelait équation imaginaire en une équivalence algébrique, relative à la variable i et au diviseur* $i^2 + 1$*. D'ailleurs ce diviseur restant le même dans toutes les formules, on pourra se dispenser de l'écrire. Il suffira d'admettre, comme nous le ferons effectivement, que le signe* $\underline{\smile}$ *indique toujous une équivalence algébrique relative au diviseur* $i^2 + 1$*. Cela posé, on passera sans peine des équations qui renferment une variable réelle aux équivalences qui devront remplacer les équations imaginaires.*

[68] [Kronecker 1887/1968], p. 260: *Der Begriff der* negativen *Zahlen kann vermeiden werden, indem in den Formen der Factor* -1 *durch eine Unbestimmte x und das Gleichheitszeichen durch das Gauss'sche Congruenzzeichen* modulo $(x + 1)$ *ersetzt wird. So wird die Gleichung* $7 - 9 = 3 - 5$ *in die Congruenz* $7 + 9x \equiv 3 + 5x \bmod x + 1$ *transformiert.*

Thus there seems to exist a filiation from Gauss to Kronecker through Cauchy, in which operative concepts and the use of indeterminates are transmitted, whose goal is to avoid the introduction of new symbolical signs (Cauchy) or new objects (Kronecker).[69]

5. Conclusion

The conquest of several mathematical areas by arithmetic, which we mentioned in the introduction, was thus achieved through two rival ways, both stemming from Gauss's work. The first one, followed by Weierstrass, Dedekind and Cantor, borrowed the conception of number from Gauss. This conception entailed a development of mathematics through the *extension* of this concept of number and the introduction of new numbers. At the close of the conquest, which was to lead, in particular, to the arithmetization of analysis, "the captive analysis captured its savage victor,"[70] and arithmetic was reduced to a simple province of analysis. The second way, followed by Kronecker who rejected this annexation of arithmetic by analysis, borrowed other concepts and methods, also from Gauss. These concepts, more related to operations than to objects, had to avoid the extension of the concept of number and the proliferation of new numbers. Thus Kronecker proposed this deployment of operations as an alternative to the development of the mathematical subject matter through conceptual extension. These two approaches – conceptual extension (and the consequent widening of the domain of objects) or operative deployment – appear more generally as distinct paths to mathematical progress. These two ways, usually coming one after the other, are combined in Gauss's work. Thus this work stops the pendular swing from the concept (or the object) to the operation and vice versa.

Acknowledgments

I would like to thank all the participants in the 2001 Oberwolfach Conference for their stimulating comments.

References

Bolzano, Bernard. 1817. Rein analytischer Beweis des Lehrsatzes, dass zwischen je zwey Werthen, die ein entgegengesetztes Resultat gewähren, wenigstens eine reelle Wurzel der Gleichung liege. Praha: Gottlieb Haase. Repr. in *Abhandlungen der Königlichen Böhmischen Gesellschaft der Wissenschaften* 5, 1–60. English transl.: S. Russ. A translation of Bolzano's paper on the intermediate value theorem. *Historia Mathematica* 7(2) (1980), 156–185. Repr. in [Ewald 1996], vol. 1, pp. 225–248.

Boniface, Jacqueline. 2002. *Les constructions des nombres réels dans le mouvement d'arithmétisation de l'analyse*. Paris: Ellipses.

[69] Kronecker described as "a classical inconsequency" (*eine geradezu klassische Inkonsequenz*) Gauss's use of imaginary quantities in the *Commentatio secunda theoriae residuorum biquadraticorum*, while he had avoided them in his first proof of the fundamental theorem of algebra, for instance; see [Kronecker 1891], p. 19, [Boniface, Schappacher 2001], p. 233.

[70] We paraphrase Horace's famous verse: *Graecia capta ferum victorem cepit* (Horace, *Epistulae*, II, 1, v. 156).

Boniface, Jacqueline, Schappacher, Norbert. 2001. “Sur le concept de nombre dans la mathématique”. Cours inédit de Leopold Kronecker à Berlin (1891). *Revue d’Histoire des mathématiques* 7, 207–275.

Brunschvicg, Léon. 1912. Les Étapes de la philosophie mathématique. Paris: Alcan. 3rd ed., PUF, 1947. Repr. with a preface by J.-T. Desanti. Paris: Blanchard, 1981.

Cantor, Georg. 1872. Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen. *Mathematische Annalen* 5, 123–132. Repr. in [Cantor 1932], pp. 92-102.

———. 1883. *Grundlagen einer allgemeinen Mannigfaltigkeitslehre. Ein mathematisch-philosophischer Versuch in der Lehre des Unendlichen.* Leipzig: Teubner. Repr. (without the preface): Über unendliche lineare Punktmannigfaltigkeiten 5, *Mathematische Annalen* 21 (1883), 545–591. Repr. in [Cantor 1932], pp. 165–209. English transl. in [Ewald 1996], vol. 2, pp. 878–920.

———. 1932. *Gesammelte Abhandlungen mathematischen und philosophischen Inhhalts*, ed. E. Zermelo. Berlin: Springer. Repr. Hildesheim: G. Olms, 1966.

Cassirer, Ernst. 1923–1929. *Philosophie der symbolischen Formen.* 3 vols. Berlin: Bruno Cassirer. 2nd ed. Darmstadt: Wissenschafliche Buchgesellschaft, 1953–1954. Repr. with annotations in *Gesammelte Werke: Hamburger Ausgabe*, ed. B. Recki, vols. 11–13. Hamburg: Felix Meiner, 2001–2002. English transl. R. Manheim, *Philosophy of Symbolic Forms.* New Haven: Yale University Press, 1953–1957.

Cauchy, Augustin Louis. 1847. Mémoire sur la théorie des équivalences algébriques substituées aux équations imaginaires. In *Exercices d’analyse et de physique*, vol. 4. Paris: Bachelier. Repr. in *Œuvres complètes*, ser. 2, vol. 14, pp. 93–120. Paris: Gauthier-Villars, 1938.

Crilly, Tony. 1986. The Rise of Cayley’s Invariant Theory (1841–1862). *Historia Mathematica* 13, 241–254.

Dedekind, Richard. 1888. *Was sind und was sollen die Zalhen?* Braunschweig: Vieweg. 2nd ed. (with a new preface), 1893; 3rd ed. (with a new preface), 1911. Repr. in [Dedekind 1930–1932], vol. 3, p. 335-391. English transl. in [Ewald 1996], vol. 2, pp. 790–833.

———. 1930–1932. *Gesammelte mathematische Werke*, ed. R. Fricke, E. Noether, O. Ore. 3 vols. Braunschweig: Vieweg. Repr. 2 vols. New York: Chelsea, 1969.

Dugac, Pierre. 1973. Eléments d’analyse de Karl Weierstrass. *Archive for History of Exact Sciences* 10, 41–176.

Ewald, William B. 1996. *From Kant to Hilbert. A Source Book in the Foundations of Mathematics.* 2 vols. Oxford: Clarendon Press. 2nd ed., Oxford: Oxford UP, 2000.

Frege, Gottlob. 1884. *Die Grundlagen der Arithmetik: eine logisch-mathematische Untersuchung über den Begriff der Zahl.* Breslau: Koebner. New critic. ed. C. Thiel. Hamburg: Meiner, 1986. English transl. J. L. Austin, *The Foundations of Arithmetic: A Logic-Mathematical Enquiry into the Concept of Number.* Oxford: Blackwell, 1950; 2nd rev. ed., 1974.

Gauss, Carl Friedrich. 1863–1929. *Werke*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. 12 vols. Göttingen: Universitäts-Druckerei (vol. 1–vol. 6), Leipzig: Teubner (vol. 7–vol. 10.1), Berlin: Julius Springer (vol. 10.2–vol. 12). Repr. Hildesheim, New York: Olms, 1981.

———. 1900. *Arithmetik und Algebra: Nachträge zu Band 1–3.* [Gauss 1863-1929], vol. VIII.

———. 1929.*Varia. Atlas des Erdmagnetismus*. [Gauss 1863-1929], vol. XII.

Gauss & Bessel. 1880. *Briefwechsel zwischen Gauß und Bessel*, ed. A. Auwers. Leipzig: W. Engelmann. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 1. Hildesheim: G. Olms, 1975.

Gauss & Schumacher. 1860–1865. *Briefwechsel zwischen C. F. Gauß und H. C. Schumacher*, ed. Chr. A. F. Peters. 6 vols. Altona: Esch. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 5. 3 vols. Hildesheim: Olms, 1975.

Granger, Gilles-Gaston. 1994. *Formes, opérations, objets*. Mathesis. Paris: Vrin.

Hilbert, David. 1897. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4 ("1894–1895"), 177–546 + Vorwort i–xviii. Repr. in [Hilbert 1932], pp. 63–363. English transl. I. Adamson, *The Theory of Algebraic Number Fields*, intr. F. Lemmermeyer, N. Schappacher. New York: Springer, 1998.

———. 1932. *Gesammelte Abhandlungen*, vol. 1. Berlin: Springer, 1932. 2nd ed., 1970.

Kant, Immanuel. 1781. *Kritik der reinen Vernunft*. Riga: Hartknoch. 2nd rev. ed., 1787. Repr. in *Kant's Gesammelte Schriften*, ed. W. Dilthey, vol. 4 and vol. 3. Berlin: Reimer, 1911.

Kronecker, Leopold. 1887. Über den Zahlbegriff. *Journal für die reine und angewandte Mathematik* 101, 337–355. Repr. in *Werke*, ed. K. Hensel, vol. 3(1), pp. 249–274. Leipzig: Teubner, 1899. Repr., New-York: Chelsea, 1968.

———. 1891. Vorlesungen Sommersemester 1891. Manuscript in Bibliothèque de l'IRMA, Strasbourg. Ed. in [Boniface, Schappacher 2002].

———. 1901. *Vorlesungen über Zahlentheorie*, ed. K. Hensel. Leipzig: Teubner.

Méray, Charles. 1892. Considérations sur l'enseignement des mathématiques. *Revue bourguignonne de l'enseignement supérieur*, 105–129; 269–295.

———. 1894. *Leçons nouvelles sur l'analyse infinitésimale et ses applications géométriques*. 1st part. *Principes généraux*. Paris: Gauthier-Villars.

Molk, Jules. 1885. Sur la notion de divisibilité et sur la théorie générale de l'élimination. *Acta mathematica* 6, 1-166.

Weierstrass, Karl. 1878. Einleitung in die Theorie der analytischen Funktionen. Sommer-Semester Vorlesung, course notes by A. Hurwitz. Manuscript in Library of the ETH, Zürich. Partial ed. in [Dugac 1973], pp. 96–118.

———. 1886. Ausgewählte Kapitel aus der Funktionenlehre. Sommer-Semester Vorlesung, notes by G. Thieme. Manuscript in Mathematisches Institut, Humboldt Universität, Berlin. Partial ed. in [Dugac 1973], pp. 129–136.

V.2

On Arithmetization

Birgit Petri and Norbert Schappacher

Hardly used today, the term "arithmetization" (*Arithmetisierung, arithmétisation*) was in use around 1900 as a generic description of various programmes which provided non-geometrical foundations of analysis, or other mathematical disciplines. These programmes included constructions of the continuum of real numbers from (infinite sets, or sequences, of) rational numbers, as well as clarifications of the notion of function, limit, etc.[1]

More or less detailed descriptions of arithmetization can be found in every history of XIX$^{\text{th}}$ century mathematics, and numerous special studies have been published.[2] The *raison d'être* of the present chapter in this book is the question whether (and in which way) Gauss's *Disquisitiones Arithmeticae*, and the image of arithmetic they created, influenced the arithmetization of analysis.[3] There is no simple-minded answer to this question because the arithmetization of analysis was a multi-faceted process which, at any given time, was represented by mathematicians with different, often conflicting agendas. For instance, the antagonism between Richard Dedekind's

[1] The word "arithmetization" was taken up in other contexts in the 1930s: for the Gödelization of formalized theories, and by Oscar Zariski to describe his rewriting of Algebraic Geometry which was inspired by Wolfgang Krull's "arithmetic" theory of ideals and valuations. Such later developments will not be treated in this chapter.

[2] From the early encyclopedia articles [Pringsheim 1898], [Molk 1909] to a special study like [Dugac 1976], and a more reflective general essay like [Jahnke, Otte 1981]. Among recent publications, we mention [Boniface 2002] and [Dugac 2003], and recommend particularly [Epple 1999/2003] as a concise introduction to the subject.

[3] The present chapter is therefore a natural continuation of J. J. Ferreirós's chap. III.2 above – cf. [Bekemeier 1987]; the retrospective usage of the word arithmetization in reference to Cauchy, Ohm, and others was encouraged by Klein, see § 3.2 below – and is partly parallel to J. Boniface's chap. V.1.

approach and Leopold Kronecker's, which was discussed in § 3.4 of chap. I.2 above in the context of the further development of Kummer's theory of ideal numbers, reappears here via conflicting programmes of arithmetization.

In order to better understand the history of arithmetization, we distinguish major periods of it. The final answer to the initial question suggested by our investigation is that Gaussian elements become blurred to the point of being undetectable as soon as the Göttingen *nostrification* presented arithmetization as a unified movement in the last years of the XIX$^{\text{th}}$ century; see § 3.2 below.

1. The End of the Theory of Magnitudes[4] in 1872

The general post-XVII$^{\text{th}}$ century notion of number, commonly accepted until the middle of the XIX$^{\text{th}}$ century, was formulated for instance by Newton like this:

> By number we understand not a multitude of units, but rather the abstract ratio of any one quantity to another of the same kind taken as unit. Numbers are of three sorts; integers, fractions, and surds: an integer is what the unit measures, the fraction what a submultiple part of the unit measures, and a surd is that with which the unit is incommensurable.[5]

Numbers were thus defined in terms of magnitudes, or quantities; the foundation of the continuum was geometry, or at any rate not arithmetic.

The year 1872 saw the publication of four papers in Germany each of which presented a new arithmetic theory of the real numbers detaching numbers from magnitudes.[6] In § 1 and § 2, we recall salient features of these theories. We start with Charles Méray from Dijon who had already published his arithmetization in France slightly earlier.

1.1. Charles Méray

Charles Méray[7] seems to have been the first to publish an arithmetization of the irrational numbers. It appeared in 1870 as part of the report of the 1869 congress of the *Sociétés savantes* and seems to have gone unnoticed on what would soon be the other side of the war lines, in Germany.[8] Yet, there were analogies: Méray and

[4] We borrow this very appropriate title from [Epple 1999/2003].

[5] [Newton 1707], p. 2: *Per numerum non tam multitudinem unitatum quam abstractam quantitatis cujusvis ad aliam ejusdem generis quantitatem quæ pro unitate habetur rationem intelligimus. Estque triplex; integer, fractus & surdus: Integer quem unitas metitur, fractus quem unitatis pars submultiplex metitur, & surdus cui unitas est incommensurabilis.*

[6] [Kossak 1872] (containing an incomplete digest of Karl Weierstrass's introduction of real numbers), [Heine 1872] (based on what he had learned from Cantor), [Cantor 1872], and [Dedekind 1872].

[7] See [Boniface 2002], pp. 48–56, for biographical notes on Méray (1835–1911).

[8] [Méray 1869]. In his 1899 report on Méray to the Academy, Henri Poincaré described Méray and Weierstrass as working on different planets; see [Dugac 1973], p. 139: *les deux savants ont travaillé d'une façon aussi indépendante que s'ils avaient habité des planètes différentes.*

Dedekind (see § 1.3 below) shared the provincial situation within their countries and dissatisfaction with the lack of foundational rigour in the usual teaching of analysis. Both considered "such an elementary and arid subject" almost unfit for an ordinary mathematical publication.[9] But both insisted that formulas such as $\sqrt{a} \cdot \sqrt{b} = \sqrt{ab}$ had to be justified. Dedekind would actually claim in 1872 that such propositions "as far as I know have never been really proved,"[10] which corroborates his lack of awareness of [Méray 1869], p. 288. On the other hand, both Méray and Cantor (see § 1.2) used Cauchy sequences of rational numbers – called *variables progressives convergentes* in [Méray 1869] – with the same unpedagogical twist of calling them convergent even before they had served to define their own limit.[11] Méray also called them sequences "having a (fictitious) limit," as opposed to those "that have a (numerical [i.e., rational]) limit."[12]

Sequences that differ by a sequence tending to zero are called *équivalentes* by Méray, but he avoided treating the equivalence classes as objects. In fact, contrary to his successors Dedekind and Cantor, Méray did not construct the continuum from rational numbers, but wanted to eliminate "the rather obscure concept of irrational number."[13] A good deal of analysis thus turned merely symbolic in Méray's view:

> Finally, a sign adequate to recall both the nature of the calculations which define v_n and the rational values of the quantities with which they are to be performed, will conveniently designate in the language the fictitious limit. The same sign could represent in the formulas the undetermined rational number which represents its approximate value, computed to a higher and indefinitely growing degree of approximation, i.e., really, any progressive variable equivalent to v.[14] ... [A]ny equation between rational or irrational quantities is really the abridged and picturesque enunciation of the fact that certain calculations performed on the rational value of those, on progressive variables which have the others as fictitious limits, and if necessary on integers tending to infinity, yield a progressive variable tending to zero independently of the relation established between these integers and independently of the way in

[9] [Méray 1869], p. 281: *C'est ce que je me propose d'exposer aussi brièvement que le commande la nature élémentaire et aride d'un pareil sujet.*

[10] [Dedekind 1872/1932], p. 330: *man gelangt auf diese Weise zu wirklichen Beweisen von Sätzen (wie z.B. $\sqrt{2} \cdot \sqrt{3} = \sqrt{6}$), welche meines Wissens bisher nie bewiesen sind.*

[11] [Méray 1869], p. 284: *Il nous faut un terme spécial pour exprimer la propriété remarquable* ... [$|v_{n+p} - v_p| \to 0$]: *je dirai que la variable progressive v est* convergente. See footnote 26 below.

[12] [Méray 1869], p. 284: *pour exprimer la convergence de la variable, on dira simplement:* elle a une limite (fictive).

[13] [Méray 1869], p. 281: ... *on échappe à la nécessité d'introduire dans le raisonnement la conception assez obscure de nombre incommensurable.*

[14] [Méray 1869], p. 285: *Enfin un signe quelconque propre à rappeler, à la fois, la nature des calculs qui définissent v_n et les valeurs numériques des quantités sur lesquelles on doit les exécuter, désignera commodément dans le langage, la limite fictive; le même signe pourra représenter dans les formules le nombre indéterminé qui en représente la valeur approchée, calculée à un degré d'approximation de plus en plus et indéfiniment élevé, c'est-à-dire, au fond, toute variable progressive équivalente à v.*

> which we change the nature of the progressive variables used for the calculation, provided they remain equivalent.[15]

The identity $\sqrt{a} \cdot \sqrt{b} = \sqrt{ab}$ is thus analyzed as saying that, "if α, β, γ are any rational sequences whose squares tend to a, b, ab, then the difference $\alpha\beta - \gamma$ tends to zero."[16] Méray's 1869 note ends with such explanations and never discusses the completeness of the continuum, even though one of the principles of the mathematical theory of limits isolated at the beginning of [Méray 1869] (p. 280) is the convergence of Cauchy sequences.[17] His goal to eliminate irrationals from the theory is a prominent point of contact with Kronecker's programme of arithmetization (see § 2 below), even though Méray's distinction betweeen *le langage*, i.e., the symbolic formalism of roots and other irrationals habitually used in analysis, and *le calcul*, performed exclusively in the domain of rational numbers, seems at odds with Kronecker's precise ideas about how to reduce analysis to general arithmetic.

The primal difference between Méray and his German successors, however, was that he was not seeking the *arithmetization* of analysis, but its *algebraization*. He shared no scientific ideal nurtured by number theory; he did not pretend, as Dedekind would, to have fathomed the essence of continuity. Méray's ideal of rigour was formal and algebraic; his hero was not the Gauss of the D.A., but Lagrange, the algebraic analyst. And when Méray pleaded for building function theory not on the turbid notion of continuity but on analyticity and the algebra of power series, this was again a reference to Lagrange, not to Weierstrass.[18]

1.2. Georg Cantor's Extension of a Result in the Theory of Trigonometric Series

According to his own *curriculum vitae*, Georg Cantor studied both Gauss's *Disquisitiones Arithmeticae* and Legendre's *Théorie des nombres* around 1866, and these readings inspired his 1867 doctoral dissertation[19] as well as his 1869 habilitation memoir.[20] One of the theses he proposed for his doctoral defense was: "In arithmetic, purely arithmetic methods are vastly superior to analytic ones."[21]

[15] [Méray 1869], p. 287: *une équation ... entre des quantités commensurables ou incommensurables: c'est l'énonciation abrégée et pittoresque du fait que certains calculs opérés sur la valeur numérique des unes, sur des variables progressives qui ont les autres pour limites fictives, et au besoin sur des nombres entiers croissant à l'infini, donnent une variable progessive qui tend vers zéro, quelque relation que l'on établisse entre ces nombres entiers et de quelque manière que l'on change la nature des variables progressives soumises au calcul, pourvu qu'elles restent équivalentes à elles-mêmes.*

[16] [Méray 1869], p. 288: *signifie que α, β, γ étant des variables commensurables quelconques, dont les carrés tendent vers a, b, ab, la différence $\alpha\beta - \gamma$ tend vers zéro.*

[17] The completeness of the continuum can be reformulated in terms of rational sequences with multiple indices; in this way it is at least implicitly treated in [Méray 1887], § 14.

[18] [Méray 1872], pp. XI–XXIII. Méray called an analytic function *fonction olotrope*.

[19] [Cantor 1932], p. 31. The dissertation is about the integral zeros of ternary quadratic forms, and picks up from D.A., art. 294.

[20] [Cantor 1932], pp. 51–62, on the transformation of ternary quadratic forms.

[21] [Cantor 1932], p. 31: *In arithmetica methodi mere arithmeticae analyticis longe praestant.*

However, contrary to Dedekind's foundational motivation – see subsection 1.3 below – Cantor's theory of "numerical magnitudes in a large sense" (*Zahlengrößen im weiteren Sinne*) was a necessary technical ingredient to formulate the main theorem of [Cantor 1872/1932], and its presentation is accordingly "sketchy" (p. 92).[22] Cantor's main theorem (§ 3, p. 99) says that a Fourier series which is zero everywhere except possibly in a point set "of the ν^{th} kind" (*Punktmenge der* ν^{ten} *Art*) is in fact identically zero. Cantor called a point set of the ν^{th} kind, if ν successive "derivations" of the set, i.e., passing to the set of its accumulation points ν times, leaves only a finite set of points.

Cantor, who had attended Weierstrass's and Kronecker's lectures in Berlin, did point out that his "definitions and operations may serve to good purpose in infinitesimal analysis" (p. 96). One gathers from §§ 1–2 that they amount to a "general, purely arithmetical theory of magnitudes, i.e., one which is totally independent of all geometric principles of intuition." But Cantor first stated this fact explicitly only in 1882.[23] In his 1872 paper, Cantor's *Zahlengrößen* serve a *dual purpose*: they allow him to define the real numbers via (equivalence classes of) Cauchy sequences, but they also give rise to particular sets of rational numbers in the continuum whose limit points are "of the ν^{th} kind."[24]

An "infinite series given by a law" $a_1, a_2, \ldots, a_n, \ldots$ such that "the difference $a_{n+m} - a_n$ becomes infinitely small as n grows" is said to "have a definite limit," or that it is a numerical magnitude in the large sense (§ 1). Given several such series, Cantor associated symbols to them, $b, b', b,'' \ldots$, and defined relations:

$$(1) \quad b = b', \qquad (2) \quad b > b', \qquad (3) \quad b < b',$$

as $a_n - a'_n$ for growing n becomes infinitely small (case 1), stays bigger than a certain positive number (case 2), or stays smaller than a certain negative number (case 3). However, the equality relation $b = b'$ thus defined does *not* mean that Cantor used the symbols $b, b', \ldots$, or the words *Zahlengröße, Grenze*, etc., for equivalence classes of Cauchy sequences: "the identification of two numerical magnitudes $b, b' \ldots$ does not include their identity, but only expresses a certain relation which takes place between the series to which they refer."[25] Cantor wrote $b * b' = b''$, for $*$ denoting any one of the operations $+, -, \times, /$, if the elements of the corresponding series satisfy $\lim(a_n * a'_n - a''_n) = 0$. From these definitions it follows in particular that $b - a_n$ becomes infinitely small for growing n. This justifies *a posteriori* the initial parlance of the "definite limit."[26]

[22] Page- or §-numbers in this subsection refer to [Cantor 1872/1932]: *nur andeutungsweise.*

[23] [Cantor 1879–1884/1932], p. 156, note: *eine allgemeine, rein arithmetische, d.h. von allen geometrischen Anschauungsgrundsätzen vollkommen unabhängige Größenlehre.*

[24] [Cantor 1872], pp. 98–99. For a presentation which focusses exclusively on the construction of real numbers, see [Cantor 1879–1884], part IV, § 9.

[25] [Cantor 1872/1932], p. 95: ... *indem ja schon die die Gleichsetzung zweier Zahlengrößen* b, b' *aus B ihre Identität nicht einschließt, sondern nur eine bestimmte Relation ausdrückt, welche zwischen den Reihen stattfindet, auf welche sie sich beziehen.*

[26] This unpedagogical twist was later avoided in [Cantor 1879–1884/1932], p. 186f. There

If B is the domain of all numerical magnitudes thus obtained, Cauchy sequences of elements of B can be formed because the condition that $b_{m+n} - b_n$ becomes infinitely small as n grows "is conceptually completely determined by the previous definitions" (p. 95).[27] After the obligatory definitions of relations and operations in the domain C thus obtained, one may again form Cauchy sequences from elements of C, and so forth. Cantor called those numerical magnitudes "of the λ^{th} kind" which are obtained as the result of exactly λ subsequent limit processes. He pointed out that, for $\lambda \geq 1$, each numerical magnitude of the λ^{th} kind can be "set equal" to a numerical magnitude of the μ^{th} kind, for all $1 \leq \mu \leq \lambda$ (the continuum is complete).[28] But he insisted on the conceptual difference between the ways in which magnitudes of different kinds are given; a magnitude of the λ^{th} kind will in general be a λ-fold infinite array of rational numbers.[29]

Given a unit, a point on an oriented line with origin o is "conceptually determined" (*begrifflich bestimmt*) by its abscissa. This is unproblematic, if the abscissa is rational. Conversely, if the point is effectively given, "for instance by a construction," then there will be a sequence of points with rational abscissas a_n which will "get infinitely close, as n grows, to the point which is to be determined." In this case, Cantor says that "the distance from o of the point to be determined equals b," where b is the numerical magnitude given by the sequence (a_n) (§ 2, p. 96). One verifies that the topological ordering of the distances to o coincides with the ordering of the corresponding numerical magnitudes. The statement that *every* numerical magnitude (of any order) also determines a point on the line with the corresponding abscissa, is postulated by Cantor as an *axiom*, "since it is in the nature of this statement that it cannot be proven."[30] It endows

> the numerical magnitudes *a posteriori* with a certain objectivity, from which they are, however, totally independent.[31]

Cantor called "fundamental series" (*Fundamentalreihen*) what we call Cauchy sequences today.

[27] Cantor's set phrase *begrifflich ganz bestimmt* sounds like a preemptive defense against constructivist criticism. According to a letter from Cantor to Hermann Amandus Schwarz (see [Cantor 1991], p. 24: March 30, 1870), Leopold Kronecker had doubts about the "Weierstrass-Bolzano Theorem" to the effect that a continuous function on a closed interval attains the boundaries of its range. For Cantor, this theorem was fundamental, and Schwarz needed it to complete a proof of Cantor's first identity theorem for Fourier series; cf. [Cantor 1870], p. 141. It was also the main goal of [Heine 1872]. The fact that the article [Cantor 1872] did not appear in *Journal für die reine und angewandte Mathematik* like most of his preceding articles on the subject, but in *Mathematische Annalen*, may be related to Kronecker's criticism.

[28] Here Cantor never read "=" as "equal," but rather as "set equal" or the like. Dedekind failed to appreciate the interest of this distinction: [Dedekind 1872/1932], p. 317.

[29] [Cantor 1872/1932], p. 95f: *im allgemeinen λfach unendlichen Reihen rationaler Zahlen.*

[30] [Cantor 1872/1932], p. 97: *weil es in seiner Natur liegt, nicht allgemein beweisbar zu sein.*

[31] [Cantor 1872/1932], p. 97: *Durch ihn wird denn auch nachträglich den Zahlgrößen eine*

Admitting this axiom, the points on the line correspond precisely to the equivalence classes of Cauchy sequences.

Already in 1872, Cantor had in mind the transfinite extension of his hierarchy of numerical magnitudes "of the λ^{th} kind":

> The results of analysis (except for a few known exceptions) can all be reduced to such identifications [of numerical magnitudes of different kinds], even though (we just touch upon this here, with a view to those exceptions) the concept of number, as far as it has been developed here, carries in itself the germ for an inherently necessary and absolutely infinite extension.[32]

The transfinite ordinals[33] thus appear as the true completion of Cantor's programme of arithmetization of analysis. They are in contradiction with Gauss's rejection of completed infinites,[34] and thus also a long way from Cantor's arithmetic beginnings in the spirit of the D.A. The theory expounded in [Cantor 1872] also violated Kronecker's constructivity requirement; Cantor gave names ("$b, b', b'', \ldots$") to objects of which it may not be decidable in a finite number of steps whether two of them can be "set equal" to one another.

Cantor's 1872 paper not only defended the freedom to form new concepts, even non-constructively, but also tried to demonstrate the usefulness of distinguishing between sets of various "kinds." The first, methodological aspect makes it similar to [Dedekind 1872]. Their respective axiomatic treatments of the relationship between the arithmetized continuum and points on a line are also quite analogous.[35] The main difference from Dedekind is Cantor's concern for hierarchies according to the way the real numbers are given.[36]

1.3. Richard Dedekind on Continuity and Irrational Numbers

It was under the influence of Dirichlet and Riemann that Richard Dedekind developed his markedly conceptual approach to mathematics. He also traced this "decision for

gewisse Gegenständlichkeit gewonnen, von welcher sie jedoch ganz unabhängig sind.

[32] [Cantor 1872], p. 95: *Auf die Form solcher Gleichsetzungen lassen sich die Resultate der Analysis (abgesehen von wenigen bekannten Fällen) zurückführen, obgleich (was hier nur mit Rücksicht auf jene Ausnahmen berührt sein mag) der Zahlenbegriff, soweit er hier entwickelt ist, den Keim zu einer in sich notwendigen und absolut unendlichen Erweiterung in sich trägt.*

[33] See [Cantor 1879–1884/1932], part IV, p. 167: Cantor had originally regarded them as "infinite whole numbers."

[34] [Cantor 1991], p. 148f: Cantor to Lipschitz, November 19, 1883. [Cantor 1879–-1884/1932], p. 189.

[35] Cf. [Cantor 1889]. In 1882, Cantor claimed that the "hypothesis of the continuity of space" could only mean that the space underlying the phenomena of our experience was in perfect one-to-one correspondence with the "purely arithmetical continuum (x, y, z)," and he referred to [Dedekind 1872] and [Cantor 1872]; see [Cantor 1879–1884/1932], part III, p. 156. To be sure, this hypothesis itself was for Cantor an arbitrary one: *die an sich willkürliche Voraussetzung.*

[36] It is tempting but anachronistic to interpret this in the light of later criticism of impredicative definitions, like for instance in [Weyl 1918].

the intrinsic against the extrinsic" back to his reading of Gauss's *Disquisitiones Arithmeticae*.[37] His little brochure [Dedekind 1872] – a present to his father on the occasion of his 50 years in office, rather than an article in a mathematical journal – is a showcase example of his method; Dedekind exhibited a conceptual analysis of the continuity of the line, and the way in which "the discontinuous domain of the rational numbers has to be completed into a continuous one" follows from it by necessity (p. 323).[38] In particular, Dedekind considered his analysis not as a purely *ad hoc* construction but was convinced that he had discovered a fundamental principle:[39]

> If all the points of the line fall into two classes in such a way that each point of the first class lies left of each point of the second class, then there is one and only one point which produces this partition into two classes, this cutting up of the line.[40]

For Dedekind this was an unprovable axiom "by which we invest the line with the idea of continuity."[41] Its validity relied on the fact that "everybody" will find it compatible with his "idea of the line." This implies neither the reality of space nor its actual continuity, if space has indeed an independent existence (p. 323).

Following this lead, Dedekind constructed the irrational real numbers by "creating" one for each cut of the rationals not produced by a rational number, and extended the order relation from rational numbers (where he had carefully analyzed it before) to these new numbers, and found that "this domain $\mathcal{R}$ now also enjoys continuity:"

> If the system $\mathcal{R}$ of all real numbers splits up in two classes $\mathcal{A}_1, \mathcal{A}_2$ in such a way that each number α_1 of the class $\mathcal{A}_1$ is smaller than each α_2 of the class $\mathcal{A}_2$, then there exists one and only one number α which gives rise to this partition.[42]

In conclusion, he proved that this "principle of continuity" is equivalent to the convergence of all bounded monotone sequences, and to the convergence of all Cauchy

[37] See C. Goldstein's and N. Schappacher's chap. I.2, § 1, footnote 52, Dedekind's quote on D.A., art. 76 cited there, and the references given.

[38] Simple page numbers in this subsection refer to [Dedekind 1872]. Another example of such conceptual work, analyzed in O. Neumann's chap. II.1, § 3, and alluded to in chap. I.2, § 3.2, is Dedekind's emphasis on the notion of irreducibility for sec. 7 of the D.A.

[39] This principle has been interpreted as Dedekind's attempt to contribute to Riemann's notion of continuous manifold; see [Ferreirós 1999], p. 73. Be this as it may, Cantor did try to find such a higher-dimensional generalization; see [Cantor 1991], p. 83: Cantor to Dedekind, September 15, 1882.

[40] [Dedekind 1872/1932], p. 322: *Zerfallen alle Punkte der Geraden in zwei Klassen von der Art, daß jeder Punkte der ersten Klasse links von jedem Punkte der zweiten Klasse liegt, so existiert ein und nur ein Punkt, welcher diese Einteilung aller Punkte in zwei Klassen, diese Zerschneidung der Geraden in zwei Stücke hervorbringt.*

[41] [Dedekind 1872/1932], p. 323: *durch welches wir die Stetigkeit in die Linie hineindenken.* The fact that, between two distinct points, there are infinitely many others appeared unproblematic for Dedekind; see Kronecker's criticism in his 1891 lectures (§ 2.2 below).

[42] [Dedekind 1872/1932], p. 329: *IV. Zerfällt das System $\mathcal{R}$ aller reellen Zahlen in zwei Klassen $\mathcal{A}_1, \mathcal{A}_2$ von der Art, daß jede Zahl α_1 der Klasse $\mathcal{A}_1$ kleiner ist als jede Zahl α_2 der Klasse $\mathcal{A}_2$, so existiert eine und nur eine Zahl α, durch welche diese Zerlegung hervorgebracht wird.*

sequences, thus completing his sketch of a "purely arithmetical and completely rigorous foundation of the principles of infinitesimal analysis."[43] At the same time, he had successfully dissociated the definition of number from the nowhere rigorously defined notion of extensive magnitude (p. 321), and based infinitesimal analysis on (infinite sets of) rational numbers, i.e., ultimately on sets of integers.

The analogy between Dedekind's introduction of irrational numbers via cuts and his replacing Kummer's ideal numbers by ideals, i.e., by infinite sets of algebraic numbers – in other words, the analogy between the ordering of rational numbers according to size, and of algebraic numbers according to divisibility – and the subsequent formal investigation of the sets obtained, strongly suggests that we view these two Dedekindian theories as variations of the same foundational theme. In this sense, Dedekind's "arithmetization"[44] is closely associated with number theory.[45]

2. Arithmetization in the Berlin Way

The publications discussed in § 1 all originated in the province. At the same time and even before 1870, Karl Weierstrass and Leopold Kronecker in Berlin had their own ideas about arithmetization, and had conveyed some of them to their students (like Georg Cantor). But Heine's, Cantor's, and Dedekind's 1872 publications, and possibly other factors, would provoke a greater explicitness in Berlin in the 1870s and 1880s.

2.1. Karl Weierstrass

Weierstrass would later be considered the central figure of arithmetization, in view of the many ambiguities he had cleared up in real and complex function theory, by counterexamples and rigorous exposition. This is why we briefly discuss him here, even though we see at least no *specific* relationship between his approach and the notion of arithmetic initiated by Gauss's *Disquisitiones Arithmeticae*.

Weierstrass's introduction of positive real numbers[46] starts from finite or infinite "aggregates" (*Aggregate*) a of positive fractions $\frac{1}{n}$, i.e., collections of (possibly multiple) copies of such fractions. Finitely many positive multiples of various $\frac{1}{n}$ can be transformed into a multiple of $\frac{1}{d}$, for a common denominator d. This effectively defined equality of finite aggregates and their linear ordering: $a_1 \leq a_2$ if a_1 is transformable by fractional arithmetic into a subaggregate of a_2. Infinite aggregates will in general not admit a common denominator. For two of them, Weierstrass defined $A_1 \leq A_2$ to mean that every finite aggregate which is equal, in the above

[43] [Dedekind 1872/1932], p. 316: *rein arithmetische und völlig strenge Begründung der Prinzipien der Infinitesimalanalysis.*

[44] In the preface of [Dedekind 1872], he spoke about "discovering the proper origin in the elements of arithmetic" (*seinen eigentlichen Ursprung in den Elementen der Arithmetilk zu entdecken*).

[45] To discover the coherence of Dedekind's contributions to various domains is one of the main goals of [Dugac 1976]. See also the thesis [Haubrich 1992], which starts with a chapter on arithmetization, and [Ferreirós 1999].

[46] Weierstrass may have had *some* such theory as early as 1841: [Kopfermann 1966], p. 80.

sense, to a finite subaggregate of A_1, is also equal to a finite subaggregate of A_2. If $A_1 \leq A_2$ and $A_2 \leq A_1$, the two infinite aggregates are said to be equal. If all finite aggregates are less than or equal to A, then A equals infinity. All other aggregates (the finite ones and those infinite aggregates which are not infinity) make up Weierstrass's domain of positive real numbers. Negatives are obtained by working with two units opposite to each other; the complex numbers etc. require even more units.

By tracing over the years the growing weight given to foundations in Weierstrass's introductory course on the theory of analytic functions, one gets a first understanding of the way the movement of arithmetization was catching on. We know four versions of this course: Wilhelm Killing's notes from Spring 1868, Georg Hettner's notes of Spring 1874, Adolf Hurwitz's of Spring 1878, and Kurt Hensel's notes, probably from the Winter 1882–1883.[47]

The whole chapter "Introduction to the concept of number" (*Einführung in den Zahlbegriff*) in Killing's notes [Weierstrass 1868] gives the impression of recalling known facts, based on the notion of magnitude or quantity (*Größe* in German). For instance: "If the numerical quantity is given by an infinite series, then it will equal another quantity, if ..."[48] We conclude that arithmetization was at least not for the students in 1868.

A keener interest in arithmetization is evident in a letter, written in December 1873 to Paul du Bois-Reymond, where Weierstrass distinguished between various approaches to analysis: either "with the notion of extensive magnitude, or coming from algebra, i.e., from the notion of number and the basic arithmetic operations necessarily implied by it. I myself hold this last path to be the only one by which analysis can be founded with scientific rigour and all difficulties can be solved."[49] In the 1874 lecture notes we read about the theory of complex numbers:

> However, for analysis we need a purely arithmetical foundation which has already been given by Gauss. Even though the geometric presentation of the complex quantities is an essential tool for their investigation, we must not use it here because analysis has to be kept clean of geometry.[50]

[47] See [Ullrich 1988], pp. xi–xiv, for the structure of Weierstrass's regular lecture cycle. Hettner's notes may have been worked out only after 1889; at any rate, the copy uses post-1880 orthography. Only Hurwitz's notes date the individual lectures. Hensel's notes in the IRMA library at Strasbourg are undated; we associate them to 1882–1883 on the basis of Hensel's curriculum and a comparison with other notes he took.

[48] [Weierstrass 1868], p. 3: *Ist die Zahlengrösse durch eine unendliche Reihe gegeben, so wird sie einer andern Grösse gleich sein, wenn ...*

[49] [Weierstrass 1923], p. 203f: *je nachdem man von geometrischen und physikalischen Vorstellungen ausgehend, also mit dem Begriff der extensiven Größe, das Gebiet der Analysis betritt oder von der Algebra aus, d.h. dem Zahlbegriff und den mit demselben notwendig gegebenen arithmetischen Grundoperationen. Ich halte den letzteren Weg für den, auf welchem allein sich die Analysis mit wissenschaftlicher Strenge begründen läßt und alle Schwierigkeiten sich beseitigen lassen.*

[50] [Weierstrass 1874], p. 6: *Wir bedürfen jedoch für die Analysis einer rein arithmetischen Begründung, die schon Gauss gegeben hat. Obgleich die geometrische Präsentation der complexen Grössen ein wesentliches Hülfsmittel zur Untersuchung derselben ist, können*

And the strongest arithmetization programme is formulated in the 1882–1883 lectures:

> For the foundation of pure analysis all that is required is the concept of number, while geometry has to borrow many notions from experience. We will try here to construct all of analysis from the concept of number.[51]

As of 1874, the lecture courses all develop the theory which we have briefly sketched in the 2nd paragraph of this subsection. A crucial point explicitly made in all three courses is that infinite sums have no meaning other than the one they receive from definitions involving only operations with finite subaggregates.[52] For instance in the 1882–1883 lectures, Weierstrass insisted that the idea of a number determined by infinitely many elements[53] is itself not any more difficult than that of the infinite sequence of natural numbers. And after the general definition of equality, special mention was made of the case where a certain law assures us of the existence of all of its elements, even if we are not able to effectively specify them.[54]

The relationship between the arithmetized numbers and points on a line was still treated as unproblematic in [Weierstrass 1874], p. 41. That each line segment corresponds to a numerical quantity was mentioned there in passing (p. 76). The problem whether to each numerical quantity also corresponds a point, was spirited away by the convention that "a single value of a complex quantity be called a point."[55] The 1878 lectures were more elaborate in this respect. For the existence of a point (on a line with marked origin P and unit) corresponding to a given numerical quantity, say a, Weierstrass considered (for a particular example) all the points X for which the segment PX is smaller than the segment corresponding to some finite quantity contained in a, and all points Y for which PY is greater than all the segments corresponding to a finite quantity contained in a. He then argued directly (without explicitly alluding to Dedekind for this intuitive cut-argument):

> The points X and the points Y now form one continuous series of points. There

wir sie hier nicht anwenden, da die Analysis von der Geometrie rein erhalten werden muss.

[51] [Weierstrass 1883], p. 1: *Die reine Analysis bedarf zu ihrer Begründung nur des Begriffes der Zahl, während z.B. die Geometrie viele Begriffe der Erfahrung entlehnen muß. Wir wollen versuchen, hier die gesammte Analysis aus dem Begriffe der Zahl zu construiren.*

[52] Cf. Cantor's compliment to Weierstrass on this point in [Cantor 1879–1884/1932], part IV, p. 185.

[53] Weierstrass's expression "element" and other features of his presentation may well go back to the tradition of algebraic analysis. See for instance [Stern 1860], p. 9. Cf. [Dirksen 1845], chap. 3, *Abschnitt* 2.

[54] [Weierstrass 1883], p. 26f. The example of $\sqrt{2}$ given thereafter carries Hensel's note in the margin: "for rational numbers one can specify all the elements, for numbers with infinitely many elements every required element can be specified." (*bei rat. Zahlen kann man alle bei den Zahlen mit unendl. vielen Elementen jedes verlangte Element angeben.)*

[55] [Weierstrass 1874], p. 116: *Wir werden häufig einen einzelnen Wert einer complexen Grösse einen Punkt nennen.*

> must therefore be a point which affords the transition from the point series of X to the point series of Y.[56]

In [Weierstrass 1883], however, only the numerical quantity corresponding to a given ratio of segments is explained in detail, whereas the inverse problem is dismissed with the remark that one may "imagine" the necessary construction "done."[57]

In conclusion, by 1874 Weierstrass's theory was built exclusively on an arithmetized notion of quantity. The relationship to extensive quantities is discussed, albeit less profoundly than by Dedekind or Cantor. One may read the evolution of Weierstrass's presentations over the years as a movement towards a more constructivist point of view, where "ideas" or "imaginations" (*Vorstellungen*), i.e., processes of the mind, are appealed to in order to smoothen the acceptance of infinites. This may have been the result of his ongoing dialogue with Kronecker.[58]

2.2. Leopold Kronecker

In Part I of this book, Leopold Kronecker's role in the history of Gauss's *Disquisitiones Arithmeticae* has been discussed under two headings: in chap. I.1, § 4.3, he appeared as a representative of the field of arithmetic algebraic analysis, whereas his theory of algebraic numbers and functions was described as one of the alternatives to Dedekind's theory of ideals in chap. I.2, § 3.4. Kronecker's programme of arithmetization was based on the same method as his theory of algebraic numbers and functions – i.e., the adjunction of indeterminates and the reduction of the polynomials obained with respect to module systems – also to incorporate all of analysis into a unified "General Arithmetic."[59]

Unlike his Berlin colleague Weierstrass, Kronecker was not concerned with designing a coherent, up-to-date presentation of function theory, including pathological counterexamples etc., for he was perfectly happy with the parts of classical analysis, especially elliptic and modular functions, that he had himself enriched. Nor was he interested in Cantor's set theoretical innovations and the completed infinites involved in them. And unlike Dedekind, Kronecker was not looking for conceptual analyses (even less, if they employed completed infinites) of such notions as continuity which for him were germane to geometry or mechanics.

[56] [Weierstrass 1878], p. 22: *Die Punkte X und die Punkte Y bilden nun eine stetige Reihe von Punkten, es muß also einen Punkt geben, der den Übergang von der Punktreihe X zur Punktreihe Y vermittelt.*

[57] [Weierstrass 1883], p. 197: *Dann läßt sich jede Z-Gr [Zahlengrösse] geometrisch dadurch darstellen, daß man eine Strecke gebildet denkt, welche aus der Längeneinheit a und deren genauen Theilen gerade so zusammengesetzt ist, wie die zu repräsentierende Z-Gr aus der Haupteinheit und deren genauen Theilen.*

[58] Their joint criticism of Riemann's use of Dirichlet's principle in the 1860s is not only confirmed by Casorati's papers (see [Neuenschwander 1978], p. 27), but is also alluded to by [Heine 1870], p. 360.

[59] *Allgemeine Arithmetik.* Kronecker also chose this as the title of his standard lecture course at the end of his life; see the beginning of Hensel's preface to [Kronecker 1901], p. V.

Kronecker published his views on arithmetization only in the 1880s.[60] In 1886, the 63 year old Kronecker published his programmatic article "On the concept of number" in a *Festschrift* dedicated to the philosopher Eduard Zeller:

> [A]rithmetic bears a similar relationship to the other two mathematical disciplines, geometry and mechanics, as mathematics as a whole bear to astronomy and the other natural sciences; arithmetic likewise renders manifold services to geometry and mechanics and receives from its sister disciplines a wealth of inspirations in exchange. Here, however, the word "arithmetic" has to be taken not in the usual restrictive sense, but one has to subsume under it all mathematical disciplines except geometry and mechanics, in particular algebra and analysis. And I actually believe that one day one will succeed in "arithmetizing"[61] the complete content of all these mathematical disciplines, i.e., to found them solely and exclusively on the notion of number taken in the strictest sense, thereby peeling away the modifications and extensions of this notion,[62] most of which have been prompted by applications to geometry or mechanics. The fundamental difference between geometry and mechanics on the one hand, and the mathematical disciplines on the other which are here being collected under the label of "arithmetic," is, according to *Gauss*, that the object of the latter, number, is *only* a product of our mind, whereas space as well as time also have a *reality outside* of our mind whose laws we cannot completely impose *a priori.*[63]

[60] As in chap. I.2, one has to consult (aside from the more philosophical [Kronecker 1887b] and his last lecture course [Kronecker 1891]) his *Grundzüge* [Kronecker 1881], the paper [Kronecker 1886] where module systems (*Modulsysteme*, introduced in 1881) are applied to algebra, and [Kronecker 1888]. Cf. J. Boniface's chap. V.1.

[61] According to his student Jules Molk, Kronecker was the first to use this verb transitively; see [Molk 1909], p. 158, note 78.

[62] Kronecker's note: "I here mean in particular the inclusion of irrational numbers and of the continuous quantities."

[63] We quote from the extended printing [Kronecker 1887b/1895–1931], vol. 3(1), p. 253: *In der Tat steht die Arithmetik in ähnlicher Beziehung zu den anderen beiden mathematischen Disciplinen, der Geometrie und Mechanik, wie die gesammte Mathematik zur Astronomie und den anderen Naturwissenschaften; auch die Arithmetik erweist der Geometrie und Mechanik mannigfache Dienste und empfängt dagegen von ihren Schwester-Disziplinen eine Fülle von Anregungen. Dabei ist aber das Wort "Arithmetik" nicht in dem üblichen beschränkten Sinne zu verstehen, sondern es sind alle mathematischen Disciplinen mit Ausnahme der Geometrie und Mechanik, also namentlich die Algebra und Analysis, mit darunter zu begreifen. Und ich glaube auch, dass es dereinst gelingen wird, den gesammten Inhalt aller dieser mathematischen Disciplinen zu "arithmetisieren," d.h. einzig und allein auf den im engsten Sinne genommenen Zahlbegriff zu gründen, also die Modificationen und Eweiterungen dieses Begriffs* (Kronecker's footnote: *Ich meine hier namentlich die Hinzunahme der irrationalen sowie der continuirlichen Grössen*) *wieder abzustreifen, welche zumeist durch die Anwendungen auf die Geometrie und Mechanik veranlasst worden sind. Der prinzipielle Unterschied zwischen der Geometrie und Mechanik einerseits und zwischen den übrigen hier unter der Bezeichnung "Arithmetik" zusammengefassten mathematischen Disciplinen andererseits besteht nach* Gauss *darin, dass der Gegenstand der letzteren, die Zahl,* bloss *unseres Geistes Product ist, während der Raum ebenso wie die Zeit auch* ausser *unserem Geiste eine* Realität *hat, der*

Kronecker went on to quote Gauss's letter to Bessel of April 9, 1830.[64] Also the method with which Kronecker would eliminate at least the *algebraic* irrationalities is described as being directly inspired by Gauss:

> [W]ith the *systematic* introduction of indeterminates (*indeterminatae*), which stems from *Gauss*, the special theory of integers was expanded into the general arithmetic theory of entire functions of indeterminates with integral coefficients. This general theory allows to eliminate all notions which are alien to arithmetic proper: that of negative, fractional, real, and imaginary algebraic numbers.[65]

Negative numbers are then multiples of an indeterminate s which is taken modulo $s+1$; a fraction $\frac{1}{b}$ is represented by q_b modulo $b \cdot q_b - 1$, and an algebraic number is handled by working with polynomials modulo its minimal equation.[66] What remains somewhat unclear is how this Kroneckerian programme was to affect the practice of analysis. At least the formal developments in Kronecker's long series of papers on elliptic functions of the late 1880s seem unaffected by the radical arithmetization one might expect from the preceding quotes. A first clue is provided by what Kronecker told the young David Hilbert when the latter paid him a visit in 1888:

> Equal is only $2 = 2$. Irrational and transcendental numbers are given 1.) by implicit representation $\sin x = 0$, $x^2 = 5$, or 2.) by approximation. In general, it is not at all difficult to build everything rigorously on this basis, avoiding Weierstrass's notion of equality and continuity. But at certain critical junctures it is difficult, and there one can never be precise and rigorous enough. Only the discrete and the singular have significance. But the rest one can also obtain, by interpolation. Therefore his goal for the elliptic functions is to admit only the singular moduli,[67] and then build everything arithmetically from there.[68]

wir a priori ihre Gesetze nicht vollständig vorschreiben können.

[64] See J. Ferreirós, chap. III.2 above, § 1.

[65] [Kronecker 1887b/1895–1931], vol. 3(1), p. 260: *[M]it der* principiellen *Einführung der "Unbestimmten"* (indeterminatae)*, welche von* Gauss *herrührt, hat sich die specielle Theroie der ganzen Zahlen zu der allgemeinen arithmetischen Theorie der ganzen ganzzahligen Functionen von Unbestimmten erweitert. Diese allgemeine Theorie gestattet alle der eigentlichen Arithmetik fremden Begriffe, den der negativen, der gebrochenen, der reellen und der imaginären algebraischen Zahlen, auszuscheiden.*

[66] Cf. [Kronecker 1887a]. [Kronecker 1887b], § 5, III, shows how to separate real conjugates.

[67] The singular moduli are analogous to algebraic numbers in that they yield algebraic values for modular and elliptic functions; the arithmetic properties of these values were one of Kronecker's central domains of research. See chap. I.1, § 4.3. Cf. [Schappacher 1998], [Vlăduţ 1991]. At the end of his life, contrary to what he told Hilbert, Kronecker studied a more general theory, deriving invariants of binary quadratic forms which also contained continuous parameters from Fourier developments of elliptic functions for *nonsingular* moduli; see [Kronecker 1932]; cf. [Kronecker 1895–1931], vol. 5, pp. 65–83.

[68] See BNUS, Cod. Ms. D. Hilbert 741, "Kronecker," pp. 1/2–1/3: *Gleich sei nur* $2 = 2$. *Irrationale und transzendente Zahlen seien 1.) durch die implizite Darstellung* $\sin x = 0, x^2 = 5$ *gegeben oder 2.) durch Annäherung. Im allgemeinen sei es gar nicht schwer*

But which transcendental functions would be accepted as implicitly defining transcendental numbers, like in the equation "$\sin x = 0$" quoted by Hilbert? It seems that what really gave meaning to transcendental functions for Kronecker, was their role as invariants of some general equivalence relation. Molk gave the concrete example of the function $\pi \cot(\pi u) = \sum_{k=-\infty}^{k=+\infty} \frac{1}{u+k}$ as an invariant of the relation which identifies u with $u + k$ for any integer k.[69]

At any rate, there would hardly be room in Kronecker's arithmetized analysis for Cantor's theory of the continuum or the budding functional analysis, and Kronecker also wanted to keep geometry relegated to its own domain: "In opposition to the notion of continuity, which is present in a certain way in geometry and mechanics, stands the discontinuity of the sequence of numbers."[70] This turns the real line (which was still referred to by way of comparison in [Kronecker 1881/1895–1932], vol. 2, p. 354) into an attempt "to somehow conjure up continuity within arithmetic," and in 1891 Kronecker explicitly stated that it was impossible to order all fractions "in a straight line,"[71] presumably because this would require infinitely many unknowns and relations.[72]

One of Kronecker's most basic *methodological tenets* was *concreteness*: defini-

auf dieser Grundlage bei Vermeidung des Weierstrass'schen Begriffs der Gleichheit und der Continuirlichkeit alles strenge aufzubauen. Aber bei gewissen kritischen Stellen sei es schwer und da könne man nicht genau und strenge genug sein. Nur das Diskrete und Singuläre habe Bedeutung. Das übrige könne man aber auch erhalten, nämlich durch Interpolation. So sei es bei den elliptischen Funktionen sein Ziel, nur die singulären Moduln zuzulassen und dementsprechend alles arithmetisch aufzubauen.

[69] See [Kronecker 1891], p. 238, and [Molk 1909], p. 162. See also the discussion of the invariance of dimension in [Kronecker 1891], pp. 246–247. Cf. [Kronecker 1901], pp. 132–142.

[70] [Kronecker 1891], p. 227; see J. Boniface's chap. V.1, footnote 64 for the original quote. In [Kronecker 1888/1895–1931], vol. 3(2), pp. 89–97, and [Kronecker 1891], p. 265, Kronecker discussed approximating a ball by cubes. He concluded more radically in 1891: "There is a volume – the ball – … But there is no number to which the convergent series of fractions tend." (*[W]ohl ist ein Volumen da – nämlich die Kugel – … Nicht aber ist eine Zahl da, welcher die konvergierenden Bruchreihen zustreben.)*

[71] [Kronecker 1891], p. 227 (see J. Boniface's chap. V.1, footnote 64) and p. 257: *Unmöglich aber ist es, nach dieser Ausdehnung der Begriffe größer und kleiner auf die Brüche diese in einer geraden Linie ihrer Größe nach anzuordnen. Für eine endliche Zahl gegebener Brüche ist diese Ordnung wohl möglich. Für eine endliche Zahl ist sie aber nicht nötig, für alle Brüche nicht möglich.*

[72] In [Kronecker 1886/1895–1931], vol. 3(1), p. 155, he did mention the "purely logical" possibility of "module systems with infinitely many elements," asking however that this "arithmetically not sufficiently precise notion" be reduced to finite module systems in "special arithmetical applications." He added a note where he explained that this caution was not followed in Dedekind's general theory of modules and ideals, and criticized in the same way the definitions of irrational numbers, thinking apparently of Heine, Dedekind, and Cantor.

tions are to be given along with an effective criterion to decide whether or not they apply to a given object;[73] infinite series have to be given so that they are amenable to computation; indirect existence proofs are either avoidable or anathema.[74] Likewise, Kronecker repeated in his 1891 lectures that there was really no need for a "theory of infinite series which define irrational numbers."[75]

Another recurrent methodological topos of Kronecker's was to use adequate equivalence relations, the celebrated model being the equivalence and composition of quadratic forms in Gauss's *Disquisitiones Arithmeticae*.[76] In [Kronecker 1888/1895–1931], vol. 3(1), p. 90, and [Kronecker 1891], p. 266, the author even stretched this idea to the mode "2.) by approximation" in which irrationals can be given (as he had told Hilbert); approximations would be identified if they were in the same "equivalence interval."

This last idea matches the "mathematics of approximation" that Felix Klein propagated as of the early 1870s. To be sure, Klein's theory of "function strips" (*Funktionsstreifen*) was not guided by Gauss's D.A.,[77] but by an analysis of the inherent lack of precision of our spacial intuition, and thus fitted well with the contemporary interest in the psychology of perception. But Klein did acknowledge an indebtedness to a conversation with Kronecker about the impossibility of effectively giving infinitely many terms of a series, which had provided "the first occasion to develop his ideas."[78]

3. Discourses on Arithmetization

By excluding extensive magnitudes from the foundation of analysis, arithmetization modified the relation between mathematics and its applications in the empirical sciences. Concretely, the move looked at first like the retreat into the ivory tower; in an academic speech in 1891, the rector of Innsbruck university, Otto Stolz, refrained from going into details about arithmetization, not just for lack of time, but because he felt "that pure mathematics has not gained in popularity by the immersion into itself in which it currently indulges."[79] (One may recall Méray's and Dedekind's initial

[73] See for instance the discussion of irreducibility in [Kronecker 1881/1895–1931], vol. 2, p. 256–257. In [Kronecker 1891], p. 240, he suggested that definitions be gathered from experience, and mathematics recognize itself as a natural science.

[74] See [Kronecker 1891], p. 240; cf. footnote 80 below.

[75] [Kronecker 1891], p. 269–271, where he went on to declare that the series $\sum \frac{c_n}{n!}$ with integers c_n such that $0 \leq c_n \leq n-1$ "really exist."

[76] [Kronecker 1881/1895–1931], vol. 2, p. 324, and [Kronecker 1891], p. 261f (esp. note 62). Cf. the way in which Kronecker paraded this arithmetic idea in his quarrel with Camille Jordan, e.g. in [Kronecker 1895–1931], vol. 1, p. 418: *En appliquant les notions de l'Arithmétique à l'Algèbre, on peut appeler équivalentes ....*

[77] He did, however, refer to Gauss the astronomer in this context; see [Klein 1921–1922], vol. 2, p. 245.

[78] [Klein 1873/1921–1922], vol. 2, p. 216, note 6: *Ich bin hierauf gelegentlich von Herrn Kronecker gesprächsweise aufmerksam gemacht worden; in seiner Bemerkung lag für mich wohl der erste Anlaß, mir die in* § *1, 2 des Textes niedergelegte Auffassung zu bilden.*

[79] [Stolz 1891], p. 4: *Auch kann ich mir denken, dass die reine Mathematik durch die*

hesitations about their publications.) Stolz, a former Berlin student, mentioned as protagonists of arithmetization Weierstrass and Kronecker, who "have not arrived at agreeing opinions."[80]

3.1. Philosophical Points of View

Contrary to Stolz's hesitations, a number of philosophically inclined mathematicians, and philosophers with their own image of mathematics, were publishing their views as the movement of arithmetization gathered momentum. Within the limits of the present article, we only mention a few names here, as scattered evidence of an ongoing, if apparently unstructured debate. The history of this whole debate is worth looking into and remains to be written.

Hermann Hankel, a student of Riemann's, already published before 1872 (and died in 1873 at age 34). In [Hankel 1867], p. 46, he explicitly doubted the scientific relevance, and in fact the possibility, of defining irrational numbers without appeal to magnitudes. At the same time, however, importing ideas from the British logical school, he began to build a "general arithmetic," i.e., an axiomatic theory of algebraic composition laws which gave him a general, formal notion of number; see [Hankel 1867], pp. VIII, 47. In spite of this modern, formal theory, the gap between arithmetic and analysis appears even wider in his encyclopedia article [Hankel 1871] where the notion of limit separates analysis from arithmetic and algebra, and appears to render any actual arithmetization impossible.

Paul du Bois-Reymond presented in his book [Bois-Reymond 1882] a dialogue between the "idealist" and the "empiricist" with the intention to help mathematicians to greater philosophical clarity, specifically about the existence of the limit of an infinite decimal fraction. The presentation is strongly influenced by the time-honoured interest in processes of thinking and perception. Magnitudes are maintained as a source of inspiration and application of analysis;[81] arithmetization is invited to formally ascertain rigorous proofs (p. 290). Hankel and Bois-Reymond were analogous in that they saw the potential of formal, structural mathematics,[82] but reacted to it conservatively. In Bois-Reymond's case, this reaction is also motivated by the conviction that mathematical analysis "is in truth a natural science." In spite of the later date of [Bois-Reymond 1882], its author (like Hankel) really reacted essentially to pre-1872 forms of arithmetization.[83]

Versenkung in sich selbst, der sie sich gegenwärtig hingiebt, an Popularität nicht gewonnen hat. [Daum 2002] suggests that mathematics remained largely untouched by the big wave of German literature popularizing the natural sciences since about 1850.

[80] [Stolz 1891], p. 4: *Dabei sind sie jedoch nicht zu übereinstimmenden Ansichten gelangt.* (Dedekind and Cantor *are* mentioned in a footnote on p. 16.) Incidentally, this speech contains the missing quote in [Kronecker 1891], p. 240, footnote 41: [Stolz 1891], p. 9. See also [Stolz, Gmeiner 1904], p. 148.

[81] [Bois-Reymond 1882], p. 54, appeals to Gauss for having called mathematics, "so correctly and profoundly, the science of magnitudes" (*die von Gauss so wahr und so tief Grössenlehre genannte Wissenschaft*).

[82] [Bois-Reymond 1882], p. 54, speaks of a symbolic game (*Zeichenspiel*).

[83] See [Bois-Reymond 1882], pp. 53–55. His comment on [Heine 1872] on p. 55 is a way

When the physicist Gustav Robert Kirchhoff opposed metaphysical reflections in physics and defined as the goal of mechanics (somewhat vaguely), to describe natural movements as simply and completely as possible, this gave a tremendous boost to the German empiricist, positivist philosophy of science.[84] Even though all variants of arithmetization could probably be made to comply with this philosophy, it was Kronecker who explicitly followed his Berlin colleague Kirchhoff and presented his own programme of arithmetization within Kirchhoff's mould, stressing the analogy of mathematics with other sciences and dividing mathematics into general arithmetic on the one hand and geometry and mechanics on the other.[85]

Against Gauss's, Kirchhoff's, and Kronecker's separation of arithmetic from geometry and mechanics, Leo Königsberger, in his speech [Königsberger 1895], pleaded for a return to Kant's foundation of all mathematics on pure intuitions.

Sightless Eugen Karl Dühring was as of 1877 the most universally hated philosopher on the Berlin academic scene.[86] Dühring considered mathematical notions to be touchstone cases for epistemology. Having determined early on the impossibility of thinking an infinite number,[87] his interest in mathematics increasingly turned into wild criticism of allegedly untenable mathematical notions and tendencies.[88] In [Dühring 1878], pp. 249–265, however, he developed a sort of philosophical programme of arithmetization turning analysis into a perfect form of arithmetic. This, however, did not diminish his polemics: against mathematics in general that he found overrated, and against higher arithmetic in particular.

Another very prolific philosopher, Wilhelm Wundt in Leipzig, tried to justify modern mathematical trends, in particular Dedekind's and Cantor's, against Berlin restrictions to potential infinites; see [Wundt 1883]. His position was neokantian: pure intuition is taken as an abstract notion, not a *Vorstellung*. For him, the fundamental theme of mathematics for the last 2000 years was the mediation between discrete numbers and the continuum. At the same time, he held a similarly skeptical

of not taking the arithmetization of irrational numbers seriously.

[84] See [Kirchhoff 1876] for a concise formulation; cf. [Cornelius 1903].

[85] [Kronecker 1881/1895–1931], vol. 2, p. 354; [Kronecker 1891], pp. 226, 252. In [Kirchhoff 1865], p. 5, Kirchhoff had called geometry and mechanics two closely related and equally certain applications of pure mathematics.

[86] [Köhnke 1986], pp. 373, 519. He would flirt with socialism (albeit not very successfully; recall Friedrich Engels's *Anti-Dühring* of 1878), and, at least after his removal from Berlin University, would be openly antisemitic, and finally founded a sect.

[87] [Dühring 1865], p. 115. Felix Klein was duly impressed by this; see [Klein 1873/1921–1922], vol. 2, p. 215, note 5. We do not know if Kronecker reacted to this early Dühring.

[88] His would-be historical treatise [Dühring 1877] has Lagrange as its absolute hero, and is in many respects written from the point of view of French mathematics of the first third of the XIX$^{\text{th}}$ century; see pp. 545–549. (This may remind one of Méray, but the contexts, professional identities and styles of both authors do not suggest a fruitful comparison.) Developments originating from the D.A. are described as "pleasures of speculation" (*Speculationsvergnügungen*) without real relevance, and the contemporary analysis and algebra is ridiculed for its hollowness. The same continues in the joint book with his son [Dühring, Dühring 1884].

position on proofs by contradiction as Kronecker, and – possibly under the influence of Klein? – he also insisted on the importance of intuition for mathematics.

Benno Kerry – a young *Privatdozent* of philosophy at Strassburg University, who died in 1899 at age 31 – is usually known today for Gottlob Frege's 1892 replique to him.[89] But in his long series of papers on intuition and its psychic processing (in Wundt's influential journal), he also dealt with Kronecker's arithmetization, criticizing the narrowness of Kronecker's concept of number in general, and the introduction of negative and fractional numbers via indeterminates and congruences in particular, quoting Cantor, Dedekind, and Elwin B. Christoffel for their criticism of Kronecker.[90]

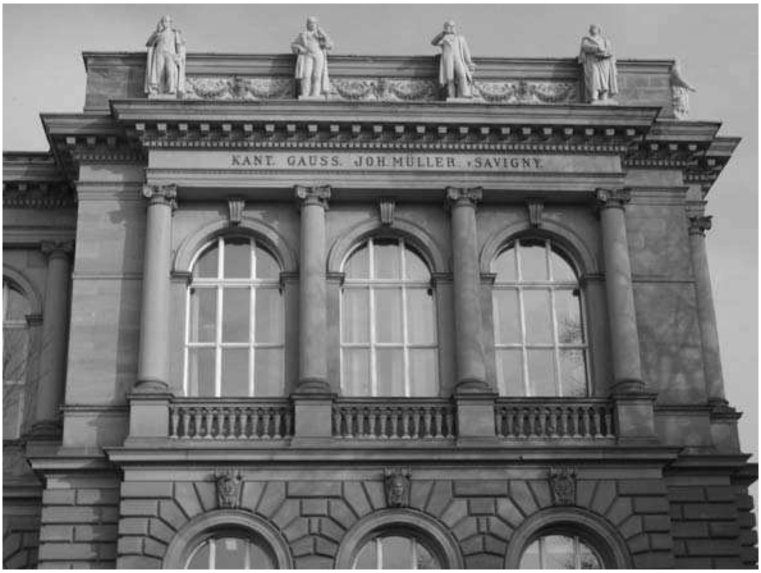


Fig. V.2. Collegiengebäude, Kaiser-Wilhelm-Universität Strassburg (1879–1884)
Four German scholars. Kant, Gauss, and J. Müller incarnate the domains entering into the discussions sketched in § 3.1: philosophy, mathematics, and physiology.

Finally, Adolf Elsas published a fundamental criticism of Fechner's psychophysics [Elsas 1886] where (starting p. 53) he criticized the mathematicians for giving up magnitudes. It is voices like his that provide some evidence *ex contrario* for the thesis in [Jahnke, Otte 1981], p. 45, that arithmetization was in fact "a response to the changed relationship between mathematics and the empirical sciences," since new sciences, treating new kinds of magnitudes, asked to be mathematized.

[89] In Frege's *Über Begriff und Gegenstand.*

[90] [Kerry 1889], pp. 89–92; [Kerry 1890], pp. 319–324. His second point seems to be misguided insofar as it tries to argue with values of the newly adjoined unknown; see [Kerry 1889], pp. 90–91. Kerry calls (p. 92) Kronecker's method "exceedingly cumbersome and complicated" (*überaus schwerfällige und umständliche Weise*).

3.2. The Göttingen Nostrification *of Arithmetization*

As the turn of the century approached, arithmetization, in one form or the other, seemed well established, and the dominant question was no longer, whether analysis should be founded independently of the notion of magnitude, but what arithmetization meant for the unity of mathematics, for the relation among the mathematical disciplines – in particular arithmetic against geometry – and for the applications of mathematics to the sciences. Indeed, the movement of arithmetization could potentially threaten the unity of mathematics, separate arithmetic from geometry, and mathematics from the sciences. It was with this potential threat in mind that Felix Klein gave his address on arithmetization to the Göttingen Academy [Klein 1895]; its timeliness, and the growing importance of the author, is underlined by the prompt translations of it that followed.[91] The speech also marked the beginning of the *nostrification* of arithmetization by the newly emerging mathematical centre at Göttingen.[92]

The starting point of the talk was Weierstrass's 80th birthday.[93] Klein presented Weierstrass as "the principal representative" of arithmetization.[94] Recalling that the XVIIIth century had been a "century of discoveries" in mathematics, Klein first described the XIXth century as an aftermath:

> Gradually, however, a more critical spirit asserted itself and demanded a logical justification for the innovations with such assurance, the establishment, as it were, of law and order after the long and victorious campaign. This was the time of Gauss and Abel, of Cauchy and Dirichlet.[95]

Although it may already seem unusual to liken these extremely creative mathematicians to administrators,[96] Klein carried on in the same vein:

[91] Already in his Leipzig inaugurational lecture, which he published 15 years after the event, [Klein 1880/1895], Klein had warned against losing the unity of mathematics.

[92] For the Göttingen concept of "nostrification," cf. [Corry 2004], sec. 9.2.

[93] October 31, 1895, three days before the address. Weierstrass would die in 1897.

[94] In preparatory notes for his 1880–1881 Leipzig classes, he had called Weierstrass's introduction of irrational numbers "arithmetical," and Dedekind's cuts "geometrical" [Klein 1880–1881], p. 264

[95] [Klein 1895], p. 966 (English); p. 232 (German).

[96] Minkowski would play on Klein's metaphor in his famous Dirichlet centennial speech [Minkowski 1905], p. 451: "One hears about the progressive arithmetization of *all* mathematical disciplines, and some therefore take arithmetic to be nothing but a convenient constitution for the extensive empire of mathematics. Well, in the end some will see it only as the high police which is authorized to check on all unlawful incidents in the widely ramified commonwealth of magnitudes and functions. – ... *man hört von der fortschreitenden Arithmetisierung* aller *mathematischen Wissenszweige sprechen, und manche halten deshalb die Arithmetik nur noch für eine zweckmäßige Staatsverfassung, die sich das ausgedehnte Reich der Mathematik gibt. Ja, zuletzt werden einige in ihr nur noch die hohe Polizei sehen, welche befugt ist, auf alle verbotenen Vorgänge im weitverzweigten Gemeinwesen der Größen und Funktionen zu achten.*

> But this was not the end of the matter. Gauss, taking for granted the continuity of space, unhesitatingly used the intuition of space as a basis for his proofs; but closer investigation showed not only that many special points still needed proof, but also that the intuition of space had led to the too hasty assumption of the generality of certain theorems which are by no means general. Hence arose the demand for *exclusively arithmetical methods of proof*… This is the Weierstrassian method in mathematics, the *Weierstrass'sche Strenge*, as it is called.[97]

Klein then simply called "arithmetization" *all* developments of this kind, from Gauss to Weierstrasss, from Kronecker to Peano, and he went even further:

> For since I consider that the essential point is not the mere putting of the argument into the arithmetical form, but the more rigid logic obtained by means of this form, it seems to me desirable – and this is the positive side of my thesis – to subject the remaining divisions of mathematics to a fresh investigation based on the arithmetical foundation of analysis. On the other hand I have to point out most emphatically – and this is the negative part of my task – that it is not possible to treat mathematics exhaustively by the method of logical deduction alone, but that, even at the present time, *intuition* has its special province.[98]

In this way, Klein dismissed any special role of number theory for arithmetization, and reduced this movement to what he saw as its "essence," i.e., to a matter of logical tidying up to ensure the necessary rigour. This point of view stresses continuous progress, and does not invite the search for historical fault lines. In fact, Klein's agenda was not history at all. A passing reference to contemporary textbooks (p. 233) suggests that he considered the arithmetization of basic analysis as accomplished, and went out to promote research in geometry and mathematical physics which would take this most modern, arithmetized analysis into account.[99] Furthermore, he pleaded the case of well-trained mathematical intuition, which "*is always ahead of logical reasoning*."[100] He hailed (p. 238) the new appeal to intuition that Minkowski's geometry of numbers brought to arithmetic,[101] and he insisted that intuition has to be trained in university courses for beginners, scientists and engineers. Klein closed his address with a holistic metaphor of mathematics as a tree for which deep roots are just as vital as high branches.

When Klein gave this speech, David Hilbert had just started his second semester of teaching in Göttingen. Back in Königsberg, in his 1891 lectures on geometry,

[97] [Klein 1895], p. 966 (English); p. 233 (German).

[98] [Klein 1895], p. 967 (English); p. 234 (German).

[99] Let us mention in passing the measure-theoretic turn that Felix Bernstein would give to this kind of approach with his "axiom of the restricted arithmetizability of observations" in [Bernstein 1911].

[100] [Klein 1895], p. 237: … daß die so verstandene mathematische Anschauung auf ihrem Gebiete überall dem logischen Denken voraneilt und also in jedem Momente einen weiteren Bereich besitzt als dieses. (Emphasis in the original.) See also the last few sentences of [Klein 1890/1921–1922], vol. 1, p. 382, where Klein insisted on the necessity of arithmetizing irrational numbers first, in order to then sharpen our intuition by transferring the abstract notions thus found into geometry.

[101] See J. Schwermer's chap. VIII.1 below.

Hilbert had still faithfully echoed the separation of arithmetic from geometry which can be traced back to Gauss.[102] Over the following decade, Hilbert's position changed significantly. By 1897, he was in tune with Felix Klein's very general, nostrified concept of arithmetization when he emphasized in the preface to his *Zahlbericht* the similar level of abstractness of all mathematical disciplines once they are treated "with that rigour and completeness … which is actually necessary."[103] The same is repeated along Klein's lines, and with a criticism of Kronecker's position, in the introduction to his 1900 Mathematical Problems:

> While insisting on rigour in the proof as a requirement for a perfect solution of a problem, I should like, on the other hand, to oppose the opinion that only the concepts of analysis, or even those of arithmetic alone, are susceptible of a fully rigorous treatment. This opinion, occasionally advocated by eminent men, I consider entirely erroneous. Such a one-sided interpretation of the requirement of rigour would soon lead to the ignoring of all concepts arising from geometry, mechanics and physics, to a stoppage of the flow of new material from the outside world, and finally, indeed as a last consequence, to the rejection of the ideas of the continuum and of the irrational number.[104]

This was written the year after the publication of his *Foundations of Geometry*, which open with the following declaration of Hilbert's arithmetization-via-axiomatization:

> Geometry, just like arithmetic, needs only a few simple basic facts to be built up from systematically. These basic facts are called *axioms*.[105]

The 1890s thus took David Hilbert from a position marked by arithmetic as the model discipline of pure mathematics to an egalitarian programme of axiomatization (which he would in fact try to extend all the way to physics). His sweeping declarations

[102] [Hilbert 2004], p. 22–23 (where Kronecker ought to have been mentioned in note 6). Note the simultaneity with [Kronecker 1891]. Cf. [Toepell 1986], p. 21.

[103] Our transl. of [Hilbert 1897/1932], p. 64: *Ich bin der Meinung, daß alle die anderen Wissensgebiete der Mathematik wenigstens einen gleich hohen Grad von Abtraktionsfähigkeit … verlangen – vorausgesetzt, daß man auch in diesen Gebieten die Grundlagen überall mit derjenigen Strenge und Vollständigkeit zur Untersuchung zieht, welche tatsächlich notwendig ist.*

[104] [Hilbert 1900a], p. 294–295: *Wenn ich die Strenge in den Beweisen als Erfordernis für eine vollkommene Lösung eines Problems hinstelle, so möchte ich andererseits zugleich die Meinung widerlegen, als seinen etwa nur die Begriffe der Analysis oder gar nur diejenigen der Arithmetik der völlig strengen Behandlung fähig. Eine solche bisweilen von hervorragenden Seiten vetretene Meinung halte ich für durchaus irrig; eine so einseitige Auslegung der Forderung der Strenge führt bald zu einer Isolierung aller aus der Geometrie, Mechanik und Physik stammenden Begriffe, zu einer Unterbindung des Zuflusses von neuem Material aus der Außenwelt und schließlich sogar in letzter Konsequenz zu einer Verwerfung der Begriffe des Kontinuums und der Irrationalzahl.*

[105] Our transl. of [Hilbert 2004], chap. 5, p. 436: *Die Geometrie bedarf – ebenso wie die Aritmnetik – zu ihrem folgerichtigen Aufbau nur weniger und einfacher Grundthatsachen. Diese Grundthatsachen heissen die* Axiome *der Geometrie.*

on arithmetization in the preface to the 1897 *Zahlbericht*[106] are best read with this evolution in mind. This preface builds up to the notion of arithmetization through a list of interactions of number theory with other mathematical disciplines. First he points to

> the close connection between number-theoretic questions and algebraic problems … The central reason for this connection is nowadays completely clear. Namely, the theory of algebraic numbers and the Galois theory of equations both have their roots in the theory of algebraic fields, and the theory of number fields has come to be the most essential part of modern number theory.[107]

Then Hilbert mentions five fruitful interactions between number theory and function theory: the analogies between number fields and function fields, the relation between the distribution of primes and the zeros of the Riemann zeta function, the transcendence of e and π, Dirichlet's analytic class number formula, and the theory of complex multiplication. All these examples motivate the inthronisation: "Thus we see how far arithmetic, the 'Queen' of mathematics, conquers broad areas of algebra and function theory and takes the lead in them."[108] Arithmetization is then added on top:

> Finally, there is the additional fact that, if I am not mistaken, the modern development of pure mathematics takes place chiefly *under the sign of number*: Dedekind's and Weierstrass's definitions of fundamental concepts of arithmetic and Cantor's general construction of the concept of number lead to an *arithmetization of function theory* and serve to realize the principle that even in function theory a fact can count as proved only when in the last resort it is reduced to relations between rational integers. The *arithmetization of geometry* is accomplished by the modern investigations in non-euclidean geometry in which it is a question of a strictly logical construction of the subject and the most direct possible and completely satisfactory introduction of number into geometry.[109]

[106] The essential building blocks of this preface to [Hilbert 1897] date back to 1895 and 1896; see [Hilbert 2004], pp. 153–156.

[107] I.T. Adamson's transl. of [Hilbert 1897], p. 64.

[108] Slight modification of I.T. Adamson's transl. of [Hilbert 1897], p. 65: *So sehen wir, wie die Arithmetik, die "Königin" der mathematischen Wissenschaft, weite algebraische und funktionentheoretische Gebiete erobert und in ihnen die Führerrolle übernimmt.*

[109] Our emendation (we correct in particular the erroneous replacement of "Weierstrass" by "Kronecker") of I.T. Adamson's transl. of [Hilbert 1897], p. 66: *Es kommt endlich hinzu, daß, wenn ich nicht irre, überhaupt die moderne Entwickelung der reinen Mathematik vornehmlich* unter dem Zeichen der Zahl *geschieht:* Dedekinds *und* Weierstrass*' Definitionen der arithmetischen Grundbegriffe und* Cantors *allgemeine Zahlgebilde führen zu einer* Arithmetisierung der Funktionentheorie *und dienen zur Durchführung des Prinzips, daß auch in der Funktionentheorie eine Tatsache erst dann als bewiesen gilt, wenn sie in letzter Instanz auf Beziehungen für ganze rationale Zahlen zurückgeführt worden ist. Die* Arithmetisierung der Geometrie *vollzieht sich durch die modernen Untrersuchungen über Nicht-Euklidische Geometrie, in denen es sich um einen streng logischen Aufbau derselben und um die möglichst direkte und völlig einwandfreie Einführung der Zahl in die Geometrie handelt.*

The ubiquity of number thus meets Hilbert's syncretist notion of arithmetization in 1897. This arithmetization touches algebra, analysis, and geometry alike. Hilbert does insist on the tremendous success of higher arithmetic, transformed into the mature theory of algebraic number fields. Arithmetization, however, is only added at the end of the argument as a general logical approach to the foundations of mathematical theories. Hardly three years later, Hilbert will speak of axiomatisation instead. His specific agenda was thus obviously different from Klein's, but the two Göttingen accounts of arithmetization resemble each other in that they retain essentially a very general idea about rigorous foundations, and brush over differences between specific arithmetization programmes.[110] We have seen in chap. I.2, § 3.6, above that inside the *Zahlbericht*, Hilbert also freely navigated between Dedekind's and Kronecker's approaches.

Reading Gauss's *Disquisitiones Arithmeticae* had provided Leopold Kronecker with a precise methodology of arithmetization, and Dedekind had interpreted the same source as a call for a particular type of mathematical conceptual analysis. Hilbert's *Zahlbericht* and his other foundational projects from the turn of the century do conjure up a very general principle of arithmetic and rigour; but the application of this principle in various parts of mathematics has emancipated itself from any Gaussian model and from the various types of arithmetization proposed since 1872; in fact, Hilbert described all of these as "genetic" in 1900, and preferred the "axiomatic" method instead.[111]

3.3. Looking Back on Arithmetization

The parallel German and French editions of the *Enzyklopädie der mathematischen Wissenschaften* provide an interesting snapshot capturing the differences between the German and the French outlook on mathematics before WW I.[112] In the case of arithmetization, however, the German text written by Alfred Pringsheim and its French arrangement by Jules Molk bear a more complicated relation to each other because Molk was not only French but also Kronecker's former student. Pringsheim's original German text on the arithmetization of irrationals focuses first on the axiomatisation of the relationship between numbers and points on the line initiated by Cantor and Dedekind. Then follow brief discussions of Paul "du Bois-Reymond's fight against the arithmetical theories," and of the "total arithmetization according to Kronecker." These two positions are described as deviating from the majority consensus and Kronecker's programe is flatly dismissed as impracticable; see [Pringsheim 1898], pp. 53–58. The French version, not surprisingly, discusses Charles Méray's approach in greater detail, insisting on its priority. Furthermore, Molk added more than four

[110] See also [Corry 1996/2004], chap. 3, and [Rowe 1989].

[111] [Hilbert 1900b], pp. 180–181.

[112] See C. Goldstein's chapter VI.1 below for a discussion of French reactions to arithmetization at the end of the century, esp. in connection with Charles Hermite's reading of the D.A. As for other countries, some initial references on the interesting Italian case can be found in [Pringsheim 1898], p. 53, note 18; p. 55, note 27; p. 57, note 37, as well as [Bohlmann 1897], p. 110.

pages describing Kronecker's programme quite carefully, explicitly stressing the constructivist principles behind it.[113]

A precious textbook reflecting the movement of arithmetization is [Stolz, Gmeiner 1902], i.e., the 2nd revised edition of Stolz's *Vorlesungen über allgemeine Arithmetik* of 1885. It is precious precisely because it looks less modern than one might expect in 1902, but covers a largely pre-set-theoretic panorama beginning with (abstract) magnitudes according to Grassmann.[114] The "Theoretical Arithmetic" treated here is characterized as the part of the foundations of analysis which does not require the notion of continuous function.[115] Both the point of view of magnitudes (sec. 5, pp. 99–119), and the arithmetization of the continuum "according to G. Cantor and Ch. Méray" (which the authors consider easiest to explain; sec. 7, pp. 138–184) are treated. Weierstrass's method is treated in exercises (e.g., pp. 177–179, 270). Kronecker's arithmetization is dismissed on the strength of the majority opinion among mathematicians. Probably the most original part for a textbook – which reminds us of the encyclopedia – is the historical sec. 6 (pp. 120–137) which takes the reader from Euclid's Book 5 – i.e., Eudoxus's theory of proportions – to Descartes, Newton, etc., and to the contemporary period.

By clearly exhibiting this traditional approach through magnitudes as a substantially different alternative to the arithmetization of the continuum, Stolz and Gmeiner displayed a keener historical sense than several of their colleagues, including even professionals of the history of mathematics. In fact, the arithmetization of real numbers was often seen as a modern replay of Eudoxos's theory of ratios. This strikes us as symptomatic of the rapidity with which arithmetization was not only nostrified in Göttingen, but lost the appearance of an innovative rearrangement of the hierarchy of mathematical disciplines, at the very time when the paradoxes of set theory began to potentially undermine the Dedekind-Cantor definitions of the continuum.

Rudolf Lipschitz would write to Dedekind already on June 8, 1876 with reference to book V of Euclid's *Elements*: "But I think that your definition of irrational numbers differs only in form, not in content from what the ancients have found."[116] Dedekind in his prompt reply naturally disliked the appeal to magnitudes, and also stressed – admitting for the sake of the argument[117] that Euclid's ratios of magnitudes

[113] [Molk 1909], pp. 147–163. In passing, Molk defends Kronecker's procedures against criticism by Couturat; see [Molk 1909], p. 160, notes.

[114] We do not attempt to survey the textbook reception of arithmetization in general. The work has not yet been done, as far as we know. The unbalanced [Bohlmann 1897], which was surely written upon Klein's request, takes arithmetization to start somehow with Euler, and fails to work out the last period for lack of time on the part of the author.

[115] [Stolz, Gmeiner 1902], p. IV: *Das von den soeben erwähnten Gegenständen gebildete Gebiet lässt sich dadurch kennzeichnen, das zur Behandlung desselben der Begriff der stetigen Function nicht erforderlich ist.*

[116] [Lipschitz 1986], p. 58 (cf. [Dedekind 1932], p. 469): *… ich aber der Meinung bin, dieselbe [Dedekinds Definition der irrationalen Zahlen] unterscheide sich nur in der Form des Ausdruckes aber nicht in der Sache von dem was die Alten festgestellt haben.* For Dedekind's reply, see pp. 64–68.

[117] Which one should not admit, because even ratios of integers were treated by Euclid as

were meant to define numbers – the absence of any discussion of completeness and continuity.

Other authors made the same observation as Lipschitz, apparently deriving a special satisfaction from this alleged coming together of great minds over many centuries. For Max Simon[118] for instance, prop. 24 of Euclid's Book V, clearly showed that Book V was really about "the foundation of the rules of computation for irrational numbers, and that Eudoxus's method differs only inessentially from that of our Weierstrass."[119] Sir Thomas Heath retorted by explaining that Dedekind's definition of his cuts was formally much closer to Euclid, Book V, def. 5, than Weierstrass's.[120]

4. Conclusion

There are a few respects which Cantor's, Dedekind's, and Kronecker's arithmetization programmes share, in spite of all their manifest incompatibility with respect to finitist or constructivist requirements. First, all three authors considered mathematics as a science with a clearly defined domain of objects: as mentioned before, Kronecker viewed mathematics as a natural science;[121] Dedekind considered his analysis of continuity via cuts as expressing the essence of this concept; Cantor seems to have considered even his transfinite numbers as something that he discovered, rather than invented.[122] For all three authors arithmetization reduced the irrational numbers to the rational – or all the way to natural – numbers whose existence was taken to be evident. Second, they all executed this reduction to elementary given objects in a way that they considered naturally adequate for the problem at hand: for Kronecker, this meant indeterminates and congruences *à la Gauss*, for Dedekind grouping together sets of primary objects was just as naturally adequate a procedure as the consideration of series of rational numbers was to Cantor. The overall image that this suggests of the movement of arithmetization in the 1870s and 1880s is therefore that of a novel theory of objects that had formerly been understood in terms of extrinsic notions (magnitudes), this novel theory being founded on an independently accepted basis (the natural numbers), and proceeding with ingredients or methods deemed to be

relations rather than objects; see [Vitrac 1992], p. 150.

[118] A teacher in Strasbourg who had obtained his docorate with Weierstrass and was from 1903 also *ordentlicher Honorarprofessor* for the history of mathematics at *Kaiser Wilhelm Universität Strassburg.*

[119] [Simon 1901], p. 122: *S[atz] 24 zeigt mit größter Schärfe, ... daß es sich im fünften Buch um nichts anderes handelt, als um die strenge Begründung der Rechnungsregeln für Irrationalzahlen, und daß der Gang des Eudoxus von dem unseres Weierstraß nur unwesentlich abweicht.* See also [Simon 1901], p. 108–110, where he acknowledged Hieronymus Zeuthen's similar observation; see [Zeuthen 1893/1902], § 16 of the part on Greek mathematics.

[120] [Heath 1926], p. 124–126. Cf. [Vitrac 1994], p. 548–551. According to [Simon 1906], p. 49, Cantor and Dedekind deluded themselves when they thought to have defined continuity arithmetically, without recourse to geometry. Cf. footnote 94 above.

[121] [Kronecker 1891], last paragraph on p. 232.

[122] [Cantor 1991], letter to Veronese, November 17, 1890, p. 330.

acceptable. From this point of view, arithmetization, in spite of all its novelty, appears not as an expression of modernity – indeed, as far as new objects were created, they were not purely formal, nor were they objectivized tools, but regularly formed from existing integers – but as a new type of solid building, erected on a traditional base in a controlled and supposedly innocuous and stable construction.

Our periodization has allowed us to isolate a transitional phase of arithmetization where Gaussian influence is detectible at least in two of the major authors. This influence operated via diverging fundamental positions (Kronecker's constructivism vs. Dedekind's completed infinites), but always in the direction of a novel but object-oriented rewriting of analysis. Gauss's after-effect ended with the onset of purely set-theoretic, axiomatic or logicist approaches, i.e., at the same time as the Göttingen nostrified image of arithmetization took shape.

References

Bekemeier, Bernd. 1987. *Martin Ohm (1792–1872): Universitätsmathematik und Schulmathematik in der neuhumanistischen Bildungsreform.* Göttingen: Vandenhoeck & Ruprecht.

Bernstein, Felix. 1911. Über eine Anwendung der Mengenlehre auf ein aus der Theorie der säkularen Störungen herrührendes Problem. *Mathematische Annalen* 71, 417–439.

Bohlmann, Georg. 1897. Übersicht über die wichtigsten Lehrbücher der Infinitesimalrechnung von Euler bis auf die heutige Zeit. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 6, 91–110.

Boniface, Jacqueline. 2002. *Les constructions des nombres réels dans le mouvement d'arithmétisation de l'analyse.* Paris: Ellipses.

du Bois-Reymond, Paul. 1882. *Die allgemeine Functionentheorie. Erster Teil. Metaphysik und Theorie der mathematischen Grundbegriffe: Grösse, Grenze, Argument und Function.* Tübingen: Laupp. Repr. Darmstadt: Wissenschaftliche Buchgesellschaft, 1968.

Cantor, Georg. 1870. Beweis, dass eine für jeden reellen Werth von x durch eine trigonometrische Reihe gegebene Funktion $f(x)$ sich nur auf eine einzige Weise in dieser Form darstellen lässt. *Journal für die reine und angewandte Mathematik* 72, 139–142.

———. 1872. Über die Ausdehnung eines Satzes aus der Theorie der trigonometrischen Reihen. *Mathematische Annalen* 5, 123–132. Repr. in [Cantor 1932], pp. 92–101.

———. 1879–1884. Über unendliche lineare Punktmannigfaltigkeiten. *Mathematische Annalen* 15 (1879), 1–7; 17 (1880), 355–358; 20 (1882), 113–121; 21 (1883), 51–58, 545–586; 23 (1884), 453–488. Repr. in [Cantor 1932], pp. 139–244.

———. 1887–1888. Mitteilungen zur Lehre vom Transfiniten. *Zeitschrift für Philosophie und philosophische Kritik* 91 (1887), 81–125; 92 (1888), 240–265. Repr. in [Cantor 1932], pp. 378–439.

———. 1889. Bemerkung mit Bezug auf den Aufsatz: Zur Weierstraß-Cantorschen Theorie der Irrationalzahlen. *Mathematische Annalen* 33, 476. Repr. in [Cantor 1932], p. 114.

———. 1932. *Gesammelte Abhandlungen mathematischen und philosophischen Inhalts*, ed. E. Zermelo. Berlin: Springer.

———. 1991. *Briefe*, ed. H. Meschkowski, W. Nilson. Berlin: Springer.

Cornelius, Hans. 1903. *Einleitung in die Philosophie.* Leipzig: Teubner.

Corry, Leo. 1996. *Modern Algebra and the Rise of Mathematical Structures.* Science Networks 17. Basel, Boston: Birkhäuser. 2nd ed., 2004.

———. 2004. *David Hilbert and the Axiomatization of Physics (1898–1918). From* Grundlagen der Geometrie *to* Grundlagen der Physik. Archimedes 10. Berlin, etc.: Springer.

Daum, Andreas W. 2002. *Wissenschaftspopularisierung im 19. Jahrhundert. Bürgerliche Kultur, naturwissenschaftliche Bildung und die deutsche Öffentlichkeit, 1848–1914.* 2nd ed. München: Oldenbourg.

Dedekind, Richard. 1872. *Stetigkeit und irrationale Zahlen*. Braunschweig: Vieweg. Repr. in *Gesammelte mathematische Werke*, ed. R. Fricke, E. Noether, O. Ore., vol. 3, pp. 315–334. Braunschweig: Vieweg, 1932. English transl. in [Ewald 1996], pp. 765–779.

Dirksen, Enno Heeren. 1845. *Organon der gesammten transcendenten Analysis. Erster Theil. Transcendente Elementarlehre.* Berlin: Reimer.

Dugac, Pierre. 1973. Eléments d'analyse de Karl Weierstrass. *Archive for History of Exact Sciences* 10, 41–176.

———. 1976. *Richard Dedekind et les fondements des mathématiques*. Paris: Vrin.

———. 2003. *Histoire de l'analyse. Autour de la notion de limite et ses voisinages*, ed. B. Bru, R. Laurent. Paris: Vuibert.

Dühring, Eugen Karl. 1865. *Natürliche Dialektik. Neue logische Grundlegungen der Wissenschaft und Philosophie*. Berlin: Mittler. Repr. Frankfurt/Main: Minerva, 1975.

———. 1877. *Kritische Geschichte der allgemeinen Prinzipien der Mechanik. Von der philosophischen Fakultät der Universität Göttingen mit dem ersten Preise der Beneke-Stiftung gekrönte Schrift*. Leipzig: Fues.

———. 1878. *Logik und Wissenschaftstheorie*. Leipzig: Fues.

Dühring, Eugen Karl, Dühring, Ulrich. 1884. *Neue Grundmittel und Erfindungen zur Analysis, Algebra, Functionsrechnung und zugehörigen Geometrie, sowie Principien zur mathematischen Reform nebst einer Anleitung zum Studium und Lehren der Mathematik*. Leipzig: Fues.

Elsas, Adolf. 1886. *Über die Psychophysik. Physikalische und erkenntnistheoretische Betrachtungen*. Marburg: Elwert.

Epple, Moritz. 1999. Das Ende der Größenlehre: Grundlagen der Analysis 1860–1910. In *Geschichte der Analysis*, ed. H.N. Jahnke, pp. 371–410. Heidelberg: Spektrum. English transl. in *A History of Analysis*, ed. H.N. Jahnke, pp. 291–323. Providence: American Mathematical Society, 2003.

Ewald, William Bragg. 1996. *From Kant to Hilbert*, vol. 2. Oxford: Oxford University Press.

Ferreirós, José. 1999. *Labyrinth of Thought: A History of Set Theory and its Role in Modern Mathematics*. Science Networks 23. Basel: Birkhäuser.

Hankel, Hermann. 1867. *Theorie der complexen Zahlensysteme insbesondere der gemeinen imaginären Zahlen und der Hamilton'schen Quaternionen nebst ihrer geometrischen Darstellung*. Leipzig: Voss.

———. 1871. Grenze. In *Allgemeine Encyklopädie der Wissenschaften und Künste, in alphabetischer Folge*, ed. J.S. Ersch, J.G. Gruber, vol. 90 of part 1, pp. 185–211. Leipzig: Gleditsch. Repr. Graz: Akademische Druck- und Verlagsanstalt, 1976.

Haubrich, Ralf. 1992. *Zur Entstehung der algebraischen Zahlentheorie Richard Dedekinds.* Dissertation, Georg-August-Universität Göttingen. Göttingen.

Heath, Sir Thomas L. 1926. *The Thirteen Books of Euclid's Elements, translated from the text of Heiberg, with introduction and commentary*, vol. 2: Books III–IX. 2nd ed. Cambridge: Cambridge University Press. Repr. New York: Dover, 1956.

Heine, Eduard. 1870. Ueber trigonometrische Reihen. *Journal für die reine und angewandte Mathematik* 71, 353–365.

———. 1872. Die Elemente der Functionenlehre. *Journal für die reine und angewandte Mathematik* 74, 172–188.

Hilbert, David. 1897. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4 ("1894–1895"), 177–546 + Vorwort 1–xviii. Repr. in *Gesammelte Abhandlungen*, vol. 1, pp. 63–363. Berlin: Springer, 1932. Engl. transl. I. Adamson: *The Theory of Algebraic Number Fields*, introd. F. Lemmermeyer, N. Schappacher. New York: Springer, 1998.

———. 1900a. Mathematische Probleme. Vortrag, gehalten auf dem Internationalen Mathematiker-Congress zu Paris 1900. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 253–297. Engl. transl., *Bulletin of the American Mathematical Society* 8 (1902), 437–479; repr. in *Mathematical developments arising from Hilbert problems*, ed. F. E. Browder, pp. 1–34. Providence: American Mathematical Society, 1976.

———. 1900b. Über den Zahlbegriff. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 8, 180–184.

———. 2004. *David Hilbert's Lectures on the Foundations of Geometry 1891–1902*, ed. M. Hallet, U. Majer. Berlin, Heidelberg: Springer.

Jahnke, Hans Niels, Otte, Michael. 1981. Origins of the program of "arithmetization of mathematics." In *Social History of Nineteenth-Century Mathematics*, ed. H. Mehrtens, H. Bos, I. Schneider. Boston, Basel, Stuttgart: Birkhäuser.

Kerry, Benno. 1889–1890. Ueber Anschauung und ihre psychische Verarbeitung. *Vierteljahrsschrift für wissenschaftliche Philosophie*. Part 5: 13 (1889), 71–124; Part 7: 14 (1890), 317–353.

———. 1890. *System einer Theorie der Grenzbegriffe. Ein Beitrag zur Erkenntnisstheorie*, ed. Gustav Kohn. Leipzig: Franz Deuticke.

Kirchhoff, Gustav Robert. 1865. *Ueber das Ziel der Naturwissenschaften: Vortrag zum Geburtsfeste des höchstseligen Grossherzogs Karl Friedrich von Baden und zur akademischen Preisvertheilung am 22. November 1865*. Heidelberg: Mohr.

———. 1876. *Vorlesungen über mathematische Physik*, vol. I: *Mechanik*. Leipzig: Teubner.

Klein, Felix. 1873. Über den allgemeinen Funktionsbegriff und dessen Darstellung durch eine willkürliche Kurve. *Sitzungsberichte der physikalisch-medizinischen Sozietät zu Erlangen*. Repr. *Mathematische Annalen* 22 (1883), 249–259. Repr. in [Klein 1921–1922], vol. 2, pp. 214–224.

———. 1880–1881. *Funktionentheorie in geometrischer Behandlungsweise. Vorlesung gehalten in Leipzig 1880/81*, ed. F. König. Leipzig: Teubner, 1987.

———. 1880. Über die Beziehungen der neueren Mathematik zu den Anwendungen (Antrittsrede 25.10.1880 Leipzig). *Zeitschrift für den mathematischen und naturwissenschaftlichen Unterricht* 26 (1895), 534–540.

———. 1890. Zur Nicht-Euklidischen Geometrie. *Mathematische Annalen* 37, 544–572. Repr. in [Klein 1921–1922], vol. 1, pp. 353–383.

———. 1895. Über Arithmetisierung der Mathematik. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Geschäftliche Mitteilungen*, 82–91. Repr. in [Klein 1921–1922], vol. 1, pp. 232–240. Engl. transl. *Bulletin of the American Mathematical Society* 2 (1895), 241–249; repr. in [Ewald 1996], pp. 965–971. Italian transl. S. Pincherle, *Rendiconti del circolo matematico di Palermo* 10 (1896), 107–117. French transl. L. Laugel, *Nouvelles Annales* 3rd ser. 16 (1897), 114–128.

———. 1921–1922. *Gesammelte mathematische Abhandlungen*. Vol. 1: *Liniengeometrie, Grundlegung der Geometrie, zum Erlanger Programm*, ed. R. Fricke, A. Ostrowski, 1921; vol. 2: *Anschauliche Geometrie, Substitutionsgruppen und Gleichungstheorie, zur mathematischen Physik*, ed. R. Fricke, H. Vermeil, 1922. Berlin: Springer.

Köhnke, Klaus Christian. 1986. *Entstehung und Aufstieg des Neukantianismus. Die deutsche Universitätsphilosophie zwischen Idealismus und Positivismus*. Frankfurt am Main: Suhrkamp.

Königsberger, Leo. 1895. *Hermann von Helmholtz's Untersuchungen über die Grundlagen der Mathematik und Mechanik. Rede zum Geburtsfeste des höchstseligen Grossherzogs Karl Friedrich und zur akademischen Preisvertheilung am 22. Nov. 1895*. Heidelberg: Hörning.

Kopfermann, Klaus. 1966. Weierstraß' Vorlesung zur Funktionentheorie. In *Festschrift zur Gedächtnisfeier für Karl Weierstraß 1815–1965*, ed. H. Behnke, K. Kopfermann, pp. 75–96. Köln: Westdeutscher Verlag.

Kossak, Ernst. 1872. *Die Elemente der Arithmetik*. Berlin: Nauck.

Kronecker, Leopold. 1881. *Grundzüge einer arithmetischen Theorie der algebraischen Grössen*. Berlin: Reimer. Repr. in *Journal für die reine und angewandte Mathematik* 92 (1882), 1–122. Repr. in [Kronecker 1895–1931], vol. 2, pp. 237–387.

———. 1883. Über bilineare Formen mit vier Variablen. *Abhandlungen der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 1–60. Repr. in [Kronecker 1895–1931], vol. 2, pp. 425–495.

———. 1886. Ueber einige Anwendungen der Modulsysteme auf elementare algebraische Fragen. *Journal für die reine und angewandte Mathematik* 99, 329–371. Repr. in [Kronecker 1895–1931], vol. 3(1), pp. 145–208.

———. 1887a. Ein Fundamentalsatz der allgemeinen Arithmetik. *Journal für die reine und angewandte Mathematik* 100, 490–510. Repr. in [Kronecker 1895–1931], vol. 3(1), pp. 209–240.

———. 1887b. Über den Zahlbegriff. *Journal für die reine und angewandte Mathematik* 101, 337–355. Repr. in [Kronecker 1895–1931], vol. 3(1), pp. 249–274. Engl. transl. in [Ewald 1996], pp. 947–955.

———. 1888. Zur Theorie der allgemeinen complexen Zahlen und der Modulsysteme. *Sitzungsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin* 429–438, 447–465, 557–578, 595–612, 983–1016. Repr. in [Kronecker 1895–1931], vol. 3(2), pp. 1–114.

———. 1891. Über den Begriff der Zahl in der Mathematik, ed. J. Boniface, N. Schappacher. In "Sur le concept de nombre en mathématique." Cours inédit de Leopold Kronecker à Berlin. *Revue d'histoire des mathématiques* 7 (2001), 207–275.

———. 1901. *Vorlesungen über Zahlentheorie*, ed. K. Hensel. Leipzig: Teubner. Repr. Berlin, Heidelberg, New York: Springer, 1978.

———. 1932. Faksimilierte Wiedergabe einer Adresse von Leopold Kronecker an Eduard Kummer zum 80. Geburtstage am 29. Januar 1890. *Journal für die reine und agewandte Mathematik* 170, 1–3.

———. 1895–1931. *Werke*, ed. K. Hensel. Leipzig: Teubner. 5 vols. Repr. New-York: Chelsea, 1968.

LIPSCHITZ, Rudolf. 1986. *Briefwechsel mit Cantor, Dedekind, Helmholtz, Kronecker, Weierstrass*, ed. W. Scharlau. Dokumente zur Geschichte der Mathematik 2. Braunschweig, Wiesbaden: Vieweg.

MÉRAY, Charles. 1869. Remarques sur la nature des quantités définies par la condition de servir de limites à des variables données. *Revue des sociétés savantes (Sciences mathématiques, physiques et naturelles)* 2nd ser. 3, 280–289. (Published in 1870.)

———. 1872. *Nouveau précis d'analyse infinitésimale*. Paris: F. Savy.

———. 1887. Sur le sens qu'il convient d'attacher à l'expression nombre incommensurable et sur le critérium de l'existence d'une limite pour une quantité variable de nature donnée. *Annales de l'Ecole Normale Supérieure* 3rd ser. 4, 341–360.

———. 1894. *Leçons nouvelles sur l'analyse infinitésimale et ses applications géométriques. 1ère partie: Principes généraux.* Paris: Gauthier-Villars.

MINKOWSKI, Hermann. 1905. Peter Gustav Lejeune-Dirichlet und seine Bedeutung für die heutige Mathematik, *Jahresbericht der Deutschen Mathematiker-Vereinigung* 14, 149–163. Repr. in *Gesammelte Anhandlungen*, ed. D. Hilbert, vol. 2. Leipzig: Teubner, 1911.

MOLK, Jules. 1909. Nombres irrationnels et notion de limite. In *Encyclopédie des sciences mathématiques pures et appliquées*, vol. I, part 3, pp. 133–208. Paris: Gauthier-Villars; Leipzig: Teubner.

NEUENSCHWANDER, Erwin. 1978. Der Nachlaß von Casorati (1835–1890) in Pavia. *Archive for History of Exact Sciences* 19, 1–89.

NEWTON, Isaac. 1707. *Arithmetica universalis, sive de compositione et resolutione arithmetica liber.* Cambridge: Tooke.

PRINGSHEIM, Alfred. 1898. Irrationalzahlen und Konvergenz unendlicher Prozesse. In *Encyklopädie der Mathematischen Wissenschaften mit Einschluss ihrer Anwendungen*, ed. W.F. Meyer, vol. I, part 1, pp. 47–146. Leipzig: Teubner.

ROWE, David. 1989. Klein, Hilbert, and the Göttingen mathematical tradition. *Osiris* (2) 5, 186–312.

SCHAPPACHER, Norbert. 1998. On the History of Hilbert's Twelfth Problem, A Comedy of Errors. In *Matériaux pour l'histoire des mathématiques au XXe siècle. Actes du colloque à la mémoire de Jean Dieudonné. Nice 1996*, pp. 243–273. Séminaires et Congrès 3. Paris: Société Mathématique de France.

SIMON, Max. 1901. *Euclid und die sechs planimetrischen Bücher, mit Benutzung der Textausgabe von Heiberg*. Leipzig: Teubner.

———. 1906. *Methodik der elementaren Arithmetik, in Verbindung mit algebraischer Analysis*. Leipzig, Berlin: Teubner.

STERN, Moritz Abraham. 1860. *Lehrbuch der algebraischen Analysis*. Leipzig, Heidelberg: Winter'sche Verlagshandlung.

Stolz, Otto. 1891. *Grössen und Zahlen.* Rede bei Gelegenheit der feierlichen Kundmachung der gelösten Preisaufgaben am 2. März 1891. Leipzig: Teubner.

Stolz, Otto, Gmeiner, J. Anton. 1902. *Theoretische Arithmetik. II. Abteilung: Die Lehre von den reellen und von den complexen Zahlen.* 2$^{\text{nd}}$ reworked ed. of O. Stolz, *Vorlesungen über allgemeine Arithmetik*, sects. V–VIII, X, XI of part I (1885), and sects. I,II,V of part II (1886). Leipzig: Teubner.

Toepell, Michael-Markus. 1986. *Über die Entstehung von David Hilberts "Grundlagen der Geometrie"*. Göttingen: Vandenhoeck & Ruprecht.

Ullrich, Peter. 1988. *Vorwort des Bearbeiters.* In [Weierstrass 1878], pp. xi–xxvii.

Vitrac, Bernard. 1992. Logistique et fractions dans le monde hellénistique. In *Histoire de fractions, fractions d'histoire,* ed. P. Benoît, K. Chemla, J. Ritter, pp. 149–172. Basel, Boston, Berlin: Birkhäuser.

———. 1994. *Euclide d'Alexandrie, Les Éléments, traduits du texte de Heiberg,* vol. 2: *Livres V–VI, Proportions et similitude*; *Livres VII–IX, Arithmétique*. Paris: Presses Universitaires de France.

Vlăduţ, Serge G. 1991. *Kronecker's Jugendtraum and Modular Functions*. Studies in the Development of Modern Mathematics 2. New York etc.: Gordon & Breach.

Weierstrass, Karl Theodor Wilhelm. 1868. *Einführung in die Theorie der analytischen Funktionen. Nach einer Vorlesungsmitschrift von Wilhelm Killing aus dem Jahr 1868.* Schriftenreihe des Mathematischen Instituts der Universität Münster, 2$^{\text{nd}}$ ser. 38, Februar 1986. Münster: Mathematisches Institut.

———. 1874. *Einleitung in die Theorien der analytischen Functionen. Nach den Vorlesungen im S.S. 1874 ausgearbeitet von G. Hettner.* Manuscript in Bibliothek, Mathematisches Institut, Göttingen.

———. 1878. *Einleitung in die Theorie der analytischen Funktionen. Vorlesung Berlin 1878 in einer Mitschrift von Adolf Hurwitz*, ed. P. Ullrich. Dokumente zur Geschichte der Mathematik 4. Braunschweig: Vieweg, 1988.

———. 1883. *Theorie der analytischen Functionen nach Vorlesungen des Professor Weierstraß.* Unpub. manuscript by K. Hensel in Bibliothèque de IRMA, Strasbourg.

———. 1886. *Ausgewählte Kapitel aus der Funktionenlehre. Vorlesung, gehalten in Berlin 1886*, ed. R. Siegmund-Schultze. Teubner-Archiv zur Mathematik 9. Leipzig: Teubner, 1988.

———. 1923. Briefe an Paul du Bois-Reymond. *Acta Mathematica* 39, 199–225.

Weyl, Hermann. 1918. *Das Kontinuum. Kritische Untersuchungen über die Grundlagen der Analysis.* Leipzig: Veit & Comp.

Wundt, Wilhelm. 1883. *Methodenlehre.* Vol. 2 of *Logik. Eine Untersuchung der Prinzipien der Erkenntnis und der Methoden wissenschaftlicher Forschung*. Stuttgart: Enke.

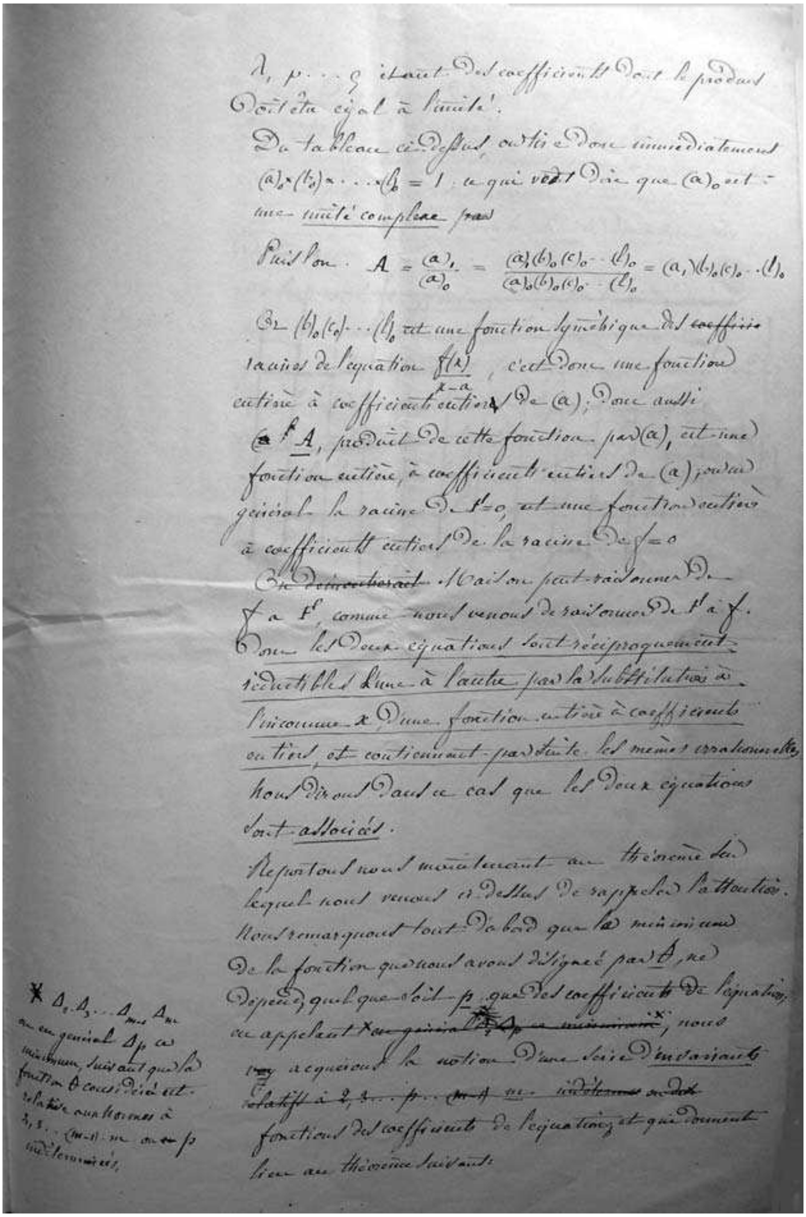
Zeuthen, Hieronymus Georg. 1893. *Forelæsning over Mathematikens Historie. Oldtid og middelalder.* København: Høst & Søn 1893. German transl. R. von Fischer-Benzon, *Geschichte der Mathematik im Altertum und Mittelalter: Vorlesungen*. Kopenhagen: Hoest 1896. French transl. J. Mascart, *Histoire des mathématiques dans l'antiquité et le moyen âge*. Paris: Gauthier-Villars, 1902.

Part VI

Number Theory and the *Disquisitiones* in France after 1850

Ces propositions d'arithmétique sont curieuses et donnent une impression de pure beauté à tous ceux qui en saisissent le sens. Mais on peut se demander si cette jouissance esthétique d'un petit nombre suffit à justifier les grands efforts des arithméticiens purs, alors qu'il existe tant de questions d'analyse, dont la solution serait du plus haut intérêt pour la mécanique et la physique, et dont la beauté esthétique n'est pas moindre. … Aussi n'y a-t-il pas lieu de regretter que la jeune école mathématique française délaisse ces études arithmétiques, en faveur en Allemagne, pour s'attacher de préférence à défricher le champ immense de recherches qui se rattachent au calcul différentiel et au calcul intégral.

Anon. [Emile Borel], *La Revue du mois*, 1906



$\lambda, \mu \dots \varsigma$ étant des coefficients dont le produit doit être égal à l'unité.

Du tableau ci-dessus, on tire donc immédiatement $(a)_0 \times (b_0) \times \dots (l)_0 = 1$, ce qui veut dire que $(a)_0$ est une unité complexe ~~pas~~

Puis l'on a $A = \frac{(a)_1}{(a)_0} = \frac{(a)_1 (b)_0 (c)_0 \dots (l)_0}{(a)_0 (b)_0 (c)_0 \dots (l)_0} = (a_1)(b)_0(c)_0 \dots (l)_0$

Or $(b)_0 (c_0) \dots (l)_0$ est une fonction symétrique des ~~coeffici~~ racines de l'équation $\frac{f(x)}{x-a}$, c'est donc une fonction entière à coefficients entiers de (a); donc aussi A, produit de cette fonction par (a), est une fonction entière, à coefficients entiers de (a); ou en général la racine de $F=0$, est une fonction entière à coefficients entiers de la racine de $f=0$

~~On démontrerait~~ Mais on peut raisonner de f à F, comme nous venons de raisonner de F à f. Donc les deux équations sont réciproquement réductibles l'une à l'autre par la substitution à l'inconnue x d'une fonction entière à coefficients entiers, et contiennent par suite les mêmes irrationnelles, nous dirons dans ce cas que les deux équations sont associées.

Reportons nous maintenant au théorème sur lequel nous venons ci-dessus de rappeler l'attention. Nous remarquons tout d'abord que le minimum de la fonction que nous avons désignée par θ, ne dépend, quel que soit p que des coefficients de l'équation, en appelant ✱ ~~en général Δ_p ce minimum~~ ✱, nous acquérons la notion d'une série d'invariants ~~relatifs à 2, 3 ... p ... (n-1) ou indéterminés~~ fonctions des coefficients de l'équation, et qui donnent lieu au théorème suivant.

✱ $\Delta_2, \Delta_3 \dots \Delta_{n-1}, \Delta_n$ ou en général Δ_p ces minimum, suivant que la fonction θ considérée est relative aux formes à 2, 3 ... (n-1) ... n ou p indéterminées,

Fig. VI.1. C. Hermite's continuous reduction of forms: a programme for algebraic numbers
Unpublished manuscript, January 1852
(Académie des sciences de l'Institut de France)

VI.1

The Hermitian Form of Reading the *Disquisitiones*

CATHERINE GOLDSTEIN

Sketching his professional biography for Gösta Mittag-Leffler in 1882, Charles Hermite presented his departure from the Ecole polytechnique:

> This was in 1843, and, since that moment, I have devoted myself entirely to the study of elliptic functions and of Gauss's *Disquisitiones Arithmeticae*.[1]

This double dedication is doubly intriguing; from the point of view of the *Disquisitiones*, and from the point of view of Hermite and the French mathematical scene. From the first because of the apparent asymmetry of the formulation: Hermite does not say "elliptic functions and number theory," nor even "elliptic functions and forms," which might seem to capture more aptly his multifarious work on invariant theory, algebraic equations, Diophantine approximation and the integration of differential equations arising out of physical problems. Nor did he restrict himself to "Jacobi's *Fundamenta nova theoriae functionum ellipticarum* and Gauss's *Disquisitiones Arithmeticae*," although we have ample testimonies of his life-long involvement with Carl Gustav Jacob Jacobi's masterpiece.[2] Hermite provides us instead with a hint to the particular status of the D.A., which appears here as a

[1] [Hermite & Mittag-Leffler 1984–1989], part I, p. 168, letter 80, September 15, 1882: *C'était en 1843, et, à partir de cette époque, je me suis entièrement consacré à l'étude des fonctions elliptiques, et des* Disquisitiones Arithmeticae *de Gauss*. According to Gaston Darboux, Hermite left the Polytechnique one year after his admission because an infirmity closed his access to the state careers usually available at graduation, see [Darboux 1905], p. 11; the letter to Mittag-Leffler, however, mentions only that Joseph Liouville, then professor at the Polytechnique, convinced Hermite's parents to let him leave the school and follow his penchant for mathematics.

[2] "Jacobi's *Fundamenta Nova* was always on his desk" (*Les* Fundamenta nova *de Jacobi étaient toujours sur sa table de travail*) wrote, for example, his son-in-law, the mathematician Emile Picard, in [Picard 1901/1905–1917], p. xxvi.

mathematical research field in itself.[3]

Then again, it is intriguing from the second point of view, that of Hermite. In his introduction to Ernst Eduard Kummer's *Collected Papers*, André Weil writes:

> The great number-theorists of the last century are a small and select group of men. The names of Gauss, Jacobi, Dirichlet, Kummer, Hermite, Eisenstein, Kronecker, Dedekind, Minkowski, Hilbert spring to mind at once. To these one may add a few more, such as the universal Cauchy, H. Smith, H. Weber, Frobenius, Hurwitz.[4]

Indeed, Hermite is the main figure on the French mathematical scene in the XIX$^{\text{th}}$ century, who was, and is still, recognized as a first-rank *number theorist*. As explained earlier (see in particular chap. I.1), the French mathematicians welcomed the D.A. early and warmly, but also read it through a specific prism, that of the theory of algebraic equations. Hermite's work itself blossomed in this particular soil; according to Emile Picard, Hermite liked to say that he had taught himself *algebra*, while still at school, by reading Joseph Lagrange's *Traité de la résolution des équations numériques* and the D.A., [Picard 1901/1905–1917], p. viii. One can thus wonder how his intense interaction with the D.A. led him to number theory, and to which number theory. Was Hermite's arithmetical work akin to that done by the contemporary German mathematicians mentioned by Weil above? Did it too shape part of the evolution of arithmetic? To answer these questions, I shall first survey the evidence we have of the role of the *Disquisitiones Arithmeticae* in Hermite's scientific biography; I shall then exemplify how the D.A. was used by Hermite, in what contexts and to what effect, through a closer reading of a few articles. Finally, I shall reflect on the specificities of the Hermitian interpretation of the D.A. and on its impact in the second half of the XIX$^{\text{th}}$ century.

1. Explicit References to Gauss in Hermite's Works

Gauss's name appears recurrently in Hermite's published writings, as well as in his correspondence, often as that of a guide and of a model of all things mathematical. In one of his first works devoted to number-theoretical questions, at the end of the 1840s, Hermite alluded for instance to "the great questions of the theory of forms, considered in a general manner, … this immense field of research which has been opened to us by M. Gauss."[5] In an 1867 letter, he claimed Gauss as the German equivalent of the influential Laplace,

> and it is to the impulse given by these two men of an extraordinary genius that are due the works realized in our time. … The way opened by the illustrious master has

[3] On this issue, see chap. I.1 above, in particular § 5.

[4] [Weil 1979], vol. 3, p. 379. Weil's judgment, as well as his list, is of course partly subjective; but it neatly illustrates the current view according to which most number-theoretical work was produced in Germany, see also on this issue J. Ferreirós's chap. III.2. The basis of this view, its anchorage in a particular hierarchy of mathematical subjects, and its limits are discussed in part I above.

[5] See [Hermite 1850/1905–1917], vol. I, p. 136: … *des grandes questions de la théorie des formes, considérée d'une manière générale. Dans cette immense étendue de recherches qui nous a été ouverte par M. Gauss…*

> been particularly fruitful. Lagrange, Legendre above all, and after him M. Cauchy in his last years, have emulated Gauss in several respects.[6]

In 1892, the names of Gauss, again, and of Jacobi, serve to measure his admiration for one of Stieltjes's results: "neither Gauss nor Jacobi ever gave me more pleasure."[7]

Praise of Gauss is of course no cause for surprise. In Hermite's case it is also part and parcel of the great admiration he felt and expressed during his entire life for German mathematics (and more generally for Germany) as a whole. He entertained epistolary contacts with Jacobi since the mid 1840s, and later on with many other German mathematicians, like Carl Borchardt, Rudolf Lipschitz, Leo Königsberger or Leopold Kronecker. He traveled at the beginning of the 1850s to Berlin, where he was met, among others, by Gotthold Eisenstein, Ernst Eduard Kummer and Peter Gustav Lejeune Dirichlet.[8] Later, visiting him would be compulsory for German mathematicians passing through Paris. In 1877, he enthusiastically participated in the ceremonies honouring Gauss's centenary in Göttingen. Hermite was widely considered in German circles as an important mediator with French mathematicians, to the point of being later criticized in France as too overtly pro-German.[9]

However, my opening quote suggests that the impact of the *Disquisitiones Arith-*

[6] Letter of January 8, 1867 to unindentified recipient, Dossier Hermite, Archives de l'Académie des sciences: *Et c'est à l'impulsion donnée par ces deux hommes d'un génie extraordinaire que sont dus les travaux accomplis à notre époque. … La voie ouverte par l'illustre maître a été singulièrement féconde. Lagrange, Legendre surtout et après lui Mr. Cauchy dans ses dernières années, ont été les émules de Gauss à plusieurs égards.* Given the respective ages of Lagrange, Legendre and Gauss, the last sentence is striking.

[7] [Hermite & Stieltjes 1905], vol. 2, p. 268: *Ni Gauss, ni Jacobi ne m'ont jamais causé plus de plaisir.*

[8] Although alluded to in his published letters to Thomas Stieltjes, [Hermite & Stieltjes 1905], vol. I, p. 387, as well as in Eisenstein's *Werke*, [Eisenstein 1975], vol. 2, p. 771, this important early trip is not mentioned in the Hermite obituaries I have seen, nor in the more recent historical literature. It is however largely documented in letters. For instance, Victor Puiseux recommended him to Dirichlet around 1851: *Je profite pour me rappeler à vous du voyage que va faire à Berlin M. Hermite dont le talent pour les mathématiques vous est bien connu et qui était tant apprécié par M. Jacobi. Plus peut-être que personne en France, M. Hermite est au courant des beaux travaux par lesquels les géomètres allemands se sont illustrés ces derniers temps.* Hermite himself mentions his mathematical discussions in Berlin, for instance in a letter to Dirichlet written in April 1853: *Dans les instants trop courts que j'ai pu passer auprès de vous lors de mon voyage à Berlin, vous m'avez annoncé en présence de notre pauvre ami Eisenstein, avoir la théorie de la transformation en elle-même d'une forme ternaire indéfinie.* Both letters are in Dirichlet's *Nachlaß*, Staatsbibliothek zu Berlin-Preussischer Kulturbesitz, Handschriftenabteilung.

[9] See for example the letter of December 17, 1875 from Borchardt to Lipschitz, in [Lipschitz 1986], p. 21: "Hermite is already perceived as pro-German and unpatriotic by some of his colleagues." His role as a mediator is extolled in his German-language obituaries. In the *Abhandlungen der naturwissenschaftlichen Gesellschaft ISIS in Dresden* (1901), Heft 1, Martin Krause praised his efforts, *das Studium der Werke von Gauss und von Jacobi heimisch zu machen*, adding: *während seines ganzen wissenschaftlichen Lebens war er*

meticae on Hermite's mathematics was even more pervasive and more specific. To be able to place it in its proper perspective, it is useful to revisit briefly Hermite's mathematical biography.[10]

Charles Hermite was born in 1822 in Dieuze, near Nancy, in the East of France,[11] studying first in Nancy, then in Paris. While preparing the entrance examination for the Ecole polytechnique, the *pépinière* for French mathematicians in the early 1840s, he was already reading on his own Euler's writings and other advanced mathematical works.[12] He also published two small papers in the *Nouvelles Annales*, one of which proves the impossibility of solving the general quintic equation by radicals. Received at the Ecole polytechnique in the summer of 1842, Hermite resigned after a year, as mentioned above; but he had already made important contributions to the study of elliptic functions and their generalizations, communicated to Jacobi from January 1843 on. The reproduction of Hermite's letters in Jacobi's own *Opuscula*, as early as 1846, bears ample testimony to the rapid international recognition of Hermite's mathematical value. His professional status in France, however, remained uncertain for a longer time. He became *répétiteur* for analysis at the Ecole Polytechnique in 1848,[13] temporarily replaced the fugitive Guglielmo Libri at the Collège de France in 1848–1849 and 1849–1850, with two courses on elliptic functions and number theory,[14] and was elected as early as 1856 to the Academy of sciences; but he did not obtain a stable and solid position in France until the 1860s.[15] During this period, however, he produced numerous works: on elliptic and Abelian functions; on quadratic n-ary forms and binary forms of various degrees, studying them arithmetically, but also algebraically in connection with Arthur Cayley and James Joseph Sylvester's work on invariant theory; and on algebraic equations, in particular on

ein Vermittler der deutschen und der französischen Mathematik; see also Emil Lampe in *Naturwissenschaftliche Rundschau*, in 1901. On Hermite's activities in promoting German mathematics, see [Archibald 2002]. For the various ways Hermite used the very idea of a French-German frontier, see [Goldstein 2006].

[10] If not otherwise indicated, the information is taken from [Picard 1901], [Darboux 1905] and letter 80 in [Hermite & Mittag-Leffler 1984–1989].

[11] Dieuze (in contrast to Nancy) became German in 1871, after the Franco-Prussian war.

[12] Emile Picard wrote at the beginning of Hermite's *Œuvres* that at this moment, Hermite bought with his own money a copy of the *Disquisitiones Arithmeticae* (see [Picard 1901], also reproduced in [Darboux 1905], p. 7). In his brief autobiographical letter sent to Mittag-Leffler in 1882, Hermite's unique allusion to the D.A. serves as my opening quote, concerning the period 1843 and onward.

[13] That same year he married Louise Bertrand, the sister of the mathematician Joseph Bertrand; one of their daughters married Emile Picard. On the family relationships among French mathematicians and on the key figure of Bertrand as an organizer and "mathematical politician," see [Zerner 1991].

[14] He did not apply for the position, once vacant. Liouville obtained it in 1851, against Cauchy, see [Belhoste & Lützen 1984], [Lützen 1990] and [Belhoste 1991].

[15] He became *maître de conférences* à l'Ecole Normale Supérieure in 1862 and finally obtained one professorship in 1869 at the Ecole polytechnique, and in 1870 another at the Sorbonne (he would abandon the first in 1876).

modular equations, Sturm's theorem and the solution of the quintic equation by elliptic functions. In the 1870s, in connection with his courses, his research mostly focused on analytical aspects and on applications of elliptic functions to differential equations and mechanics. However, he retained a life-long interest in approximations and the generalizations of continued fractions – an interest culminating with his proof of the transcendence of *e* in 1873. By the last decades of the century, he had become an icon of the French mathematical community, visited by a continuous flow of visitors, with an intensive and varied international correspondence – besides Mittag-Leffler and the German mathematicians already alluded to, may be mentioned Hermann Amandus Schwarz, Angelo Genocchi, James Joseph Sylvester, Thomas Stieltjes, Mathias Lerch, and many others. His Jubilee in December 1892, a few days before that of Louis Pasteur, epitomized these various aspects of his scientific status. He died at the beginning of 1901, just after two last mathematical notes on approximation, continued fractions, and zeros of special functions.

Hermite had studied the *Disquisitiones Arithmeticae* early[16] and as a part of an essentially autodidactic, though intense, training, which included books by Lagrange, Legendre and Jacobi as well. Contrary to most authors in France, who, before 1850, concentrated principally on congruences and on the seventh section of the D.A., Hermite's focus was definitely on its fifth section. In his obituary of Kronecker, Hermite asserted that "the theory of quadratic forms is the most important part of the Disquisitiones Arithmeticae of Gauss,"[17] and other mathematicians would follow this lead in describing Hermite's predilections as well as in sketching his links to Gauss; at Hermite's Jubilee, Henri Poincaré declared for instance:

> You have never stopped cultivating the highest parts of the mathematical sciences, those where pure number reigns: analysis, algebra, arithmetic. … You made your first discoveries in the nascent theory of algebraic forms and, while successively attacking all the interesting questions in arithmetic, you enlarged and illuminated with a new light the admirable structure raised by Gauss.[18]

[16] Which text did Hermite use? Most references are to article numbers which are the same in all versions. According to Picard, Hermite had bought the French translation by Poullet-Delisle (thus still available around 1840), and there is indeed an 1861 mention of "Gauss. Rec. Arith. p. 288" ([Hermite 1905–1917], vol. 2, p. 116), relative to ambiguous forms, which confirms this natural hypothesis. However, on December 8, 1891 for instance, Hermite advises Stieltjes to consult the "Disquisitiones Arithmeticae. Digressio continens tractatum de formis ternariis" ([Hermite & Stieltjes 1905], vol. 2, p. 199), and another mention of the Latin title of a paragraph of the D.A. also appears in an 1886 paper; at that date, an amended version of Gauss's Latin work, cleaned of its original misprints, had been made available as the first volume of Gauss's *Werke*, see chap. I.2, § 1 above.

[17] [Hermite 1905–1917], vol. 4, p. 341: *La théorie des formes quadratiques est la plus importante partie des Disquisitiones Arithmeticae de Gauss.*

[18] [Hermite 1893], p. 6: *Vous n'avez cessé de cultiver les parties les plus élevées de la Science mathématique, celles où règne le nombre pur, l'Analyse, l'Algèbre et l'Arithmétique. … Vous faisiez vos premières découvertes sur la théorie naissante des formes algébriques et, attaquant successivement toutes les questions intéressantes de l'Arithmétique, vous agrandissiez et vous éclairiez d'une lumière nouvelle l'admirable édifice élevé par Gauss.*

Indeed, every explicit reference to the D.A. in the four volumes of Hermite's works concerns the fifth section. For instance, Hermite commented on the "complete identity of the previous theorems with those of the paragraphs 154, 155, and 168 of the work of M. Gauss" in a 1854 paper on quadratic forms, and reflected in 1886 on the "beautiful theorems on the mean value of the number of primitive classes stated by Gauss in the *Disquisitiones Arithmeticae*, art. 302, and that M. Lipschitz was the first to succeed in proving."[19] Such precise references to specific articles of the DA, however, are relatively rare, a mere dozen in the published works (in comparison with, say, Dirichlet, in whose papers the regular use of references to the D.A. reminds the reader of the manner in which ancient authors referred to Euclid's *Elements*). Besides them, and general statements on the role of the D.A. and of Gauss already mentioned,[20] one also finds allusions to notations and concepts, like those of "determinant" and "adjoint." For instance, a letter to Borchardt published in 1857 in his *Journal* describes the discriminant of an algebraic equation as "the determinant of M. Gauss" ([Hermite 1905–1917], vol. 1, p. 416) and in his 1855 note on the transformation of Abelian functions, Hermite used "what M. Gauss calls an *adjoint substitution* to a given substitution" ([Hermite 1905–1917], vol. 1, p. 449). This last example testifies to important point: the use of the *Disquisitiones Arithmeticae* did not remain strictly confined to number-theoretical topics, some of the ideas and concepts of the D.A. were adapted or extended to other situations, in particular by dropping integrality assumptions. We get here a first glimpse of the intertwining of arithmetic, algebra and analysis, alluded to by Poincaré, which we will meet again as a key to Hermite's conception and practice of mathematics.

However, to restrict oneself to picking up such explicit traces is to minimize the effects of the D.A. on Hermite's mathematical writings. Many of his results were published as letters to editors of mathematical journals, in which his style is generally loose. Following a then accepted habit, Hermite often provides only a sketch of his results, giving neither all the details of his proofs and computations, nor explanations of the origins of his ideas or notations.[21] In such a case, a close reading can bring to light less obvious affinities and adaptations, perhaps taken for granted by Hermite, in any case unrecorded. For reasons of length, I shall concentrate in what follows on Hermite's early arithmetical papers, which already provide a survey of the different ways in which Hermite inserted the *Disquisitiones Arithmeticae* into his practice.

[19] Resp. [Hermite 1905–1917], vol. I, p. 242: *On remarquera la complète identité des théorèmes qui précèdent avec ceux des paragraphes 154, 155 et 168 de l'ouvrage de M. Gauss*, and [Hermite 1905–1917], vol. 4, p. 222: *les belles propositions sur la valeur moyenne des classes de formes primitives énoncées par M. Gauss dans les* Disquisitiones Arithmeticae*, article 302, et que M. Lipschitz a le premier réussi à démontrer.*

[20] In 1882, Hermite even proposed *Disquisitio Mathematica* as a possible title for the new journal launched by Mittag-Leffler (which would finally become *Acta Mathematica*), see [Hermite & Mittag-Leffler 1984–1989], part I, pp. 173–174, letter 84.

[21] Several mistakes were detected and sometimes corrected by the team in charge of the edition of Hermite's *Œuvres*; in particular, far from negligible differences exist between the original publications and the versions contained in his *Œuvres*.

2. The Letters to Jacobi on Number Theory

The first written trace for Hermite's work in number theory can be dated back to 1847 in the first of four letters to Jacobi, all published in 1850 in the fiftieth issue of the *Journal für die reine und angewandte Mathematik*.[22] Besides these letters, Hermite also published between 1848 and 1850 several short papers connected with the same topics, before his celebrated article of 1851 on the introduction of continuous variables into number theory, [Hermite 1851]. This section will be devoted to the 1847–1850 letters to Jacobi on number theory and to their immediate developments.

2.1. Jacobi's Setting.

The direct incentives to Hermite's results reported in these letters appear to be two statements by Jacobi. The first opened a 1835 article on periodic functions of complex variables, [Jacobi 1835], which Hermite had already used in his previous work on Abelian functions. There, Jacobi proved that an analytic one-valued function of a complex variable cannot have "three periods [that] cannot be reduced to two" (*si tres periodos ad duas recoveri no possint*), without being constant. The main step of Jacobi's proof goes roughly as follows: let a, a', a'' and b, b', b'', be, respectively, the real and the imaginary parts of three periods. Let us denote by A, A', A'' the three quantities $a'b'' - a''b'$, $a''b - ab''$, $ab' - a'b$, and assume that they are neither equal to 0, nor verify a $\mathbf{Z}$-linear relation.[23] It is then possible to find three non-zero integers α, α', α'' such that $\mid \alpha\frac{A'}{A} - \alpha' \mid$ is smaller than any given positive quantity and $\mid \alpha\frac{A''}{A} - \alpha'' \mid$ smaller than 1/2. The first construction comes from the approximation of any real by a rational, obtained at the time by the theory of continued fractions; the second construction expresses that, for any irrational x, there is an integer in the open interval $(x - 1/2, x + 1/2)$. But then the numbers $a''' = \alpha a + \alpha' a' + \alpha'' a''$ and $b''' = \alpha b + \alpha' b' + \alpha'' b''$ are the real and imaginary parts of another period of the function and can be chosen strictly smaller than $\frac{a''}{2}$ and $\frac{b''}{2}$ respectively. Reiterating the procedure with a', a'', a''' and b, b', b''' instead of a, a', a'' and b, b', b'' provides

[22] We have here concordant testimony. The first letter refers to a communication from Jacobi on August 6, 1845, as being "almost two years ago"; the letters mention that Carl Borchardt is visiting Paris, a visit which, according to the latter's own correspondence, took place in 1847. In an 1854 letter to Borchardt published in the *Journal für die reine und angewandte Mathematik*, Hermite also mentioned his "research on arithmetical questions that, since the year 1847, directed my attention to quadratic forms composed of a sum of squares of similar functions of roots of a single equation" (*des recherches sur des questions arithmétiques qui depuis l'année 1847 ont appelé mon attention sur les formes quadratiques composées d'une somme de carrés de fonctions semblables des racines d'une même équation*). The date of 1845 (or even August 6, 1845) sometimes given in the secondary literature obviously stems from a confusion with the date of *Jacobi*'s letter.

[23] These cases lead to dependence conditions among the initial three periods. The concept of linear independence was not obvious at the time, but Jacobi carefully links the coefficients m, m', m'' of a $\mathbf{Z}$-linear relation between three periods, $mi + m'i' + m''i'' = 0$, to the quantities $a'b'' - a''b'$, $a''b - ab''$, $ab' - a'b$ (up to a proportionality factor), and explicitly constructs in this case the two new periods from which i, i', i'' can be derived.

an infinite sequence of non-zero periods, strictly decreasing towards 0 – the function is thus constant. This is that "so singular an algorithm" which specially struck Hermite:

> Is [it] not the first example of a new mode of approximation, where the principal questions of the theory of continued fractions present themselves again, from a wider point of view?[24]

and gave rise to a recurring topic of his research up to his death.

The second theorem of Jacobi alluded to states that a prime of the form $5n + 1$ can be decomposed into a product of four complex numbers "built up from the 5th roots of unity," that is, for Jacobi, of the form $a_0 + a_1\alpha + a_2\alpha^2 + a_3\alpha^3 + a_4\alpha^4$, with a_i integers, and $\alpha^5 = 1$. (Although this terminology was not yet adopted, I shall refer to such numbers as 5-cyclotomic numbers.) It was presented, with analogous statements for 8- and 12-cyclotomic numbers, at the Berlin Academy of Sciences on May 16, 1839, published without proof in Crelle's *Journal* as [Jacobi 1839], and translated into French in 1843. These statements, in connection with the search of higher reciprocity laws, also played a role in the development of Kummer's ideas on algebraic numbers,[25] but Hermite, while recognizing the potential consequences on higher reciprocity laws, insisted on the link with his preceding work:

> Until now in this research, I have had in sight, above all, the application which presents itself naturally to the theory of the division of Abelian functions depending on the integral $\int \frac{dx}{\sqrt{1-x^5}}$.[26]

But Hermite then brought to the forefront a further ingredient to bind them all:

> It is in some very elementary properties of quadratic forms with an arbitrary number of variables that I found the principles of analysis which I request permission to discuss with you.[27]

[24] [Hermite 1905–1917], vol. 1, p. 101: *L'algorithme si singulier, par lequel vous réduisez à un degré de petitesse arbitraire les deux expressions $ma + m'a' + m''a''$, $mb + m'b' + m''b''$ n'est-il pas le premier exemple d'un mode nouveau d'approximation, où les principales questions de la théorie des fractions continues viennent se représenter, sous un point de vue plus étendu?*

[25] See R. Bölling's chap. IV.1 above. The uses of Jacobi's note, [Jacobi 1839], by several number theorists are analyzed in chap. I.1 above, § 4.

[26] [Hermite 1905–1917], vol. 1, p. 102: *Jusqu'ici j'ai eu plutôt en vue, dans cette recherche, l'application qui s'offre d'elle-même à la théorie de la division des fonctions abéliennes dépendant de l'intégrale* $\int \frac{dx}{\sqrt{1-x^5}}$. Such a link, in the simpler quartic case, between prime numbers of the form $4n + 1$, Gaussian integers, biquadratic reciprocity laws and lemniscatic function (as well as the cubic equivalent) had been already stressed in Jacobi's paper, see chap. I.1, § 4.1.

[27] [Hermite 1850/1905–1917], vol. 1, p. 101: *C'est dans quelques propriétés très élémentaires des formes quadratiques, à un nombre quelconque de variables, que j'ai rencontré les principes d'Analyse dont je vous demande la permission de vous entretenir.*

This constellation is typical of Hermite's work, which circulates among approximations, quadratic forms, and Abelian functions. The same themes will recurrently appear in his number-theoretical publications and nourish, as we shall see, his studies on algebraic numbers and on equations. Quadratic forms, in particular, will offer both a unified frame for many problems and the clues to solve them. It is noticeable that none of these ingredients is *per se* arithmetical – Hermite's forms do not necessarily have integral coefficients. The characterization of arithmetical phenomena becomes thus particularly interesting.

2.2. The Main Theorem

At the core of Hermite's work lies the determination of an upper bound for the minimal value at integers of a quadratic form. Let f be a $n+1$-ary quadratic form, that is a homogenous polynomial of degree 2 in $n+1$ variables, $x_0, \ldots, x_n$; its coefficients here are real numbers (that is, *not* necessarily integral). The linear system of equations

$$\begin{gathered}\frac{1}{2}\frac{df}{dx_0}(x_0,\ldots,x_n) = X_0\\ \frac{1}{2}\frac{df}{dx_1}(x_0,\ldots,x_n) = X_1\\ \vdots\\ \frac{1}{2}\frac{df}{dx_n}(x_0,\ldots,x_n) = X_n\end{gathered}$$

determines a new set of variables $(X_0, X_1, \ldots X_n)$ and Hermite first defines the determinant D of the quadratic form f as the determinant of this change of variables.[28] The key result provides a $n+1$-uple of integers at which the absolute value of f is less than a bound, which does not depend on the coefficients of the form, but only on its determinant D and the number $n+1$ of variables:

Theorem. Let f be a $n+1$-ary quadratic form, with non-zero determinant D. There exist $n+1$ integers α, β, γ, ..., λ, such that

$$\mid f(\alpha,\beta,\gamma,\ldots,\lambda)\mid < (\frac{4}{3})^{n/2}\sqrt[n+1]{\mid D\mid}.$$

Hermite then sketches a proof, which proceeds through a complete induction. The result, he writes, is "easy for binary forms"; it is indeed a spin-off of the reduction theory for these forms[29] that for any binary quadratic form f with non-zero determi-

[28] For $n=1$ and $f(x_0,x_1) = ax_0^2 + 2bx_0x_1 + cx_1^2$, for instance, one obtains $X_0 = ax_0 + bx_1$ and $X_1 = bx_0 + cx_1$, and the determinant is $ac - b^2$, the negative of the expression given in D.A., art. 154.

[29] For forms with integral coefficients, it is proved in D.A., art. 171, but also, even more explicitly, in [Legendre 1830], arts. 54–56. Moreover, the constructions given there do not depend on the integrality of the coefficients.

nant D, it is possible to find an equivalent[30] form g whose first coefficient is smaller than $2\sqrt{\frac{|D|}{3}}$; this coefficient is the value at (1, 0) of the form g, thus, obviously, a value at certain integers of the first form f, which provides the result in this case.

Hermite's trick to launch the induction is then to introduce a certain $n+1$-ary form related to the form of departure f, called the adjoint form of f, and to interpret its value, for any set of $n+1$ arbitrary integers fixed in advance, as the determinant of a suitable n-ary form. The adjoint form F of the form f is defined by the relation $f(x_0, x_1, \ldots, x_n) = \dfrac{F(X_0, \ldots, X_n)}{D}$, where the set of variables $X_0, X_1, \ldots, X_n$ is given as above.

Gauss's *Disquisitiones Arithmeticae* is never mentioned in this first letter and seems indeed quite far; neither the notation nor the setting *per se*, in particular the fact that forms with real coefficients are being dealt with, seems to be borrowed from it directly. Gauss's emphasis was on the form itself (often represented by its coefficients), not on its values. But the notion of adjoint form, in the case of a ternary form, and all the paraphernalia associated with it, were introduced by Gauss in art. 267,[31] and the whole "digression containing a treatise on ternary forms," arts. 266–285, is worth a closer look. First of all, Gauss showed in art. 272 how any ternary quadratic form is equivalent, up to a constant, to one whose first coefficient is smaller than $\sqrt[3]{D}$.[32] Again, this coefficient is the value for some integers of any form of the same equivalence class and thus Gauss's result is Hermite's main theorem for ternary forms with integer coefficients. But even more decisively, Gauss's study of the representation of numbers and of binary forms by ternary forms, from art. 278 on, provides the key to Hermite's proof.

When a substitution of variables $x = mt + nu, \quad x' = m't + n'u, \quad x'' = m''t + n''u$ gives the relation $f(x, x', x'') = \phi(t, u)$, the binary form ϕ is said to be represented by the ternary form f. In art. 280, Gauss showed that, in such a case, the adjoint form F of f represents the determinant d_ϕ of ϕ, more precisely that

$$d_\phi = F(m'n'' - m''n', m''n - mn'', mn' - m'n),$$

and reciprocally, that all representations of a number d by a ternary form F arise in this way from a binary form ϕ, of which d is the determinant, and which itself can be represented by a ternary form f of adjoint F. Neither the statements, nor their proofs, depend at all on the integrality of the coefficients of the forms. That is, Gauss's digression on ternary forms, planned to complete his theory of binary forms,

[30] Here, as in the classical case of forms with integral coefficients, two equivalent forms are forms which can be deduced from each other by an invertible linear change of the variables with *integral* coefficients. See chap. I.1, § 1.2 and chap. VIII.1.

[31] In order to define the adjoint form of a ternary form f, Gauss simply listed its coefficients as explicit polynomials of the coefficients of f; this adjoint coincides with that of Hermite for ternary forms. As already mentioned above, the concept of adjoint is one of those specifically attributed to Gauss by Hermite in the sequel of his work.

[32] In these paragraphs, Gauss disregards the sign of the determinant and Hermite adopts the same convention in his own paper.

also provides, when read and used backwards, several tools to reduce statements on ternary forms to those on binary forms, and thus launch an induction.

Hermite's proof, indeed, mimics, for $n+1$-ary forms (with real coefficients), the Gaussian constructions for ternary forms, arts. 278–280. He assumes that his theorem is true for n-ary forms and considers then a $(n+1)$-ary form f.[33] First of all, if f_0 is a n-ary form represented by f, the very definition of the adjoint shows, as above for $n = 2$ (cf. art. 280), that the adjoint F of f represents the determinant of f_0, that is, there exist $n+1$ integers $\alpha, \beta, \ldots, \lambda$, not all 0, such that $F(\alpha, \beta, \ldots, \lambda) = D_{f_0}$. Reciprocally, for any such set of $n+1$ integers $\alpha, \beta, \ldots, \lambda$, Hermite exhibits a linear change of $n+1$ variables into n variables, with integral coefficients, which transforms f into a n-ary (positive definite) form f_0, such that $D_{f_0} = F(\alpha, \beta, \ldots, \lambda)$. This lemma can also be applied to F, whose adjoint is $D^{n-1}f$; that is, there is a n-ary form F_0, which is represented by F and such that $D_{F_0} = D^{n-1}f(\alpha, \beta, \ldots, \lambda)$. By the induction hypothesis applied to the n-ary form F_0, there exist integers $x_1, \ldots, x_n$ such that

$$F_0(x_1, \ldots, x_n) < \left(4/3\right)^{\frac{1}{2(n-1)}} \sqrt[n]{D^{n-1}f(\alpha, \ldots, \lambda)}.$$

Since F represents (any value of) F_0, one obtains, for an appropriate set of integers $(\alpha_0, \beta_0, \ldots, \lambda_0)$

$$F(\alpha_0, \beta_0, \ldots, \lambda_0) < \left(4/3\right)^{\frac{1}{2(n-1)}} \sqrt[n]{D^{n-1}f(\alpha, \ldots, \lambda)}.$$

Again, by constructing f_0 such that $D_{f_0} = F(\alpha_0, \beta_0, \ldots, \lambda_0)$ and applying this time the induction hypothesis to f_0, there exist integers $x'_1, \ldots, x'_n$ such that

$$f_0(x'_1, \ldots, x'_n) < \left(4/3\right)^{\frac{1}{2(n-1)}} \sqrt[n]{F(\alpha_0, \ldots, \lambda_0)},$$

that is, integers $(\alpha', \beta', \ldots, \lambda')$ such that

$$f(\alpha', \beta', \ldots, \lambda') < \left(4/3\right)^{\frac{1}{2(n-1)}} \sqrt[n]{F(\alpha_0, \ldots, \lambda_0)}.$$

Combining the two inequalities gives then, for any set of integers $(\alpha, \beta, \ldots, \lambda)$ a new set $(\alpha', \beta', \ldots, \lambda')$ such that

$$f(\alpha', \beta', \ldots, \lambda') < \left(4/3\right)^{\frac{n^2-1}{2n}} \sqrt[n^2]{D^{n-1}f(\alpha, \beta, \ldots, \lambda)}.$$

Reiterating the procedure provides the set of integers on which the value of f satisfies the desired inequality.

[33] Here, we suppose that the form is positive definite, that is, takes only strictly positive values at any non-zero set of real variables; a few details are different in the case of indefinite forms.

2.3. Arithmetical Applications

Hermite provides a vast range of applications by means of the same basic procedure: encapsulate the phenomenon under study by a positive definite quadratic form (more specifically, its value at integers); then use the inequality stated by the theorem, either directly or in the form of a finite set of equalities obtained through coupling it to integrality conditions. Let us illustrate this point with some significant examples, extracted from these letters to Jacobi.

The first example returns to the opening theme of the letter, approximations by rational numbers. For two fixed real numbers A and B,[34] Hermite considers the (positive definite) ternary form

$$f(x, x', x'') = (x' - Ax)^2 + (x'' - Bx)^2 + \frac{x^2}{\Delta},$$

where Δ is an arbitrary positive real number. The determinant of f is Δ^{-1}. The main theorem, applied to this form, then asserts that there exist three integers m, m', m'' such that

$$f(m, m', m'') = (m' - Am)^2 + (m'' - Bm)^2 + \frac{m^2}{\Delta} < \frac{4}{3}\frac{1}{\sqrt[3]{\Delta}},$$

hence the three inequalities

$$\begin{aligned} \mid m' - Am \mid &< \frac{2}{\sqrt{3}}\frac{1}{\sqrt[6]{\Delta}}, \\ \mid m'' - Bm \mid &< \frac{2}{\sqrt{3}}\frac{1}{\sqrt[6]{\Delta}}, \\ \mid m \mid &< \frac{2}{\sqrt{3}}\sqrt[3]{\Delta}. \end{aligned}$$

Using the last inequality to get an upper bound for $\frac{1}{\sqrt[6]{\Delta}}$ and eliminate Δ, Hermite obtains finally:

$$\mid \frac{m'}{m} - A \mid < \frac{2\sqrt{2}}{\sqrt[4]{27}}\frac{1}{\mid m\sqrt{\mid m \mid} \mid}$$

$$\mid \frac{m''}{m} - B \mid < \frac{2\sqrt{2}}{\sqrt[4]{27}}\frac{1}{\mid m\sqrt{\mid m \mid} \mid}$$

that is, simultanous approximations of A and B by rational numbers with the same denominator m and an error of order less than $m\sqrt{\mid m \mid}$.

[34] The same proof works, *mutatis mutandis*, for any number of reals. Moreover, in the third letter, Hermite explains how to apply the same argument to the approximation of complex numbers by quotients of Gaussian integers, see [Hermite 1850/1905–1917], vol. 1, p. 142.

Similarly, Hermite revisits Jacobi's result on periods of analytic functions, extending it in his fourth letter to prove that analytic functions of n variables cannot have more than $2n$ (independent) periods. Let us assume, for instance, that $p = a + b\sqrt{-1}$, $p' = a' + b'\sqrt{-1}$, $p'' = a'' + b''\sqrt{-1}$ are three periods of a non-constant analytic function of one complex variable (with the a's and b's real); to them Hermite associates the ternary form

$$f = (ax + a'y + a''z)^2 + (bx + b'y + b''z)^2 + \frac{z^2}{\Delta^2},$$

the determinant of which is $D = (\frac{ab'-ba'}{\Delta})^2$. If this determinant is not zero, the main theorem asserts, for each value of Δ (or of D), the existence of integers x, y, z such that $f(x, y, z)$ is smaller than $\sqrt[3]{2D}$. In particular, then

$$(ax + a'y + a''z)^2 + (bx + b'y + b''z)^2 < \sqrt[3]{2D}.$$

Thus, for any positive number, there would exist a period of the initial function, $xp + yp' + zp''$, whose norm would be smaller than it, which is impossible. The case where $D = 0$, that is $ab' - ba' = 0$, is handled by means of a binary form.

As announced earlier, the first letter also contains a proof of Jacobi's statement concerning the decomposition of certain primes into a product of cyclotomic algebraic numbers. It exemplifies the second way of using the main theorem alluded to above. But it also introduces Hermite's programme for the study of algebraic numbers, this central topic of number theory in the second half of the XIX$^{\text{th}}$ century.

Let $F(x) = x^n + Ax^{n-1} + \ldots + Kx + L = 0$ be an algebraic irreducible equation with integral coefficients; its roots[35] are denoted by $\alpha, \beta, \ldots, \lambda$. Hermite assumes that, for a certain fixed integer N, there exists an integer a satisfying the congruence $F(a) \equiv 0 \bmod N$. He then introduces the form $\mathcal{F} = \phi(\alpha)\phi(\beta)\cdots\phi(\lambda)$, where

$$\phi(\alpha) = Nx_0 + (\alpha - a)x_1 + (\alpha^2 - a^2)x_2 + \ldots + (\alpha^{n-1} - a^{n-1})x_{n-1}.$$

That is, the various factors $\phi(\alpha), \phi(\beta), \ldots$, are linear forms with complex coefficients in n variables $(x_0, x_1, \ldots, x_{n-1})$. Their product $\mathcal{F}$ is an n-ary form of degree n, with integer coefficients – such forms will be known later as *decomposable* forms. More precisely, the coefficient of each term of the form $\mathcal{F}$ is a symmetric function of the roots $\alpha, \beta, \ldots, \lambda$ multiplied either by N (if the term contains the variable x_0), or by $(\alpha - a)(\beta - a)\cdots(\lambda - a)$ (if the term contains only the variables $x_1, \ldots, x_{n-1}$), that is either by N or by $F(a)$, which by hypothesis is a multiple of N. Thus, the coefficients of the form $\mathcal{F}$ are all multiples of N, and this is thus also true for the values of the form at integers.

In order to link this situation to the main theorem, Hermite then associates to the decomposable form, $\mathcal{F}$, a *continuous family* of quadratic positive definite n-ary forms: if all the roots of the equation F are real, for instance, he chooses the forms

$$f = D_0\phi^2(\alpha) + D_1\phi^2(\beta) + \ldots + D_{n-1}\phi^2(\lambda),$$

[35] As usual at this time, Hermite implicitly considers these roots to be complex numbers.

where the D_i are arbitrary strictly positive real numbers.[36] For each choice of the D_i, the main theorem, applied to the corresponding quadratic form f, provides a set of integers $(x_0, x_1, \ldots, x_{n-1})$ at which the value of f is less than $(4/3)^{\frac{n-1}{2}} \sqrt[n]{D}$, with D being the determinant of the form. But the product of the (positive) terms composing the sum f, that is $D_0 D_1 \cdots D_{n-1} (\mathcal{F})^2$, is less than its maximal value, $\left(\frac{f}{n}\right)^n$, obtained when all the terms are equal, and thus it is less than $\dfrac{(\frac{4}{3})^{\frac{n(n-1)}{2}}}{n^n} D$.

A straightforward computation of the determinant D then shows that there exist integers $x_0, x_1, \ldots, x_{n-1}$ such that $\mathcal{F}(x_0, x_1, \ldots, x_{n-1}) = MN$, with the integer M less than

$$\left(\frac{4}{3}\right)^{\frac{n(n-1)}{4}} \left(\Delta n^n\right)^{\frac{1}{2}},$$

where Δ is the resultant of the equation $F = 0$, that is, the product of the $n(n-1)$ differences of the roots $\alpha, \beta, \ldots, \lambda$.[37]

Hermite finally specializes this result to the cyclotomic equation $F(x) = \frac{x^p - 1}{x - 1}$, for p a prime number (5 or 7 in the cases he discusses) and N any prime number of the form $kp + 1$. Here, $\Delta = p^{p-2}$. Moreover, as p divides $N - 1$, there exists an integer a of order p modulo N, that is $a^p \equiv 1 \bmod N$ and $a \not\equiv 1 \bmod N$,[38] and thus the preceding discussion applies.

If $p = 5$, the bound provided for M is smaller than 2; M being an integer, it is necessary that $M = 1$ and thus $\mathcal{F} = N$.[39] This proves that any prime number N congruent to 1 modulo 5 can be written as a product of four complex numbers built from the fifth roots of unity (the $\phi(\alpha)(x_0, x_1, x_2, x_3)$ and its three conjugates, for the integers (x_0, x_1, x_2, x_3) provided by the theorem). This is precisely the result stated (without proof) by Jacobi in 1839. Hermite also proves it for $p = 7$, as well as an analogous result for the decomposition of primes congruent to -1 modulo 7, as a product of three complex numbers constructed with the roots of the polynomial $F(x) = x^3 + x^2 - 2x - 1$.[40]

[36] If the roots are not all real, the term corresponding to a pair of conjugate roots β, γ is taken as $d\phi(\beta)\phi(\gamma)$, with an arbitrary strictly positive real number d.

[37] We note that the coefficients $D_0, \ldots, D_{n-1}$ are eliminated from the final result. This means that there are in fact infinitely many systems of integers for which $\mathcal{F}(x_0, x_1, \ldots, x_{n-1})$ is equal to a fixed multiple MN of N.

[38] Such basic facts on power residues were established in sec. 3 of the D.A. Hermite does not even bother to justify the existence of a.

[39] We see here, as explained above, exactly how the integrality condition converts the bound provided by the main theorem into an equality.

[40] This result for primes congruent to 1 modulo 5 (or 7) is linked in modern terms to the fact that unique factorization holds in the ring of integers of the corresponding cyclotomic fields. In a short paper published during the same period, [Hermite 1905–1917], vol. 1, pp. 274–275, Hermite also stated more generally that if a prime number p *divides* the norm of an m-cyclotomic number, an adequate power of p *is* a norm, that is a product of m-cyclotomic numbers.

2.4. The Reduction of Forms

As already mentioned in our discussion of Hermite's main theorem, the proof is closely related to the problem of reduction of quadratic forms – that is to the problem of choosing good representatives of the equivalence classes, the reduced forms, and of finding the substitutions which transform ("reduce") a given form into such a representative of its class.[41] In the binary case, the reduced forms can be described by means of a finite number of (linear) inequalities on their coefficients (implying in particular that their number, and thus the number of classes, is finite in the case of forms with integral coefficients), but Hermite displaced the emphasis:

> What one has to do above all in the theory of reduction, is to discover the integral values of the indeterminates for which a given definite form is *the smallest possible*.[42]

In his letters to Jacobi he addressed the case of definite quadratic forms, but with an arbitrary number of variables and with arbitrary real coefficients, and proposed three successive definitions of the reduced forms, corresponding to three different methods of construction. His repeated attempts were motivated by a wish to obtain a unique reduced form in each class (as in the case of binary forms) and more effective procedures of reduction. For reasons of space, I shall discuss here only the second attempt,[43] which clearly illustrates these components, as well as the dependence on the D.A.

After his first attempt, Hermite was seeking "a method of reduction which is simpler and, above all, closer to Lagrange's algorithm for binary forms."[44] He introduced for this purpose what he called the "derived forms", which are "intimately linked [...] to M. Gauss's adjoint forms," but "considered in an explicit manner."[45]

[41] See chap. I.1, § 1.2 for the point of view of the D.A., and J. Schwermer's chap. VIII.1 for the historical development of the topic. For a description of the various theories of reduction before 1920, see [Dickson 1919–1923], vol. 3, chap. IX.

[42] [Hermite 1850/1905–1917], vol. 1, p. 142: *Ce qu'on devait se proposer avant tout, dans la théorie de la réduction, était de découvrir les valeurs entières des indéterminées pour lesquelles une forme définie donnée était* la plus petite possible.

[43] The first attempt focused on the special quadratic forms associated to decomposable forms, and defined reduced forms inductively, by combining the usual definition of reduction for a binary form and the process of induction used in the proof of the main theorem (here there is no uniqueness in general). The third proposal, which does provide a unique reduced form per class, was developed and described later as the method of successive minima, see J. Schwermer's chap. VIII.1, § 2.3. All the proposals yield the finiteness of the number of classes in the case of forms with integer coefficients. Hermite was not satisfied by any of his constructions and decades later, advised his student Léon Charve to use Eduard Selling's theory of reduction instead his own. In the fourth and last letter, Hermite also commented on the reduction of forms with real coefficients to a form of the type $\sum_i x_i^2 - \sum_j x_j^2$.

[44] [Hermite 1905–1917], vol. I, p. 122: *Depuis [la première lettre], j'ai été amené à une méthode de réduction plus simple et surtout plus analogue à l'algorithme de Lagrange pour les formes binaires.*

[45] [Hermite 1850/1905–1917], vol. I, p. 122: *L'idée principale de cette méthode consiste*

For an $(n+1)$-ary form

$$f(x_0, x_1, \dots, x_n) = \sum_0^n \sum_0^n a_{ij} x_i x_j,$$

such that $a_{ij} = a_{ji}$, Hermite defined the derived form g_0 by

$$g_0(y_1, \dots, y_n) = \sum_1^n \sum_1^n b_{ij} y_i y_j,$$

with $b_{ij} = a_{00}a_{ij} - a_{0i}a_{0j}$; analogous definitions, *mutatis mutandis*, give the other derived forms g_i, for the indices $i = 1, \dots, n$. We remark that, for ternary forms, the three derived forms are simply the three binary forms which arise from the adjoint form, by taking each indeterminate in turn to be 0. These binary forms had been specifically used by Gauss in his discussion of the reduction of ternary forms, see D.A., art. 272.

Reduction for $(n+1)$-ary definite forms is then defined by induction. If one assumes a theory of reduction for n-ary forms, an $(n+1)$-ary form f is called reduced if one of its diagonal coefficients, say $a_{\mu\mu}$, is the smallest possible in the class,[46] if moreover $a_{\mu i} < 1/2a_{\mu\mu}$ for all indices $i \neq \mu$, and if finally the associated derived form g_μ is a reduced n-ary form. Hermite proved that any $(n+1)$-ary form can be transformed by a modular transformation into such a reduced form, and, moreover, that the coefficients of a reduced form are bounded, with bounds depending only on the determinant and the number of indeterminates. For example, the product of the diagonal coefficients of a reduced form is less than $(\frac{4}{3})^{\frac{1}{2}n(n+1)} \mid D \mid$. These bounds permit him, for instance, to show that, for $2 \leq n \leq 6$,[47] there is a unique class of n-ary forms with integer coefficients of determinant 1 (the class represented by a sum of n squares).

Another important application, and the last to be described here, links the question of reduction to Hermite's general programme concerning algebraic numbers:

> Perhaps one will succeed in deducing from this a complete system of characters for each species of these kinds of quantities, analogous for instance to those given by the theory of continued fractions for the roots of quadratic equations. … What an immense task it is for number theory and integral calculus, to penetrate into the nature of such a multitude of entities created by reason, classifying them into mutually irreducible groups, to constitute them all individually through characteristic and elementary definitions![48]

dans l'introduction de certaines formes liées intimement, comme je suis parvenu à le reconnaître, aux formes adjointes de M. Gauss, mais qu'il me semble indispensable de considérer d'une manière explicite.

[46] The null case is not taken into account.

[47] Optimistically and helped by some miscomputations, Hermite stated the result up to $n = 8$. For a survey on these issues, see for instance [Serre 1970], chap. V.

[48] [Hermite 1850/1905–1917], vol. 1, p. 131: *Peut-être parviendra-t-on à déduire de là un*

The model provided by continued fractions is very well explained by Léon Charve in his 1880 thesis:

> One knows that if one expands a quadratic irrational as a continued fraction, the computation is periodic. This periodicity constitutes a very remarkable property of the roots of quadratic equations, and can even serve as a definition of these irrationals. But the theory of continued fractions is closely linked to the theory of binary quadratic forms, such that the expansion into a continued fraction of a root α of a quadratic equation is identical to the search for successive minima of the expression
>
> $$(x-\alpha y)^2 + \Delta(x-\beta y)^2$$
>
> where β is the second root of the equation under consideration and Δ a quantity which increases positively from 0 to ∞. From another point of view, the search for these minima comes back to the reduction of the binary form
>
> $$f = (x-\alpha y)^2 + \Delta(x-\beta y)^2$$
>
> for every value of Δ. Carrying out this reduction, one finds that the sequence of reduced forms equivalent to f for every value of Δ is obtained by a periodic computation. One is thus led to wonder if some type of approximation of the quantities would not give an analogous periodicity for irrationals of higher degree than the second. It is the consideration of quadratic forms which leads to this extension of the theory of continued fractions and yields these new methods of approximation.[49]

système complet de caractères pour chaque espèce de ce genre de quantités, analogue par exemple à ceux que donne la théorie des fractions continues pour les racines des équations du second degré.... [Q]uelle tâche immense pour la théorie des nombres et le calcul intégral, de pénétrer dans la nature d'une telle multiplicité d'êtres de raison, en les classant en groupes irréductibles entre eux, de les constituer tous individuellement par des définitions caractéristiques et élémentaires.

[49] [Charve 1880], pp. 36–37: *On sait que, si l'on développe en fraction continue une irrationelle du second degré, le calcul est périodique. Cette périodicité constitue une propriété très remarquable des racines des équations du second degré, et elle peut même servir de définition à ces irrationnelles. Or la théorie des fractions continues est liée étroitement à la théorie des formes quadratiques binaires, de sorte que le développement en fraction continue d'une racine α d'une équation du second degré est identique à la recherche des minima successifs de l'expression $(x-\alpha y)^2+\Delta(x-\beta y)^2$, où β désigne la deuxième racine de l'équation considérée et Δ une quantité qu'on fait croître positivement de 0 à ∞. D'un autre côté, la recherche de ces minima revient à la réduction de la forme binaire $f=(x-\alpha y)^2+\Delta(x-\beta y)^2$ pour toute valeur de Δ. En opérant cette réduction, on trouve alors que la suite des formes réduites équivalentes à f pour toute valeur de Δ s'obtient par un calcul périodique. On est alors conduit à se demander si quelque mode d'approximation des quantités ne donnerait pas une périodicité analogue pour les irrationnelles d'un degré supérieur au second. C'est la considération des formes quadratiques qui conduit à cette extension de la théorie des fractions continues, et donne ces nouvelles méthodes d'approximation.*

Hermite tests his programme on the simplest situation, that of an algebraic equation $x^3 - A = 0$, with A an integer. Let α be the real cubic root of A, β and γ the two conjugate associated complex roots. To this situation can be associated[50] a family of definite ternary forms

$$F_\Delta = (x + \alpha y + \alpha^2 z)^2 + \Delta(x + \beta y + \beta^2 z)(x + \gamma y + \gamma^2 z),$$

the determinant of which is $D = \frac{27}{4}\Delta^2 A^2$. Using the bounds which characterize the coefficients of a reduced form, as explained before, Hermite concludes that the reduction of the series of forms F_Δ comes down to that of a finite number of them; the same modular substitutions, repeated periodically, operate all the reductions.[51]

3. The Method of Continual Reduction

Up to now, we have seen how Hermite borrowed from the *Disquisitiones Arithmeticae* the construction of specific concepts (like the derived forms), proofs (like that of the main theorem) and, in a more diffuse way, the pervasive project of a refined classification of mathematical objects. Another mode of inspiration is displayed in one of the most influential article written by Hermite, on "the introduction of continuous variables into number theory," published in Crelle's *Journal* in 1851, a year after the letters to Jacobi. The first paragraph runs once again through familiar themes:

[50] The construction is a particular case of that explained above, with $\phi(\alpha) = x + \alpha y + \alpha^2 z$, that is $N = 1$ and $a = 0$.

[51] In his thesis, Charve computed several numerical examples. For instance, see [Charve 1880], pp. 45–53, let us take $\alpha = \sqrt[3]{2}$; the point of departure is the form

$$F_{0,\Delta} = (x + y\sqrt[3]{2} + z\sqrt[3]{4})^2 + 2\Delta(x + \lambda y\sqrt[3]{2} + \lambda^2 z\sqrt[3]{4})(x + \lambda y\sqrt[3]{2} + \lambda^2 z\sqrt[3]{4}),$$

with λ a non-trivial third root of unity; this form is already reduced when Δ belongs to a certain interval $[\Delta_0, \Delta_1]$, but then, when Δ becomes greater than Δ_1, it should be reduced to another form, say $F_{1,\Delta}$. This form, again, is already reduced for Δ belonging to a certain interval, and on either side of the interval must be reduced to another form, etc. The point is that one obtains the series of reduced forms $F_{0,\Delta}, F_{1,\Delta}, F_{2,\Delta}, F_{3,\Delta}, F_{4,\Delta}, \ldots$, and again $F_{0,\Delta}, F_{-1,\Delta}, F_{-1,\Delta}, \ldots$, by applying *periodically* and successively the same three transformations, with respective coefficients

$$\begin{matrix} 1 & -1 & -1 \\ 0 & 0 & -1 \\ 1 & 0 & -1 \end{matrix}, \quad \begin{matrix} 1 & -1 & 0 \\ 0 & -1 & 0 \\ 1 & -1 & -1 \end{matrix}, \quad \begin{matrix} -1 & 0 & 0 \\ -1 & 0 & 0 \\ 0 & 0 & -1 \end{matrix}.$$

This corresponds to relations between $F_{n,\Delta}$ and $F_{n+3,\Delta'}$, for instance $F_{3,\Delta} = (1 + \sqrt[3]{2} + \sqrt[3]{4})^2 F_{0,\Delta(\sqrt[3]{2}-1)^3}$. Note that the multiplier $(1 + \sqrt[3]{2} + \sqrt[3]{4})^2$ is the square of a unit; the converse is also true. More generally, as a side product of his study, Hermite sketched a proof that all units built from the roots of a irreducible algebraic equation, with integral coefficients and m real roots and couples of conjugate roots, can be obtained as powers of only $m - 1$ such units. That these independent generators indeed exist was proved by Dirichlet in 1846.

the origin of Hermite's arithmetical interests in the theory of Abelian functions, his objective of basing a study of algebraic numbers on the theory of decomposable forms, and finally his method:

> As for the method, its principal character consists in the introduction, through a general and very simple procedure, of continuous variables which make questions relative to integers dependent upon the most elementary analytic principles.[52]

But the core of the article consists of revisiting sec. 5 of the D.A., as an explicit test for Hermite's method. It begins with a review of the classical case of definite binary quadratic forms, characteristically presenting the conditions of reduction in terms of minimal values.

Then, we are treated literally to a browsing through the D.A. with occasional specific interventions when Hermite's approach allows him to obtain the results of the D.A., or analogous ones, in a different way.[53] The reduction of indefinite binary forms will illustrate this point. Hermite considers more generally a binary form of degree n, decomposable into μ real linear factors $(x + \alpha_i)$ and ν complex linear conjugate factors $(x + \beta_j y)(x + \gamma_j y)$, with $\mu + 2\nu = n$:

$$f(x, y) = a_0x^n + a_1x^{n-1}y + \ldots + a_{n-1}xy^{n-1} + a_ny^n$$
$$= a_0(x+\alpha_1 y)(x+\alpha_2 y)\ldots(x+\alpha_\mu y)(x+\beta_1 y)(x+\gamma_1 y)\ldots(x+\beta_\nu y)(x+\gamma_\nu y)$$

According to a now familiar pattern, with f he associates the family of definite binary quadratic forms

$$\phi_{t,u}(x, y) = t_1^2(x + \alpha_1 y)^2 + t_2^2(x + \alpha_2 y)^2 \ldots + t_\mu^2(x + \alpha_\mu y)^2$$
$$+ 2u_1^2(x + \beta_1 y)(x + \gamma_1 y) + \ldots + 2u_\nu^2(x + \beta_{nu} y)(x + \gamma_\nu).$$

The reduction of f is defined through the reduction of this family. For each set of real values of the t_i and u_j, there is a modular transformation of the variables x and y which reduces the corresponding form $\phi_{t,u}$; it also transforms the initial form f. When one carries out this *continual reduction* for all $t's$ and $u's$, one then obtains a series of forms, transforms of f; it is the same for two equivalent forms. The reduced forms of the class of f are then chosen among the forms of this series, to be those realizing the minimum of the quantity[54]

$$\theta = \frac{a_0^2 D^{\frac{1}{2}n}}{(t_1t_2\cdots t_\mu u_1^2u_2^2\cdots u_\nu^2)^2}.$$

[52] [Hermite 1851/1905–1917], vol. 1, p. 164: *Pour la méthode, son principal caractère consiste dans l'introduction, par un procédé général et très simple, de variables continues, qui font dépendre les questions relatives aux nombres entiers des principes analytiques les plus élémentaires.*

[53] If not, the topic is simply alluded to: "The complete search of equivalence conditions of two forms with negative determinant should now simply be a consequence of the results just obtained, but for that I can only reproduce the book of M. Gauss itself," wrote Hermite for instance at the beginning of the fifth part before going on to another topic.

[54] Hermite shows that this quantity provides a bound for the coefficients, more precisely that the product of coefficients a_ia_{n-1} is bounded by $\theta(\frac{4}{3})^{n/2}n^{-n}((n-1)\cdots(n-i+1))^2(i!)^{-2}$.

This minimum is baptized by Hermite the determinant of the form, and it is shown that all forms with integral coefficients and same determinant belong to a finite number of equivalent classes.

In the particular case handled by Gauss of a binary indefinite form with integer coefficients $f = ax^2+2bxy+cy^2 = a(x+\alpha y)(x+\alpha' y)$, one has simply to consider the family of definite binary quadratic forms $\phi_\lambda = (x+\alpha y)^2 + \lambda(x+\alpha' y)^2$, with λ a real parameter. The quantity θ is constant, equal to $4(b^2-ac)$. The reduced forms are all those deduced from f by the transformations which successively reduce the ϕ_λ; among them, Hermite calls principal reduced forms those for which the corresponding reduced transform of ϕ_λ has equal extreme coefficients; the others he calls intermediate reduced forms. In this new, more general framework, Hermite is able to recover the results of the D.A. for binary quadratic forms of positive determinant:

> We can thus reason as does M. Gauss, art. 187... Then one will have obtained all different classes of determinant D, each represented, not by a unique form, but by an infinitely repeated period of a small number of principal reduced forms.[55]

Several other results of the D.A. are then deduced from these considerations. For example, Hermite uses his simple construction to link the decomposition into 2 squares of a prime number $p = 4n+1$ to the period of the quadratic form $(1, 0, -p)$ – a link established by Gauss in art. 265 by more intricate arguments.

4. Dealing with New Matters: The Example of Hermitian Forms

We know that the first sections of the D.A. constituted for Gauss himself a model for the arithmetic of the Gaussian integers.[56] In 1842, Dirichlet continued the enterprise, studying binary quadratic forms with Gaussian integers as coefficients (and indeterminates),[57] along the lines of Gauss's sec. 5. While underlining again the similarities between the methods usable in the real and in the complex cases, Hermite signaled in 1853 that new principles might nonetheless be required. The example he chose to present touches upon a celebrated new concept attached to his name, Hermitian forms.

Hermite wrote them as $f = Avv_0 + Bvw_0 + B_0wv_0 + Cww_0$, where the coefficients A and C are real and B and B_0 are conjugate complex numbers. The

[55] [Hermite 1851/1905–1917], vol. 1, p. 183: *[Les réduites] se reproduiront dés lors périodiquement en faisant croître λ jusqu'à l'infini.... Nous pouvons donc raisonner comme le fait M. Gauss, § 187... Alors on aura obtenu toutes les classes différentes de déterminant D, représentées chacune, non par une forme unique, mais par une période répétée indéfiniment d'un petit nombre de réduites principales.* Note that, while the overall result is the same as that of Gauss, the reduced forms and the periods obtained by Gauss, arts. 183–187, are slightly different.

[56] See chap. I.1 above, § 3.2.

[57] See [Dirichlet 1842]. This paper was published in Crelle's *Journal*, but in French. We note that, as was usual then, Dirichlet calls "complex integers" what we now call Gaussian integers, seeing in them the complex equivalent of the usual real integers (and not yet, in this context, an example among others of a ring of algebraic integers).

variables $v = x + \sqrt{-1}\,y$, $w = z + u\sqrt{-1}$ are complex, with conjugates v_0 and w_0. These forms, Hermite remarks, are thus special quaternary quadratic forms, when seen as forms of the real variables x, y, z, u. But instead of classifying them up to the usual modular transformations (with real integer coefficients), Hermite proposes to take into account only a particular group of these transformations, those which can be expressed as

$$\begin{aligned} v &= aV + bW, & w &= cV + dW \\ v_0 &= a_0 V_0 + b_0 W_0, & w_0 &= c_0 V_0 + d_0 W_0 \end{aligned}$$

where a, b, c, d are complex integers and a_0, b_0, c_0, d_0 their conjugates.

> One is then led to attribute to them a mode of existence singularly annalogous to that of binary quadratic forms, although they essentially contain four indeterminates.[58]

The analogy again runs in accordance with the main steps of sec. 5 of the D.A., defining the determinant (or "invariant") $\Delta = BB_0 - AC$, equivalence, reduction, and representation of numbers by these forms. The promised novelties arrive, concerning firstly the various types of equivalence, since the determinant of the relevant transformations, $ad - bc$, may now take four values, $1, -1, \sqrt{-1}, -\sqrt{-1}$, and secondly quadratic reciprocity, the relevant congruence in the study of the representation of a number M by the form now being $x^2 + y^2 \equiv \Delta \bmod M$, instead of $x^2 \equiv \Delta \bmod M$.[59] The particular representation by the form $vv_0 + uu_0$ leads to a new derivation of Jacobi's result on the number of decompositions of an integer as a sum of four squares. In a letter to Borchardt, published in 1857, Hermite used the reduction of these forms to prove that the roots of algebraic equations, with Gaussian integers as coefficients, give rise to only finitely many "distinct irrationalities" for a fixed degree and a fixed discriminant.[60]

5. Another Glimpse at Hermite's Sources

These multiple uses testify to a close and familiar reading of the D.A. by Hermite. However, it would overly confine Hermite's background to restrict it merely to the D.A. Distinct ways of framing questions and of stating priorities pervade Hermite's reading of the D.A. For instance, it was Lagrange, not Gauss who posed as the

[58] [Hermite 1854/1905–1917], vol. 1, p. 238: *On est alors conduit à leur attribuer un mode d'existence singulièrement analogue à celui des formes quadratiques binaires, bien qu'elles contiennent essentiellement quatre indéterminées.*

[59] This is one of the very rare instances in Hermite's work of a result directly bearing on congruences; this one is of course a direct prolegomenon for questions concerning forms.

[60] See [Hermite 1905–1917], vol. 1, p. 414. In modern terms, this means that these roots generate finitely many number fields over $\mathbf{Q}(i)$. The result for equations with real coefficients had been proved by Hermite three years earlier, by the same method: to these roots, one associates quadratic forms (Hermitian forms in the complex case) following the construction given above, and one proves that they correspond to finitely many reduced forms. But forms corresponding to the same reduced form are arithmetically equivalent and the roots of the corresponding equations generate the same number field.

second problem of his “Additions” to Euler’s *Algebra* the minimization of the value for integers of a binary homogeneous polynomial $Ap^m + Bp^{m-1}q + \ldots + Rq^m$, with integer coefficients A, B, ..., R, and who, in the following problem, connected this question for $m = 2$ to the continued fraction expansion of $-B/2A$. More generally, the recurrent interest in continued fractions and approximations is reminiscent of Lagrange and Legendre, two authors whom Hermite read thoroughly in his youth.[61] Transformations of expressions like $a_0 + a_1\alpha + a_2\alpha^2 \ldots$ (with α a root of a certain algebraic equation), which play a key role in Hermite’s approach to the study of algebraic numbers, are used in both Lagrange and Legendre.[62]

As for the idea – presented as a matter of fact and not an innovation by Hermite – of adapting reduction to forms with arbitrary coefficients, it is often attributed, within number theory, to a 1831 commentary of Gauss on Ludwig August Seeber’s thesis.[63] But there is no reason to doubt Hermite’s honesty in thanking Jacobi around 1848 (and thus after his first letter on number theory) for the communication of this paper via Borchardt. Lagrange’s *Mécanique analytique* already offered a study of linear transformations of real forms of higher degree.[64] On the other hand, both Cauchy and Fourier derived results on algebraic equations by continously varying their coefficients.[65]

More difficult to pinpoint, but quite characteristic, the flavour of Hermite’s mathematical prose itself reminds the reader strongly of these French authors. The style is discursive and oriented towards the description of processes. It is interesting in this respect to contrast Gauss’s and Hermite’s ways of handling periodic phenomena, which also play an important role in the D.A. Gauss called attention to the cyclic structures this periodicity displays: for congruences, forms, and roots of cyclotomic equations (see chap. I.1, § 1.4). Hermite, on the other hand, focused on the finitely many transformations which bring out the periodicity; concordantly, he devoted several papers to the complete determination of the relevant transformations (and their substitution group structure), for various types of forms and various types of equivalence.[66]

[61] Gauss used continued fractions, but only marginally, while Legendre devoted the whole first part of [Legendre 1830] to them.

[62] See for instance [Lagrange 1867–1892], vol. 2, p. 527 and vol. 7, p. 6, pp. 45–49; [Legendre 1830], vol. 1, 1$^{\text{ère}}$ partie, vol. 2, 4$^{\text{e}}$ partie, § 16.

[63] On Seeber’s thesis and Gauss’s commentary, see J. Schwermer’s chap. VIII.1 below.

[64] Karen Parshall has argued that this was a decisive text for the birth of invariant theory in Great Britain, cf. [Parshall 1989], and it is certainly quoted, besides the D.A., in George Boole’s founding paper. Also, [Jacobi 1839] alluded to the fact that reduction theory applies without change to binary quadratic forms with Gaussian integers as coefficients.

[65] Hermite himself refers to Cauchy’s *Exercices de mathématiques* in this context; see also [Fourier 1820]. These papers are particularly relevant to Hermite’s work on the Sturm theorem, where quadratic forms also intervene.

[66] That group structures and field structures had emerged in quite different contexts and thus have distinct histories, only to merge much later, is now well established, thanks to [Corry 1996]. Hermite’s work has still to be examined in this perspective.

6. Hermite and Arithmetic Algebraic Analysis

Just before his death, Hermite wrote to Eugen Jahnke, the editor of *Archiv der Mathematik und Physik*:

> I have always been and will be until the end the disciple of your great mathematicians, Gauss, Jacobi, Dirichlet. Others, like Kronecker, Borchardt, M. Lipschitz, etc. have been the companions of my studies and my devoted friends.[67]

Although limited, for the occasion, to German names, the list is significant. It points to the research field Norbert Schappacher and I have called "arithmetic algebraic analysis," see chap. I.1, § 3, a field to which Hermite actively contributed since the late 1840s.

Hermite's papers exemplify the high reactivity to the work of other contributors, which allowed us, a posteriori, to delimit this research field. He quickly responded to Jacobi's papers at the beginning of his career, as we have seen, and gave a new proof of Seeber's bound for the product of diagonal coefficients of a reduced ternary form only a few months after he received Gauss's review of Seeber's thesis. At the end of his 1851 paper he assimilated, from his own point of view, some very recent results of Eisenstein on cubic forms[68] and in 1857 he presented to the French Academy a memoir of Kummer on ideal numbers. Later on, he would repetitively cross Kronecker's path when dealing with the quintic equation, modular equations, and formulas for the classes of quadratic forms.[69] As for Dirichlet, from forms with complex coefficients to approximations to the structure of complex units, it is obvious how close his research themes were to Hermite's. The interplay of continuous real tools and arithmetic is also a feature both authors shared. Even if the way they introduced it was, of course, different, during the XIX$^{\text{th}}$ century they offered the two main patterns to follow in this direction.[70] In 1853, Hermite wrote to Dirichlet:

> Sir, During the too short moments I was able to pass with you during my trip to Berlin, you announced in the presence of our poor friend Eisenstein to have the theory of the transformation into itself of an indefinite ternary form. I had myself already carried out some investigations on this difficult question, but without success

[67] *Archiv der Mathematik und Phyisk* 3$^{\text{rd}}$ ser. 1 (1901), p. 20, also quoted in [Darboux 1905], p. 48: *J'ai toujours été et je serai jusqu'à mon dernier jour le disciple de vos grands géomètres, Gauss, Jacobi, Dirichlet. D'autres, comme Kronecker, Borchardt, M. Lipschitz, etc. ont été les compagnons de mes études et mes amis dévoués.*

[68] In 1852, Eisenstein would write to him: *vous vous êtes extrêmement approché d'une théorie que j'ai imaginée* (you have come extremely close to a theory that I have imagined), see [Eisenstein 1975], vol. 2, p. 771.

[69] On these interactions with Kronecker, see C. Houzel's chap. IV.2 above. Kronecker himself refers to Hermite's work, for instance, in [Kronecker 1895–1931], vol. 1, p. 161 on the transformation of Abelian functions; p. 308, on Sturm's theorem; vol. 4, pp. 43–48, on the quintic equation; p. 203, on definite quadratic forms, etc. One could multiply these examples with other mathematicians contributing to the field, for instance Borchardt and Peter Friedrich Arndt, and outside Germany, Cayley and Liouville.

[70] This proximity was noted by others, see for instance Jacobi's note to Hermite, fourth letter, [Hermite 1850/1905–1917], p. 160.

> and I was not surprised to hear you say that the principles on which you had based the solution were quite hidden. A short time ago, I was again led to this topic, obeying I think a law of my destiny not to do anything in arithmetic other than unearth some of the discoveries you made a long time ago.[71]

The theme of unity, dear to Dirichlet, is also very present in Hermite's discourse. He stressed it when describing Dirichlet's (and Kronecker's) work:

> The main thought which inspired Dirichlet is shown in his famous memoir, entitled On the application of infinitesimal analysis to number theory. It was a revelation that there was a close link between two regions so widely separated in the scientific domain, integers on one hand, and on the other, the continuous variables of analysis. One could glimpse in Dirichlet's discovery the testimony of a deep unity, one that had never been suspected, among the most diverse branches of mathematics. M. Kronecker has pursued with brilliant success the investigations carried out in this direction.[72]

In a manner characteristic of algebraic analysis, this unity is anchored in analytical formulas. After explaining an application of elliptic functions to sums of squares, Hermite commented to Angelo Genocchi, in June 1883:

> If one denotes by $f(n)$ the number of decompositions of an integer $n \equiv 5 \text{ Mod } 8$ into five odd squares whose roots are assumed to be positive, one has
>
> $$f(5) + f(13) + \ldots + f(n) = \sum_a E\left[\frac{\sqrt{n - 4aa'} + 1}{2}\right].$$
>
> In this formula, $E(x)$ represents the integer contained in x, and the sum is extended to all odd numbers a and a' such that $n - 4aa' > 0$. ... Is not this arithmetical character, proper to formulas of the theory of elliptic functions, a very singular thing, and may

[71] Nachlaß Dirichlet, Staatsbibliothek Berlin, Preussischer Kulturbesitz, Handschriftenabteilung, extract of a letter from Hermite, April 6, 1853: *Monsieur, Dans les instants trop courts que j'ai pu passer auprès de vous lors de mon voyage à Berlin, vous m'avez annoncé en présence de notre pauvre ami Eisenstein, avoir la théorie de la transformation en elle-même d'une forme ternaire indéfinie. J'avais moi-même déjà fait quelques recherches sur cette question si difficile, mais sans succès, et je n'ai pas été surpris de vous entendre dire que les principes sur lesquels vous aviez fondé la solution étaient très cachés. Depuis peu, j'ai été ramené sur ce sujet, obéissant je crois à une loi de ma destinée, de ne jamais rien faire en arithmétique que retrouver quelque chose de découvertes que vous avez faites depuis longtemps.*

[72] Dossier Hermite, Archives de l'Académie des sciences, Paris, letter to require the *légion d'honneur* for Kronecker, May 19, 1882: *La pensée qui a principalement inspiré Dirichlet se montre dans son mémoire célèbre qui est intitulé sur l'application de l'analyse infinitésimale à la théorie des nombres. C'était une révélation qu'il y eut ainsi un lien étroit entre deux régions si éloignées dans le domaine de la science, les nombres entiers d'une part, et de l'autre les variables continues de l'analyse; on pourrait entrevoir dans la découverte de Dirichlet le témoignagne d'une unité profonde et qui n'avait jamais été soupçonnée entre les branches les plus diverses des mathématiques. Mr Kronecker a poursuivi avec d'éclatants succès les recherches entreprises dans cette voie.*

> we not conclude that Analysis and number theory are at heart one and the same theory?[73]

Unity is here gained by explicitly constructing bridges between objects and between proofs or by exporting constructions and techniques from one area to another. We have already met several instances, for instance Hermite's use of adjoint substitutions, and self-adjoint forms in four variables, in his 1855 study of the transformation of Abelian functions.[74] His series of papers on Sturm's theorem is another perfect illustration.[75] For a given algebraic equation, Charles Sturm had exhibited in the 1830s a finite chain of real functions such that the difference of the variations of the sign of its values at a real a and at a real b provides the number of real roots of the equation between a and b. Sturm's proof relied on Rolle's theorem. A few years later, Sylvester constructed more directly a chain of Sturm functions for the task. Associating to the equation a family of quadratic forms with real coefficients, according to his favourite procedure, Hermite showed how to obtain Sylvester's functions directly from the invariants of the forms.[76] Poincaré's address at Hermite's Jubilée could be read as a vibrant homage to the specific interactions among arithmetic, algebra and analysis which characterize arithmetic algebraic analysis:

> Arithmetic was the first to reap the fruit of its alliance, but Analysis also would largely gain from it. Were not your groups of similar transformations in fact discontinuous groups and did they not generate uniform transcendental functions, useful in the theory of linear equations? For the same reason, you were bound to be seduced by the properties of elliptic functions and by the almost mysterious ease with which arithmetical theorems are derived from them.[77]

[73] [Hermite & Genocchi 2003], p. 98: *Si l'on désigne par $f(n)$ le nombre des décompositions d'un entier $n \equiv 5 \text{ Mod } 8$ en cinq carrés impairs dont les racines sont supposées positives, on a*

$$f(5) + f(13) + \ldots + f(n) = \sum_a E\left[\frac{\sqrt{n-4aa'}+1}{2}\right].$$

Dans cette formule $E(x)$ représente l'entier contenu dans x, et la somme s'étend à tous les nombres impairs a et a' tels que l'on ait: $n - 4aa' > 0$. ... N'est-ce pas une chose bien singulière que ce caractère arithmétique propre aux formules de la théorie des fonctions elliptiques, et n'est-on pas en droit d'en conclure que l'Analyse et la théorie des nombres ne sont au fond qu'une seule et même doctrine? I am very grateful to Giacomo Michelacci who communicated to me his edition of these letters.

[74] See [Hermite 1905–1917], vol. 1, pp. 448-452. A parallel with the study of Hermitian forms and binary forms is indicated p. 452.

[75] See [Sinaceur 1991], ch. 7, which also illuminates Hermite's algebraic environment outside the D.A., evoked above – including the algebraic writings of Lagrange and Fourier, the theory of elimination, and Cauchy's and Borchardt's work on the "secular equation," that is the equation giving the secular inequality of the elliptic orbits of planets. The later impact on linear algebra of these writings is discussed in [Brechenmacher 2006].

[76] "I have thus found again, in a purely algebraic investigation, this special species of quadratic forms which I considered so many times in my arithmetical investigations," wrote Hermite at the end of his paper, see [Hermite 1905–1917], vol. 1, p. 287.

[77] [Hermite 1893], pp. 6–7: *C'était l'Arithmétique qui recueillait les premiers fruits de son*

Hermite shared another conception with several mathematicians in the field, in particular Kronecker:[78] he considered mathematics a science. To Thomas Stieltjes, he wrote in May 1894:

> I feel very happy to learn you are in such good shape that you have transformed yourself into a natural scientist, to observe the phenomena of the arithmetical world. Your doctrine is mine. I believe that the numbers and the functions of Analysis are not the arbitrary product of our mind; I think they exist outside of us, with the same necessary character as the things of objective reality, and that we meet them or discover them, and study them, like physicists, chemists, and zoologists, etc.[79]

This conviction resonates well not only with the emphasis on classification in his programme for algebraic integers, but also with his requirement of effective procedures. To Stieljtes again:

> I conceived I could penetrate inside the world of irrational numbers defined by equations, $F(x) = 0$, with integer coefficients, by studying the continuous reduction of the form $\sum \alpha_i \bmod^2(x + x_i y + x_i^2 z + \ldots)$, with x_i designating the roots of the equation[80] ... I took a first step by recognizing that a finite number of operations is sufficient; one should have been able to perform them. Arithmetical investigations absolutely require examples where observation can be exercised, otherwise we remain in a vacuum – which is unfortunately what happened to me.[81]

Though classifying forms, of course, occupies an important place in the D.A., and computations are part and parcel of Gauss's number theory, Hermite borrowed both elements with some twists; for him, classification is the true task of science in

alliance, mais l'Analyse en devait aussi largement profiter. Vos groupes de transformations semblables n'étaient-ils pas en effet des groupes discontinus, et ne devaient-ils pas engendrer des transcendances uniformes, utiles dans la théorie des équations linéaires. Pour la même raison, vous deviez être séduit par les propriétés des fonctions elliptiques et par cette facilité presque mystérieuse avec laquelle on en déduit des théorèmes arithmétiques. The quotes goes on with more examples of the same type.

[78] See J. Boniface's chap. V.1, § 3.

[79] [Hermite & Stieljtes 1905], vol. 2, p. 398: *Je me sens tout joyeux de vous savoir en si bonne disposition que vous vous transformez en naturaliste pour observer les phénomènes du monde arithmétique. Votre doctrine est la mienne, je crois que les nombres et les fonctions de l'Analyse ne sont pas le produit arbitraire de notre esprit ; je pense qu'ils existent en dehors de nous avec le même caractère de nécessité que les choses de la réalité objective, et que nous les rencontrons ou les découvrons, et les étudions, comme les physiciens, les chimistes et les zoologistes, etc.*

[80] Here, mod designates the modulus of a complex number.

[81] [Hermite & Stieltjes 1905], vol. 2, p. 390: *Je m'étais figuré devoir pénétrer dans le monde des irrationnelles définies par des équations à coefficients entiers $F(x) = 0$ en étudiant les circonstances de la réduction continuelle de la forme $\sum \alpha_i \bmod^2(x + x_i y + x_i^2 z + \ldots)$, x_i désignant les racines de cette équation. ... Je n'ai fait qu'un premier pas, en reconnaissant qu'un nombre fini d'opérations suffit ; il aurait été indispensable de pouvoir les effectuer. Les recherches d'Arithmétique exigent absolument des exemples où l'observation puisse s'exercer; autrement on reste dans le vide, ce qui m'est arrivé pour mon malheur.*

general and the observation of examples[82] – even experimenting on them – is the clue to discovery. The role of these distinctive elements[83] is explicitly brought out by a letter of March 2, 1876:

> The feelings expressed in that passage of your last letter where you say to me "the more I reflect on all these things, the more I realize that mathematics is an experimental science, like all the other sciences," and in that other passage "It seems to me that the main task now [for mathematics] just as for descriptive natural history consists in gathering as much material as possible, and in discovering principles by classifying and describing this material" – this feeling, I say, is also mine, and in a simple and precise form you have summarized with regard to mathematics the intimate and deep conviction of my entire life as a mathematician. I therefore believe that even the most abstract analysis is an observational science; I assimilate absolutely the complex of notions, known and yet to be known, in this domain of analysis to those of the natural sciences, the ideas of analysis having their proper individuality, their figures so to speak, and their multiple correlations, to the same degree as animals and plants.[84]

7. Analysis Takes the Lead

There is at least one feature however, traditionally attached to Gauss's heritage and, even more specifically, to the academic discipline of number theory, that Hermite did not adopt:[85] the model of the D.A. as an epitome of rigourous demonstrations and meticulous thinking. For Hermite the keywords of good mathematical practice were naturalness and simplicity; rigour should follow, almost spontaneously, from the development of research, not be a leading motivation for it – and rigorous presentation

[82] Unlike Gauss, Hermite did not seem to take any particular pleasure in nor display any talent for computations. His mistakes and complaints about both are abundant, see for instance [Hermite & Mittag-Leffler 1984–1989], part III, p. 28, [Hermite & Stieljtes 1905], vol. I, p. 15, or vol. 2, p. 417.

[83] For a study of the way they operate in Hermite's conception of mathematics, and a more complete sample of citations, see [Goldstein 2008].

[84] File H 1850 (6) Hermite, Charles, Staatsbibliothek zu Berlin, Preussischer Kulturbesitz, Handschriftenabteilung (the "unknown" adressee is Leo Königsberger): *Le sentiment exprimé dans ce passage de votre dernière lettre où vous me dîtes "plus je réfléchis sur toutes ces choses, plus je reconnais que les mathématiques forment une science expérimentale, aussi bien que toutes les autres sciences" et dans cet autre passage: "Il me semble que la tâche principale, actuellement, de même que pour l'histoire naturelle descriptive, consiste à amasser le plus possible de matériaux, et à découvrir des principes en classant et décrivant ces matériaux," ce sentiment dis-je est aussi le mien, et sous une forme simple et précise vous avez résumé à l'égard des mathématiques l'intime et profonde conviction de toute ma vie de géomètre. Je crois donc que l'analyse la plus abstraite est en grande partie une science d'observation, j'assimile absolument le complexe des notions connues et à connaître dans ce domaine de l'analyse à celles des sciences naturelles, les notions de l'analyse ayant leur individualité propre, leur figure si je puis dire, et leurs corrélations multipliées, au même degré que les animaux et les plantes.*

[85] In this respect, his writings constitute an excellent point of departure to distinguish between research development and the academic discipline of number theory in the 1860s.

for its own sake was particularly to be rejected in teaching. Concerning Peano's editing of a course given by Genocchi, he commented:

> A large place is made for these very modern demands for rigour. … As for me, I am so frightened by the complicated apparatus of certain demonstrations in M. Darboux's memoir on discontinuous functions … that never, of my own free will, shall I consent to let them into my lectures at the Sorbonne.[86]

Although often associated with mathematicians Hermite particularly admired, like Karl Weierstrass or Kronecker, the trend towards arithmetization did not then find a positive echo with him.[87] On the contrary, perhaps under the pressure of his lectures,[88] he will progressively give the first place to analysis, and perceive its development as the unifying force of arithmetic algebraic analysis. In 1861, he wrote in a letter to Joseph Liouville:

> The demonstrations of Father Joubert spring from the [theory of complex multiplication] where the concept of the class of quadratic forms appears in the most necessary way and plays a most important role. I attach a great price to these demonstrations because they illuminate and extend the arithmetical theory of forms, while showing that the theorems given a long time ago by Gauss are just so many properties of elliptic functions; they add one of the most remarkable examples of those hidden links which bind transcendental analysis to arithmetic.[89]

[86] [Hermite & Genocchi 2003], p. 150: *Il y est fait grandement place aux exigences toutes modernes en fait de rigueur. … Je suis pour mon compte tellement effrayé de l'appareil compliqué de certaines démonstrations du mémoire de Mr Darboux sur les fonctions discontinues … que jamais, de mon plein gré, je ne consentirai à les faire entrer dans mes leçons de la Sorbonne.* It does not mean, as it is often said, that Hermite rejected discontinuous functions, or Darboux's work in general, see [Goldstein 2008].

[87] Thanks to his direct construction of a Sturmian series of functions, Hermite was able to prove Sturm's theorem without any recourse to Rolle's theorem (which Sturm used) or, more generally, to "continuity" (as Hermite himself points out). However, his interest here seems to me more to multiply the approaches in arithmetic algebraic analysis than to eliminate analysis per se, see [Hermite 1905–1917], vol. 2, p. 255.

[88] While we have concordant testimonies that lectures on number theory in Berlin in the second half of the century could attract hundreds, the situation was different in France. Hermite complained in 1879 that certain of his lectures at the Polytechnique were not well understood and had to be left outside the programme for the final exam: one of them concerned "the applications to arithmetic of the theory of elliptic functions and had the same fate. German students would give you more satisfaction on these matters." (File H 1850 (6) Hermite, Charles, Staatsbibliothek zu Berlin, Preussischer Kulturbesitz, Handschriftenabteilung.)

[89] [Hermite 1905–1917], vol. 2, p. 108: *Les démonstrations du P. Joubert découlent de [la théorie de la multiplication complexe] où la notion de classe de formes quadratiques s'offre de la manière la plus nécessaire et joue le rôle le plus important. J'attache à ces démonstrations un grand prix car elles éclairent et étendent la théorie arithmétique des formes en montrant que les théorèmes donnés il y a longtemps par Gauss sont autant de propriétés de fonctions elliptiques et elles ajoutent un des plus remarquables exemples de ces liens cachés qui réunissent l'analyse transcendante à l'arithmétique.* For the mathematical context of this quote, see C. Houzel's chap. IV.2 above.

The word "necessary" again is quite typical and coherent with Hermite's representation of mathematics as a natural science: the freedom of the mathematician is constrained, contrary to Dedekind's famous conception of mathematical objects as free constructions. To Kronecker, Hermite wrote on January 29, 1881:

> I see in [your work] a confirmation of what I think I told you once, that arithmetic is mainly an anticipation of the theory of elliptic functions. From which you draw, like me, the conclusion that over and beyond individual efforts left to free will, which every day provide science with its building materials, there is a force which binds them and coordinates them, which imparts to them a direction, independently of ourselves, making of us fellow-workers through the centuries.[90]

In his comments on Cauchy's work at the inauguration of the new Sorbonne, in 1890, analysis fullfills all his criteria for good mathematics:

> Analysis, while extending its domain, smooths the path, so arduous, so difficult to follow, of its first inventors; its principles gain in power and become more accessible, its methods take on a complete rigour and Cauchy has the greatest role in these important advances.[91]

The evolution of Kronecker towards a strong programme of arithmetization left Hermite particularly confused and unhappy[92] and, despite his admiration for Kronecker's *Grundzüge*, he would ignore this work in his obituary, choosing rather to stress those aspects of Kronecker's work more akin to his own preferences.[93] The theme of anticipation, and the subordinate role of arithmetic, can be found again and

[90] A copy of this unpublished letter to Kronecker is kept in Hermite's file in the Archives de l'Académie des sciences: *J'y vois une confirmation de ce que je crois vous avoir dit un jour, que l'arithmétique n'est en grande partie qu'une anticipation de la théorie des fonctions elliptiques. D'où vous tiriez comme moi la conclusion qu'en dehors et au-dessus des efforts individuels et abandonnés au libre arbitre qui chaque jour apportent à la science ses matériaux, il est une force qui les associe et les coordonne, qui leur imprime à notre insu une direction en nous faisant à travers les siècles les coopérateurs les uns des autres.* The last sentence could almost be used as the very characterization of a research field, see chap. I.1., § 5. However, the religious tone of the end is here unmistakable.

[91] [Hermite 1905–1917], vol. 3, p. 307: *L'Analyse, en étendant son domaine, aplanit la voie si laborieuse, si difficile à suivre des premiers inventeurs; ses principes gagnent en puissance et deviennent d'un accès plus facile, les méthodes prennent une complète rigueur et Cauchy a la plus grande part à ces importants progrès.* Note how rigour is supposed here to appear naturally, not to be imposed a priori. It is also interesting to contrast this with the preface of Hilbert's *Zahlbericht*, see chap. I.2, § 3.6 above. Almost the same diagnosis of the past leads to different, and even contradictory, solutions: algebraic number fields versus analysis.

[92] See for instance [Hermite & Mittag-Leffler 1984–1989], part II, p. 104.

[93] See for instance, [Hermite 1905–1917], vol. 4, p. 341: *M. Kronecker a mis en complète évidence que la théorie des formes quadratiques, de déterminant négatif, a été une anticipation de la théorie des fonctions elliptiques, de telle sorte que les notions de classes et de genres, celle des déterminants réguliers et de l'exposant d'irrégularité, auraient pu s'obtenir par l'étude analytique et l'examen des propriétés de la transcendante.*

again in Hermite's correspondence, and they lead him to a reevaluation of number theory since the D.A. For instance, he advised Sylvester:

> But what is as important as to discover extremely interesting results, is to engage your students and your collaborators in Baltimore in this fruitful path, where number theory joins Analysis, following Gauss and Jacobi, Dirichlet and Eisenstein. It is a singular thing, but absolutely certain, that arithmetic has no proper method, unlike Geometry, Algebra or integral calculus; it only develops by allying itself closely to Algebra or Analysis, and the admirable fruits it produces owe their birth to a force which lies outside itself.... In my opinion, Gauss's theory of quadratic forms is, in many respects, only an anticipation of the theory of elliptic functions and it is a provable fact that it is to this theory that are owed all the results since Gauss and Dirichlet.[94]

8. Hermite's Heritage

Hermite's case illustrates a general phenomenon: how quite different readings and developments of the D.A. could be produced on different soils – by amalgating it with other traditions and by selecting and emphasizing different parts of Gauss's book itself. The D.A., and more specifically its fifth section, provided Hermite, implicitly or explicitly, with a large range of problems such as reduction, of concepts such as adjoint form, of models of proofs such as the induction used in his main theorem, and of theory, or perhaps more accurately, of a predefined agenda for the study of a topic, a list of properties and proposals to prove. What Hermite, in turn, produced is a vast, synthetic domain of research, where forms and complex functions are at the forefront (relegating congruences and reciprocity laws to the background). This domain is of its kind as coherent as the D.A., although the nature of this coherence, as we have seen, is not the same.[95]

[94] [Parshall 1998], p. 221:*Mais ce qui est aussi important que de découvrir des résultats extrêmement intéressants, c'est d'engager vos élèves et collaborateurs de Baltimore dans cette voie féconde, où la théorie des nombres se joint à l'Analyse, à la suite de Gauss et de Jacobi, de Dirichlet et d'Eisenstein. C'est une chose singulière, mais absolument certaine que l'arithmétique n'a point de méthode propre comme la Géométrie, l'Algèbre ou le calcul intégral; elle ne se développe qu'en s'alliant étroitement à l'Algèbre ou à l'Analyse et les fruits admirables qu'elle produit doivent leur naissance à une force qui est en dehors d'elle. ... A mon sentiment, la théorie des formes quadratiques de Gauss n'est à beaucoup d'égards qu'une anticipation de la théorie des fonctions elliptiques et par le fait il est prouvé que c'est à cette théorie que sont dus tous les résultats depuis Gauss et Dirichlet.*

[95] This coherence could be extended to Hermite's political and religious views, as shown by his correspondence. He shared the concerns of the French Catholic Church, then opposed on several fronts to what was described as "modernity" (republicanism, free conceptual creation, formalism, etc.). For reasons of space, this point will not be further discussed here, but see above the end of the letter to Kronecker of January 29, 1881, and [Goldstein 2008]. Hermite's Platonic realism was perceived as extreme in its extent (see [Poincaré 1912/1913], p. 95), but several of its components, as we have seen, found a sympathetic echo in his correspondents.

And his programme was not a marginal one: "We are Hermite's heirs," Kyparissos Stephanos is reported to have said to his students.[96] In France, Poincaré, Emile Picard and Camille Jordan, among others, followed in his tracks in many respects. Elsewhere, Luigi Bianchi, Aleksandr Korkin, and Egor Zolotarev, developed his work on Hermitian forms, quadratic forms, minima, and it is to Hermite that Hermann Minkowski dedicated his 1896 *Geometrie der Zahlen*.[97] Until the First World War at least, his articles directly fed a large, international cluster of investigations and fostered one of the important research traditions originating in the D.A.[98]

His views on analysis were shared by many mathematicians in his environment. This shows that a fruitful and life-long involvement with the D.A. did not always accompany a disciplinary defence of the hegemony of number theory.[99] It was thus fitting that Poincaré chose Hermite's arithmetical work to illustrate his own views at the First International Congress of Mathematics, held in Zürich in 1897 – using words which sound like a reply to Hilbert's preface to his *Zahlbericht* and, even more, a rejoinder against arithmetization.[100]

> The only natural object of mathematical thought is the integer. It is the external world which has imposed its content on us; we have invented it no doubt – but it has forced us to invent it. Without it there would be no infinitesimal analysis; all of mathematical science would be reduced to arithmetic and the theory of substitutions. Yet it is to the study of the continuous that we have consecrated nearly all our time and all our effort. Who will regret it? Who will believe that this time and this effort have been wasted? Analysis unfolds for us infinite perspectives that arithmetic has not dreamed of; it shows us at a glance a grandiose composition, whose arrangement is simple and symmetric. Against this, in number theory, where the unforeseen reigns, the view is so to speak blocked at every step. Doubtless, you will be told that outside of the integer there is no rigour, and consequently no mathematical truth; that everywhere [the integer] lies hidden and that effort must be expended to render transparent the veils that hide it, even at the price of submitting to eternal repetitions.

[96] Kyparissos Stephanos defended a thesis in Paris on binary forms and elimination in 1884 and returned to Greece to become Professor of Mathematics at the University of Athens. See [Phili 1997], p. 85.

[97] This last book encapsulates in a unified setting many themes and applications dear to Hermite, from approximation to minima of forms to algebraic numbers, see J. Schwermer's chap. VIII.1 below. The setting is geometric (lattices), but Minkowski's geometry has a strong analytic component, see [Gauthier 2008].

[98] The one we called H-K in chap. I.2.

[99] There were other ways of developing the D.A. and number theory in France, see in particular A.-M. Décaillot's chap. VI.2 below. For the place of analysis in France at the end of the XIX$^{\text{th}}$ century, see [Gispert 1991].

[100] Poincaré could not go to Zürich and his text was read *in absentia*. We know that Hermite approved these views, see [Hermite & Mittag-Leffler 1984–1989], part III, p. 54, letter of September 1, 1898. On the other hand, it is interesting that Minkowski discouraged Hilbert from countering Poincaré in his own talk at the next International Congress, in Paris; see [Minkowski & Hilbert 1973], p. 119: *Die Züricher Rede von Poincaré habe ich wieder durchlesen. Ich finde, dass man alle seine Behauptungen bei der milden Form, in der sie gehalten sind, gut unterschreiben kann.*

Let us not be purists but grateful to the *continuous* which, even if all stems from the integer, is alone capable of extracting so much from it.

Need I moreover remind you of the surprising profit M. Hermite has obtained from his introduction of continuous variables into the theory of numbers? In this fashion, the very domain of the integer has been itself invaded and this invasion has reestablished order there where disorder reigned.[101]

References

Archibald, Thomas. 2002. Charles Hermite and German mathematics in France. In *Mathematics Unbound. The Evolution of an International Mathematical Research Community (1800-1945)*, ed. K. Parshall, A. Rice, pp. 123–137. Providence (R.I.): Americam Mathematical Society; London: London Mathematical Society.

Belhoste, Bruno. 1991. *Augustin-Louis Cauchy. A Biography*. New York: Springer.

Belhoste, Bruno, Lützen, Jesper. 1984. Joseph Liouville et le Collège de France. *Revue d'histoire des sciences* 37(3-4), 255–304.

Brechenmacher, Frédéric. 2006. Histoire du théorème de Jordan de la décomposition matricielle (1870–1930). Thèse, EHESS. Paris.

Charve, Léon. 1880. *De la réduction des formes quadratiques ternaires positives et de leur application aux irrationnelles du troisième degré*. Thèse présentée à la faculté des sciences de Paris. Paris: Gauthier-Villars. Repr. *Annales de l'École normale supérieure* 2nd ser. 9, 3–156 (supplement).

Corry, Leo. 1996. *Modern Algebra and the Rise of Mathematical Structures*. Science Networks 17. Basel, Boston, Berlin: Birkhäuser. 2nd ed., 2004.

Darboux, Gaston. 1905. *Notice historique sur Charles Hermite*. Paris: Gauthier-Villars.

Dickson, Leonard Eugene. 1919–1923. *History of the Theory of Numbers*. 3 vols. Washington: The Carnegie Institute. Repr. New York: Chelsea, 1956.

[101] [Poincaré 1897], pp. 26–27: *Le seul objet naturel de la pensée mathématique, c'est le nombre entier. C'est le monde extérieur qui nous a imposé le continu, que nous avons inventé sans doute, mais qu'il nous a forcés à inventer. Sans lui, il n'y aurait pas d'analyse infinitésimale ; toute la science mathématique se réduirait à l'arithmétique ou à la théorie des substitutions. Au contraire, nous avons consacré à l'étude du continu presque tout notre temps et toutes nos forces. Qui le regrettera? Qui croira que ce temps et ces forces ont été perdus? L'analyse nous déroule des perspectives infinies que l'arithmétique ne soupçonne pas; elle nous montre d'un coup d'œil un ensemble grandiose, dont l'ordonnance est simple et symétrique; au contraire, dans la théorie des nombres, où règne l'imprévu, la vue est pour ainsi dire arrêtée à chaque pas. Sans doute, on vous dira qu'en dehors du nombre entier, il n'y a pas de rigueur, et par conséquent pas de vérité mathématique; que partout il se cache, et qu'il faut s'efforcer de rendre transparents les voiles qui le dissimulent, dût-on pour cela se résigner à d'indéterminables redites. Ne soyons pas si puristes et soyons reconnaissants au continu qui, si tout sort du nombre entier, était seul capable d'en faire tant sortir.*
Ai-je besoin, d'ailleurs, de rappeler que M. Hermite a tiré un parti surprenant de l'introduction des variables continues dans la théorie des nombres? Ainsi, le domaine propre du nombre entier est envahi lui-même, et cette invasion a rétabli l'ordre là où régnait le désordre.

DIRICHLET, Johann Peter Gustav LEJEUNE-. 1842. Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. *Journal für die reine und angewandte Mathematik* 24, 291–371. Repr. in *Werke*, ed. L. Kronecker, vol. 1, pp. 533–618. Berlin: Reimer, 1889.

EISENSTEIN, Gotthold. 1975. *Mathematische Werke*, ed. A. Weil. 2 vols. New York: Chelsea.

FOURIER, Joseph. 1820. Sur l'usage du théorème de Descartes dans la recherche des limites des racines. *Bulletin des sciences de la société philomatique de Paris*, 156–165; 181–187.

GAUTHIER, Sébastien. 2008. Justifier l'utilisation de la géométrie en théorie des nombres: des exemples chez C. F. Gauss et H. Minkowski. In *La Justification en mathématiques*, ed. D. Flament, P. Nabonnand. Paris: Maison des sciences de l'homme. Preprint.

GISPERT, Hélène. 1991. *La France Mathématique. La Société Mathématique de France (1870-1914).* Cahiers d'histoire et de philosophie des sciences 34. Paris: SFHST, SMF.

GOLDSTEIN, Catherine. 2006. Du Rhin et des nombres : quelques réflexions sur l'usage de la notion de "transfert culturel" en histoire des mathématiques. In *Sciences et frontières*, ed. P. Hert, M. Paul-Cavallier. Bruxelles: Éditions Modulaires Européennes, to appear.

———. 2008. Un arithméticien contre l'arithmétisation : les principes de Charles Hermite. In *La Justification en mathématiques*, ed. D. Flament, P. Nabonnand. Paris: Maison des sciences de l'homme. Preprint.

HERMITE, Charles. 1850. Extraits de lettres de M. Hermite à M. Jacobi sur différents objets de la théorie des nombres. *Journal für die reine und angewandte Mathematik* 40, 261–278; 279–315. Repr. (with corrections) in [Hermite 1905–1917], vol. 1, pp. 100–163.

———. 1851. Sur l'introduction des variables continues dans la théorie des nombres. *Journal für die reine und angewandte Mathematik* 41, 191–216. Repr. (with corrections) in [Hermite 1905–1917], vol. 1, pp. 164–192.

———. 1854. Sur la théorie des formes quadratiques. Second mémoire. *Journal für die reine und angewandte Mathematik* 47, 343–368. Repr. (with corrections) in [Hermite 1905–1917], vol. 1, pp. 234–263.

———. 1893. *1822-1892. Jubilé de M. Hermite*. Paris: Gauthier-Villars.

———. 1905–1917. *Œuvres*, ed. E. Picard. 4 vols. Paris: Gauthier-Villars.

HERMITE & GENOCCHI. 2003. *Le Lettere di Charles Hermite a Angelo Genocchi (1868–1887)*, ed. G. Michelacci. Quaderni matematici (2^{nd} ser.) 546. Trieste: Dipartimento di scienze matematiche.

HERMITE & MITTAG-LEFFLER. 1984–1989. Lettres de Charles Hermite à Gösta Mittag-Leffler, [ed. P. Dugac]. *Cahiers du séminaire d'histoire des mathématiques* 5, 49–285 (letters 1874–1883); 6, 79–217 (letters 1884–1891); 10, 1–82 (letters 1892–1900).

HERMITE & STIELTJES. 1905. *Correspondance d'Hermite et de Stieltjes*, ed. B. Baillaud, H. Bourget. 2 vols. Paris: Gauthier-Villars.

JACOBI, Carl Gustav Jacob. 1835. De functionibus duarum variabilium quadrupliciter periodicis, quibus theoria transcendentium Abelianarum innititur. *Journal für die reine und angewandte Mathematik* 13, 55–78. Repr. in *Gesammelte Werke*, vol. 2, ed. K. Weierstrass, pp. 28–50. Berlin: Reimer, 1882.

———. 1839. Über die complexen Primzahlen, welche in der Theorie der Reste der 5ten, 8ten und 12ten Potenzen zu betrachten sind. *Journal für die reine und angewandte Mathematik* 19, 314–318. Repr. in *Gesammelte Werke*, vol. 6, ed. K. Weierstrass, pp. 275–280. Berlin: Reimer, 1891. French transl. *Journal de mathématiques pures et appliquées* 1st ser. 8 (1843), 268–272.

Kronecker, Leopold. 1895–1931. *Werke*, ed. K. Hensel. 5 vols. Leipzig: Teubner; repr. New York: Chelsea, 1968.

Lagrange, Joseph Louis. 1867–1892. *Œuvres*, ed. J.-A Serret. 14 vols. Paris: Gauthier-Villars, 1879; repr. Hildesheim, New York: Olms, 1973.

Legendre, Adrien-Marie. 1830. *Théorie des nombres*. 2 vols. Paris: Didot.

Lipschitz, Rudolf. 1986. *Briefwechsel mit Cantor, Dedekind, Helmholtz, Kronecker, Weierstrass*, ed. W. Scharlau. Dokumente zur Geschichte der Mathematik 2. Braunschweig, Wiesbaden: Vieweg.

Lützen, Jesper. 1990. *Joseph Liouville 1809-1882: Master of Pure and Applied Mathematics*. New York: Springer.

Minkowski & Hilbert. 1973. *Herman Minkowski. Briefe an David Hilbert*, ed. L. Rüdenberg, H. Zassenhaus. Berlin, Heidelberg, New York: Springer.

Parshall, Karen. 1989. Toward a History of Nineteenth-Century Invariant Theory. In *The History of Modern Mathematics*, ed. D. Rowe, J. McCleary, vol. 1, pp. 157-206. Boston: Academic Press.

———. 1998. *James Joseph Sylvester: Life and Work in Letters*. Oxford: Oxford University Press.

Picard, Emile. 1901. Leçon sur l'Œuvre scientifique de Charles Hermite. Repr. Préface, in [Hermite 1905–1917], vol. I, pp. vii-xl.

Phili, Christine. 1997. Sur le développement des mathématiques en Grèce durant la période 1850–1950. *Istorico-matematicheskie issledovania* 3, special issue ed. S. Demidov, M. Hormigon, 80–102.

Poincaré, Henri. 1897. Les rapports de l'analyse et de la physique mathématique. *Acta Mathematica* 21, 331–341. Repr. *Revue générale des sciences pures et appliquées* 8, 857–861. Repr. in *L'analyse et la recherche*, ed. G. Ramunni. Paris: Hermann, 1991.

———. 1912. La logique de l'infini. *Scientia* 12-25, 1–11. Repr. in *Dernières pensées*, pp. 84–96. Paris: Flammarion, 1913.

Serre, Jean-Pierre. 1970. *Cours d'arithmétique*. Paris: PUF.

Sinaceur, Hourya. 1991. *Corps et modèles*. Mathesis. Paris: Vrin.

Weil, André. 1979. *Oeuvres scientifiques. Collected papers*. 3 vols. New York, Berlin, etc.: Springer.

Zerner, Martin. 1991. Le règne de Joseph Bertrand (1874-1900). In [Gispert 1991], pp. 299–322.

VI.2

Number Theory at the *Association française pour l'avancement des sciences*

Anne-Marie Décaillot

The *Association française pour l'avancement des sciences* (AFAS) was launched with some brilliance in 1872 by a group of renowned scientists – including Claude Bernard, Marcelin Berthelot, Louis Pasteur, Jean-Baptiste Dumas, and Adolphe Wurtz – who wished to contribute to the moral recovery of their country after the disastrous conflict between France and Prussia. "Through science, for the nation,"[1] such is the motto of the Association which developed with the Third Republic and faded with it. The period after the war was indeed favourable to the promotion of science. In order to disseminate its results to a large public, the AFAS established a series of annual congresses, taking place in turn in various provincial towns: during these congresses, well-known scientists explained their most recent research, but enlightened amateurs could also present their work. The public at these congresses was composed of the same social classes on which the new Third Republic was relying: the industrial world with a strong presence of engineers, the teaching world with high-school or university teachers, the medical world, as well as a variety of amateur scientists, among whom were many military men.

Already before the 1870 conflict, French mathematics felt the need for international relations. Between 1872 and 1914, around forty foreign scientists participated in the congresses of the association – unlike, for instance, those of the French mathematical society, [Gispert 1991]. Their presence witnesses the attempts of the Association to establish international links, a policy which was particularly successful for mathematics: important foreign mathematicians, like James Joseph Sylvester or Pafnuti Lvoviš Čebyšev, exerted from the beginning a decisive influence on the

[1] "Par la science, pour la patrie." On the AFAS, see [Gispert 2002].

Association. However, there was a significant exception: on nationalistic grounds, German mathematicians were not invited before 1894, when Georg Cantor participated in a meeting of the AFAS in Caen.[2]

Either occasionally or regularly, famous French mathematicians, like Charles Hermite, Georges Halphen, Gaston Darboux, Henri Poincaré, Paul Appell or Emile Borel, contributed to the Association during the whole period under study. But the most original feature of the AFAS comes from the scientific expression of personalities who situated themselves far from the traditional scientific milieu: they developed original directions of research, often at the margins of academic mathematics.[3] The Deputy Charles-Ange Laisant, a mathematician trained at the Ecole polytechnique and a pillar of the AFAS, states that new channels of authentic research, connected with the range of its French membership, appeared within the Association française pour l'avancement des sciences, before fertilizing mathematics in-the-large.[4]

1. The References to Gauss's *Disquisitiones Arithmeticae* in the AFAS

The following analysis is based on a study of the annual *Comptes rendus* published by the Association between 1872 and 1914; the communications presented at the congresses are classified by discipline. Among the 1200 papers read in the sections involving mathematical sciences (including geodesy, astronomy and mechanics), one may evaluate at about 120 those concerning number theory. Numerous studies also come under the headings "geometry of situation" or "recreational mathematics": despite manifest combinatorial or numerical aspects, they cannot be confused with number-theoretical ones and we have systematically disgarded them.

We observe that in arithmetic and number theory, the main contributors are not the great names of French mathematics – with the interesting exception of Henri Poincaré. The reservation of the French academic milieu with respect to arithmetic is well-known.[5] Hermite expresses this point of view in a letter to Sylvester on February 19, 1883:

> This is a singular thing, although absolutely certain, that arithmetic has no proper method, as geometry, algebra or integral calculus; it only develops by allying itself closely with algebra or analysis and the fruits that it produces owe their birth to a force which is outside it.[6]

[2] Through this invitation, initiated by Charles-Ange Laisant, the AFAS wanted to promote the idea of an International Congress of Mathematics: the first one, in Zurich, in 1897, included Laisant among the French delegates.

[3] See [Gispert 1999].

[4] [Laisant 1880], p. 63: *Plusieurs questions originales ont pris naissance dans l'Association française et se sont ensuite développées et accrues en passant dans d'autres milieux.*

[5] On the number-theoretical production published in France during this period, see [Goldstein 1994] and [Goldstein 1999].

[6] [Parshall 1998], p. 220: *C'est une chose singulière, mais absolument certaine, que l'arithmétique n'a point de méthode propre, comme la géométrie, l'algèbre ou le calcul intégral; elle ne se développe qu'en s'alliant étroitement à l'algèbre ou à l'analyse, et les fruits qu'elle produit doivent leur naissance à une force qui est en dehors d'elle.* [Editors' note: For details on Hermite's perspective, see C. Goldstein's chap. VI.1.]

At the AFAS, the most productive authors in arithmetic are foreign mathematicians such as Sylvester, Čebyšev, or Eugène Catalan, a professor of analysis who had emigrated to Liège under the Second Empire; highschool teachers as Edouard Lucas or Ernest Lebon; an amateur as Gaston Tarry, a controller of finance in Algeria; Jules Molk's student André Gérardin, editor in Nancy of the journal of recreational mathematics *Sphinx-Œdipe*.

Among the themes they developed, the most frequent are the arithmetical study of prime numbers and divisibility questions (more than forty-five contributions). In this area, both professional and amateur mathematicians mingle together. Besides the theoretical results of Lucas, one also finds explicit decompositions of specific large integers or construction of tables of prime factors, by passionate amateurs as Tarry or Gérardin. About ten papers, on Bernoulli numbers, Mersenne numbers, or amicable numbers, are linked to the preceding theme. Lucas also uses Sylvester's anallagmatic chess-board to decompose numbers which are sum of squares. Cantor's intervention in Caen, [Cantor 1895], is a paradigm of the studies in empirical arithmetic, as it intends to support Goldbach's so-called "theorem" by checking it up to 1000. A last important topic is linked to the evaluation of the number of primes between two given numbers and to Dirichlet's theorem on the distribution of primes in arithmetical progressions: six contributions (by Sylvester, Catalan, Lebon, …) touch upon these issues. Čebyšev states for instance in the Paris congress, [Čebyšev 1879], that prime numbers of the form $4n + 1$ appear more frequently than those of the form $4n - 1$.

A second theme is that of Diophantine equations (18 contributions), almost exclusively handled by amateurs; Gérardin is the most active author in this field. On the other hand, the few papers involving cyclotomy and periods of roots of unity (6 contributions) are all written by experienced mathematicians, like Sylvester, Lucas or the university professor of Clermont-Ferrand, Auguste Pellet.

The theory of congruences is the subject of about 15 papers. Of particular interest is the application made by Lucas to the "geometry of fabrics" and to the study of primality, to which we shall return. So-called figurative algebra, by Laisant and Gabriel Arnoux, presents in tabular form the finite structures of integers modulo various primes, and investigates in this framework the question of the irreducibility of polynomials with coefficients in such structures.

As perhaps could be expected in such a milieu dedicated to linking industry, technology and science, 14 contributions concern arithmetic machines: here we meet again Čebyšev, who invented an adding machine using continuous motion, as well as the French railway engineer, Henri Genaille or Torrès y Quevedo, an engineer from Madrid. The history itself of computation and of computational instruments is discussed in four papers, for instance by Edouard Lucas or Charles Henry, then librarian at the Sorbonne university (and coeditor of Pierre Fermat's works).

Two presentations stand apart. Ole Broch, a former minister and professor at the University of Christania, explains at the Lille congress, in 1874, the work of the Danish astronomer, Thorvald Thiele, concerning the generalization to complex numbers of quadratic residues. However, his point is the graphic representation of such residues, which "often strikes the eyes by the beauty of the mosaic drawing that it offers"[7] and connects his lecture to the visual and practical trends of the other speakers. The second remarkable intervention, for different reasons, is that of Poincaré, [Poincaré 1882]: he is the only one to discuss the theory of forms and the question of invariants.

Although explicit references are rare in these congress proceedings, one can still find traces of a few sources: the most quoted name is that of Pierre Fermat. Gauss's results are known of course through the French 1807 translation of the *Disquisitiones Arithmeticae*, by A.-C.-M. Poullet-Delisle, but also through the last edition of Adrien-Marie Legendre's *Théorie des nombres* in 1830. Dirichlet's articles on the distribution of prime numbers in arithmetical progressions appear to be familiar to the most learned speakers; on the contrary, as we have seen, communications involving complex integers or the theory of forms are exceptional. Edouard Lucas is the only one to mention other names, like Augustin Cauchy, Carl Gustav Jacobi or Ernst Kummer. In the preface of his own *Théorie des nombres*, [Lucas 1891], Lucas underlines the influence of Gauss on his own research, in particular what concerns congruences and cyclotomy. It is thus to the analysis of certain aspects of Lucas's works, at the crossroads of higher and recreational mathematics, that we shall now turn, in order to delineate more precisely the impact of Gauss's masterpiece.

2. Congruences and Geometry of Fabrics

Edouard Lucas (1842–1891) was born in Amiens, in the north of France. A former student at the Ecole normale supérieure, *agrégé de mathématiques* in the same promotion as Gaston Darboux, he became associate astronomoner at the Observatoire de Paris from 1864 to 1869, at a moment when bitter conflicts opposed the director of the observatory, Urbain Le Verrier, and the astronomers themselves.[8] Lucas sometimes took refuge from this unpleasant atmosphere in his hometown: he discovered then the problems relative to weaving, thanks to the works of Edouard Gand,[9] whom Lucas quoted in his first publication, [Lucas 1867]. One may suggest that Edouard Lucas's interest for number theory, and in particular for prime numbers, originated from the question of industrial fabrics and that this interest first expressed itself in the tradition of local industrial societies. After the 1870 war, Edouard Lucas became a highschool teacher and a very active member of the Association française pour l'avancement des sciences, intervening for the first time in 1876, at the occasion of the Clermont-Ferrand congress.

[7] [Broch 1875], p. 1175: ... *souvent frappe les yeux par la beauté du dessin en mosaïque qu'elle offre.*

[8] On this issue, see for instance [Décaillot 1998] and [Décaillot 1999].

[9] Edouard Gand (1815–1891) was also born in Amiens. He began his career in the textile industry, where he became a mechanical draughtsman and a *liseur*, that is an analyst, for Jacquard punchcards. In 1861, he was the main founder of the Société industrielle d'Amiens, a society which comissioned him to organize a theoretical and practical course on weaving and another on mechanical design, for which he wrote several works.

It is at the Association française pour l'avancement des sciences that Lucas took on the theme of fabrics, in connection with arithmetic – an original question developed in the Association.[10]

The theory of congruences allowed Lucas to construct and classify fabrics with a rectilinear weaving, called "regular satins." They can be represented as drawings on cross-ruled paper, called *armures* (weaves): on a square chess-board of size $p \times p$ (p is called the modulus of the weave) are indicated the "weaving points" (*points de liage*) which correspond to the points of the fabric where the warp thread crosses the woof thread. The weave of a regular satin consists of p weaving points placed on the chess-board in such a way that two points cannot be on the same warp or woof thread; on the square chess-board, the warp threads are represented by columns, the woof ones by rows and the weaving points by darkened squares. The weaving of a regular satin is described by the modulus p and the shift (*décochement*) a, less than p and prime to p: the darkened points are the points of coordinates (x, ax), where x denotes the column number (chosen between 0 and $p - 1$) and ax the row number, calculated modulo p. It is indeed well-known that the residues in $\mathbf{Z}/p\mathbf{Z}$ of the various numbers $0, a, 2a, 3a, \ldots, (p-1)a$ define a permutation of the numbers $0, 1, 2, 3, \ldots, p - 1$.

Lucas classified satins of modulus p using the properties of $\mathbf{Z}/p\mathbf{Z}$. Every shift a prime to p has an opposite $p-a$ and an "associate" a', according to the terminology attributed to Euler in the *Disquisitiones Arithmeticae* (art. 77), that is such that $aa' \equiv 1 \bmod p$.[11] The shifts a and $p-a$ construct satins which are symmetric with respect to the horizontal direction; the shifts a and a' lead to satins whose drawings are deduced from each other by an exchange between warp and woof threads. The four satins corresponding to the shifts a, $p-a$, a', $p-a'$ are considered by Lucas as satins of the same "group": the same weave represents them, up to a symmetry or a rotation.

If $p > 2$, the four satins of a group reduce to two in two cases only. The first occurs when $a = a'$. The corresponding satins have weaving points which are symmetric with respect to the main diagonal of the chess-board. The shift a gives then a solution in $\mathbf{Z}/p\mathbf{Z}$ of the equation $x^2 - 1 = 0$. To these satins belong the serge-like fabrics, associated to the shifts 1 and $p - 1$. The second case occurs when $a = p - a'$. The corresponding satins are called "square satins" and are considered to be the most elegant among the regular satins. The lattice of their weaving points remains invariant under a rotation of a quarter turn around any of its points; neighbouring weaving points delineate squares, as can be seen in the example

[10] Two contributions by Lucas at the AFAS, in 1876 and 1878, concern this topic; unfortunately, no text on these first attempts has come down to us. In 1880, a memoir on the same theme appeared in the Italian *Ingenere civile*, which would be translated posthumously for the 1911 AFAS congress, [Lucas 1912]. The theme of mosaics and fabrics, as developed in mathematics at this time, is studied in [Décaillot 2002].

[11] The existence of a' results for instance from Bachet's theorem applied to coprime numbers p and a: it states that there exists two numbers x and y such that $ax + py = 1$. The residue class of the associate a' is of course the inverse of the residue class of a, in current terminology.

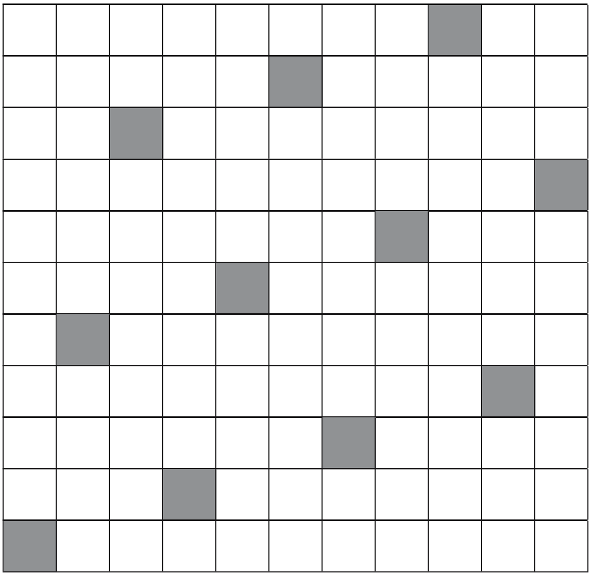


Fig. VI.2A. A satin of modulus 11 and shift 4

$p = 13, a = 5$ below. The shift a of a square satin gives a solution in $\mathbf{Z}/p\mathbf{Z}$ of the equation $x^2 + 1 = 0$.

Laisant summarized Lucas's work on the geometry of fabrics in his opening lecture of the 1879 congress:

> Using theorems by Fermat, Euler and Gauss, on the decomposition of certain numbers as the sum of two squares, and on the theory of associate numbers according to a prime or composite modulus [Gauss, *Disquisitiones Arithmeticae*, art. 77], one can easily obtain the table of the fundamental weaves, and thus the classification of the fabrics, according to the laws of arithmetic. In particular, one should consider the more regular weaving denoted by the author square satins and symmetrical satins, as the faithful geometrical representation of the roots of the congruencies[12]
>
> $$x^2 + 1 \equiv 0 \bmod p \qquad x^2 - 1 \equiv 0 \bmod p.$$

[12] [Laisant 1880], p. 84–85: *En se servant des théorèmes de Fermat, d'Euler et de Gauss, sur la décomposition de certains nombres en deux carrés, sur la théorie des nombres associés suivant un module premier ou composé [Gauss,* Disquisitiones Arithmeticae*, art. 77], on peut obtenir aisément le tableau des armures fondamentales, et par suite la classification des tissus, d'après les lois de l'arithmétique. En particulier, on doit considérer les armures plus régulières désignées par l'auteur sous le nom de satins carrés et de satins symétriques, comme la fidèle représentation géométrique des racines des congruences:* $x^2 + 1 \equiv 0 \bmod p$, $x^2 - 1 \equiv 0 \bmod p$.

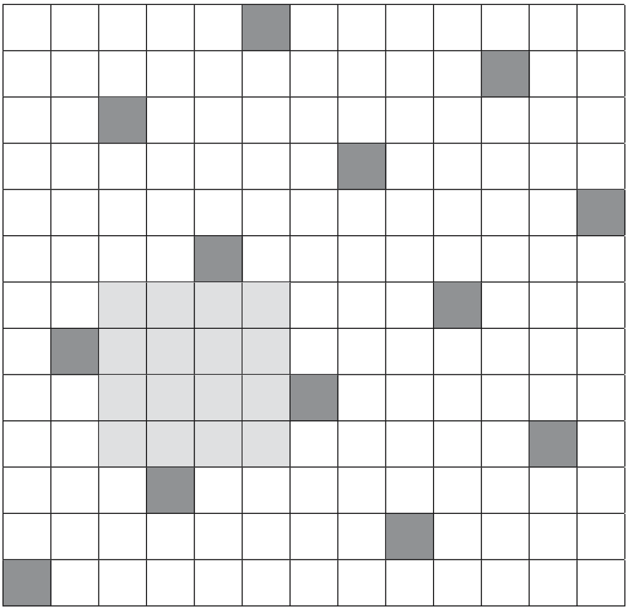


Fig. VI.2A'. Square satin of modulus 13 and shift 5

The study of the existence conditions of a square satin, for a given modulus, provided Lucas with an elegant approach to the theorem due to Fermat, according to which every prime p of the form $4n + 1$ is a sum of two squares.[13] Practicians of weaving, as Edouard Gand, had observed that a modulus p can be used to construct a square satin if it is the sum of two squares (this is the case, for instance, for the moduli 5, 13, or 25) and that there exists a square satin of prime modulus only if this modulus is of the form $4n + 1$. Lucas demonstrated these results on the chess-board and the classification of satins for a prime modulus allowed him to obtain Fermat's theorem thanks to the geometry of fabrics:

> For an odd prime modulus, one cannot have a square satin if p is of the form $4n + 3$; one has two complementary square satins if p is of the form $4n + 1$.[14]

For a prime odd p, the polynomial $x^2 + 1$ is reducible in $\mathbf{Z}/p\mathbf{Z}$ if p is of the form $4n + 1$ (resp. irreducible if p is of the form $4n + 3$), which also expresses the fact that -1 is a quadratic residue modulo p (resp. is not). A proof of these results using Fermat's Little Theorem[15] appears in the first publication of Lucas, [Lucas 1867], pp. 8–9.

[13] Letter to Mersenne on December 25, 1640, [Fermat 1891], pp. 293–294.

[14] [Lucas 1912], p. 80: *Pour un module premier impair p, on ne peut avoir de satin carré si p est de la forme* $4n + 3$*; on a deux satins carrés complémentaires si p est de la forme* $4n + 1$. See [Décaillot 2002].

[15] That is, the fact that $a^{p-1} \equiv 1 \bmod p$ if p is a prime number and a an integer prime to p.

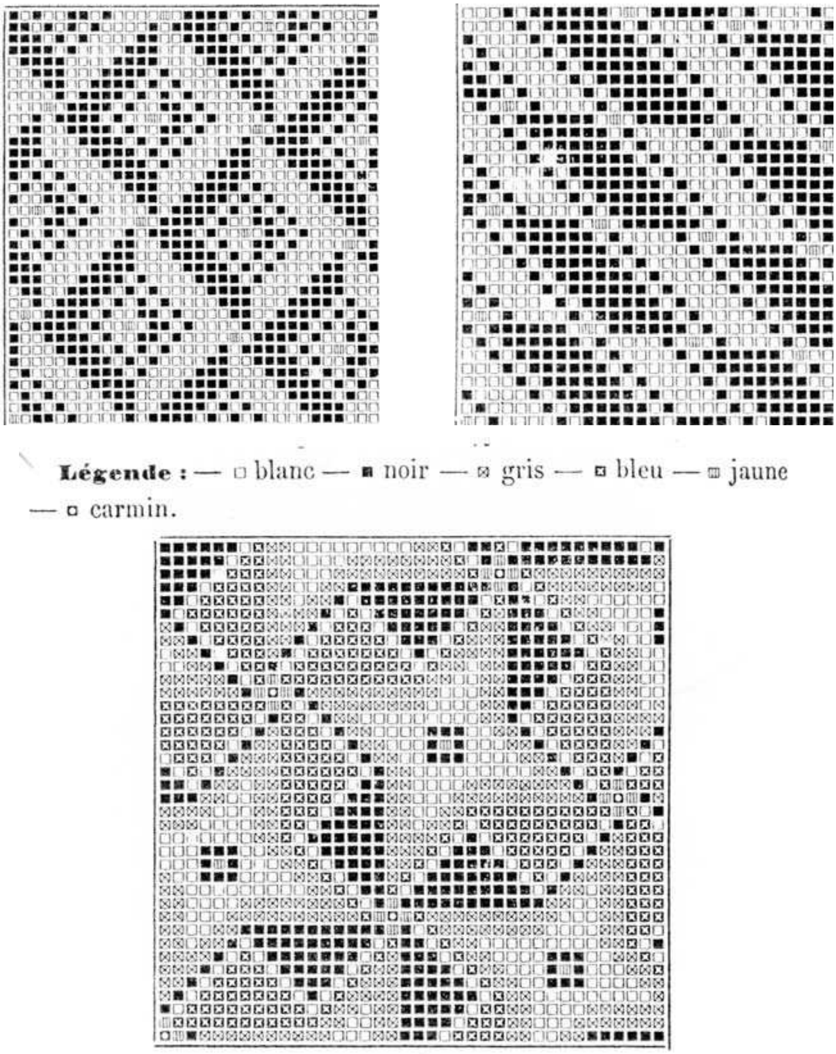


Fig. VI.2B. Number-theoretical constructions of fabrics by the industrial Édouard Gand
See [Gand 1867b], p. 286 and p. 296
(Courtesy of Bibliothèque municipale d'Amiens)

Left: *ombré* on a square satin of modulus 82 and shift 9; right: *jaspé* on a square satin of modulus 65 and shift 8. In the center, a mosaic effect on a square satin of modulus 185.

At the AFAS, Edouard Lucas entered into scientific and friendly relations with Čebyšev. In a letter to him on March 16, 1890,[16] Lucas mentions a proof of the quadratic reciprocity law obtained through weaving; the proof was published the same year in the *Bulletin de l'Académie impériale des sciences de Saint-Pétersbourg*, [Lucas 1890]. It relies upon Gauss's lemma which is easy to interpret on the chessboard. Indeed, according to this lemma, the Legendre symbol $\left(\frac{a}{p}\right)$ is equal to $(-1)^{\mu(a,p)}$, where $\mu(a, p)$ can be read on the weave of a satin (of modulus p and shift a) as the number of weaving points situated in the first $\frac{p-1}{2}$ columns and whose ordinate is greater or equal to $\frac{1}{2}p$. Lucas then succeeded in establishing the reciprocity law while formalizing the results displayed on the chessboard.[17]

The work of Lucas on the geometry of fabrics gave an impulse to new directions of research in the years 1878–1879, at the Société mathématique de France as well as the AFAS, on the theme of the "geometry of quiconxes." The objects of this study are regular lattices of points in the plane or the space.[18] One may add that calculation of congruences, joint with symbolic calculation of differences, led Lucas to a beautiful proof of the theorem of Thomas Clausen and Karl von Staudt on Bernoulli numbers.[19]

3. From Fermat's Little Theorem to the Invention of the Gaussian.

In 1785, Legendre had stated that "there are infinitely many prime numbers in any arithmetical progression whose first term and common difference are coprime":[20] the first proof, using analytic methods, was given by Lejeune-Dirichlet in 1837, in [Dirichlet 1837], and included as an appendix in the various editions of Dirichlet's *Vorlesungen über Zahlentheorie*. In a "Mémoire sur les nombres premiers", presented in 1848 at Saint-Petersburg, Čebyšev also used analytical means to prove that, for any $a > 3$, there is at least one prime number greater than a and smaller than $2a - 2$, a *postulatum* (Čebyšev's term) due to Joseph Bertrand in 1845.[21]

The search for prime numbers was thus launched for several decades in sources well-known to Lucas, but the most significant results relied on analysis. At the 1877 AFAS Congress, Lucas also noticed about Dirichlet's result:

> To summarize, all this research is based on the consideration of arithmetical progressions. We owe to the illustrious Fermat deep studies on the doctrine of prime numbers and based on the consideration of problems on geometrical progressions.[22]

[16] This letter is kept in the Academic Archives of Russia (Moskva), File: Čebyšev, Correspondence.

[17] For the proof, see [Décaillot 2002].

[18] Lattices of points were of course also studied in an independent context, in connection with crystallography, quadratic forms and complex functions, see [Cohn-Vossen, Hilbert 1923]. [Editors' note: see also J. Schwermer's contribution, chap. VIII.2.]

[19] On this proof, see [Décaillot 1999], vol. 1, pp. 107–110.

[20] [Legendre 1785], p. 552: *Il y a une infinité de nombres premiers compris dans toute progression arithmétique dont le premier terme et la raison sont premiers entre eux.*

[21] See [Čebyšev 1852] and [Bertrand 1845].

[22] [Lucas 1878a], p. 161: *En résumé, toutes ces recherches sont basées sur la considération*

Lucas's research then moved to the study of the primality of large numbers by means of geometrical progressions or of other connected series:

> It is ... through the observation of the Fibonacci series $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$, in which every term is the sum of the two terms that precede it, that we have met a new proposition which constitutes the converse of Fermat's theorem. We have deduced from it a great number of corollaries which allow us to know if a given number p of twenty or thirty digits is prime or not.[23]

Lucas described Fermat's Little Theorem as a result "remarkable by its elegance and its utility" and mentioned several proofs of this result, including that of Gauss, *Disquisitiones Arithmeticae*, art. 51.[24] Gauss gave in fact a stronger form, already stated by Fermat:

> If p is a prime number which does not divide a and if a^t is the smallest power of a congruent to 1 [mod p], the exponent t is $p - 1$ or an aliquot part of $p - 1$. (*Disquisitiones Arithmeticae*, art. 49.)

Checking the congruence $2^{37.73-1} \equiv 1 \bmod 37.73$, Lucas put into light the fact that Fermat's Little Theorem does not characterize prime numbers:

> This congruence shows that Fermat's theorem can apply to composite numbers and that, consequently, it has no converse.[25]

The "true converse" of Fermat's theorem was established by Lucas in 1876: if a and p are coprime numbers,

> if $a^x - 1$ is divisible by p for x equal to $p - 1$ and is not divisible by p for x equal to any aliquot part of $p - 1$, then the number p is prime.[26]

The participants to the Clermont-Ferrand congress of the Association française pour l'avancement des sciences were the first to hear this interesting theoretical result, expressed as a primality test relying on the divisibility of a certain series – an approach which we will see again. Lucas introduced the series $S_n = a^n - 1$, with a prime to p: if S_n is divisible by p for $n = p - 1$ and not previously, the number p is a prime number, [Lucas 1877a], p. 63. A proof of the result, based on a *reductio ad absurdum* was then published two years later in the *American Journal of Mathematics*.

des progressions arithmétiques. On doit à l'illustre Fermat des recherches profondes sur la doctrine des nombres premiers et basées sur la considération des problèmes des progressions géométriques.

[23] [Lucas 1891], préface, pp. xi-xii: *C'est ... par l'observation de la suite de Fibonacci* $0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, \ldots$*, dans laquelle chaque terme est la somme des deux termes qui le précèdent, que nous avons rencontré une proposition nouvelle qui consitue la réciproque du théorème de Fermat. Nous en avons déduit un grand nombre de corollaires qui permettent de savoir si un nombre donné p de vingt ou trente chiffres est premier ou non.*

[24] [Lucas 1891], pp. 421–422.

[25] [Lucas 1878a], p. 161 and [Lucas 1891], pp. 422–423.

[26] [Lucas 1891], p. 441: *si* $a^x - 1$ *est divisible par p, pour x égal à* $p - 1$*, et n'est pas divisible par p pour x égal à une partie aliquote de* $p - 1$*, le nombre p est premier.*

In his *Théorie des nombres*, Lucas develops the study of these congruences. He acknowledged particularly the influence of Dirichlet's lectures on the conception of his own book:

> It would be too long to give the list of works which have been published in Germany, in the last years, on the topic that concerns us. We will limit ourselves to mention the lessons of Lejeune-Dirichlet, published by M. Dedekind: *Vorlesungen über Zahlentheorie*; the third edition of this delicious treatise (Brunswick, 1881 [sic]) includes, besides the proof of Dirichlet's celebrated theorem on the presence of prime numbers in arithmetical progressions, noticeable and important additions by the editor on General Arithmetic.[27]

The third part of Lucas's book, devoted to arithmetical divisibility, presents manifest analogies with the two first parts of the German treatise. However, Lucas chose a terminology which underlines Gauss's impact on the topic. When he dealt with the determination of the solutions of the equation $a^x \equiv 1 \bmod n$, for a and n coprime integers:

> Among all powers of a which give 1 as residue, the most important to consider is that of the smallest exponent, disregarding the exponent zero. Let thus be g the smallest exponent such that one has $a^g \equiv 1 \bmod n$. ... We will say that g is the Gaussian of a for the modulus n. ... The exponents of the powers of a which, divided by n, give the residue 1, are all the multiples of the Gaussian.[28]

Fermat's Little Theorem has been generalized by Euler to arbitrary moduli: if $\phi(n)$ (the totient function or Euler indicator) denotes the number of prime numbers coprime with n and smaller than n, one has, for any a coprime with n:

$$a^{\phi(n)} \equiv 1 \bmod n.$$

A prime p can be characterized by the fact that its Euler indicator is equal to $p-1$. The Gaussian g of a for the modulus n satisfies the inequalities $g \leq \phi(n) \leq n-1$. The converse of Fermat's theorem relies on the fact that if $g = n-1$, then $\phi(n) = n-1$ and the number n is prime. One can also notice that Lucas's counter-example $2^{37.73-1} \equiv 1 \bmod 37.73$ uses the Gaussian: that of 2 is 36 for the modulus 37 as well

[27] [Lucas 1891], p. viii: *Il serait trop long de donner la liste des ouvrages qui ont paru en Allemagne, dans ces dernières années, sur le sujet qui nous occupe. Nous nous bornerons à citer les leçons de Lejeune-Dirichlet, publiées par M. Dedekind:* Vorlesungen über Zahlentheorie*; la troisième édition de ce délicieux traité (Brunswick, 1881* [sic]*) contient, en dehors de la démonstration du célèbre théorème de Dirichlet sur la présence des nombres premiers dans les progressions arithmétiques, de remarquables et importantes additions de l'éditeur sur l'Arithmétique générale.*

[28] [Lucas 1891], pp. 439–440: *Parmi toutes les puissances de a qui donnent 1 pour reste, la plus importante à considérer est celle du plus petit exposant, en ne tenant pas compte de l'exposant zéro. Soit donc g le plus petit exposant tel que l'on ait* $a^g \equiv 1 \bmod n$. ... *Nous dirons que g est le gaussien de a pour le module n. ... Les exposants des puissances de a qui, divisées par n, donnent pour reste 1, sont tous les multiples du gaussien.* For more details on the introduction of the "Gaussian," see [Décaillot 1999], vol. 1, pp. 87–88.

as for the modulus 73, thus it is also 36 for the modulus 37.73. But $37.73 - 1 = 2700$ is a multiple of 36, thus the sought-for congruence.

4. Prime Numbers in Fibonacci Series

Lucas devoted to Leonardo of Pisa a bulky memoir published in Italy in 1877, [Lucas 1877b]. But his own original contribution, developed in several articles, consists in revealing the "law of apparition of prime numbers" inside the Fibonacci series:

> If p is prime number not equal to 2 or to 5, one has $u_{p-1} \equiv 0$ or $u_{p+1} \equiv 0 \bmod p$, depending whether 5 is or is not a quadratic residue of p.[29]

As is well-known, the Fibonacci series is a linear recurring series defined by $u_{n+2} = u_{n+1} + u_n$, with $u_0 = 0$ and $u_1 = 1$; Lucas calls u_n the "term of rank n." The general term of the series can been expressed in terms of $\sqrt{5}$, 5 being the discriminant of the associated characteristic equation $x^2 - x - 1 = 0$. One has

$$u_n = \frac{1}{\sqrt{5}}\Big[\Big(\frac{1+\sqrt{5}}{2}\Big)^n - \Big(\frac{1-\sqrt{5}}{2}\Big)^n\Big].$$

In the case when 5 is a quadratic residue of p (that is when $x^2 - 5 = 0$ has a solution modulo p, or $\sqrt{5}$ can be defined in $\mathbf{Z}/p\mathbf{Z}$), Fermat's theorem, applied to the term of rank $p - 1$ of the series under consideration, shows that p divides u_{p-1}.

In the case when $\sqrt{5}$ is not defined in $\mathbf{Z}/p\mathbf{Z}$ (that is, when $x^2 - 5 = 0$ has no solution modulo p), Lucas noticed that p appears in the term of rank $p + 1$ of the series, that is $u_{p+1} \equiv 0 \bmod p$; the result was inspired by a lemma of Joseph Lagrange.[30] Taking into account Lagrange's result allowed Lucas to open the field of primality tests defined by the converse of Fermat's theorem.

He proposed indeed the following primality criterion:

> If in one of the recurring series u_n, the term u_{p-1} is divisible by p, while p does not divide any term of the series whose rank is a divisor of $p - 1$, the number p is prime; similarly, if u_{p+1} is divisible by p, while p does not divide any term of the series whose rank is a divisor of $p + 1$, the number p is prime.[31]

This result constitues a sufficient condition of primality which application is all the easiest when the divisors of $p + 1$ or $p - 1$ are readily accessible, as it is for instance the case for Mersenne or Fermat numbers: for Mersenne numbers, the test is applied to the rank $p + 1$, for Fermat numbers, to the rank $p - 1$.

[29] [Lucas 1877a], pp. 64–65 and [Lucas 1878b], pp. 296–297: *Si p est un nombre premier non égal à 2 ou à 5, on a $u_{p-1} \equiv 0$ or $u_{p+1} \equiv 0 \bmod p$ selon que 5 est ou non résidu quadratique de p.*

[30] This is lemma VII in [Lagrange 1775], pp. 782–783.

[31] [Lucas 1877a], p. 66 and [Lucas 1878b], p. 302: *Si dans l'une des séries récurrentes u_n, le terme u_{p-1} est divisible par p, sans qu'aucun des termes de la série dont le rang est un diviseur de $p - 1$ le soit, le nombre p est premier; de même, si u_{p+1} est divisible par p, sans qu'aucun des termes de la série dont le rang est un diviseur de $p + 1$ le soit, le nombre p est premier.*

The use of the Fibonacci series is a particular case. More generally, Lucas took into account the series $u_n = \frac{a^n - b^n}{a-b}$ (with first terms $u_0 = 0, u_1 = 1$) and $v_n = a^n + b^n$ (with first terms $v_0 = 2$, $v_1 = 1$), where a and b are the two roots of a quadratic equation ($r^2 - r - 1 = 0$ in the case of the Fibonacci series).[32] The decomposition of the even terms $u_{2n} = u_n.v_n$ and the relation $v_{2n} = v_n^2 - 2(-1)^n$ guarantee that the method is fast, its application to Mersenne numbers being particularly efficient.

A Mersenne number $p = 2^n - 1$ is proved to be prime if $u_{2^n} = 0$ and $u_{2^k} \neq 0$ for every integer $k \leq n-1$. Considering the series $w_k = v_{2^k}$, whose terms are given by the recurrence relation $w_k = w_{k-1}^2 - 2$, with the first term $w_1 = v_2 = 3$, Lucas was able to state:

> In order to test the primality of $p = 2^n - 1$, one builds the series of numbers $w_1 = 3, w_2 = 7, w_3 = 47, w_4 = 2207, \ldots, w_k = w_{k-1}^2 - 2$. If the first term that is divisible by p has rank $n - 1$, the number p is prime.[33]

According to Lucas, his test allowed him to check the primality of most of the numbers Mersenne originally listed.[34] For the number $2^{127} - 1$, he indicated:

> I have thus checked, but, I must admit, only once, that the number $A = 2^{127} - 1$ is prime. … I have used for this last number the system of binary numeration, while operating on a 127 × 127 chess-board.[35]

Using the same method, Jules Hudelot[36] checked in 54 hours the primality of $2^{61} - 1$ and the engineer Henri Genaille conceived of an arithmetical machine to test "large prime numbers." This machine was presented at the AFAS congress in 1891:

> The arithmetical piano allows us to give a practical sequel to the method that was formulated by M. E. Lucas, at the Clermont-Ferrand congress, for checking large prime numbers. By a simple adjustment of a few pins, checking prime numbers of the form $2^n - 1$ is reduced in most cases to a few hours work.[37]

[32] These series u_n and v_n appeared in Lagrange's resolution of the so-called Pell-Fermat equation: "an arbitrary non-square integer being given, to find a square such that the product of the two numbers increased by 1 be a square,"[Lagrange 1766-1769], p. 695.

[33] [Lucas 1878a], p. 162 and [Lucas 1878b], p. 310: *Pour tester la primalité de* $p = 2^n - 1$, *on forme la suite de nombres* $w_1 = 3, w_2 = 7, w_3 = 47, w_4 = 2207, \ldots, w_k = w_{k-1}^2 - 2$. *Si le premier des termes divisibles par p est de rang égal à n* − 1, *le nombre p est premier.*

[34] See [Dickson 1919-1923], vol. 1, pp. 12–13, pp. 22–33 and pp. 395–401. Mersenne gave $2^n - 1$ as primes, for $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$. Of those, $2^{67} - 1$ and $2^{257} - 1$ are composite.

[35] [Lucas 1877b], pp. 152–158: *J'ai ainsi vérifié, mais une seule fois, je l'avoue, que le nombre* $A = 2^{127} - 1$ *est premier. … J'ai employé pour ce dernier nombre le système de la numération binaire, en opérant sur un échiquier de 127 cases de côté.* We remind the reader that Mersenne primes have all their digits equal to 1 in binary numeration.

[36] Quoted in [Lucas 1887]. The primality of this number was communicated to the Academy of Saint-Petersburg by Ivan M. Pervušin as soon as 1883, see [Dickson 1919–1923], vol. 1, p. 25.

[37] [Genaille 1891]: *Le piano arithmétique permet de donner une suite pratique à la méthode formulée par M. E. Lucas, au Congrès de Clarmont-Ferrand, pour la vérification des*

Lucas's method is not always conclusive, as it offers only sufficient conditions for primality. It was improved by Théophile Pépin, [Pépin 1877] and [Pépin 1878], but above all by Derrick Henry Lehmer, between 1927 and 1932, [Lehmer 1927], [Lehmer 1930], [Lehmer 1932]: the so-called Lucas-Lehmer test is still a crucial tool for the search of very large primes in cryptography. In France, however, Lucas's works fell almost into oblivion after the early death of their author. André Gérardin, one of his few followers, conceived in 1912 the principle of a "congruence machine" for the decomposition of large numbers into prime factors, relying on a sieve method. Such a machine was constructed in 1920 by the Carissan brothers and recently rediscovered, [Shallit, Williams, Morain 1995]. Gérardin himself intervened on the theme of algebraic machines at the Fifth International Congress of Mathematics in 1912 in Cambridge, see [Gérardin 1913].

5. International Aspects of Number Theory at the AFAS

The Association française pour l'avancement des sciences, an enterprise devoted to the promotion and development of French science, was nonetheless impregnated from the beginning by foreign influences: the English influence, with the presence of Sylvester, the Russian influence with Čebyšev who also decisively wanted to link mathematics to its concrete applications.[38] The German influence, however, was less connected with the actual presence of scientists, whom the AFAS refused to invite before 1894, than to the reading of treatises and to the exploration of specific themes, in particular those of the theory of numbers.

The activities of the Association are indeed noticeable in fields which were often neglected by academic science. The taste of engineers, teachers and simple amateurs – all participants of these congresses – for an accessible and useful science led the AFAS, as we have seen, to make room for numerical issues. If the theoretical aspects of number theory were never ignored, the figurative representation of arithmetical or algebraic problems, the "curious" observations on numbers, the construction of numerical tables or of elaborate computing machines, were put to the forefront. On the other hand, these observations could be reinforced by theoretical concepts which in turn were characteristically able to make the theorems appear "curious" and interesting for the AFAS members: this is how Gauss's work, continued by Dirichlet and Dedekind, entered into the deeply original approach of Edouard Lucas.

References

Bernstein, Sergei Natanovich. 1947. Chebyshev's influence on the development of mathematics [in Russian]. *Uchenye Zapiski Moskovskogo Gosudarstvennogo Universiteta* 91, 35-45. English transl. O. Sheynin, *Mathematical Scientist* 26-2 (2001), 63–73.

grands nombres premiers. Par la manœuvre simple de quelques chevilles, la vérification des nombres premiers de la forme $2^n - 1$ *se trouve réduite dans la plus grande partie des cas à un travail de quelques heures.*

[38] See [Bernstein 1947]. On the international links of the French arithmeticians, see [Goldstein 1999].

Bertrand, Joseph. 1845. Mémoire sur le nombre de valeurs que peut prendre une fonction quand on permute les lettres qu'elle renferme. *Journal de l'Ecole polytechnique* 30e cah. 18, 123–140.

Broch, Ole-Jacob. 1875. Sur la représentation graphique des nombres complexes. In *Association française pour l'avancement des sciences. 3. Compte rendu de la 3e session. Lille 1874*, pp. 1174–1176 + pls. xii and xiii. Paris: AFAS.

Cantor, Georg. 1895. Vérification jusqu'à 1000 du théorème empirique de Goldbach. In *Association française pour l'avancement des sciences. 23. Compte rendu de la 23e session. Caen 1894*, 2nd part: *Notes et essais*, pp. 117–134. Paris: AFAS.

Čebyšev, Pafnuti L. 1852. Mémoire sur les nombres premiers (lu à l'Académie impériale de Saint-Pétersbourg en 1848). *Journal de mathématiques pures et appliquées* 17, 366–390.

———. 1879. Sur une transformation des séries numériques. In *Association française pour l'avancement des sciences. 7. Compte rendu de la 7e session. Paris 1878*, p. 87. Paris: AFAS.

Décaillot, Anne-Marie. 1998. L'arithméticien Edouard Lucas (1842–1891): théorie et instrumentation. *Revue d'histoire des mathématiques* 4, 191–236.

———. 1999. *Edouard Lucas (1842–1891): le parcours original d'un scientifique français dans la deuxième moitié du XIXe siècle*. Thèse, Université René Descartes. Paris.

———. 2002. Géométrie des tissus. Mosaïques. Echiquiers. Mathématiques curieuses et utiles. *Revue d'histoire des mathématiques* 8, 145–206.

———. 2004. La géométrie des tissus. *Pour la Science*, avril, 78–83.

Dirichlet, Johann Peter Gustav Lejeune-. 1837. Beweis des Satzes, dass jede unbegrenzte arithmetische Progression, deren erstes Glied und Differenz ganze Zahlen ohne gemeinschaftlichen Factor sind, unendlich viele Primzahlen enthält. *Abhandlungen der Königlich Preussischen Akademie der Wissenschaften*, 45–81. Repr. in *Werke*, vol. 1, pp. 313–342. Berlin: Reimer, 1889–1897.

———. 1863. *Vorlesungen über Zahlentheorie*, ed. with supplements by R. Dedekind. Braunschweig: Vieweg. 2nd ed., 1871. 3rd ed., 1879. 4th ed., 1894.

Fermat, Pierre. 1891. *Œuvres*, ed. P. Tannery and C. Henry. Vol. 1. Paris: Gauthier-Villars.

Gand, Édouard. 1867a. Nouvelles méthodes de construction des satins réguliers, pairs et impairs. Théorie des nombres premiers appliquée aux pointés de ces armures. *Bulletin de la Société industrielle d'Amiens*, janvier, 57–88.

———. 1867b. Nouvelles méthodes de construction des satins réguliers, pairs et impairs. Armures (tissus), armures (dessin), mosaïques. *Bulletin de la Société industrielle d'Amiens*, juillet, 257–300.

Genaille, Henri. 1892. Piano arithmétique pour la vérification des grands nombres premiers. In *Association française pour l'avancement des sciences. 20. Compte rendu de la 20e session. Marseille 1891*, 1st part, p. 159. Paris: AFAS.

Gérardin, André. 1913. Rapport sur diverses méthodes de solutions employées pour la décomposition des nombres en facteurs. In *Association française pour l'avancement des sciences. 41. Compte rendu de la 41e session. Nîmes 1912*, 2nd part: *Notes et mémoires*, pp. 54–57. Paris: AFAS.

Gispert, Hélène. 1991. *La France mathématique, la Société mathématique de France (1870-1914).* Cahiers d'histoire et de philosophie des sciences 34. Paris: Société française d'histoire des sciences et des techniques, Société mathématique de France.

———. 1999. Réseaux mathématiques en France dans les débuts de la Troisième République. *Archives internationales d'histoire des sciences* 49, 122–149.

———. ed. 2002. *"Par la science pour la patrie", l'AFAS, un projet politique pour une société savante*. Collection Carnot. Rennes: Presses universitaire de Rennes.

Goldstein, Catherine. 1994. La théorie des nombres dans les *Comptes rendus de l'Académie des sciences* (1870–1914) : un premier examen. *Rivista di Storia della Scienza* 2nd ser. 2, 137–160.

———. 1999. Sur la question des méthodes quantitatives en histoire des mathématiques : le cas de la théorie des nombres en France (1870–1914). *Acta historiæ rerum naturalium necnon technicarum* New ser. 3, 187–214.

Hilbert, David, Cohn-vossen, Stephan. 1932. *Anschauliche Geometrie*. Berlin: Springer. English transl. *Geometry and the Imagination*. New York: Chelsea, 1952.

Lagrange, Joseph-Louis. 1766–1769. Solution d'un problème d'arithmétique. *Miscellanea Taurinensia* 4. Repr. in *Œuvres*, vol. 1, pp. 671–731. Paris: Gauthier-Villars, 1867.

———. 1775. Recherches d'arithmétique. Seconde partie. *Nouveaux mémoires de l'Académie royale des sciences et belles-lettres de Berlin. Année 1775* (1777), 323–356. Repr. in *Œuvres*, vol. 3, pp. 695–795. Paris: Gauthier-Villars, 1869.

Laisant, Charles-Ange. 1880. Discours d'ouverture. Notice historique sur les travaux des première et deuxième sections jusqu'en 1878 inclusivement. In *Association française pour l'avancement des sciences. 8. Compte rendu de la 8e session. Montpellier 1879*, pp. 61–116. Paris: AFAS.

Legendre, Adrien-Marie. 1785. Recherches d'analyse déterminée. *Histoire de l'Académie royale des sciences. Année 1785. Avec les mémoires de mathématique et de physique pour cette année* (1788), Part. Mémoires, 465–559.

Lehmer, Derrick Henry. 1927. Test for primality by the converse of Fermat's theorem. *Bulletin of the American Mathematical Society* 33, 327–340. Repr. in [Lehmer 1981], vol. 1, pp. 69–82.

———. 1930. An extended theory of Lucas's functions. *Annals of Mathematics* 31, 419–448. Repr. in [Lehmer 1981], vol. 1, pp. 10–40.

———. 1935. On Lucas's test for the primality of Mersenne's numbers. *Journal of the London Mathematical Society* 10, 162–165. Repr. in [Lehmer 1981], vol. 1, pp. 86–89.

———. 1981. *Selected Papers*, ed. D. Mccarthy. 3 vols. Winnipeg: Charles Babage Center.

Lucas, Edouard. 1867. *Applications de l'arithmétique à la construction de l'armure des satins réguliers*. Paris: Retaux.

———. 1877a. Sur la recherche des grands nombres premiers. In *Association française pour l'avancement des sciences. 5. Compte rendu de la 5e session. Clermont-Ferrand 1876*, pp. 61–68. Paris: AFAS.

———. 1877b. Recherches sur plusieurs ouvrages de Léonard de Pise et sur diverses questions d'Arithmétique supérieure. *Bulletino di Bibliografia e di Storia delle scienze matematiche e fisiche* 10, 129–193 and 239–293.

———. 1878a. Considérations nouvelles sur la théorie des nombres premiers et de la division géométrique de la circonférence en parties égales. In *Association française pour l'avancement des sciences. 6. Compte rendu de la 6e session. Le Havre 1877*, pp. 159–167. Paris: AFAS.

———. 1878b. Théorie des fonctions numériques simplement périodiques. *American Journal of Mathematics* 1, 184–240 and 289–321.

———. 1887. Sur le neuvième nombre parfait. *Mathesis* 7, 45–46.

———. 1890. Sur la loi de réciprocité des résidus quadratiques. *Bulletin de l'Académie impériale des sciences de Saint-Pétersbourg* 33, 495–496.

———. 1891. *Théorie des nombres*. Vol. 1 [no other pub.]: *le calcul des nombres entiers, le calcul des nombres rationnels, la divisibilite arithmetique*. Paris: Gauthier-Villars. Repr. Paris: Blanchard, 1961; Paris: Gabay, 1981.

———. 1912. Les principes fondamentaux de la géométrie des tissus. In *Association française pour l'avancement des sciences. 40. Compte rendu de la 40e session. Dijon 1911*, 2nd part: *Notes et mémoires*, pp. 72–88. Paris: AFAS.

PARSHALL, Karen. 1998. *James Joseph Sylvester. Life and Work in Letters*. Oxford: Clarendon Press.

PÉPIN, Théophile. 1877. Sur la formule $2^{2^n} + 1$. *Comptes rendus de l'Académie des sciences* 85, 329–331.

———. 1878. Sur la formule $2^n - 1$. *Comptes rendus de l'Académie des sciences* 86, 307–310.

POINCARÉ, Henri. 1882. Sur les invariants arithmétiques. In *Association française pour l'avancement des sciences. 10. Compte rendu de la 10e session. Alger 1881*, pp. 109–117. Paris: AFAS.

SHALLIT, Jeffrey, WILLIAMS, Hugh C., MORAIN, François. 1995. Discovery of a lost factoring machine. *The Mathematical Intelligencer* 17-3, 41–47.

Part VII

Spotlighting Some Later Reactions

It is true now as formerly, a fact which Gauss and Dirichlet lamented, that only a small number of mathematicians busy themselves deeply with the theory of numbers and attain to a full enjoyment of its beauty. Especially outside Germany and among the younger mathematicians arithmetical knowledge is little disseminated. Every devotee of the theory of numbers will desire that it shall be equally a possession of all nations and be cultivated and spread abroad, especially among the younger generation to whom the future belongs.

David Hilbert, Introduction to Legh Wilber Reid's
The Elements of the Theory of Algebraic Numbers, 1910

VII.1

An Overview on Italian Arithmetic after the *Disquisitiones Arithmeticae*

ALDO BRIGAGLIA

1. The Early (Non)Reception of the *Disquisitiones Arithmeticae* in Italy

The decades around 1800 were not a period in which pure mathematics in general, and number theory in particular, flourished in Italy, see [Bottazzini 1994]. It is significant in this respect that Joseph Louis Lagrange, whose birth and early studies took place in Torino, finally became a prominent representative of the French mathematical school and that, decades later, Guglielmo Libri still spent most of his academic career in France. Thus, Gauss's *Disquisitiones Arithmeticae* did not have an immediate resonance in Italian mathematical circles.

Gianfrancesco Malfatti, a professor in Ferrara, already seventy years old at the time of the publication of the *Disquisitiones Arithmeticae*, was one of the rare Italian mathematicians who manifested some interest in arithmetic, and above all in the theory of algebraic equations, in the last decades of the eighteenth century.[1] In 1804, he criticized Ruffini's first attempts to prove that equations of degree higher than 4 are not solvable by radicals and thus contributed to Ruffini's later works.[2] A year later, Malfatti published what was probably the best Italian paper on arithmetical matters at that time, [Malfatti 1805], in which he studied the following problem using simple divisibility properties: multiply a given integer by a square, in such a way that it may be expressed as a sum of a given number of squares. However, none of these papers mentions Gauss and his masterwork. In fact, Malfatti did not display a serious knowledge of the recent developments in number theory; the short historical discussion in his 1805 paper only says:

[1] He worked on partitions, proposed a new method of elimination and introduced the so-called Malfatti resolvent for fifth-degree equations, [Brioschi 1863], [Biasini, Capra, Fiorentini, Pepe 1982].

[2] See [Malfatti 1804] and [Brioschi 1863].

> And while the sciences were re-establishing themselves in our countries, spreading through one country or another, having defeated the barbarism of the preceding centuries, valuable men appeared who more and more increased this branch of science of numbers, confronting products and squares and seeking integers which would satisfy all general formulas of their imagination. Among those distinguish themselves Frenicle, de Fermat and other famous names; nowadays the great geometer Lagrange does not disdain to dedicate himself seriously to this, he who has given us in the proceedings of Berlin a long and deep dissertation on similar problems.[3]

New traces of interest in number theory can be detected only from the 1820s: the first memoir of Libri concerns Diophantine analysis, and Leonard Dickson mentions in his *History of Number Theory* some contributions by Libri and G. de Paoli on congruences in 1829 and 1832, although none had an immediate impact on Italian mathematics as a whole.[4]

During the 1850s, however, in a climate of general development of mathematical studies in Italy (about which I refer to [Bottazzini 1994]), things began to change. Enrico Betti in Pisa, the most important Italian algebraist at the time, displays his fluency with congruences and Gauss's techniques for binomial equations, through his work on algebraic equations and Galois theory. In 1851, for instance, he proved that the transformations $x \to ax + b$ and $x \to (ax + b)^2 + c$ define permutations on $\mathbf{Z}/5\mathbf{Z}$, and indeed give all the 120 permutations of five numbers. Ten years later, in the context of the new national unity which launched the desire to renovate mathematics and its teaching, Betti translated into Italian Joseph Bertrand's treatise on algebra, [Bertrand 1862], adding as notes several arithmetical observations that showed his continuing interest in number theory, again in connection with algebra: one might cite for instance his treatment of the integral solution of an integral linear equation in n variables with coprime coefficients.

A more direct link with Gauss's *Disquisitiones Arithmeticae* can be witnessed in Pavia, where Francesco Brioschi and Luigi Cremona studied: Gaspare Mainardi, one of their teachers, published in 1858 a paper on binary quadratic forms where, according to Dickson, he "gave a more direct solution than had Gauss of the problem to find all transformations of one form into another, given one such transformation," [Dickson 1919–1923], vol. 3, p. 25. One might also evoke the names of Giovanni

[3] [Malfatti 1805], in [Malfatti 1981], vol. 2, pp. 761–762: *E allorchè, vinta la barbarie de' Secoli precedenti, si ristabilirono le Scienze nelle nostre contrade, andarono pullulando, or nell' uno, or nell' altro paese, de' valent' uomini, che dilatarono, sempre più, questo ramo di Scienza su i numeri, confrontando i produtti, e quadrati, e cercando quai numeri interi soddisfacessero alle generali formole da loro immaginate. Tra gli altri si distinsero il Frenicle, il de Fermat, ed altri di nome celebre nè sdegnò a' nostri giorni di occuparvisi seriamente il sommo Geometra Lagrange, che in problemi di simil sorta ci ha fatto dono negli Atti di Berlino di una lunga e profonda dissertazione.*

[4] See [Dickson 1919–1922], vol. 1, p. 55. Of course, Libri's arithmetical work published in the 1820s and 1830s as memoirs of the Académie royale des sciences or as articles in Crelle's journal displayed a good knowledge of the *Disquisitiones Arithmeticae*, in particular of congruences and equations, and won him international recognition, see [Libri 1835].

Plana and Giusto Bellavitis, who, although mainly known in other fields, displayed some interest in number theory.

A whole series of contributions also appeared in the first issues of the Roman *Annali di Scienze Matematiche e Fisiche* about the number of representations of a given integer as a sum of two squares (see *Disquisitiones Arithmeticae*, art. 182). However, most of the people involved in that elementary problem were not specialists in arithmetic, with the important exception of Angelo Genocchi, to whom we shall return. For instance, Paolo Volpicelli, who seems to have initiated the series, was then a school teacher in Rome – he became professor of mathematical physics in 1872;[5] Domenico Chelini, who proposed in 1852 using Gaussian integers to prove the result, but who did not complete the proof, was professor of mechanics at the university of Bologna.

2. Angelo Genocchi: an "Indefatigable," but Isolated Contributor

Even on such a simple problem, Genocchi's contributions, [Genocchi 1853] and [Genocchi 1854], offer a striking contrast: Genocchi made extensive use of the arithmetical properties of Gaussian integers to prove the formula, added results on other quadratic forms and also studied the number of representations of certain types of integers as a sum of four squares, while suitably criticizing the shortcomings of other articles.

Angelo Genocchi, born in 1817, may certainly be considered as the first mathematician working in Italy with a thorough knowledge of Gauss's arithmetical treatise, and, while mainly an autodidact in the field, was at least correctly informed of contemporary trends in number theory: in his 1854 article, for instance, he alluded not only to Gauss, but also to Cauchy and Kummer. Just after his death, Felice Casorati described him as "the most indefatigable devotee of this field in Italy."[6] Genocchi first studied law at the university of Parma, while reading mathematical journals and treatises on his own, but after the 1848 revolution, he left for Torino which then "hosted all the Italians who loved freedom,"[7] and devoted himself to mathematics. Teaching from 1857 onwards at the university of Torino – he counted among his students Corrado Segre and Giuseppe Peano – he had a large international correspondence in the second half of the nineteenth-century and was a visible figure in the Italian mathematical landscape, being, for instance, president of the Royal Academy of sciences [Conte, Giacardi 1991]. Peano recalls in his obituary that

[5] At first he was convinced that the formula for this number of representations, stated without proof in the *Disquisitiones Arithmeticae*, contained some misprints – as shown by Genocchi, it was merely a question of including or not zero among the integers. He finally published variants of his case-by-case proof not only in the *Annali*, but also in the *Comptes rendus de l'Académie des sciences* in 1853 and in Crelle's journal in 1855.

[6] In a letter to Francesco Siacci, quoted in [Viola 1991], p. 12, n. 2: *Le pubblicazioni risguardanti la Teoria dei numeri lo designavano come il più strenuo cultore di questio campo in Italia.*

[7] [Siacci 1889], p. 465: *a questa Torino, che ospitava amorevolmente gl'italiani amanti di libertà.*

> the whole of mathematics and particularly abstruse number theory were for him an irresistible fascination. While a student in law, he spent long hours in the library with mathematical books; the *Disquisitiones Arithmeticae* of the great Gauss was, as he told me, his favourite reading.[8]

Gauss's masterpiece is directly linked to what has been often described as Genocchi's most important work, his memoir on residues presented at the Academy of Belgium, [Genocchi 1852].[9] In the *Disquisitiones Arithmeticae*, Gauss had computed the square of

$$G = \sum_{1}^{p-1} \left(\frac{n}{p}\right) e^{2\pi i \frac{n}{p}},$$

for a prime p, where $\left(\frac{n}{p}\right)$ is the Legendre symbol: it is equal to p if $p \equiv 1 \bmod 4$ and $-p$ if $p \equiv -1 \bmod 4$. However, the computation of the sign of G (or iG) itself eluded him for several years.[10] In his 1852 paper, Genocchi obtained a simple, new proof of this computation; he also derived a proof of the quadratic reciprocity law, "through rather simple transformations and without the recourse to integral calculus," [Genocchi 1852], p. 1. According to Kronecker, who published a comparative analysis of it in the context of his own work on the reciprocity law, [Kronecker 1885] and [Kronecker 1889], Genocchi's proof relies on the fact that the excess of the number of positive values of

$$\frac{h}{m} + \frac{k}{n} - \frac{1}{2} + \frac{1}{2mn}, \qquad (k = 1, 2, \dots, \frac{1}{2}(n-1))$$

over the number of positive values of

$$\frac{h}{m} - \frac{k}{n}$$

is equal to $\frac{1}{2}\big(1 - \mathrm{sgn} R(\frac{hm}{m})\big)$. Here $R(a)$ denotes the difference between a and the nearest integer, m and n are coprime odd numbers, and h is an integer between 1 and $\frac{1}{2}(m-1)$. If m and n are prime numbers, Gauss's lemma implies that:

$$\mathrm{sgn} \prod_{h} R(\frac{hm}{m}) = \left(\frac{n}{m}\right),$$

[8] [Peano 1889-1890]: *... tuttavia la Matematica, e specialmente l'astrusa teoria dei numeri furono per lui un fascino irresistibile. Studente in leggi, passava lunghe ore in biblioteca su libri di matematica; le Disquisitiones Arithmeticae del sommo Gauss, erano, com'egli mi disse, sua lettura favorita.*

[9] In letters required by Francesco Siacci from Genocchi's colleagues and correspondents to complete his obituary of Genocchi, Catalan describes the memoir as Genocchi's "major work" (*œuvre capitale*), [Siacci 1889], p. 476, and Kronecker writes that it "outclasses in scope as well as in significance all other number-theoretical publications of Genocchi (*Denn die bezeichnete Abhandlung überragt wie an Umfang so auch an Bedeutung alle andern zahlentheoretischen Publicationen Genocchi's*), [Siacci 1889], p. 480.

[10] On the computations of these Gauss sums, see chap. VIII. 2 by Samuel J. Patterson [Editors' note].

where again $\left(\frac{n}{m}\right)$ is the Legendre symbol. Thus Genocchi's proof can be characterized as "a logarithmic version" of the third proof of the reciprocity law by Gauss.[11] Although Kronecker underlines that the key result can be deduced easily from Eisenstein's analytic formula expressing the Legendre symbol as a product of circular functions,[12] while Genocchi's work on Gauss sums appears as a particular case of Dirichlet's work, he added: "this may decrease the importance of Genocchi's memoir for mathematical literature, but increases at the same time our consideration for his mathematical talent."[13]

Thus, during the 1860s, Genocchi may be considered the unique Italian specialist in number theory. Among the other number-theoretical problems that interested him, we can mention a theorem[14] stated by Euler in a 1742 letter to Goldbach, according to which every integer not of the form $4ab - a - b$ can be expressed in the form $x^2 + y^2 + y$; Bernoulli numbers; Fermat's last theorem for $n = 7$, for which he found a simpler proof that Lamé's one, see [Genocchi 1884]; sums of cubes, as in [Genocchi 1868–1869], where he proved that the double of any prime of the type $8n - 1$ is a sum of three squares, or in [Genocchi 1885] where he found solutions[15] to equations like $x^3 + (x + r)^3 + (x + 2r)^3 = y^3$; congruent numbers and related Diophantine equations, which he studied in relation with his historical interest in Fibonacci's *Liber quadratorum* and *Liber abbacci*. However, his large activity, which displayed a lasting involvment with the topic and which put Genocchi in contact with contemporary research in other European countries, did not succeed in creating an Italian school for the theory of numbers: Genocchi had no direct student in this area.

3. Number Theory in Italy in the Aftermath of the Unification

A renewed interest in number theory took place in the last decades of the century, and two translations of important arithmetical books appeared at that time in Italy. The first was the translation, in 1881, of the third edition of Dirichlet's famous *Vorlesungen über Zahlentheorie*, containing Dedekind's appendices, [Dirichlet 1881]. The translator Aureliano Faifofer (1843–1909), was a school teacher, and had been the teacher of one of the most famous Italian mathematicians of his generation,

[11] [Kronecker 1885], repr. in [Kronecker 1895–1931], vol. 3, p. 135: *Die Genocchi'sche Beweismethode ... ist daher selbst als eine "logarithmische Umgestaltung" des dritten Gauss'schen Beweis zu charakterisieren.*

[12] Genocchi himself first derived his key result from expressions also involving roots of unity, then established it directly in the next section of his paper. "Mr Genocchi has in no way borrowed the principle of his proof from Eisenstein's developments, but has autonomously found it, independently of them, by purely arithmetical ways," writes Kronecker, [Kronecker 1885], repr. in [Kronecker 1895–1931], pp. 135–136.

[13] [Siacchi 1889], p. 482: *Dies verringert die Bedeutung der Abhandlung Genocchi's für die mathematische Literatur, vermehrt aber zugleich unsere Achtung vor seinem mathematischen Talent.*

[14] Genocchi proved the statement in [Genocchi 1853] and later noted a gap in the proof given by V. A. Lebesgue in 1854.

[15] Genocchi gave for instance the solution $149^3 + 256^3 + 363^3 = 408^3$.

Guido Castelnuovo. The second book was the 1895 translation of Čebyšev's book on congruences, [Čebyšev 1895], by a woman mathematician, Iginia Massarini, who extended the original table of indices. Neither of the translators seemed to have published anything else in number theory. The marginal situation of number theory in Italian mathematical curriculum is nonetheless shown by the absence of indigenous textbooks on this topic: one needs to wait until the turn of the century to find two original textbooks, the first one in 1897, [Scarpis 1897] and the second in 1903, [Gazzaniga 1903], whose authors also contributed some original research. Umberto Scarpis (1861–1921) wrote papers on systems of linear congruences, binary quadratic forms, Wilson's theorem, the Euler function, and Galois fields, all published after his book.

Paolo Gazzaniga (1853–1930),[16] mainly an algebraist, is an interesting figure among Italian mathematicians interested in number theory. He had been a student of Felice Casorati in Pavia, where he took his degree in 1878, but during the years 1880–1881, he studied in Berlin under the supervision of Weierstrass and Kronecker. From 1885, he was a professor at the *Lyceum "Tito Livio"* in Padua, but he was also entitled by the mathematical faculty to teach as *libero docente* a course on number theory, one of the very few in Italy. The book of mimeographed notes, [Gazzaniga 1885–1886], which he wrote for this course, later became the already mentioned printed volume, [Gazzaniga 1903]. Also in this year 1885, he wrote a paper on binomial congruences ([Gazzaniga 1885]) which remains his only original work on the subject. The preface of his textbook begins with characteristic regrets:

> Number theory which has always exercised a powerful fascination on all those who cultivated it, is still little diffused among us, probably because of the lack of familiarity which the young men of our university have with the language in which most of the relevant works are written. In this book, I have set myself the task of gathering and relating to each other the fundamental propositions and some of the most important questions of arithmology[17] with the objective to help our young students and to prepare them and motivate them to explore with some profit the classical works of the great masters.[18]

At the end of the nineteenth century, every scholar engaged in number theory felt clearly the failure of Italian universities to give due attention to this discipline, whose importance was growing abroad. Among them, one can mention Ernesto

[16] For whom I refer to [Emaldi 1994].

[17] The word *arithmologie* was also coined at the time by some French authors to designate number theory [Editors' note].

[18] [Gazzaniga 1903], p. I: *La "teoria dei numeri", che pure ha sempre esercitato su quanti la coltivarono un fascino potentissimo, è ancor poco diffusa tra noi, probabilmente per la scarsa famigliarità che i giovani delle nostre Università hanno con la lingua, nella quale è scritta la maggior parte dei lavori che ad essa si riferiscono. In questo libro mi sono proposto di raccogliere e di coordinare fra loro le proposizioni fondamentali e alcune tra le più importanti questioni di aritmologia, allo scopo di venire in aiuto ai nostri giovani studiosi e di prepararli e invogliarli a cercare poi con qualche profitto le opere classiche dei grandi Maestri.*

Cesàro (1859–1906), a professor at the universities of Palermo and Napoli, who may be considered as a *protegé* of the Belgian number theorist Eugène Catalan. During his Belgian period, in the 1870s and the first half of the 1880s, Cesàro engaged himself enthusiastically in the study of elementary number theory, dealing with triangular numbers, divisors of integers and other analogous topics; he published many short papers, solving and asking questions in journals like the *Nouvelle Correspondance de mathématiques*, the *Nouvelles Annales de Mathématiques*, *Mathesis*, but also book-length studies, like [Cesàro 1885].

In [Cesàro 1883], he established the following identity: if $a', b', c', \ldots$ are all the divisors of an integer x, f and g two arithmetical functions and if one puts $F(x) = f(a') + f(b') + f(c') + \ldots$, and $G(x) = g(a') + g(b') + g(c') + \ldots$, then one has

$$G(a)f(\frac{n}{a}) + G(b)f(\frac{n}{b}) + \ldots = g(a)F(\frac{n}{a}) + g(b)F(\frac{n}{b}) + \ldots,$$

where $a, b, c, \ldots$ are the divisors of n. Replacing f and g by various numerical functions – for instance, ϕ associating to each x the number of integers less than x and coprime with it, or the function λ taking the value 1 on integers which have an even number of prime factors, and -1 on the others – Cesàro derived thus in an unified way several relations on divisors of integers that Joseph Liouville had found, apparently separately, and published without proof. Cesàro also made some contributions on mean values and asymptotic evaluations of arithmetical functions, in the tradition of Dirichlet and Mertens.[19] For instance, he generalized to the m^{th} powers of divisors the theorem, due to Alexandre Berger (and publicized by Catalan) according to which the mean value of the sum of the inverses of divisors of a number is $\pi^2/6$; Cesàro showed that the asymptotic mean value of $\sum_{d|x} \frac{1}{d^m}$ is $\zeta(m+1) = 1 + \frac{1}{2^{m+1}} + \ldots$. Although Cesàro, not surprisingly, sees in Dirichlet "the true inventor of this theory [of means]," (see [Cesaro 1964-1965], vol. 1, pars prima, p. 134) he also mentions that Gauss,

> in his *Disquisitiones*, states, about the mean value of the genera of a given determinant, a theorem also proved by Dirichlet and which, quite simply, depends on the mean value of $\omega(N)$.[20] The expression $\omega(N)$ designates the number of ways in which a number N can be decomposed into two coprime factors.

In other memoirs, Cesàro gave various asymptotic or probabilistic estimations, concerning the greatest common divisor, or least common multiple, of several numbers, or the greatest quadratic divisor of a number, or other quantities. In [Cesàro 1886–1887], for example, he established relations between the number of the first $2n$ triangular numbers relatively prime to n and the number of products of two consecutive integers, taken between 1 and $n+1$ and prime to n, and gave the probability

[19] Several are erroneous, see [Dickson 1919–1923], vol. 1, p. 294 and [Bachmann, Hadamard, Maillet 1910–1915], p. 365.

[20] [Cesàro 1964–1965], vol. 1, pars prima, p. 134: *Dans ses* Disquisitiones*, [Gauss] énonce, à propos du nombre moyen des genres d'un déterminant donné, un théorème, démontré aussi par Dirichlet, et qui dépend tout simplement de la valeur moyenne de* $\omega(N)$.

that two triangular numbers taken at random should be relatively prime. But, in this region of number theory, perhaps his most important result[21] is the well-known asymptotic expansion of the k^{th}-prime number p_k:

$$p_k \sim k \log k + \log\log k - 1 + \frac{\log\log k - 2}{\log k} - \frac{\log\log^2 k - 6\log\log k + 11}{2\log\log k}.$$

Cesàro had at least one follower, Gabriele Torelli (1849–1931), also professor (of algebra) at Palermo and Napoli. Although he was older, Torelli may be indeed considered as Cesàro's student for questions about the distribution of prime numbers: one of his most important works pertaining to this matter, [Torelli 1901], was written largely under the influence and the guidance of Cesàro.[22] Besides academic mathematicians like Torelli and Cesaro, teachers in highschools or technical institutes like P. A. Fontebasso, Giacomo Candido or Giovanni Frattini (whose name is known to group theorists for the famous Frattini subgroup) also contributed to elementary number-theoretical questions, sometimes in the setting of new mathematical journals at an intermediate level; that is, addressed to teachers, engineers and students, like Candido's *La Matematica elementare*. Frattini, in particular, published several papers on Wilson's theorem, roots of unity, congruences, sums of squares, Pell's equation and Čebyšev theorem.

Thus, by the 1870s and 1880s, Italian studies on arithmetic had expanded, but the topic was not an important part of university curriculum and very few mathematicians were induced to undertake an academic career based on it.

4. Luigi Bianchi and His Students

Things seemed to begin to change in Pisa under the guidance of Luigi Bianchi (1856–1928). Bianchi himself studied in Pisa, at the Scuola Normale Superiore and was a pupil of Enrico Betti and Ulisse Dini. He took his degree in 1877 and, immediately after, he spent a couple of years in München and Göttingen, where he studied under the supervision of Felix Klein and became acquainted with some of the latest results on number theory and automorphic functions. Bianchi is renowned above all as a differential geometer, and the largest part of his huge mathematical production – his *Opere* comprise eleven volumes – is dedicated to this subject. But, in the period from 1889 to 1894, number theory seems to have been his main object of interest. Bianchi studied closely Dedekind's edition of Dirichlet's *Vorlesungen über Zahlentheorie*,[23] and his first papers dealt with observations and generalizations related to it, in particular with Dedekind's supplements.

[21] See [Cesàro 1895], and the development [Cipolla 1902] given by Michele Cipolla, who studied both in Palermo and Pisa.

[22] The work interested Edmund Landau, who however found a gap in the proofs. For further details about Cesàro and Torelli and their contributions to number theory, see [Carbone, Nastasi, Palladino 1996], where one can find interesting letters between the two scholars.

[23] Both Gazzaniga and Veronese had studied in Göttingen, as well as Bianchi, and they wanted a renewal of Italian teaching. Thus, I suspect that it was through Bianchi's incentive that Faifofer undertook the translation of Dirichlet's book.

As well as Dirichlet and Dedekind, Bianchi's researches in that period were deeply influenced by Poincaré, Picard, Fricke and Klein and they all focused on the extension of arithmetical methods used by Gauss for quadratic forms with integral coefficients to forms whose coefficients are Gaussian integers or to Hermitian forms.

In his first paper on these subjects, [Bianchi 1889], Bianchi followed the steps of [Dirichlet 1842], a paper in which Dirichlet began to generalize Gauss's theory of real quadratic forms to quadratic forms $ax^2 + 2bxy + cy^2$, with a, b, c, Gaussian integers. If the form is primitive (i. e. if the g. c. d. of a, b, c is 1), the so-called *divisor* of the form, the g. c. d. of the coefficients a, $2b$, c, may be 1, $1 + i$ or 2, and according to it, the forms are classified as forms of the first, the second and the third species. Dirichlet had computed by means of transcendental methods the number of equivalent forms[24] of the first species with a given determinant, and indicated that his method could be also applied to the other species. Bianchi's aim was to compute directly the ratios of the number of classes of the second and the third species to that of the first species, by means of purely arithmetical methods.[25] Observing that Dedekind, in the X$^{\text{th}}$ supplement to Dirichlet's *Vorlesungen*, had proved that the composition for forms with complex coefficients has the same properties as for real forms, Bianchi was able to adapt the method that Gauss had proposed for real forms in the *Disquisitiones Arithmeticae* (arts. 253 sq.).

Both the subject and the style of Bianchi's paper were completely new for Italian mathematicians; they lifted Bianchi's work into one of the most advanced areas of European research. A year later, in [Bianchi 1890b], he filled a gap in the study of Hermitian forms whose coefficients are Gaussian integers: in [Picard 1884], Picard had used continual reduction to determine the finiteness of the number of equivalence classes, noticing that the case in which the determinant is the sum of two squares required a different method. Bianchi showed how to find a complete system of forms[26] for such a determinant, by a purely arithmetical procedure; he showed that the number of classes is 2 or 3 according to the parity of the determinant. The same year, he also began a detailed study, [Bianchi 1890b], of what is now called the Picard group – i. e. the subgroup of PGL(2, $\mathbf{C}$) of linear substitutions of one complex variable with determinant 1, whose coefficients are Gaussian integers – and of the analogous subgroup with coefficients in $\mathbf{Z}[\epsilon]$, where ϵ is a non-trivial cubic root of 1.[27] There, Bianchi was deeply influenced by the geometrical interpretation of linear substitutions in the Moebius plane as displacements in the Poincaré model

[24] Two quadratic forms with Gaussian integers as coefficients are said to be (properly) equivalent if they are obtained from each other by a linear substitution with Gaussian integers as coefficients and with determinant 1.

[25] As Bianchi pointed out, Lipschitz already proposed such an arithmetical method, relying on the use of substitutions with Gaussian coefficients and determinant $1 + i$, in [Lipschitz 1857]. Bianchi's approach was different.

[26] That is, such that every form with this determinant is equivalent to exactly one form of this sytem.

[27] This group is a particular case of what is called now a Bianchi group. In [Humbert 1920], Humbert called Bianchi groups all the groups of linear transformations with coefficients in a quadratic field, thus giving due attention to the work of the Italian scholar.

of hyperbolic space (see [Poincaré 1883]) and strengthened to this method to develop systematically the study of these groups and of their fundamental polyhedra and to apply it to the reduction of Hermitian forms. Let

$$a\xi\xi_0 + b\xi\eta_0 + b_0\xi_0\eta + c\eta\eta_0,$$

be an Hermitian form, with a and c positive real numbers and $bb_0 - ac < 0$; here ξ_0, η_0, etc., designate the conjugates of ξ, η, etc. Bianchi calls the "index" of the form the point of the 3-space of coordinates $x = -\frac{m}{a}$, $y = \frac{n}{a}$, $z = \frac{\sqrt{ac-bb_0}}{a}$, where m and n are the real and imaginary parts of b. Two equivalent forms have the same index (and conversely), and a Hermitian form is reduced if its index lies inside the fundamental polyhedron of the Picard group, delimited by the four planes $x = \pm\frac{1}{2}$, $y = \pm\frac{1}{2}$ and the sphere $x^2 + y^2 + z^2 = 1$. Bianchi could thus prove that every Hermitian form is equivalent to a reduced form.

These studies are summarized and expanded in Bianchi's important paper [Bianchi 1891a] (written in German), in which he gives a complete exposition of his work on quadratic and Hermitian forms. The first part is devoted, as [Bianchi 1890b], to the Picard and the Bianchi groups, the determination of their fundamental polyhedra and their main properties. In the second part, Bianchi applies these results to Dedekind's theory of concordant quadratic forms, that is, of forms $ax^2+2bxy+cy^2$ and $dx^2 + 2exy + fy^2$, with the same determinant, such that the coefficients a, d and $b + e$ are coprime,[28] extending Dirichlet's results on the number of classes to forms with coefficients in $\mathbf{Z}[\epsilon]$. In the third part, he uses the same approach to study equivalence of Hermitian forms on the same rings of complex integers. This paper, which extensively used for the first time the Picard group in arithmetic and successfully demonstrated the strong analogy between the arithmetic of quadratic and of Hermitian forms, received a large international reception. At the beginning of his paper, Bianchi inscribed himself in Klein's lineage:

> The geometrical method, on which Professor Klein bases the arithmetical theory of the ordinary binary quadratic forms [Fricke, Klein 1890] may be applied with the same success on a larger scale. To prove this is the aim of the following developments which will treat in the same way the theory of Dirichlet forms with integral complex coefficients and indeterminates and of Hermitian forms with integral complex coefficients and conjugate indeterminates.[29]

[28] On concordant conditions for forms, due to Dirichlet or Dedekind, see chapters I.1 and II.2 [Editors' note].

[29] [Bianchi 1891a], p. 313: *Die geometrische Methode, auf welche Herr Professor Klein die arithmetische Theorie der gewöhnlichen binären quadratischen Formen gründet, kann mit demselben Erfolge in weiterem Umfange angewandt werden. Dies zu zeigen ist der Zweck der folgenden Entwickelungen, welche in ähnlichem Sinne die Theorie der Dirichlet'schen Formen mit ganzen complexen Coefficienten und Veränderlichen, und der Hermite'schen Formen mit ganzen complexen Coefficienten und conjugierten Veränderlichen behandeln sollen.*

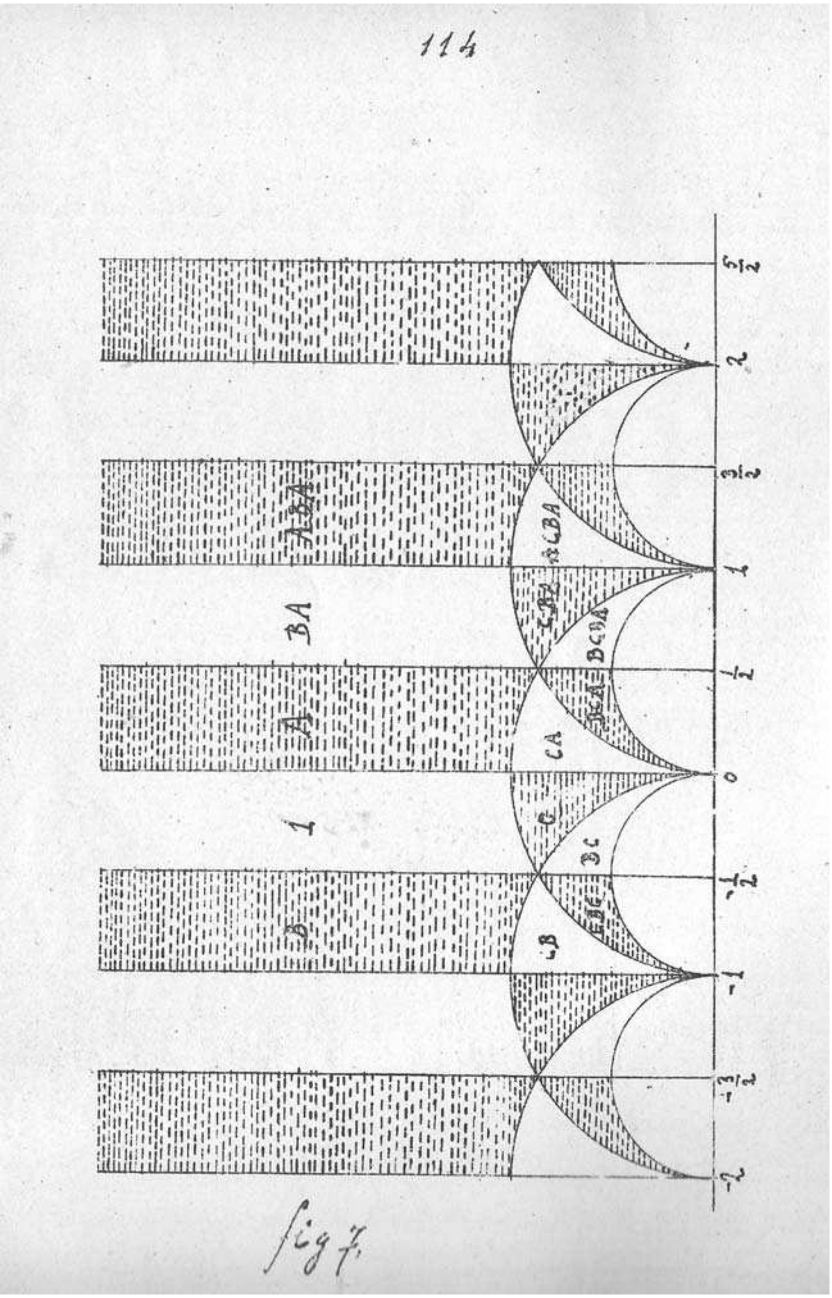


Fig. VII.1A. A tesselation of the half-plane
in Bianchi's 1912 *Lezioni sulla teoria aritmetica delle forme*
(Courtesy of the Library of the Mathematical Department, University of Palermo)

Conversely, in their fundamental *Vorlesungen über die Theorie der automorphen Funktionen*, Klein and Fricke closely followed Bianchi's method:

> Recently, Bianchi, not aware at first of Picard's results, has pursued the investigation of these objects in much detail and reported on it on several occasions; see in particular the note "Sui gruppi di sostituzione lineari a coefficienti interi complessi" as well as the detailed work "Geometrische Darstellung ...."[30]

Bianchi quickly recognized Picard's priority on the study of the group that bears his name: he quotes a letter of Picard to Klein referring to [Picard 1884] at the very beginning of the paper [Bianchi 1891b], an announcement of new results which would be proven in a series of papers published in the German journal *Mathematische Annalen* between 1891 and 1893. In these papers, Bianchi systematically applied Poincaré's and Klein's theory of automorphic functions to extend Dirichlet's and Hermite's theories of equivalence to various imaginary quadratic fields, for forms over Gaussian integers and for Hermitian forms, respectively.

In [Bianchi 1892a], for example, he studied the rings of numbers of the form $m + n\sqrt{-D}$, for m and n integers, where $D = 1, 2, 3, 5, 6, 7, 10, 11, 13, 15, 19$. As before, he used Poincaré's geometrical representation of the groups of linear transformations, but he also needed here what he called the notion of the "ampliamento del gruppo per riflessione" (extension of the group by reflections) developed by Fricke and contained in [Klein 1890]; again, he determined the fundamental polyhedron in each case. He stated in particular that the number of singular vertices (that is, the vertices at infinity) of each polyhedron is equal to the number of classes of ideals of the corresponding quadratic ring.[31] As before, the computation of the fundamental polyhedra gave him access to the theory of quadratic and Hermitian forms over the given quadratic fields. In the last part of the paper, he began to apply his results to the study of involutions and of orthogonality between quadratic and Hermitian forms over a quadratic field.[32]

[30] [Fricke, Klein 1897], p. 93: *In neuerer Zeit hat Bianchi, ohne zunächst mit den Picard'schen Resultaten bekannt zu sein, diese Gegenstände sehr ausführlich in Untersuchung gezogen und bei verschiedenen Gelegenheiten darüber berichtet; verg. namentlich die Note "Sui gruppi di sostituzione lineari a coefficienti interi complessi" sowie die ausführliche Arbeit "Geometrische Darstellung ... ".*The first article is [Bianchi 1890a], the second [Bianchi 1891a].

[31] To prove this theorem, Bianchi defined the G-equivalence between fractions in a quadratic field, for one of the groups G and the associated field: $\frac{a}{b} \sim \frac{a'}{b'}$ if and only if $\frac{a'}{b'} = \frac{\alpha\frac{a}{b}+\beta}{\gamma\frac{a}{b}+\delta}$, where α, β, γ, δ are the coefficients of a substitution in G. The number of these equivalence classes of fractions (representing the singular vertices) is then equal to the number of ideal classes of the quadratic field. Soon after, Hurwitz extended these results to any number field, see [Hurwitz 1895a] and [Hurwitz 1895b].

[32] To a Dirichlet form $a^2x^2 + 2bxy + cy^2$, whose determinant is not a perfect square, one associates an index circle, whose diameter is the segment joining the two roots of $a^2z^2 + 2bz + c = 0$; to a Hermitian form, is associated analogously an index sphere. A Dirichlet form and a Hermitian form are in involution (resp. orthogonal) if the index circle of the first is situated on (resp. is orthogonal to) the index sphere of the latter.

The following paper [Bianchi 1892b] began by dealing with the fact that some of the groups of substitutions studied before were distinguished subgroups of larger groups: Bianchi proved that the elements of these new groups have also algebraic coefficients, but this time in a higher-degree number field. In the second part of the paper, he

> indicated how the theory of the groups [of linear substitutions with complex coefficients] is linked to the arithmetical study of quaternary quadratic forms, reducible through real linear transformations to the type
>
> $$u_1^2 + u_2^2 + u_3^2 - u_4^2.$$
>
> This is an extension of the noteworthy principle established by M. Poincaré according to which the arithmetical group which corresponding to an arithmetical indefinite ternary form can be put in isomprhic correspondence with a properly discontinuous group of linear substitutions of one variable z,
>
> $$z' = \frac{\alpha z + \beta}{\gamma z + \delta},$$
>
> with *real* coefficients. Similarly the arithmetical group reproducing a quaternary form of the indicated type is in isomorphic correspondence with a discontinuous group of linear substitutions with complex coefficients. [... To this group] corresponds a regular tessellation of the non-Euclidean space; every polyhedron of the tessellation will be called for short a *fundamental polyhedron of the form.*[33]

Indeed, to the substitution $z' = \frac{\alpha z+\beta}{\gamma z+\delta}$, with α, β, γ, δ complex numbers such that $\alpha\delta - \beta\gamma = 1$, Bianchi associates the homogenous linear substitution S of 4 variables and of determinant 1, defined by the matrix

$$\begin{pmatrix} A & B & C & D \\ A' & B' & C' & D' \\ A'' & B'' & C'' & D'' \\ A''' & B''' & C''' & D''' \end{pmatrix}$$

with $A = \alpha\alpha_0, \quad B = \alpha\gamma_0 + \alpha_0\gamma \quad C = i(\alpha\gamma_0 - \alpha_0\gamma) \quad D = \gamma\gamma_0$

$$A' = \tfrac{1}{2}(\alpha\beta_0 + \alpha_0\beta), \quad B' = \tfrac{1}{2}(\alpha\delta_0 + \alpha_0\delta + \beta\gamma_0 + \beta_0\gamma)$$

[33] [Bianchi 1893b], pp. 237–238: ... *ho indicato come alla teoria di questi gruppi si collega lo studio aritmetico delle forme quadratiche quaternarie, riducibili con trasformazione lineare reale al tipo $u_1^2 + u_2^2 + u_3^2 - u_4^2$. É questa un'estensione del notevole principio stabilito dal sig. Poincaré [Poincaré 1887], mediante il quale al gruppo aritmetico riproduttivo di una forma aritmetica, ternaria indefinita si può porre in corrispondenza isomorfa un gruppo propriamente discontinuo di sostituzioni lineari sopra una variabile z, $z' = \frac{\alpha z+\beta}{\gamma z+\delta}$, a coefficienti* reali. *Così col gruppo aritmetico riproduttivo di una forma quaternaria del tipo indicato sta in corrispondenza isomorfa un gruppo discontinuo di sostituzioni lineari a coefficienti complessi. [... Al gruppo aritmetico riproduttivo] corrisponde una divisione regolare dello spazio non-euclideo; ciascun poliedro della divisione si dirà brevemente un* poliedro fondamentale della forma.

$$\begin{aligned}
C' &= \tfrac{1}{2}(\alpha\delta_0 - \alpha_0\delta + \beta\gamma_0 - \beta_0\gamma), \quad D' = \tfrac{1}{2}(\gamma\delta_0 + \gamma_0\delta)\\
A'' &= \tfrac{1}{2}(\alpha_0\beta - \alpha\beta_0), \quad B'' = \tfrac{1}{2}(-\alpha\delta_0 + \alpha_0\delta + \beta\gamma_0 - \beta_0\gamma)\\
C'' &= \tfrac{1}{2}(\alpha\delta_0 + \alpha_0\delta - \beta\gamma_0 - \beta_0\gamma) \quad D'' = \tfrac{1}{2}(-\gamma\delta_0 + \gamma_0\delta)\\
A''' &= \beta\beta_0 \quad B''' = \beta\delta_0 + \beta_0\delta \quad C''' = i(\beta\delta_0 - \beta_0\delta), \quad D''' = \delta\delta_0.
\end{aligned}$$

Here, as above, α_0, etc., designates the conjugate of α, etc. The substition S leaves invariant the quaternary quadratic form $x_2^2 + x_3^2 - x_1x_4$. The transformation $x_1 = u_4 + u_1, x_2 = u_2, x_3 = u_3, x_4 = u_4 - u_1$, changes the form into $u_1^2 + u_2^2 + u_3^2 - u_4^2$.

Bianchi then linked the groups that he had studied previously to the study of the form $y^2 + Dz^2–xt$, where D has the same meaning as above, and determined their fundamental polyhedra.

Lastly, he also indicated the relation between this arithmetical theory and Picard's analytical theory of hyperabelian functions and hyperabelian groups, as published in [Picard 1885]. This research continued in [Bianchi 1893a, b], where Bianchi studied various groups associated with other quaternary quadratic forms, as $x_1^2 + x_2^2 + \mu(x_3^2 - \nu x_4^2)$, where μ and ν are usual integers. The problem: given an arithmetical quaternary form, find the fundamental polyhedron connected with it, is obviously linked with the two main problems of the theory of quaternary forms: to establish if two quaternary forms with the same discriminant are equivalent or not; and to find all the transformations from one form to an equivalent one. In [Bianchi 1893b], studying a vast class of polyhedral groups, Bianchi solved the problem for specific types of quaternary forms and completed his work with numerous detailed examples in [Bianchi 1894 a,b]. He also explained why his methods for constructing the groups associated to the forms, and thus for reducing the forms, were simpler and more efficient than those of Fricke,[34] [Fricke 1893]. But, at that point, Bianchi turned to other topics and interrupted his arithmetical work for almost twenty years.

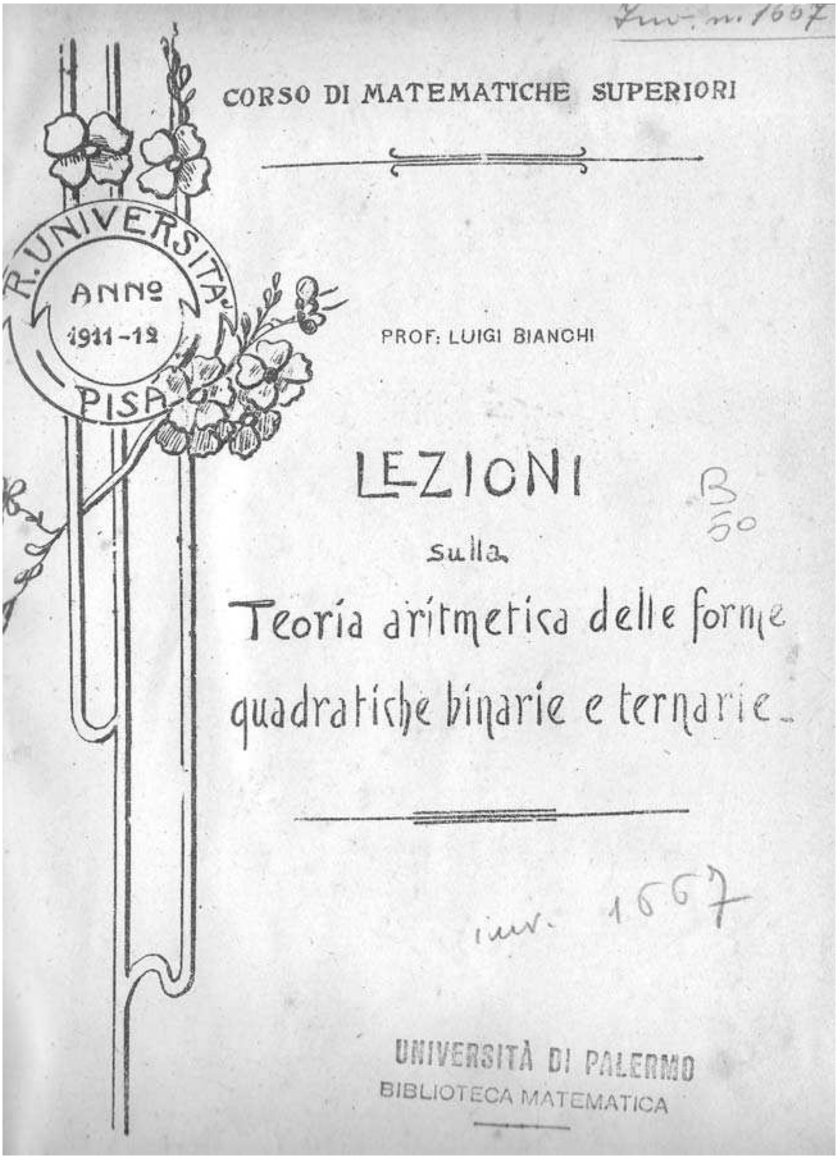
However, during this productive period, Bianchi had produced a mass of work that could put Italian mathematics at the forefront of modern (in the sense of algebraic and ideal-theoretic) number theory. In Gaetano Scorza's opinion:

> his beautiful research on the modular group and imaginary quadratic fields, ..., research which constitutes the most notable part of Italian contributions to arithmetic in the nineteenth century.[35]

Another student of Bianchi, Giovanni Sansone, echoes these words in his preface to the papers of his master:

[34] According to Dickson, [Dickson 1919–1923], vol. 3, p. 201, J. V. Uspenskij gave an algorithm in 1910 to reduce binary quadratic forms over integral numbers of a given field and remarked that while Bianchi's method was theoretically complete, it required too complicated computations to be really applicable to all numerical examples.

[35] [Scorza 1930], quoted in [Bianchi 1952], vol. 1, parte prima, p. 29: *Cadono appunto in codesto periodo di tempo le Sue belle ricerche sul gruppo modulare nei corpi quadratici immaginari ... ricerche che costituiscono la parte più ragguardevole delle contribuzioni italiane all'aritmetica pura nel secolo XIX.*



Inv. n. 1667

CORSO DI MATEMATICHE SUPERIORI

R. UNIVERSITÀ
ANNO
1911-12
PISA

PROF: LUIGI BIANCHI

LEZIONI

sulla

Teoria aritmetica delle forme quadratiche binarie e ternarie.

B
50

inv. 1667

Fig. VII.1B. Mimeographed course by Bianchi
on binary and ternary quadratic forms
(Courtesy of The Library of the Mathematical Department, University of Palermo)

> Those, in their still fresh style, in the harmonious perfection of all their parts, constitute a body of research which makes him the deepest Italian devotee of the geometrical Theory of Numbers in the last twenty years of the past century.[36]

Therefore we might ask why Bianchi, after 1894, left aside for such a long period the field of research that he had pursued with such enthusiasm and success. The main reasons for this choice are probably to be found in his growing interest in differential geometry, but another reason could be the scarce and even non-existent response to those studies in Italian academia. Bianchi was one of the leading professors at the *Scuola Normale Superiore* in Pisa, where most of the best Italian students were educated. He was deeply aware of the need to include number theory in a complete mathematical education of the future researchers. But of his many students at the end of the century, few devoted themselves to number theory. Adolfo Viterbi (1873–1917), who extended in [Viterbi 1898] Bianchi's study to substitution groups with coefficients in any number field, had worked under his supervision in Pisa: Bianchi then sent him to Göttingen to complete his studies with Felix Klein, confirming the tight links between the two scholars. However, in the first years of the twentieth century, Viterbi committed himself to applied mathematics – one of many young Italian scholars that changed their direction from number theory to other parts of mathematics – and unfortunately died during the First World War. The most important student of Bianchi was Guido Fubini, but he, too, is above all known as an applied mathematician or for his studies in projective differential geometry.

Thus, we stress that even Bianchi couldn't create an Italian school of number theory at that time. But he returned to number theory in 1912, trying hard to develop the field through his lectures; he wrote mimeographed notes, first [Bianchi 1912], on the topic he had favoured twenty years ago, the theory of forms, then [Bianchi 1921], on number fields, which developed into the splendid book [Bianchi 1923], offering to Italian students the most up-to-date textbook of that time.[37] Bianchi's efforts this time were in greater part successful, as demonstrated by the long list of his students who devoted themselves to algebra or number theory:[38] Onorato Nicoletti (1872–1929) was an expert in the theory of Hermitian forms; Gaetano Scorza (1876–1939), the author of *Corpi Numerici ed Algebre*, mainly worked on the theory of algebras; Giovanni Sansone (1888–1979) began his scientific career with important studies on the Picard group; Pacifico Mazzoni (1895–?) was interested in finite groups and Galois theory; Alberto Mario Bedarida (1890–1957), who was in epistolary contact with Edmund Landau, worked on ideal-theoretical aspects, as well as Luigi Fantappiè (1901–1956) and Tito Chella (1881–1923); Michele Cipolla (1880–1947) devoted himself to the study of congruences and group theory; Giovanni Ricci (1904–1973) contributed to some advances in additive number theory, in particular on the

[36] [Bianchi 1952], p. 192: *Esse, nel loro stile ancora fresco, nella perfezione armonica di tutte le parti, costituiscono un corpo di ricerche che fa del Nostro il più profondo cultore italiano della Teoria geometrica dei Numeri dell'ultimo ventennio del secolo scorso.*

[37] Bianchi also wrote a few research papers, in connection with the content of his course, on ideal theory in number fields.

[38] On the development of Bianchi's school in the 1920s, see [Brigaglia, Scimone 1998].

Goldbach conjecture, and on the seventh Hilbert problem – he was also the teacher of Enrico Bombieri in Milano. However, this promising group was rapidly dispersed. With the exception of Scorza, Ricci and to a lesser extent Cipolla, Bianchi's students changed their principal interests: for example, Sansone and Fantappiè became two of the most significant Italian scholars in analysis; Mazzoni in financial mathematics. Some of the others – Bedarida, Chella – were never fully subsumed into the Italian mathematical community. Only in the 1960s would a new interest in this discipline emerge.

5. Some Concluding Remarks

Luigi Bianchi wrote in the preface of his 1923 treatise:

> With the simplicity of its foundations, the rigor of its deductions and above all the beauty and harmony of its truths, arithmetic, this antique branch of the mathematical sciences, has always exerted a powerful fascination on the minds of the greatest mathematicians. But it is only in the past century, through the works of almost exclusively German mathematicians, that arithmetic has found, if I may say, the *royal* road, leading up to the general arithmetic of algebraic fields. And here appear fully the many links of arithmetical truths with the theory of algebra, with the theory of finite and infinite groups, and with the properties of the most remarkable transcendents of analysis, such as the exponential, the elliptic and modular functions, the automorphic functions in general, the Riemann $\zeta(s)$ function, etc. Even in geometry, arithmetical concepts find applications and essential analogies.[39]

With this by then standard motto, Bianchi, more than a century after the publication of Gauss's treatise, seems to establish a link between the Italian school he was trying to create and the German tradition of Gauss, Dirichlet, Kummer and Dedekind. However, as we have seen, his own work of the 1890s also integrated the approach of Klein and Poincaré, and the group-theoretical and geometrical aspects of the theory of complex functions occupy a crucial role in his papers, side-by-side with the purely arithmetical techniques inherited from the *Disquisitiones Arithmeticae* and from the *Vorlesungen* of Dirichlet and Dedekind.

This aspect might indicate why Italian mathematics had such a feeble tradition of higher arithmetic, even in the university curriculum. Although Genocchi, Cesàro, Bianchi, all referred to Gauss's *Disquisitiones Arithmeticae*, they relied on very different sections, and all combined their arithmetical interests with analytic ones:

[39] [Bianchi 1923], p. iii: *L'aritmetica, questo antico ramo delle scienze matematiche, colla semplicità dei suoi fondamenti, col rigore delle sue deduzioni, e soprattutto colla bellezza ed armonia delle sue verità ha sempre esercitato un fascino potente sulle menti dei più grandi matematici. Ma soltanto nel secolo scorso, per opera quasi esclusiva di matematici tedeschi, l'aritmetica ha trovato, si può dire, la via* regia*, elevandosi ad aritmetica generale dei corpi algebrici. E qui sono apparsi, completamente, i molteplici legami delle verità aritmetiche colle teorie dell'Algebra, colla teoria dei gruppi finiti ed infiniti, e colle proprietà delle più notevoli trascendenti dell'analisi, quali le esponenziali, le funzioni ellittiche e modulari, le funzioni automorfe in generale, la $\zeta(s)$ di Riemann ecc. Persino nella geometria i concetti aritmetici trovano applicazioni e corrispondenze essenziali.*

integral calculus, series, complex functions. Of course, the most algebraic aspects of the *Disquisitiones Arithmeticae*, in connection with the theory of equations, also influenced developments in Italy.[40] But the most extreme aspects of the movement of arithmetization, trying to eliminate both geometry and the theory of functions, did not seem to find their ways to Italy:[41] the problem of the reception of Gauss's treatise is thus perhaps related to the difficulties of Italian algebraic geometry to keep pace with the arithmetization of algebraic geometry in the 1930s.[42]

References

Bertrand, Joseph. 1862. *Trattato di algebra elementare*, trad. E. Betti. Firenze: Le Monnier. Original ed. *Traité élémentaire d'algèbre*. Paris: Hachette, 1850.

Bianchi, Luigi. 1889. Sulle forme quadratiche a coefficienti e a indeterminate complessi, *Atti della Reale Accademia dei Lincei. Rendiconti* 4th ser., 5(1), 589–599. Repr. in [Bianchi 1952], vol. 1, parte prima, 193–207.

———. 1890a. Sopra una classe di gruppi Fuchsiani riducibili a gruppi modulari. *Atti della Reale Accademia dei Lincei. Rendiconti* 4th ser., 6(1), 375–384. Repr. in [Bianchi 1952], vol. 1, parte prima, 208–220.

———. 1890b. Sui gruppi di sostituzioni lineari a coefficienti interi complessi. *Atti della Reale Accademia dei Lincei. Rendiconti* 4th ser., 6(1), 331–339. Repr. in [Bianchi 1952], vol. 1, parte prima, 221–232.

———. 1891a. Geometrische Darstellung der Gruppen linearer Substitutionen mit ganzen komplexen Koeffizienten nebst Anwendungen auf die Zahlentheorie. *Mathematische Annalen* 38, 313–333. Repr. in [Bianchi 1952], vol. 1, parte prima, 233–258.

———. 1891b. Sui gruppi di sostituzioni lineari e sulle forme quadratiche di Dirichlet e di Hermite. *Atti della Reale Accademia dei Lincei. Rendiconti* 4th ser., 7(2), 3–11. Repr. in [Bianchi 1952], vol. 1, parte prima, 259–269.

———. 1892a. Sui gruppi di sostituzioni lineari con coefficienti appartenenti a corpi quadratici immaginari. *Mathematische Annalen* 40, 332– 412. Repr. in [Bianchi 1952], vol. 1, parte prima, 270–373.

———. 1892b. Sui gruppi di sostituzioni lineari. *Mathematische Annalen* 42, 30–57. Repr. in [Bianchi 1952], vol. 1, parte prima, 374–409.

———. 1893a. Sopra alcune classi di gruppi di sostituzioni lineari a coefficienti complessi. *Mathematische Annalen* 43, 101–135. Repr. in [Bianchi 1952], vol. 1, parte prima, 410–453.

———. 1893b. Ricerche sulle forme quaternarie quadratiche e sui gruppi poliedrici. *Annali di matematica pura ed applicata*, 2nd ser., 21, 237–288. Repr. in [Bianchi 1952], vol. 1, parte prima, 454–515.

[40] On algebra in Italy in the XIXth and early XXth centuries, see [Brigaglia 1984], [Brigaglia 1989] and [Brigaglia, Ciliberto, Sernesi 1994].

[41] This issue should also be related to the role of applied mathematics, as opposed to pure mathematics, in the Italian tradition. On this question, see [Israel, Nurzia 1989].

[42] See [Brigaglia, Ciliberto 1995].

———. 1894a. Sulle forme quaternarie quadratiche e sui gruppi poliedrici. *Atti della Reale Accademia dei Lincei. Rendiconti* 5th ser., 3(1), 3–12. Repr. in [Bianchi 1952], vol. 1, parte prima, 516–528.

———. 1894b. Complemento alle ricerche sulle forme quaternarie quadratiche e sui gruppi poliedrici. *Annali di matematica pura ed applicata*, 2nd ser., 23, 1–44. Repr. in [Bianchi 1952], vol. 1, parte prima, 529–580.

———. 1912. *Lezioni sulla teoria aritmetica delle forme quadratiche e ternarie*. Pisa: Spoerri.

———. 1921. *Lezioni sulla teoria dei numeri algebrici e principi d'aritmetica analitica*. Pisa: Spoerri.

———. 1923. *Lezioni sulla teoria dei numeri algebrici*. Bologna: Zanichelli.

———. 1952. *Opere*, ed. Unione matematica Italiana. 11 vols. Roma: Edizioni Cremonese.

Biasini, Luciano, Capra, Luciano, Fiorentini, Mario, Pepe, Luigi. 1982. *Gianfrancesco Malfatti nella cultura del suo tempo*. Ferrara: Università degli Studi.

Bottazzini, Umberto. 1994. *Va' Pensiero*. Bologna: Il Mulino.

Brigaglia, Aldo. 1984. La teoria generale delle algebre in Italia dal 1919 al 1937. *Rivista di storia della scienza* 1, 2, 199–237.

———. 1989. L'introduction de l'algèbre moderne en Italie. *Cahier du séminaire d'histoire des mathématiques* 10, 323–349. Errata, *ibid.* 11, 129–132.

Brigaglia, Aldo, Ciliberto, Ciro. 1995. *Italian Algebraic Geometry between the Two World Wars*. Queen's Papers in Pure and Applied Mathematics 100. Kingston: Queen's University.

Brigaglia, Aldo, Ciliberto, Ciro, Sernesi, Edoardo (eds.). 1994. *Algebra e geometria (1860–1940): il contributo italiano*. Supplemento ai *Rendiconti del Circolo Matematico di Palermo*, IIe s., 36.

Brigaglia, Aldo, Scimone, Aldo. 1998. Algebra e Teoria dei Numeri. In *La Matematica Italiana dopo l'Unità.*, ed. S. Di Sieno, A. Guerraggio, P. Nastasi. Milano: Marcos y Marcos. pp. 505–567.

Brioschi, Francesco. 1863. Sulla risolvente di Malfatti per le equazioni del quinto grado. *Memorie del Reale Istituto Lombardo* 3e ser., 9, 215–231. Also pub. in *Annali di matematica pura ed applicata* 5, 233–250.

Carbone, Lucio, Nastasi, Pietro, Palladino, Franco. 1996. I Carteggi Torelli– Cesaro, Landau–Cesaro, Cipolla–Cesaro, e alcune questioni connesse. *Nuncius* 11, 152–225.

Čebyšev, Pafnuti Lvovič. 1895. *Teoria delle Congruenze*, trad. I. Massarini. Roma: Loescher.

Cesáro, Ernesto. 1883. Sur diverses questions d'arithmétique. *Mémoires de la Société royale des sciences de Liège* 2nd ser., 10, 1–360. Repr. in [Cesàro 1964–1965], pars prima, pp. 10–362.

———. 1885. Excursions arithmétiques à l'infini. Paris: Hermann. Repr. in [Cesàro 1964–1965], pars secunda, pp. 1–134.

———. 1886-1887. Fonctions énumératrices. *Annali di Matematica Pura ed Applicata* 2nd s. 14, 141–158. Repr. in [Cesàro 1964–1965], pars secunda, pp. 210–230.

———. 1894. Sur une formule empirique de M. Pervouchine. *Comptes rendus de l'Académie des sciences* 119, 848–849. Repr. in [Cesàro 1964–1965], pars secunda, pp. 417–418.

———. 1964–1965. *Opere scelte*, ed. Unione matematica italiana. Vol. 1 (in two parts): *Algebra. Serie. Teoria dei numeri*. Roma: Edizioni Cremonese.

Cipolla, Michele. 1902. La determinazione assintotica dell' n^{imo} numero primo. *Rendiconti dell'Accademia delle Scienze Fisico-matematiche di Napoli* 3th ser. 8, 132–166.

Conte, Alberto, Giacardi, Livia (eds.). 1991. *Angelo Genocchi e i suoi interlocutori scientifici. Contributi dall'epistolario.* Studi e Fonti per la Storia della Università di Torino IV. Torino: Deputazione subalpina di storia patria.

Dickson, Leonard Eugene. 1919–1923. *History of the Theory of Numbers*. 3 vols. Washington: Carnegie Institute.

Dirichlet, Johann Peter Gustav Lejeune-. 1842. Recherches sur les formes quadratiques à coefficients et à indéterminées complexes. *Journal für die reine und angewandte Mathematik* 24, 291–371. Repr. in *Werke*, ed. L. Kronecker, vol. 1, pp. 533–618. Berlin: Reimer, 1889.

———. 1887. *Lezioni sulla Teoria dei Numeri*, trad. A. Faifofer. Venezia: Tip. Emiliana.

Fricke, Robert. 1893. Über indefinite quadratische Formen mit drei und vier Veränderlichen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse*, 705–721.

Fricke, Robert, Klein, Felix. 1897. *Vorlesungen über die Theorie der automorphen Funktionen*, vol. 1. Leipzig: Teubner.

Gazzaniga, Paolo. 1885. Sui residui di ordine qualunque rispetto ai moduli primi. *Atti del Reale Istituto veneto di scienze, lettere ed arti* 6th ser., 4, 1271–1280.

———. 1885–1886. *Lezioni sulla teoria dei numeri*. Mimeographed notes. Padova.

———. 1903. *Gli elementi della teoria dei numeri*. Verona, Padova: Drucker.

Genocchi, Angelo. 1852. Note sur la théorie des résidus quadratiques. *Mémoires couronnés et mémoires des savants étrangers, Académie royale des sciences, des lettres et des beaux-arts de Belgique* 25, 1–54.

———. 1853. Démonstration d'un théorème d'Euler. *Nouvelles Annales de Mathématiques* 12, 235–236.

———.1854. Note sur une formule de M. Gauss relative à la décomposition d'un nombre en deux carrés et sur quelques formules analogues. *Nouvelles Annales de mathématiques* 13, 158–170.

———. 1864. Intorno all'equazione $x^7 + y^7 + z^7 = 0$. *Annali di matematica pura ed applicata* 1st ser., 6, 287–288.

———. 1865. Intorno ad alcune somme di cubi. *Annali di matematica pura ed applicata* 1st ser., 7, 151–158.

———. 1868–1869. Intorno ad alcune forme di numeri primi. *Annali di matematica pura ed applicata* 2nd ser. 2, 256–267.

———. 1875–1876. Intorno a tre problemi aritmetici di Pietro Fermat. *Atti della Reale Accademia delle scienze di Torino* 11, 811–829.

———. 1883. Démonstration d'un théorème de Fermat. *Nouvelles Annales de mathématiques* 3th ser., 2, 306–310.

———. 1887. Intorno alla funzione $\Gamma(x)$ ed alla serie dello Stirling che ne esprime il logaritmo. *Memorie di matematica e fisica della Società Italiana delle Scienze (detta dei XL)* 3th ser., 6-2, 1–24.

Humbert, Georges. 1920. Sur les groupes de M. Bianchi. *Comptes rendus de l'Académie des sciences* 170, 625–630.

Hurwitz, Adolf. 1895a. Die unimodularen Substitutionen in einem algebraischen Zahlenkörper. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen. Mathematische-physikalische Klasse*, 332–356. Repr. in *Mathematische Werke*, vol. 2, pp. 244–268. Basel, Stuttgart: Birkhäuser, 1963.

———. 1895b. Letter to L. Bianchi, 24 June 1895. In L. Bianchi, *Opere*, vol. XI, pp. 103–105. Roma: Edizioni Cremonese, 1959.

Israel, Giorgio, Nurzia, Laura. 1989. Fundamental Trends and Conflicts in Italian Mathematics between the Two World Wars. *Archives internationales d'histoire des sciences* 39, 111–143.

Klein, Felix. 1890. *Vorlesungen über die Theorie der elliptischen Modulfunctionen*, augm. and compl. R. Fricke, vol. 1. Leipzig: Teubner.

Kronecker, Leopold. 1885. Die absolut kleinsten Reste reller Grössen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaft zu Berlin vom Jahre 1884*, pp. 383–396 and 1045–1049. Repr. in [Kronecker 1895–1931], vol. 3, pp. 111–136.

———. 1889. Beweis des Reciprocitätsgesetzes für die quadratischen Reste. *Journal für die reine und angewandte Mathematik* 104, 348–351. Repr. in [Kronecker 1895–1931], vol. 3, pp. 137–143.

———. 1895–1931. *Werke*, ed. K. Hensel. 5 vols. in 6 parts. Leipzig, Berlin: Teubner.

Libri, Guglielmo. 1835. *Mémoires de mathématiques*. Berlin: Reimer.

Lipschitz, Rudolf. 1857. Zur Theorie der quadratische Formen. *Journal für die reine und angewandte Mathematik* 54, 193–196.

Malfatti, Gianfrancesco. 1804. Dubbij proposti al socio Paolo Ruffini sulla sua dimostrazione dell'imposibilità di risolvere le equazioni superiori al quarto grado. *Memorie di Matematica e Fisica della Società Italiana Delle Scienze* 11, 579–607. Repr. in *Opere*, ed. Unione matematica italiana, vol. 2, pp. 723–751. Roma: Edizioni Cremonese, 1981.

———. 1805. Saggio di alcuni problemi numerici. *Memorie di Matematica e Fisica della Società Italiana Delle Scienze* 12, 296–317. Repr. in *Opere*, ed. Unione matematica italiana, vol. 2, pp. 761–782. Roma: Edizioni Cremonese, 1981.

Mammone, Pasquale. 1989. Sur l'apport d'Enrico Betti en théorie de Galois. *Bolletino di storia delle scienze matematiche* 9, 143–169.

Peano, Guiseppe. 1889-1890. Angelo Genocchi. *Annuario della Royale Universit‡ di Torino*, 195–202. Repr. in *Opere scelte*, ed. Unione matematica italiana, vol. III, pp. 317–322. Roma: Edizioni Cremonese, 1959.

Picard, Emile. 1884a. Mémoire sur les formes quadratiques binaires indéfinies à indéterminées conjuguées. *Annales de l'Ecole Normale Supérieure* 3rd s., 1, 9–54. Repr. in *Œuvres*, vol. 1, pp. 381–426. Paris: CNRS, 1978.

———. 1884b. Sur un groupe de transformations des points de l'espace situés du même côté du plan. *Bulletin de la Société mathématique de France* 12, 43–47. Repr. in *Œuvres*, vol. 1, pp. 499–504. Paris: CNRS, 1978.

———. 1885. Sur les fonctions hyperabéliennes. *Journal de mathématiques pures et appliquées*, 4e s., 1, 87–128. Repr. in *Œuvres*, vol. 1, pp. 543–584. Paris: CNRS, 1978.

POINCARÉ, Henri. 1883. Mémoire sur les groupes kleinéens. *Acta mathematica* 3, 49–92. Repr. in *Œuvres*, vol. 2, pp. 258–299. Paris: Gauthier-Villars, 1916.

———. 1887. Les fonctions fuchsiennes et l'arithmétique. *Journal de mathématiques pures et appliquées* 4$^{\text{e}}$ ser., 3, 405–459. Repr. in *Œuvres*, vol. 2, pp. 461–511. Paris: Gauthier-Villars, 1916. Partial repr. in *Œuvres*, vol. 5, pp. 278–280 and 285–290. Paris: Gauthier-Villars, 1950.

SCARPIS, Umberto. 1897. *Teoria dei Numeri*. Milano: Hoepli.

SCORZA, Gaetano. 1930. In memoria di Luigi Bianchi. *Annali della Reale Scuola Normale Superiore di Pisa. Scienze fisiche e matematiche* 16, 27 pp.

SIACCI, Francesco. 1889. Cenni necrologici di Angelo Genocchi. *Memorie della reale Accademia delle Scienze di Torino* 2$^{\text{th}}$ ser., 39, 463–495.

TORELLI, Gabriele. 1901. Sulla totalità dei numeri primi fino ad un limite assegnato. *Atti dell'Accademia delle scienze fisiche e matematiche. Sezione della Società Reale di Napoli* 2$^{\text{nd}}$ ser., 11, n° 1, 1–222.

VIOLA, Carlo. 1991. Alcuni aspetti dell'opera di Angelo Genocchi riguardanti la teoria dei numeri. In [Conte, Giacardi 1991], pp. 11–29.

VII.2

Zolotarev's Theory of Algebraic Numbers

Paola Piazza

In the 1870s, the Russian mathematician Egor Ivanovič Zolotarev generalized Ernst Eduard Kummer's theory of ideal prime numbers from cyclotomic to more general extensions of the rational numbers in two stages. His first theory, [Zolotarev 1874], was based on Gauss's method of higher congruences, and did not apply to all finite extensions of the rationals; his second theory was completely general, but appeared only in 1880, [Zolotarev 1880], two years after the author's death. Indeed, Zolotarev was born in 1847, and died very young in 1878 in a carriage accident.

The fate of these theories was about as unlucky as that of their author. In spite of its originality and completeness, and in contrast to the solid mathematical reputation in Europe which Zolotarev had managed to build for himself by works on other subjects during his short life, his second theory of algebraic numbers could not hold its own as an alternative path to Dedekind's and Kronecker's approaches. This seems to be largely due to the unlucky circumstances surrounding Zolotarev's publications on the theory of algebraic numbers.

His first theory was based on a direct generalization of Kummer's theory of ideal cyclotomic primes. It worked explicitly with integral generators x of the given extension of the rationals, the decomposition of a given rational prime p in this extension being modelled by the decomposition of the minimal polynomial of x modulo p. Zolotarev himself acknowledged Gauss's theory of higher congruences, along with Joseph Alfred Serret's treatment of it, as historical inspirations and theoretical framework behind this approach.[1] Richard Dedekind claimed that he himself had first tried this kind of generalization of Kummer's approach, but had given up on it,

[1] Cf. G. Frei, chap. II.4 in this volume. Zolotarev referred to Gauss's manuscript of the planned *Caput Octavum* of the *Disquisitiones Arithmeticae*, as it appeared posthumously in vol. II of Gauss's *Werke*. He also quoted the second volume of Serret's *Cours d'Algèbre supérieure* – see [Zolotarev 1880], p. 52, footnote.

> because the theory thus constructed suffers mainly from two imperfections. The first one lies in the fact that a domain of algebraic integers is studied by first considering a certain algebraic integer and its corresponding equation, which is viewed as a congruence, and that the definitions of ideal numbers (or more precisely, of the divisibility by the ideal numbers) thus obtained, from that particular way of representing the algebraic integers, do not directly reveal the *invariance* that these notions do in fact possess. The second imperfection of this approach consists in occasional peculiar exceptional cases which require a special treatment.[2]

Dedekind's much celebrated example, from [Dedekind 1878], for the existence of such "occasional" difficulties is the extension of the rationals generated by a root of the polynomial $X^3 - X^2 - 2X - 8$. All discriminants of elements of the domain are divisible by 4, but the discriminant of the corresponding number field is not. In Kronecker's terminology, this situation is expressed by saying that the prime number 2 is an *außerwesentlicher Diskriminantenteiler* of the field in question.

Now, while Zolotarev was perfectly aware of the limitations of his first theory, he did choose to explain it once more in great detail in the first half of his long paper "Sur la théorie des nombres complexes," [Zolotarev 1880], before expounding on his second theory. He gave this paper in the summer of 1876 to Henry Resal for publication in the *Journal de mathématiques pures et appliquées*. But, as mentioned above, it was only published posthumously.

This explains why Dedekind did not know Zolotarev's second theory of algebraic numbers at the time of writing and publishing [Dedekind 1878]. But in a footnote on page 218 of [Dedekind 1878], he went on to speculate that the second theory, which Zolotarev had announced already in his 1874 thesis [Zolotarev 1874], would also be bound to fail to deal with the general case. Dedekind based this speculation on a sentence in the *Jahrbuch*-review of Zolotarev's Russian thesis. This was apparently sufficient to convince Leopold Kronecker that Zolotarev had no valid general theory, at a time when Kronecker could have known better by reading more than the beginning pages of Zolotarev's article in Liouville's *Journal*:

> Zolotarev's work in the latest issue of Resal's journal [Zolotarev 1880] contains an attempt to deal also with the divisors of the discriminant, by a theory based on that restricted way of representing the complex numbers (as entire functions of a single algebraic integer). But I think that this attempt is faulty, and according to Dedekind's publications of 1871 to which Zolotarev refers at the beginning of his paper, and which explain most clearly and acutely the necessity to abandon this

[2] [Dedekind 1878], p. 202: *weil die so entstandene Theorie hauptsächlich an zwei Unvollkommenheiten leidet. Die eine besteht darin, daß die Untersuchung eines Gebietes von ganzen algebraischen Zahlen sich zunächst auf die Betrachtung einer bestimmten Zahl und der ihr entsprechenden Gleichung gründet, welche als Kongruenz aufgefaßt wird, und daß die so erhaltenen Definitionen der idealen Zahlen (oder vielmehr der Teilbarkeit durch die idealen Zahlen) zufolge dieser bestimmt gewählten Darstellungsform nicht von vornherein den Charakter der Invarianz erkennen lassen, welcher in Wahrheit diesen Begriffen zukommt; die zweite Unvollkommenheit dieser Begründungsart besteht darin, daß bisweilen eigentümliche Ausnahmefälle auftreten, welche eine besondere Behandlung verlangen.*

> restricted foundation of complex number theory, any attempt to stick to it nonetheless, was bound to fail from the outset, because it went against the nature of things.[3]

An analogous reaction can be found in Paul Bachmann who writes at the end of a discussion of Eduard Selling's variant of Kummer's theory of ideal numbers:

> But it is unquestionable that this theory of Selling's is extraordinarily difficult and lacks transparency, and that it has been desirable to replace it with an different one. A paper by Zolotarev based on similar principles [Zolotarev 1874] does not, as far as I know, deal with the exceptional cases produced by the divisors of the discriminant at all.[4]

Notwithstanding the better reception of Zolotarev's work in Russia,[5] this is why Zolotarev's second theory of algebraic numbers, alongside his first one, failed to be taken seriously by the main actors of the 1870s and 1880s in the theory of algebraic numbers. In his famous *Zahlbericht* of 1897 (almost 20 years after Zolotarev's death), David Hilbert gave equal weight and credit to Dedekind's and Kronecker's approaches (the latter one being also represented by Kronecker's pupil Kurt Hensel) as far as the problem of *außerwesentliche Diskriminantenteiler* was concerned – see [Hilbert 1897], §13. But he did not mention at all either of Zolotarev's theories of algebraic numbers. This may well have been the ultimate fatal blow for the recognition of Zolotarev's work in this area of research. In fact, Hilbert's *Zahlbericht* became *the* authoritative source and textbook in algebraic number theory for more than one generation of mathematicians.

Looking back at this course of events today, Zolotarev's second theory of algebraic numbers looks more potent to us than his influential contemporaries would have it. We will reconstruct in section 1 below the key features of this theory in

[3] [Kronecker 1882], p. 383: *Ein Versuch auch diese [= die Primfactoren der Diskriminante] in einer Theorie mit zu umfassen, welche auf jener beschränkten Darstellungsweise der complexen Zahlen (als ganze Funktionen einer einzigen ganzen algebraischen Zahl) aufgebaut ist, liegt in der Zolotareff'schen Arbeit vor, die im neuesten Bande des Resal'schen Journals veröffentlicht ist. Dieser Versuch ist aber, wie ich glaube, verfehlt; und nach den von Zolotareff im Eingange seiner Arbeit citirten Dedekindschen Publikationen aus dem Jahre 1871, in welchen mit voller Klarheit und Schärfe die Nothwendigkeit dargethan ist, jene beschränkte Grundlage der complexen Zahlentheorie aufzugeben, musste ein Versuch, dieselbe dennoch beizubehalten, von vorn herein, als der Natur der Sache widersprechend, aussichtslos erscheinen..*

[4] [Bachmann 1905], p. 153: *Man kann jedoch nicht leugnen, dass diese Sellingsche Theorie außerordentlich schwierig und unübersichtlich, und es wünschenswert gewesen ist, sie durch eine andere zu ersetzen. Eine auf ähnlicher Grundlage beruhende Arbeit von Zolotareff* [here Bachmann quotes Zolotarev's thesis with a French title, not giving any precise reference] *über denselben Gegenstand geht, soviel mir bekannt ist, auf die Ausnahmefälle, welche die Diskrimantenteiler verursachen können, überhaupt nicht ein.*

[5] When Korkin presented Zolotarev for promotion to "extraordinary professor" of mathematics in St. Petersburg in 1876, he pointed out that the young mathematician had obtained a complete generalization of Kummer's theory of ideal numbers, without exceptions. On Zolotarev's reception in Russia, see [Piazza 1999] and references given there.

terms of localizations at rational primes p of the ring of integers of a number field, comparing it in particular to Dedekind's approach. Presented in this way the theory appears as quite analogous to a divisor theory constructed from the various p-adic completions of the number field.[6]

In section 2, we will point out technical aspects of Zolotarev's theory that seem to be analogous to Gauss's theory of complex numbers which Zolotarev surely knew.[7]

In his thesis [Zolotarev 1874], and on several other occasions, Zolotarev showed that he also knew Dedekind's ideal theory of 1871 well. Recall that Dedekind published in that year his first version of the X$^{\text{th}}$ Supplement of the *Vorlesungen über Zahlentheorie* of J. Peter G. Lejeune-Dirichlet's [Dirichlet 1871], §§159–163, pp. 423–462. In this work, Dedekind's approach still appeared in a sense closer to Kummer's theory of ideal numbers (see also section 6.2 of [Piazza 1998]), and it is conceivable that Dedekind's ideal theory of 1871 was interpreted by Zolotarev still as a generalization of Kummer's theory, in terms of ideal numbers. Dedekind presented his ideal theory again in [Dedekind 1876–77]. This second exposition was already based entirely on the concept of ideal which was presented as an independent concept. To my knowledge, Zolotarev never referred to this second version of Dedekind's theory of algebraic numbers. However, since he surely knew Dedekind's ideal theory of 1871, he may well have learned from Dedekind the definition of the ring $\mathcal{O}$ of all algebraic integers of a finite extension of the field $\mathbf{Q}$ of rational numbers, as well as the idea of generalizing Kummer's theory of ideal numbers to all such rings $\mathcal{O}$.

1. Biographical Notes on Zolotarev

Despite his young age, Zolotarev was not an outsider, but quite well-known and appreciated in the mathematical Europe of the middle 1870s. He belonged to the influential mathematical school around Pafnuti Čebyčev, a school that had high reputation at that time especially in France and in Germany. During his years of studies, Zolotarev had the opportunity to visit Berlin, Heidelberg and Paris, for four months (precisely, in the summers of 1872 and 1876). He attended lectures by Karl Weierstrass, Gustav Kirchhoff, and Kummer. During his stay abroad, he also met Charles Hermite who was very much interested in work of Zolotarev and Aleksandr Korkin on the arithmetic theory of quadratic forms. Zolotarev's impressions and evaluations of various theories and trends of mathematics in Germany and in France at that time are contained in several letters he wrote to Korkin.[8]

[6] Cf. the recent paper [Neumann 2002].

[7] Zolotarev showed his knowledge of Gauss's theory of the Gaussian integers $\mathbf{Z}[i]$ in particular in [Zolotarev 1874], in the introduction and in a short paragraph on the history of algebraic numbers – see [Zolotarev 1931–1932], pp. 240–241. Specifically, he pointed out in that paragraph that the Euclidean algorithm is valid in $\mathbf{Z}[i]$ and in some other domains of algebraic integers, but that it does not hold in general (for which he refers to Kummer's theory of ideal numbers for cyclotomic integers).

[8] This correspondence consists of 64 letters, all contained in the second volume of [Zolotarev 1931-1932]. These letters also contain queries concerning concrete mathematical problems.

Fig. VII.2. Egor Ivanovich Zolotarev (1847–1878)
From [Zolotarev 1931]

In 1876, Zolotarev was appointed professor and elected member of the St. Petersburg Academy of Sciences, which counted among its members many French and German mathematicians.[9] Zolotarev collaborated with the *Jahrbuch über die Fortschritte der Mathematik* from the very beginning of the seventies until 1877.[10]

Thus, Zolotarev was well appreciated in Russia and in Europe. At the same time, his writings show that he was perfectly familiar with mathematical developments in his fields of interest in Russia as well as in France and Germany. Already in his thesis [Zolotarev 1874] for instance, he refers to Dirichlet, Kummer, Hermite, Kronecker, Eisenstein, Serret, Bachmann, and Carl Gustav Jacob Jacobi.

[9] For instance Joseph Liouville and Carl Wilhelm Borchardt. Borchardt was at that time the principal editor of the *Journal für die reine und angewandte Mathematik*. In a letter to Čebyčev of 1879, Borchardt expressed his gratitude for the election as a member of the Academy and he recalled the late mathematician Zolotarev with most respectful words: "I am very moved by the honour conferred to me to be elected as a corresponding member of your famous Academy. Some years ago, I had the great pleasure to receive the visit of your fellow-countryman and pupil Zolotarev. I later sent him a reprint of my memoir on the arithmetic-geometric means of four numbers, and I was deeply grieved when the post office sent it back with the mention of his death" – see Section 8.1 of [Piazza 1998].

[10] Zolotarev was referred to in the *Jahrbuch* as *Prof. Zolotareff in Petersburg* even before his appointment in 1876.

As to the poor reception of his second theory of algebraic numbers (outside Russia), which was already discussed in the introduction, we know that Zolotarev submitted his work "Sur la théorie des nombres complexes" to the *Journal de Mathématiques pures et appliquées* as early as 1876, but the paper was published only in 1880. It was reported on also in the *Jahrbuch*, but that report was not at all exhaustive, and much shorter than the one about [Zolotarev 1874]. The only hint at Zolotarev's second theory of algebraic numbers in this review is the statement that "the thorough treatment of division is new."[11] The reasons for the delay of the publication of Zolotarev's main paper [Zolotarev 1880] are not completely clear. It may have had something to do with the change of editor of Liouville's *Journal* in 1875, when Resal took the journal over from Liouville.

2. Zolotarev's Second Theory of Algebraic Numbers

Let us briefly look back to the origin of the theory of ideal numbers. Ernst Eduard Kummer had been the first to overcome the failure of unique factorization in domains of cyclotomic integers. He assumed that irreducible elements which are not prime were actually products of ideal prime factors. In 1871, Richard Dedekind generalized Kummer's theory to every ring $\mathcal{O}$ of algebraic integers. His fundamental idea was to replace Kummer's concept of ideal number by the concept of ideal. Specifically, he substituted Kummer's ideal number with the set of algebraic integers that this number divides and called this set an *ideal*. Following the example of the divisibility laws in $\mathbf{Z}$, he proved that every ideal in $\mathcal{O}$ could be factorized uniquely into a product of prime ideals. In order to prove this, Dedekind needed a definition of divisibility among ideals: an ideal $\mathcal{A}$ divides another ideal $\mathcal{B}$ if and only if $\mathcal{B} \subset \mathcal{A}$. This definition is connected with that of the product; there exists an ideal $\mathcal{C}$ such that $\mathcal{AC} = \mathcal{B}$. Moreover, it was necessary to define something that could play the role of the absolute value in $\mathbf{Z}:$ the (absolute) norm of an ideal, i.e., the cardinality of $\mathcal{O}/\mathcal{A}$. Finally, Dedekind had to introduce the concept of prime ideal, which in this context is an ideal with only two divisors, namely itself and the ring $\mathcal{O}$ of algebraic integers in question. These prime ideals played just the same role for the new theory as the prime numbers for the divisibility theory in $\mathbf{Z}$.

In his second theory of algebraic numbers, Zolotarev also generalized completely Kummer's theory by developing a construction which we will re-interpret here in modern terms as a divisibility theory in the ring $\mathcal{O}_{(p)}$ of the so-called algebraic p-integers, where p is a fixed rational prime number. This modern re-writing is presented for the convenience of the modern reader. Zolotarev himself did not take such a structural approach to these algebraic questions, but developed a certain divisibility theory for algebraic integers relative to the fixed prime p, establishing for it step by step the existence of greatest common divisors, and whatever else he needed to finally prove unique factorization into ideal factors – see [Zolotarev 1880], §§ 27 ff.

[11] *Jahrbuch über die Fortschritte der Mathematik* 12 (1880), 125, review of [Zolotarev 1880] by Dr. Simon, Berlin: *Neu ist die eingehende Behandlung der Division.*

Let

$$\mathbf{Z}_{(p)} = \{s \in \mathbf{Q} \mid s = \frac{M}{N},\ M, N \in \mathbf{Z},\ N \notin p\mathbf{Z}\}.$$

Given a finite algebraic extension K of the rational number field $\mathbf{Q}$ of degree n, the ring $\mathcal{O}_{(p)}$ of algebraic p-integers of K can be defined to be the integral closure of $\mathbf{Z}_{(p)}$ in K. Explicitly

$$\mathcal{O}_{(p)} = \{\alpha \in K \mid \alpha = \frac{\beta}{N},\ \beta \in \mathcal{O},\ N \in \mathbf{Z},\ N \notin p\mathbf{Z}\}.$$

In terms of modern commutative algebra, $\mathcal{O}_{(p)}$ is a semilocal principal ideal domain (PID). Let $\pi_1, \pi_2, \ldots, \pi_g$ be the prime elements of $\mathcal{O}_{(p)}$. Then $\pi_1\mathcal{O}_{(p)}, \ldots, \pi_g\mathcal{O}_{(p)}$ are all the distinct prime ideals of $\mathcal{O}_{(p)}$.

Let us go back to Zolotarev's original construction and analyze its main steps. Starting from the domain $\mathcal{O}$ of all algebraic integers of K, and introducing the concept of *divisibility with respect to the modulus p* among its elements,[12] Zolotarev gave the following definitions. Call the p-norm of an algebraic p-integer α, denoted by $n(\alpha)$, the highest power of p dividing the norm $N_{K/\mathbf{Q}}(\alpha)$. Every element $\alpha \in \mathcal{O}$ (or in $\mathcal{O}_{(p)}$) such that $n(\alpha) = 1$ is regarded by Zolotarev as unit with respect to the modulus p (it *is* a unit in $\mathcal{O}_{(p)}$).

Then, Zolotarev fixed a certain system of representatives in $\mathcal{O}$ of the residue classes of $\mathcal{O}/p\mathcal{O} = \mathcal{O}_{(p)}/p\mathcal{O}_{(p)}$. Zolotarev considered the prime number p to stay prime in $\mathcal{O}$ if every representative of a non-trivial class of $\mathcal{O}/p\mathcal{O}$ is a unit in $\mathcal{O}_{(p)}$. For the other prime numbers p, Zolotarev chose a particular set of representatives for the residue-classes of $\mathcal{O}/p\mathcal{O}$; he took representatives which have minimal p-norm within their residue-class. Let

$$A = \{\alpha_1, \ldots, \alpha_r\}, \qquad r = p^n - 1.$$

be a set of such minimal representatives of the non-trivial classes of $\mathcal{O}/p\mathcal{O}$. Then he proved the key technical result of his theory – cf. [Zolotarev 1878]:

Zolotarev's Fundamental Lemma. (1) Let $\alpha \in A$. Then α divides p in $\mathcal{O}_{(p)}$.
(2) Let $\beta \in \mathcal{O}_{(p)}$, but $\beta \notin p\mathcal{O}_{(p)}$, and assume that $n(\beta) > 1$. Then there exists $\alpha \in A$ such that $n(\alpha) > 1$ and α divides β in $\mathcal{O}_{(p)}$.

Given this, Zolotarev looked for elements $\pi \in \mathcal{O}$ which are irreducible with respect to to the modulus p, i.e., irreducible in $\mathcal{O}_{(p)}$. Specifically, he defined:[13]

Definition. Let $\pi \in \mathcal{O}_{(p)}$ with $n(\pi) > 1$. Then π is irreducible in $\mathcal{O}_{(p)}$ if π divides γ in $\mathcal{O}_{(p)}$ for every $\gamma \in \mathcal{O}$ not coprime with π in $\mathcal{O}_{(p)}$.

[12] This notion, extended to the ring $\mathcal{O}_{(p)}$, amounts to divisibility there – see [Zolotarev 1880], in particular §§27 ff. Explicitly, if $\alpha, \beta \in \mathcal{O}$, then α *divides* β *with respect to the modulus* p, if there exist $\delta \in \mathcal{O}$ and $H \in \mathbf{Z}$, $H \notin p\mathbf{Z}$, such that $\alpha\delta = \beta H$.

[13] Notice that two elements α and β in $\mathcal{O}$ are not coprime with respect to to the modulus p, i.e., not coprime in $\mathcal{O}_{(p)}$, if they have a common non-unit factor in $\mathcal{O}_{(p)}$. Note that in the following definition it is equivalent to allow γ in $\mathcal{O}$ or in $\mathcal{O}_{(p)}$.

If an irreducible element π exists, then by condition (2) of Zolotarev's Fundamental Lemma, π can be taken with minimal p-norm in its residue-class, i.e., π can be taken to belong to A. Using his Fundamental Lemma again, Zolotarev easily proved that irreducible elements π do exist. Inside A we find (up to units) all the finitely many irreducible π's of $\mathcal{O}_{(p)}$. Zolotarev proved that they are prime elements. It is then straightforward to show that $\mathcal{O}_{(p)}$ is a unique factorization domain with finitely many prime elements, and in fact is a Dedekind domain.[14]

Zolotarev essentially reached these results by exploiting some properties of the p-norm, and one may note that these same steps were essentially followed also by Kummer in the case of cyclotomic integers. More precisely, let $\pi_1, \pi_2, \ldots, \pi_g$ be the distinct irreducible elements in $\mathcal{O}_{(p)}$. Then Zolotarev proved that, if $\beta \in \mathcal{O}_{(p)}$ is divisible by π_i exactly λ_i times, then $n(\beta) = p^{\lambda_1 f_1 + \cdots + \lambda_g f_g}$, where $n(\pi_i) = p^{f_i}$. (This is proved using the fact that, if p decomposes into irreducibles in $\mathcal{O}_{(p)}$ (up to units) as $\pi_1^{e_1} \cdots \pi_g^{e_g}$, and if $\alpha \in \mathcal{O}_{(p)}$ is divisible by π_i at least $e_i s$ times, for $i = 1, \ldots, g$, with a certain $s > 0$, then p^s divides α in $\mathcal{O}_{(p)}$.)

From these results, Zolotarev deduced the

Theorem. Let α and β be in $\mathcal{O}$. Then β divides α in $\mathcal{O}$ if and only if β divides α in $\mathcal{O}_{(p)}$, for every prime number p.

To every irreducible element π in $\mathcal{O}_{(p)}$, Zolotarev associated an ideal prime factor $\mathcal{P}$ of p in $\mathcal{O}$ by the rule that for all $\alpha \in \mathcal{O}_{(p)}$ and all $k \geq 0$ one have

$$\mathcal{P}^k \mid\mid \alpha \qquad \Longleftrightarrow \qquad \pi^k \mid\mid \alpha \quad \text{in } \mathcal{O}_{(p)}.$$

The elements in $\mathcal{O}_{(p)}$ this correspond bijectively to formal products of prime divisors. It then follows from the above theorem that, if $\alpha, \beta \in \mathcal{O}$ have the factorizations

$$\alpha = \mathcal{P}_1^{a_1} \cdots \mathcal{P}_g^{a_g}, \qquad \beta = \mathcal{P}_1^{b_1} \cdots \mathcal{P}_g^{b_g},$$

then $\beta \mid \alpha$ in $\mathcal{O}$ if and only if $b_i \leq a_i$ for all $i = 1, \ldots, g$.[15]

3. The Gauss-Kummer Tradition

In this section, we point out a few technical details which are shared by Carl Friedrich Gauss and some of his followers, including Zolotarev. Gauss's study of the ring $\mathbf{Z}[i]$ represents the first historical example of an analysis of the divisibility theory in a ring of algebraic integers different from $\mathbf{Z}$. When proving the unicity of the factorization in $\mathbf{Z}[i]$ in his 1832 "Theoria residuorum biquadraticorum commentatio secunda," Gauss stressed the analogies between the properties of divisibility in $\mathbf{Z}$ and in the ring $\mathbf{Z}[i]$, which is also an Euclidean domain.[16] Gauss based his proofs on the properties of the norm in $\mathbf{Z}[i]$, and particularly on the nature of the norm of

[14] Cf. [Piazza 1998].

[15] See [Piazza 1998] for a detailed discussion of how this induces a theory of divisors on $\mathcal{O}$.

[16] See [Gauss 1863/1876], p. 118, where he proved the Euclidean algorithm; the unique factorization for $\mathbf{Z}[i]$ is proved a few pages earlier, [Gauss 1863/1876], p. 108.

complex primes. It may or may not have been due to a direct influence of Gauss, that Zolotarev (and before him also Kummer) exploited the properties of the norm in order to prove the unique factorization in ideal prime numbers.

In a similar vein, one may note that minimal (in a suitable sense) systems of representatives have played an important role in divisibility theories before Zolotarev was led to his representatives that have minimal p-norm in their residue class. Taking the lead from the classical representatives for the integers *modulo n* described in the *Disquisitiones Arithmeticae*, art. 4, Gauss naturally chose representatives of $\mathbf{Z}[i]$ modulo β whose norms are $\leq \frac{1}{2}N(\alpha)$ – see [Gauss 1863/1876], pp. 113-114. To my knowledge, Gauss was the first mathematician to have chosen a system of representatives where each representative is taken with minimal norm in its residue-class.

Let us mention in passing the paper of Gotthold Eisenstein [Eisenstein 1844], in which he proves the cubic reciprocity law by using the ring $\mathbf{Z}[\rho]$, where ρ is a cubic root of unity. Here Eisenstein underlined the general analogies between the divisibility laws in $\mathbf{Z}[i]$ and $\mathbf{Z}[\rho]$, claiming that one can find in $\mathbf{Z}[\rho]$ a complete system of representatives modulo a given element in the way described by Gauss for $\mathbf{Z}[i]$ – see [Eisenstein 1844], p. 290.

Finally, note that some fundamental ideas of Gauss's divisibility theory in $\mathbf{Z}[i]$ are to be found in Kummer's theory of ideal numbers for cyclotomic integers. It was already observed that Kummer's proof of unique factorization into ideal prime numbers is based on the properties of the norm of cyclotomic integers. Furthermore, the starting point of Kummer's theory was the search of a cyclotomic integer whose norm is exactly equal to a prime number p. In fact, this implies that this integer stays prime in the cyclotomic extension considered. In the case of $\mathbf{Z}[i]$, Gauss had already shown that an integer of norm exactly equal to p is necessarily prime – see [Gauss 1863/1876], p. 105. Besides, in order to find a cyclotomic integer of norm p, Kummer remarked first that if p divides the norm of a cyclotomic integer, then that integer contains a prime factor of p – see [Kummer 1975], p. 200, p. 222 and p. 226.

In the easy case where $\mathbf{Z}[\alpha]$, with $\alpha \neq 1$ a primitive n-th root of 1, is a unique factorization domain, it was clear to Kummer how to find the prime factors of p. In fact, he just had to choose among the cyclotomic integers whose norm is divisible by p the elements with minimal norm.[17] If $\mathbf{Z}[\alpha]$ is not a unique factorization domain, Kummer realized that he was able to find integers whose norm is divisible exactly by p but not equal to p. Those elements he regarded as integers containing just one prime factor of p.

In conclusion, whether or not consciously following up Gauss's lead on these technical matters, both Kummer (for cyclotomic integers) and Zolotarev (in complete generality) carried out a kind of local approach to the divisibility theory of algebraic integers, which was one of the historical avenues of the further development of Gauss's higher arithmetic.

[17] [Kummer 1975], p. 185:... *et ex omnibus iis numeris, quarum normae ... factorem p habent, eam eligimus quae simplicissima sit, et norman quam minimam habere videatur.*

References

BACHMANN, Paul. 1905. *Zahlentheorie.* vol. V: *Allgemeine Arithmetik der Zahlenkörper*. Leipzig: B.G. Teubner.

DEDEKIND, Richard. 1930–32. *Gesammelte mathematische Werke*, ed. R. Fricke, E. Noether, O. Ore. 3 vols. Braunschweig: Vieweg.

———. 1876–77. Sur la théorie des nombres entiers algébriques. *Bulletin des sciences mathématiques et astronomiques* 1st ser. 11 (1876), 278–293; 2nd ser. 1 (1877), 17–41, 69–92, 144–164, 207–248. Partly repr. in [Dedekind 1930–32], vol. 3, pp. 263–296.

———. 1878. Über den Zusammenhang zwischen der Theorie der Ideale und der Theorie der höheren Kongruenzen. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften zu Göttingen* 23, 1–23. Repr. in [Dedekind 1930–32], vol. 1, pp. 202–232.

DIRICHLET, J. Peter Gustav LEJEUNE-. 1871. *Vorlesungen über Zahlentheorie*, ed. R. Dedekind. 2nd ed. Braunschweig: Vieweg.

EISENSTEIN, Gotthold. 1844. Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. *Journal für die reine und angewandte Mathematik* 27, 289–310.

GAUSS, Carl Friedrich. 1863. *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen. Göttingen: Universitäts-Druckerei. 2nd ed., 1876.

HILBERT, David. 1897. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4, 175–546. Repr. in *Gesammelte Abhandlungen*, vol. 1, pp. 63–363. Berlin, Heidelberg, etc.: Springer, 1932; 2nd ed., 1970.

KRONECKER, Leopold. 1882. *Grundzüge einer arithmetischen Theorie der algebraischen Grössen. Festschrift zu Herrn Ernst Kummers fünfzigjährigem Doctor-Jubiläum, 10. September 1881.* Berlin: Reimer. Repr. in *Journal für die reine und angewandte Mathematik* 92, 1–122. Repr. in *Werke*, ed. K. Hensel, vol. 2, pp. 239–387. Leipzig: Teubner, 1897.

KUMMER, Ernst Eduard. 1975. *Collected Papers*, vol. I, ed. A. Weil. Berlin, etc.: Springer.

NEUMANN, Olaf. 2002. Was sollen und was sind Divisoren? *Mathematische Semesterberichte* 48, 139–192.

PIAZZA, Paola. 1998. *Zolotarev's foundation of algebraic number theory*. Doctoral Dissertation, Università degli Studi di Messina. Messina-Palermo.

———. 1999. Egor Ivanovitch Zolotarev and the theory of ideal numbers for algebraic number fields. *Rendiconti del circolo matematico di Palermo* 2nd ser. 61, 123–150.

ZOLOTAREV, Egor Ivanovich. 1931–32. *Polnoe Sobranie Sochineny Egora Ivanovicha Zolotareva* (Collected Papers of Egor lvanovich Zolotarev). 2 vols. Leningrad: V.A. Steklov Institute of Physics and Mathematics.

———. 1874. *Teoriia tsielykh kompleksnykh chisel s prilozheniem k integral'nomu ischisleniin* (Theory of complex integer numbers, with an application to the integral calculus). Doctoral Dissertation. St. Petersburg: Tip. Iakobsona. Repr. in [Zolotarev 1931–1932], vol. 1, pp. 161–300.

———. 1878. Sur les nombres complexes. *Bulletin de l'Académie de St. Petersbourg*, 3rd ser. 24, 310–317. Repr. in [Zolotarev 1931–1932], vol. 1, pp. 361–368.

———. 1880. Sur la théorie des nombres complexes. *Journal de mathématiques* 3rd ser. 6, 51–94, 129–166. Repr. in [Zolotarev 1931–1932], vol. 1, pp. 72–179.

VII.3

Gauss Goes West: The Reception of the *Disquisitiones Arithmeticae* in the USA

DELLA FENSTER

1. Early Mathematics in the USA

When Gauss's *Disquisitiones Arithmeticae* appeared in 1801, the 25-year-old United States of America consisted of 16 states that geographically spanned the east coast from New Hampshire to Georgia and included Kentucky and Tennessee. Settled primarily by farmers, clergyman, and artisans in the sixteenth and seventeenth centuries, the needs for mathematics were very limited. The "slender source" for mathematics in the sixteenth- and seventeenth-centuries was Astronomy, to aid the clergy as they set the days of Easter, Christmas, and the various Saints holidays.[1] Harvard College was founded in 1636 to train clergy with no attention to mathematics. The College of William and Mary was established in 1693 with public funds but no focus on mathematics.

> The century that saw the work of Galileo, Kepler, Gilbert, Napier, Fermat, Descartes, Pascal, Huygens, Newton, and Leibniz in countries from which the settlers had come, saw among the intelligentsia no apparent appreciation of the discoveries of scholars of this class.[2]

The eighteenth century brought a slight interest in mathematics to America, largely within the broader framework of learned societies like The American Philosophical Society, founded in 1743, and the American Academy of Arts and Sciences, founded in 1780, and their publications. America produced no mathematicians of any international significance in the eighteenth century. Two classes of scholars existed: (1) astronomers and (2) public leaders such as Thomas Jefferson and Benjamin Franklin who promoted the study of mathematics.

[1] See [Smith, Ginsburg 1934], p. 5.

[2] See [Smith, Ginsburg 1934], pp. 13–14.

This was the mathematical terrain in America when Gauss unraveled the genesis of the *Disquisitiones Arithmeticae* in his preface. "What happened was this", Gauss began.

> Engaged in other work I chanced on an extraordinary arithmetic truth (if I am not mistaken, it was the theorem of art. 108). Since I considered it so beautiful in itself and since I suspected its connection with even more profound results, I concentrated on it all my efforts in order to understand the principles on which it depended and to obtain a rigorous proof of it. When I succeeded in this I was so attracted by these questions that I could not let them be. Thus as one result led to another ....[3]

As Gauss described the very essence of mathematical research in 1801, advanced mathematics was essentially unknown across the Atlantic.

Things began to change in the final quarter of the nineteenth century. Karen Parshall and David Rowe, [Parshall, Rowe 1994], suggest that an American mathematical research community emerged from 1876 to 1900. As the title of their book indicates, the efforts of the Englishman James Joseph Sylvester, the German Felix Klein, and the American Eliakim Hastings Moore significantly influenced this development.

Sylvester had arrived in 1876 to head the mathematics department at the brand new Johns Hopkins University, the first American institution of higher education focused not only on teaching but also on graduate studies and research. His mathematics department soon produced research-level work that caught the attention of mathematicians abroad [Parshall 1988]. When Sylvester returned to England in 1883 to occupy the Savilian Chair of Geometry at New College, Oxford, however, the other American colleges could not adequately fill the void he left; they simply did not have faculties equipped to pursue mathematics at the research level.

Americans next turned primarily to Felix Klein in Germany for their training in mathematics. The extent of Klein's influence on American mathematics was made clear in 1893, when he participated both at the Americans' invitation and as the official emissary of the Prussian government in the Mathematical Congress held in Chicago in conjunction with the World's Columbian Exposition. He followed this visit with a two-week-long Colloquium in nearby Evanston, Illinois. The timing of the Congress and the Colloquium lectures proved crucial to the American mathematical community in general and to the one-year-old University of Chicago in particular.

The "notable and inspiring group"[4] of Chicago mathematicians helped pave the way for the fledgling New York Mathematical Society (founded in 1888) to grow into the American Mathematical Society in 1894. Moreover, Klein's visit "clearly signaled his desire to bow out gracefully after a decade of involvement in the American mathematical scene." The University of Chicago Department of Mathematics, with Eliakim Hastings Moore serving as its chair, soon emerged "not

[3] See Gauss, *Disquisitiones Arithmeticae*, preface. The "theorem of art. 108" alluded to states that -1 is a quadratic residue of all prime numbers of the form $4n + 1$ and a nonresidue of prime numbers of the form $4n + 3$.

[4] See [Birkhoff 1938], p. 273.

only as the leading center for mathematics in the United States but also as the first American institution of higher education to offer mathematical training comparable to that available at leading European universities."[5]

Owing to its successful implementation and continuation of a commitment to high research standards, the University of Chicago held a unique position among American institutions in the closing decade of the nineteenth century. Moore and his German colleagues, Oskar Bolza, and Heinrich Maschke sought to build and succeeded in forming a mathematics department that promoted original research, quality publications, and a broad view of the American mathematical community. The strong institutional and departmental philosophy inherent in these goals thus made the University of Chicago a viable option for Leonard Eugene Dickson as well as other aspiring American mathematicians, including Oswald Veblen, Gilbert Bliss, George D. Birkhoff, and R.L. Moore.

2. Leonard Dickson's Historical Project

Born in 1874 in Independence, Iowa, Dickson spent his boyhood in Cleburne, Texas, and attended the University of Texas for his undergraduate and master's training in mathematics. While Dickson pursued a Ph.D. at the young Chicago Mathematics Department from 1894 to 1896, the then group-theoretically minded E.H. Moore inspired him to write a thesis on what we would call permutation groups. Although group theory would remain among Dickson's research interests throughout his career, he would add finite field theory, invariant theory, the theory of algebras and number theory to his repertoire of research interests. In the spring of 1900, just a few months past his twenty-sixth birthday and roughly one hundred years after the appearance of the *Disquisitiones Arithmeticae*, the Chicago Mathematics Department invited Dickson to join them as an assistant professor. From this position, Dickson made significant contributions to the consolidation and growth of the algebraic tradition in America. Specifically, Dickson spent forty years (all but the first two) of his professional career on the faculty at Chicago where he directed 67 Ph.D. students, wrote 18 books and roughly 300 manuscripts, served as editor of the *American Mathematical Monthly* and the *Transactions of the American Mathematical Society*, and guided the American Mathematical Society as its president from 1916 to 1918.

Dickson arrived on the mathematical scene as America's mathematical research community came together and pursued his career as that group consolidated and grew. Thus Dickson's mathematical contributions constitute a prominent and influential example of how Gauss's ideas took shape in America's young research community. The somewhat surprising genesis of many of these investigations begins with Dickson's three-volume *History of the Theory of Numbers*.

This 1500 page historical account of the theory of numbers appeared in three installments in 1919, 1920, and 1923 and is still in print today.[6] This latter fact would

[5] The last two quotes are from [Parshall, Rowe 1994], pp. 360–361.

[6] Thus, one may consider Dickson's *History of the Theory of Numbers*, as among the "[f]ew books on the history of mathematics" that were "written over fifty years ago" and continue "to attract many readers today." [Rowe 2001], p. 590.

certainly please Dickson. He not only consulted an impressive amount of sources from American and European libraries to write the text, but he also labored to secure – and maintain – a publisher for this work. Aided by Felix Klein, Dickson's first book, *Linear Groups with an Exposition of the Galois Field Theory*, had appeared in 1901 under the Teubner label.[7] But Dickson wanted an American publisher for his historical compendium. He approached the Carnegie Institution, one of America's new philanthropic organizations, with his idea.

In 1902, Andrew Carnegie, the Scottish born American emigrant who built an empire of steel in the last half of the nineteenth century, allocated $10,000,000 in bonds to found the Carnegie Institution of Washington (CIW) to improve and extend "the opportunities for study and research" in America.[8] Dickson had this precise goal for mathematics, and for more than three decades he appealed to the CIW on behalf of American mathematics.

In February of 1911, with his mathematical research interests focused primarily in invariant theory, Dickson proposed what must have been an intriguing idea to R. S. Woodward, president of the Carnegie Institution. Dickson began:

> It would seem desirable to have undertaken in this country something of the kind done by the British Association, the Deutsche Mathematiker-Vereinigung, etc., in the preparation by specialists of note of extensive Reports each covering an important branch of science. Experience has shown that frequently such a report contains important new results to which the author was led in attempting to complete certain investigations, or to connect them with other lines.... To take a specific case, the theory of numbers ...[9]

Dickson made this appeal to Woodward at a time when American mathematicians "felt a growing independence from Europe in research" but still "saw the need to gain independence with respect to the publication system as well" [Siegmund-Schultze 1997], p. 141. In his address and subsequent publication "Mathematical Progress in America," retiring American Mathematical Society President Thomas Fiske had called for an "English translation of the new German encyclopedia of mathematics ... to spread throughout this land of seventy-five million inhabitants a knowledge of, and an interest in, advanced mathematics."[10] With his fierce devotion to placing American mathematics on a firm foundation, Dickson would have never proposed such a translation. In fact, Dickson made a more nationalistic proposal: the publication of an encyclopedia of the same quality and influence, only written and published by American sources. Perhaps, this same nationalism motivated, at least in part, Dickson's plans for the *History*.[11]

[7] See [Parshall 1991].

[8] See [Carnegie 1902], p. xi.

[9] Leonard Dickson, letter to R.S. Woodward, February 11, 1911. Carnegie Institution Archives, Washington DC, Dickson Papers.

[10] Quoted from [Siegmund-Schultze 1997], p. 140.

[11] In his letter to R. S. Woodward of April 26, 1919 (Carnegie Institution Archives, Washington DC, Dickson Papers), for example, Dickson again indirectly associated his *History of the Theory of Numbers* with the German and French encyclopedias. Note in passing

Dickson clearly wanted an American publisher, but he recognized that finding one would be difficult. At the close of his two-page letter to Woodward, he expressed doubt "that an [A]merican publisher of textbooks would undertake quite so ambitious a volume as I plan." Consequently, he continued, "it occurred to me to try to enlist the good offices of the Carnegie Institution of Washington. Would you be inclined to favor such a publication in case your referees should report favorably as to the value of the work?" When Woodward replied positively, Dickson began an extended correspondence intended to sell his idea to the Carnegie Institution. This effort supports Reinhard Siegmund-Schultze's conclusion that "the lack of governmental support [for publishing mathematical research] and the undeveloped state of commercial scientific publishing up until the end of the 1930s forced American mathematicians to look for other sources of support, especially philanthropic foundations."[12]

Dickson had not always been successful with his requests for funds from the Carnegie Institution. In 1903, for example, Dickson asked the one-year-old Carnegie to publish a book entitled *Analytic Group Theory in a General Field*. Frank Morley, an influential member of the CIW's Mathematics Advisory Committee, described the printing of the manuscript as "eminently desirable."[13] Morley, however, situated his comments within his larger aims for CIW support for mathematics. Consequently, Dickson's book proposal landed in a morass of policies – or, more accurately, lack of policies – regarding CIW funds for publications in mathematics. Although the CIW had recommended publishing his text as one of their shorter monographs among themselves, they had, apparently, not communicated this information to Dickson.[14] This confusion contributed to Dickson's decision to withdraw the manuscript and submit, instead, an application for a six-month appointment as a Carnegie *Investigator*.[15] The CIW approved Dickson's application for a *Research Assistant* from April–October, 1904.[16] In his formal letter of acceptance, Dickson indicated to Charles Walcott, Secretary of the CIW, that, with help from the University of Chicago, he planned to stretch these six months into a full year of "solid" research, "the opportunity I have so much hoped for."[17] By comparison, at about the same time, the Carnegie denied support to solid American mathematicians such as C.S. Peirce and Oswald Veblen. Dickson maintained a consistent correspondence with the Carnegie regarding mathematical results he obtained during his tenure as a

that Dickson's work was not the first historical study of mathematics by an American; the priority is Florian Cajori's, see [Cajori 1894]. For a brief overview of early American contributions to the history of mathematics see [Smith, Ginsburg 1934], pp. 160–162.

[12] See [Siegmund-Schultze 1997], pp. 159–160.

[13] See letter Morley to Gilman, April 18, 1903. All letters quoted here are from the Carnegie Institution Archives, Washington DC.

[14] See letter Walcott to Billings, May 15, 1903.

[15] See letter Dickson to Gilman, September 10, 1903.

[16] The nebulous application process at the CIW is reflected in Dickson's application as an Investigator and his appointment as a Research Assistant. For more on the CIW and its early support of mathematics see [Fenster, 2003].

[17] See letter Dickson to Walcott, March 4, 1904.

research assistant. But he did not request funds for another project until he broached the idea of his historical study in 1911.

Other notable – and, for that matter, not so notable – mathematicians received support from the Carnegie Institution in its early years. Ernest J. Wilczynski and Arthur B. Coble were among the few who succeeded in securing funds. James Byrnie Shaw published the first book on mathematics with the Carnegie Institution, [Shaw 1907]. Derrick N. Lehmer, who earned his Ph.D. under E.H. Moore at the University of Chicago in 1901, published his *Factor Table for the First Ten Millions*, [Lehmer 1910], with the CIW. In 1914, they published Lehmer's *List of Prime Numbers from 1 to 10,006,721*, [Lehmer 1914].

The titles of these publications alone suggest a trend in Carnegie support. It seems the Carnegie Institution was more inclined to publish compendia or tables, that is, works seen as being of general interest rather than specialized research monographs. Dickson's proposed history fit this prescript. These efforts not only pre-date the first world war, but their focus stands in marked contrast to Oswald Veblen's efforts in the 1920's to secure external funds for American mathematics by linking it with the natural sciences. Factor tables and lists of prime numbers belong to the most pure branch of mathematics. The Carnegie Institution could not foresee how this extensive work would influence Dickson's mathematical researches. But perhaps Dickson could?

A. Adrian Albert, Dickson's most distinguished student, reported that "[Dickson] always stated that he had always wished to work in the theory of numbers and that he wrote his monumental three-volume *History of the theory of numbers* so that he could know all of the work which had been done in the subject."[18] Although Dickson described his motivation in more altruistic terms, a look at his subsequent mathematics seems to confirm Albert's comment. Let us now first take a look at Dickon's *History* as a text, and then move on to the mathematics that grew out of it.

3. The Text of Leonard Dickson's *History of the Theory of Numbers*

Dickson's description of this historical undertaking as "serious, useful work"[19] proved more than accurate. This was no hastily written history of number theory. On the contrary, Dickson had planned both the content of his project and the precise method he would follow to present the details of his study. He revealed the scope of his plans in the preface to the first volume when he explicitly stated his bold intention to "give an adequate account of the entire literature of the theory of numbers."[20] As for his method, Dickson viewed it as

> inconceivable that any one would desire this vast amount of material arranged other than by topics. … What is generally wanted is a full and correct statement of the facts, not an historian's personal explanation of those facts. The more completely the historian remains in the background or the less conscious the reader is of the historian's personality, the better the history. Before writing such a history, he

[18] See [Albert 1955], p. 333.

[19] See [Dickson 1919–1923], vol. 2, p. xxi.

[20] See [Dickson 1919–1923], vol. 1, p. iii.

> must have made a more thorough search for all the facts than is necessary for the conventional history.[21]

This historiographically naive postulation of given "topics" and "facts" hides, and, consequently, knowingly or otherwise, protects from further discussion the organization of the material done by the author in the background. How exactly did Dickson single out what counted as a "fact" in the history of number theory and how did he decide where to place it in his three volumes? Illustrating this point, Catherine Goldstein has commented on the place Dickson reserved for Fermat's and Frenicle's proofs that there is no right triangle with rational (or integer) sides whose area is a perfect square. She explains that Dickson classified these texts (which, *in fact*, avoid the algebraic formalism altogether) differently from other historians such as J. Itard, J.E. Hofmann, and from the mathematician A. Weil:

> [These texts] appear in [Dickson's] chapter on the equations of degree 4, where they are preceded by a mention of Fibonnacci's statement[22] and followed by a host of proofs concerning the impossibility of $x^4 \pm y^4 = z^4$ (in nonzero integers). This bespeaks a historical narrative which is result-oriented, but which also takes the significant state of the results to be the one which is fixed by their algebraic reformulation.[23]

Dickson clearly had perused Gauss's *Disquisitiones Arithmeticae*. This is witnessed by volumes 1 and 3 of his *History*, where large portions of Gauss's D.A. are often reported on almost line by line. However, in volume 2 (with more than 800 pages the largest of the three), Dickson's interests and priorities clearly did not coincide with those of Gauss; many scattered questions of Diophantine analysis find their place in this second volume. It thus tends to reflect above all the production of writers like J.J. Sylvester, A. Cunningham, A. Desboves, A. Genocchi, E. de Jonquières, T. Pépin, and many other authors, in particular in France and Great-Britain.

In his purportedly comprehensive *History of the Theory of Numbers*, Dickson omitted the "crown jewel of elementary number theory:" the quadratic reciprocity law.[24] The historical record suggests that Dickson did not intend for this omission to occur.[25] In his closing remarks in the preface to volume II, Dickson refers to a volume III as the "concluding" volume in the series.[26] Volume III appeared in 1923, "promptly" prepared, as Dickson described it in the preface, owing to the "favorable

[21] See [Dickson 1919–1923], vol. 2, p. xx.

[22] To the effect that a congruent number cannot be a square, or equivalently, that there is no perfect square which, added to or subtracted from a square, still yields squares.

[23] See [Goldstein 1995], p. 108: *Ils paraissent dans le chapitre sur les équations de degré 4, y sont précédés par la mention de l'énoncé de Fibonacci* [explanatory footnote] *et suivis d'une foule de preuves concernant l'impossibilité de $x^4 \pm y^4 = z^4$ (en entiers non nuls). Trace d'un récit historique orienté sur les résultats, mais aussi pour lequel l'état significatif des énoncés est fixé par la réécriture algébrique.*

[24] See [Kaplansky 1993], p. 1155.

[25] A brief overview of this omission follows. For more details, see [Fenster 1999c].

[26] See [Dickson 1919–1923], vol. 2, p. xii.

reception accorded to the first two volumes of this history."[27] Early in the text of this third volume, nestled in his history of binary quadratic forms, Dickson points his reader forward to a fourth volume that was to include, among other topics, the quadratic reciprocity law.[28]

The planned fourth volume involved Albert Everett Cooper, a University of Chicago graduate student from 1924 to 1926. Cooper earned his Ph.D. in mathematics in the spring of 1926 under Dickson's guidance with his historical dissertation, "A Topical History of the Theory of Quadratic Residues" [Cooper 1926]. This dissertation was intended to be a chapter in the fourth volume of Dickson's *History*. This fourth volume would contain a separate chapter on the history of quadratic reciprocity. While the Carnegie Institution of Washington agreed to issue the "fourth and final volume" of Dickson's *History*,[29] Dickson proposed that the Carnegie Institution no longer plan to publish it, but instead publish one of his two new forthcoming treatises on Number Theory. Dickson attempted to secure publication for the fourth volume elsewhere, but with no success. Although Cooper apparently prepared the manuscript of the fourth volume for the Carnegie Institution in 1929, they did not print it.[30]

In contrast to his typically high standards of excellence and completeness, it seems that Dickson's new texts on number theory compromised the completion of his history project. Consequently, Dickson left untreated the theorem Gauss had considered the pivotal result of number theory.

To be sure, this does not mean that Dickson did not value the quadratic reciprocity law. In his *Introduction to the Theory of Numbers*, he introduced it as follows:

> The quadratic reciprocity law is doubtless the most important tool in the theory of numbers and occupies the central position in its history. Its generalizations form a leading topic, past and present, in the theory of algebraic numbers.[31]

In this same textbook, he succinctly presented Gauss's third and second proofs of quadratic reciprocity (the latter as an exercise) as well as Eisenstein's proof via lattice counting.[32] Moreover, to a large extent, Dickson's chapters I-III, V, VII, and IX follow the layout of Gauss's *Disquisitiones Arithmeticae*. In addition, Dickson devoted his *Studies in the Theory of Numbers* [Dickson 1930] to the arithmetic of quadratic forms, a subject largely created by Gauss.

[27] See [Dickson 1919–1923], vol. III, p. iii.

[28] See [Dickson 1919–1923], vol. III, p. 3: "… to be quoted under the quadratic reciprocity law in Vol. IV."

[29] See letter W.M. Gilbert to L.E. Dickson, December 20, 1927; CIW Archives, Washington, D.C., Dickson Papers.

[30] In a telegram to the CIW on June 25, 1929, Cooper announced that "I have ready the manuscript for the fourth volume. How many copies do you think should be printed?"

[31] See [Dickson 1929], p. 30.

[32] See [Dickson 1929], pp. 34–36, 148.

4. Leonard Dickson as a Number Theorist

Dickson wrote his *History* as a comprehensive literature review for the needs of mathematicians – professional and amateur. This foray into the historical field interrupted, but did not stop Dickson's pure mathematical researches – cf. [Fenster 1999]. In fact, Dickson concurrently pursued his various interests and, in 1920, he brought together two of these seemingly disparate areas of mathematics in one of the most prestigious talks of his career, his plenary address at the International Congress of Mathematics in Strasbourg [Dickson 1921d]. By presenting one of these plenary lectures, Dickson joined the ranks of mathematicians like Felix Klein, Giuseppe Peano, Henri Poincaré, Émile Picard, Simon Newcomb, and Edmund Landau. The topic he chose for it came from the theory of numbers, that is, in Dickson's words,[33] from "the literature … I had been examining minutely in the preparation and publication of the first volumes of my History of the Theory of Numbers. I shall approach a few typical problems of the theory of numbers through the medium of other branches of mathematics." Thus Dickson's historical study inspired his four-part International Congress address. Following his introductory remarks, he applied algebro-geometric methods to the problem of finding all rational solutions of certain Diophantine equations. In the final two parts, he made use of the theory of algebraic invariants to determine the integers for which a given binary cubic form equals a square.[34] He devoted the majority of his attention, however, to Part II, where he applied algebraic and hypercomplex numbers to the problem of finding all integer solutions to certain diophantine equations:

> While seeking interesting material which would illustrate this topic, I was led to the discovery of a very simple general method of finding explicit formulas which give all the integral solutions of homogeneous quadratic equations in several variables. For equations in four variables, the method makes use of some simple properties of integral algebraic numbers; while for equations in six variables, use is made of properties of integral quaternio[n]s." [35]

Explicitly, Dickson studied equations such as[36]

$$x_1^2 + x_2^2 + x_3^2 = x_4^2 \quad \text{and} \quad x_1^2 + \ldots + x_5^2 = x_6^2. \qquad [1]$$

The analysis proceeds via the study of all integral solutions of various associated equations including

$$x^2 + y^2 = zw, \qquad [2a]$$

which, in turn, is accomplished by bringing to bear the arithmetic of the Gaussian integers $\mathbf{Z}[\sqrt{-1}]$.

[33] See [Dickson 1921d], p. 41.

[34] See [Dickson 1921d], pp. 42–46, 55–56.

[35] See [Dickson 1921d], p. 41.

[36] For a more comprehensive analysis of these results and their place in Dickson's overall research program, see [Fenster 1999]. Six months after the Strasbourg congress, he would generalize his results back in the United States at an AMS meeting [Dickson, 1921b].

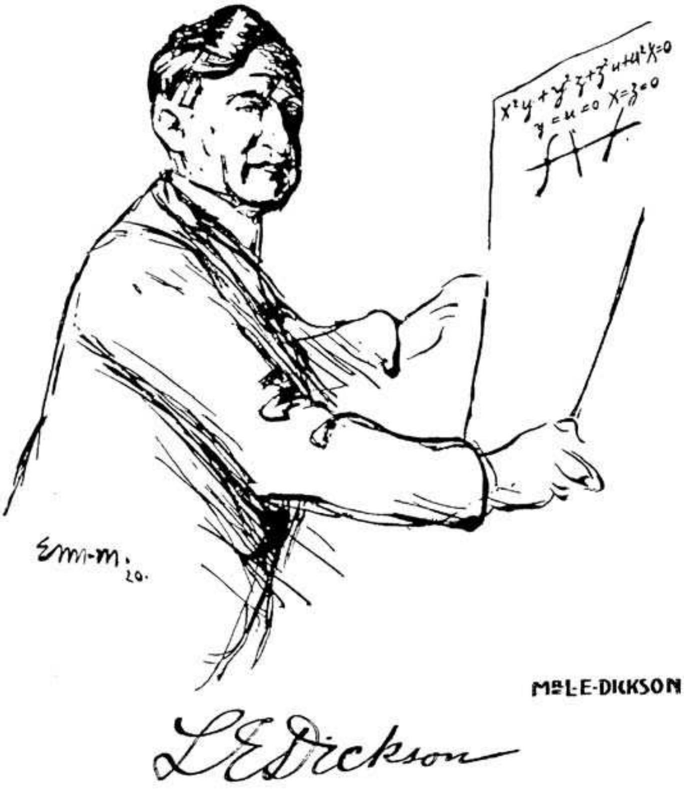


Fig. VII.3. Sketch of Dickson's plenary lecture at the 1920 ICM in Strasbourg
From: D.J. Albers, G.L. Alexanderson, C. Reid,
ICMs 1893–1986, Springer 1987, p. 17.

On several occasions in the context of such diophantine problems, Dickson emphasized the genuinely arithmetic nature of the problem of effectively determining the integral solutions of equations such as [2a]. He expressed this most forcefully in a little note written several months after the Strasbourg Congress:

> Numerous writers have claimed to find all integral solutions of various homogeneous equations when they have actually found merely the rational solutions. … It has been regarded as self-evident by all writers, who have mentioned the topic, that the problem of solving a non-homogeneous equation in rational numbers is equivalent to the problem of solving the corresponding homogeneous equation in integers. Let us examine this question for the particular homogeneous equation
>
> $$x^2 + 5y^2 = zw \tag{1}$$
>
> and the corresponding non-homogeneous equation
>
> $$X^2 + 5Y^2 = Z. \tag{2}$$

> ... If $x, y, z, w (w \neq 0)$ are integers satisfying (1) and if we write
>
> $$\frac{x}{w} = X,\ \frac{y}{w} = Y,\ \frac{z}{w} = Z, \tag{3}$$
>
> we obtain rational numbers satisfying (2). Conversely, if X, Y, Z are rational numbers satisfying (2), we may express them as fractions (3) with a common denominator and obtain integers x, y, z, w satisfying (1).
>
> Here there is nothing wrong with the algebraic work, nor with the facts deduced. The fallacy lies in the failure to perceive that these facts do not warrant the conclusion that, in the converse case, we have shown how to find all integral solutions.[37]

Thus Dickson emphasized that the rational solutions of (2) do not automatically lead to an explicit determination of the least common denominators of X, Y, Z. Information about these denominators is, however, needed to deduce all integral solutions of (1).

But Dickson's text contained no ordinary footnote. Dickson referred to art. 300 of Gauss's D.A. as an example of one such text that presented the topic as self-evident. Gauss claimed here that "it is thus clear that the solution of this equation $[ax^2 + 2bxy + cy^2 + 2dx + 2ey + f = 0]$ by rational numbers is identical with the solution by integers of the equation $at^2 + 2btu + cu^2 + 2dtv + 2euv + fv^2 = 0$."[38]

This footnote illustrates Dickson's use of rhetoric in his mathematical publications. Throughout his work in the theory of the arithmetic of algebras, for example, Dickson consistently criticized the work of his predecessors.[39] In the case at hand, Dickson offered a considered (negative) assessment of Carl Friedrich Gauss. Perhaps here too, Dickson made this comment to underscore the originality of his own observation.

Returning to Dickson's Strasbourg address, his method to find the integral solutions of the first equations [1] employed simple properties of integral algebraic numbers: norm, unique division, and (unique) factorization of Gaussian integers. He then analogously applied the arithmetic of the integral quaternions to deduce all integral solutions to $x_1^2 + ... + x_5^2 = x_6^2$. For this part of his work, Dickson relied on what he referred to as Adolf Hurwitz's "perfect" arithmetic of quaternions.[40] Hurwitz's arithmetic hinged on his definition of integral quaternions as those with coordinates either integers or all halves of odd integers. Moreover, like the method used by Gauss for determining the primes in the complex numbers, Hurwitz established an association between the prime integral quaternions and the prime integers. Even still, Dickson found "the presence of the denominators 2 in certain integral quaternions an inconvenience"[41] that he would try to eliminate.

[37] See [Dickson 1921c], p. 313.

[38] In fact, in art. 300 of the D.A., Gauss only used his observation in the uncontested direction, in order to derive the rational solutions of the first equation from the integral solutions of the second equation, which he had obtained in art. 299 of the D.A.

[39] See [Fenster 1998].

[40] See [Hurwitz 1896]. For Dickson's comment see [Dickson 1921b], p. 225.

[41] See [Dickson 1921b], pp. 225–226.

He fully developed these ideas in his more number-theory friendly "Arithmetic of Quaternions" [Dickson 1921b]. As the title suggests, he considered not only the notion of an integral quaternion but also the attendant concepts of prime, greatest common divisor, and unique factorization of integral quaternions. He clearly spelled out the motivation behind his research in this direction when he wrote that "[q]uaternions have recently been applied to the solution of several important problems in the theory of numbers. For this purpose it is necessary to make a choice of the quaternions which are to be called integral."[42] Thus, with the integral quaternions a necessary component in the search for solutions to certain Diophantine equations, Dickson found himself compelled to come to terms with the arithmetic of this specific algebra initially and with more general algebras later. As Dickson described it in the introduction to his celebrated text on the subject, *Algebras and their Arithmetics,*

> The chief purpose of this book is the development for the first time of a general theory of the arithmetics of algebras, which furnishes a direct generalization of the classic theory of algebraic numbers. The book should appeal not merely to those interested in either algebra or the theory of numbers, but also to those interested in the foundations of mathematics. Just as the final stage in the evolution of number was reached with the introduction of hypercomplex numbers (which make up a linear algebra), so also in arithmetic, which began with integers and was greatly enriched by the introduction of integral algebraic numbers, the final stage of its development is reached in the present new theory of arithmetics of linear algebras.[43]

Inasmuch as his previous efforts to define a set of integral elements in an arbitrary algebra formed what he viewed as "the final stage in the evolution of number," this book spelled out the associated theory of arithmetic. Moreover, although the quaternions and their application to diophantine equations may have initially lured him into this subject, the generalization of the algebraic numbers represented a key component in the measurement of his theory's success.

As Dickson intended for his *Algebras and their Arithmetics* to reach a wide audience, he devoted the first eight chapters to the development of the general theory of algebras. In particular, he called attention to Wedderburn's structure theorems of algebra which had previously remained "somewhat overlooked." Moreover, Dickson's definition of a set of integral elements generally gained acceptance "in the extensive German development of a unitary theory of ideals, by Emil Artin, Helmut Hasse, Emmy Noether, B.L. van der Waerden, and others."[44] Thus Dickson's work had strong ties to key mathematical ideas from the past, a broad presentation which brought many aspects of the general theory of algebras into focus, and links with the (future) work of the influential German algebraists. His impressive theory earned him the American Association for the Advancement of Science Prize in 1924 and the American Mathematical Society's Cole Prize in 1928 for this book.[45]

But these were temporary rewards. His more long-term influence came in the

[42] See [Dickson 1921b], p. 225.

[43] See [Dickson 1923], p. vii.

[44] Both preceding quotes from [Birkhoff 1938], p. 287.

[45] Cf. [Fenster 1998].

theory of algebras when he tackled the problem spurred by Wedderburn's structure theorems of algebra, namely, the determination of all division algebras. Concurrent with other mathematical researches, Dickson spent more than twenty years on this problem. In the process, he introduced the notion of cyclic algebras (although he did not use that term) and came close to the theory of crossed products, a concept Emmy Noether would fully generalize later.[46]

Moreover, when Dickson turned his attention elsewhere, quaternion algebras remained a topic of study for others, including the Swiss mathematician Rudolf Fueter.[47] As we have seen, Dickson's arithmetic of quaternions arguably served a more important role in his own work in terms of the catalyst it provided for other research. More important to the current study, perhaps, is what Fueter's work suggests about the reception of the German translation (and partial revision) of Dickson's *Arithmetic of Algebras*, namely, his *Algebren und ihre Zahlentheorie*.[48] For his paper [Fueter 1932], Fueter relied extensively on the ideas put forth by Dickson in this book [Dickson 1927]. Furthermore, Fueter was not only aware of Dickson's work, but also of that of his students.[49]

But recall the diophantine problems which interested Dickson in the first place:

$$x_1^2 + x_2^2 + x_3^2 = x_4^2 \quad \text{and} \quad x_1^2 + ... + x_5^2 = x_6^2 \qquad [1]$$

and their corresponding auxiliary equations:

$$x^2 + y^2 = zw, \quad \text{and} \quad x^2 + y^2 + z^2 + w^2 = sn. \qquad [2a, b]$$

While he wrote the historical study that inspired his interest in these types of problems, Dickson maintained an especial interest in Fermat's Last Theorem and the four and eight square theorems. Thus, it comes as no surprise that the pure number theoretic problem that attracted his attention for the closing decade of his career was the so-called ideal Waring theorem.

In 1770, Edward Waring (1734–1798) conjectured, apparently based on short tables, that every integer can be expressed as the sum of at most r_n many n^{th} powers, for some r_n depending on n; this conjecture was proved by David Hilbert in 1909.[50]

[46] Cf. [Scharlau 1999], pp. 44–46. Scharlau further asserts there that "[t]he theory of cyclic algebras is often attributed to Dickson, but it seems that Wedderburn's contributions are more significant. He gave clear and correct proofs with precise insight while Dickson's attempts often lead only into a morass of calculations." See also Scharlau's statement that "most of Dickson's work is not very pleasant to read." [Scharlau 2000], p. 237. On the same and the following page, Scharlau points out the lack of reception of Dickson's work on quadratic forms in a general field.

[47] See [Fueter 1932] and [Fueter 1934].

[48] Cf. [Fenster, Schwermer 2005], sections 1, 2.

[49] See [Fueter 1934], p. 199, footnote 2, where Fueter refers to the work of C.G. Latimer, Dickson's 26th student (of 67). Fueter's references to other work (a Hamburg Dissertation, a Russian manuscript, etc.) suggest a solid acquaintance with the relevant literature.

[50] See [Kline 1972], vol. 2, p. 609; [Dickson 1919–1923], vol. 2, chap. XXV; and [Dickson 1936].

About two years after Waring, J.A. Euler, son of Leonhard Euler, stated that, in order to express every positive integer as a sum of positive n^{th} powers, *at least* I terms are necessary, where

$$I = \left[\left(\frac{3}{2}\right)^n\right] + 2^n - 2. \qquad (*)$$

(Here $[x]$ denotes the greatest integer $\leq x$.) From 1919 to 1927, Hardy and Littlewood did what Dickson would refer to as "pioneer work" to establish an upper bound, and in 1934, Vinogradow obtained what Dickson considered "astonishing" results which improved the upper bound considerably. In Dickson's words, "[t]he ideal Waring Theorem states that every positive integer is a sum of I integral n^{th} powers ≥ 0, for I in (*)."[51] In a long series of papers, Dickson and his students proved this theorem.

Dickson must have held this result in high regard. When invited to the 1936 Harvard Tercentenary as one of four distinguished mathematicians in the world, along with G.H. Hardy, Tullio Levi-Civita and Élie Cartan, Dickson chose to speak on "The Waring Problem and its Generalizations." He opened his talk with a brief history of the theorem, gave his proof of the ideal Waring theorem, and gave some generalizations of the theorem, including "remarkable new results" which provided a method to count the number of powers which appeared in pairs.[52]

5. Conclusion

If the history is in the problems, then the problems Dickson chose to present on more distinguished occasions must be taken into special consideration. From this perspective, the historical record reveals Dickson's interest in and emphasis on the mathematics behind solving Diophantine Equations that express integers as sums of squares, cubes, or fourth powers, etc. In that sense his orientation differed sharply from Gauss's rather theory-oriented approach to the theory of numbers.

But Gauss outlined his desire for the *Disquisitiones Arithmeticae* in a general way when he expressed in the preface his "greatest hope" for the book: that it "pleases those who have at heart the development of science, either by supplying solutions that they have been looking for or by opening the way for new investigations." The example of Leonard Dickson shows that Gauss's hope was indeed achieved in the early years of America's mathematical research community, if perhaps in ways Gauss could not even have imagined.

Inspired by his historical researches, Dickson made extensive use of the Gaussian integers and their properties to solve equations such as $x^2 + y^2 = zw$. But Gauss's work was also present elsewhere in Dickson's solution. In particular, just as Gauss expanded the concept of an integer with his complex integers, Dickson stretched the notion of an integer in an algebra, all the time making certain that his set of integral elements in an algebra would fit the existant theory of integral algebraic numbers.

Ultimately, it seems, his comprehensive historic study of number theory led him to isolate problems of interest and seek solutions of increasing generality. Not

[51] See [Dickson 1936], p. 834.

[52] See [Dickson 1936], p. 836.

surprisingly, he spent the final decade of his mathematical career focused on establishing and generalizing a celebrated, unsolved number-theoretic problem. Thus this study highlights not only how Dickson conceived of a historical study of number theory but also how he used the history of mathematics to inform his mathematical researches. This work also highlights one of Dickson's mathematical tenets, that is, his emphasis on generalization. He was, in part, setting the standard for a still young American mathematical community.[53] In the process, he also opened new American venues for mathematics publications

Although the *Disquisitiones Arithmeticae* appeared three-quarters of a century before America had a budding mathematical research community and a full century before that group began to take root and grow, Dickson's research provides one example of how Gauss's ideas penetrated American mathematics in both detail and scope.

References

Albert, A. Adrian. 1955. Leonard Eugene Dickson 1874–1954. *Bulletin of the American Mathematical Society* 61, 331–345.

Birkhoff, George D. 1938. Fifty Years of American Mathematics. In *Semicentennial Addresses of the American Mathematical Society*, ed. R.C. Archibald, pp. 270-315. New York: American Mathematical Society.

Cajori, Florian. 1894. *A History of Mathematics*. New York: MacMillan.

Carnegie Institution of Washington. 1902. *Yearbook*. Washington: Carnegie Institution of Washington.

Cooper, Albert E. 1926. *A Topical History of the Theory of Quadratic Residues*. Unpublished dissertation, University of Chicago. University of Chicago Archives.

Dickson, Leonard E. 1975. *The Collected Mathematical Papers*, vols I-IV. New York: Chelsea.

———. 1983. *The Collected Mathematical Papers*, vol. VI. New York: Chelsea.

———. 1901. *Linear Groups with an Exposition of the Galois Field Theory*. Leipzig: B.G. Teubner, 1901. Repr. New York: Dover, 1958.

———. 1907. On Quadratic Forms in a General Field. *Bulletin of the American Mathematical Society* 14, 108–115. Repr. in [Dickson 1975], vol. IV, pp. 512–519.

———. 1917. Fermat's Last Theorem and the Origin and Nature of the Theory of Algebraic Numbers. *Annals of Mathematics* 18, 161–187. Repr. in [Dickson 1975], vol. I, pp. 595–621.

———. 1919. On Quaternions and their Generalization and the History of the Eight Square Theorem. *Annals of Mathematics* 20, 155–171, 297. Repr. in [Dickson 1975], vol. I, pp. 623–639.

———. 1919–1923. *History of the Theory of Numbers*. vol. 1: *Divisibility and Primality*, 1919; vol. 2: *Diophantine Analysis*, 1920; vol. 3, *Quadratic and Higher Forms*, with a chapter on the class number by G.H. Cresse, 1923. Washington: Carnegie Institution of Washington. Repr. New York: Chelsea, 1952.

[53] Cf. [Fenster, 1997].

———. 1921a. A New Method in Diophantine Analysis. *Bulletin of the American Mathematical Society* 27, 353–365. Repr. in [Dickson 1975], vol. IV, pp. 619–631.

———. 1921b. Arithmetic of Quaternions. *Proceedings of the London Mathematical Society* 20, 225–232. Repr. in [Dickson 1975], vol. III, pp. 397–404.

———. 1921c. Fallacies and Misconceptions in Diophantine Analysis. *Bulletin of the American Mathematical Society* 27, 312–319. Repr. in [Dickson 1975], vol. IV, pp. 611–618.

———. 1921d. Some Relations Between the Theory of Numbers and Other Branches of Mathematics. In *Comptes Rendus du Congrès International des Mathématiciens, Strasbourg 1920*, ed. H. Villat, pp. 41–56. Toulouse: Privat. Repr. in [Dickson 1975], vol. II, pp. 579–594.

———. 1923. *Algebras and Their Arithmetics*. Chicago: University of Chicago Press.

———. 1927. *Algebren und ihre Zahlentheorie*. Zürich: Orell Füssli.

———. 1929. *Introduction to the Theory of Numbers*. Chicago: University of Chicago Press.

———. 1930. *Studies in the Theory of Numbers*. Chicago: University of Chicago Press.

———. 1936. The Waring Problem and its Generalizations. *Bulletin of the American Mathematical Society* 42, 833–842. Repr. in [Dickson 1975], vol. V, pp. 51–60.

Fenster, Della D. 1997. Role Modeling in Mathematics: The Case of Leonard Eugene Dickson (1874–1954). *Historia Mathematica* 24, 7–24.

———. 1998. Leonard Eugene Dickson and His Work in the Arithmetics of Algebras. *Archive for History of Exact Sciences* 52, 119-159.

———. 1999a. Leonard Dickson's *History of the Theory of Numbers*: An Historical Study with Mathematical Implications. *Revue d'histoire des mathématiques* 5, 159–179.

———. 1999b. The Development of the Concept of an Algebra: Leonard Eugene Dickson's Role. *Supplemento ai Rendiconti del Circolo Matematico di Palermo* 61, 59–122.

———. 1999c. Why Dickson left Quadratic Reciprocity out of the History of the Theory of Numbers, *American Mathematical Monthly* 106, 618–626.

———. 2003. Funds for Mathematics: Carnegie Institution of Washington Support for Mathematics from 1902–1921. *Historia Mathematica* 30, 195–216.

Fenster, Della D., Schwermer, Joachim. 2005. A Delicate Collaboration: A. Adrian Albert and Helmut Hasse and the Principal Theorem in Division Algebras in the Early 1930's. *Archive for History of Exact Sciences* 59, 349-379.

Fiske, Thomas. 1905. Mathematical Progress in America. *Bulletin of the American Mathematical Society* 11, 238–246.

Fueter, Rudolf. 1934. Quaternionenringe. *Commentarii mathematici Helvetici* 6, 199–222.

———. 1932. Über eine spezielle Algebra. *Journal für die reine und angewandte Mathematik* 167, 52–61.

Goldstein, Catherine. 1995. *Un théorème de Fermat et ses lecteurs*. Saint-Denis: Presses Universitaires de Vincennes.

Hurwitz, Adolf. 1896. Über die Zahlentheorie der Quaternionen. *Nachrichten von der königlichen Gesellschaft der Wissenschaften zu Göttingen*, 113–340. Repr. in *Mathematische Werke*, vol. II, pp. 303–330. Basel, Stuttgart: Birkhäuser, 1963.

Kaplansky, Irving. 1993. Quadratic Reciprocity in Dickson's History. *Notices of the American Mathematical Society* 40, 1155.

Kline, Morris. 1972. *Mathematical Thought from Ancient to Modern Times*. 3 vols. New York: Oxford University Press.

Kohler, Robert. 1991. *Partners in Science: Foundations and Natural Scientists, 1900-1945*. Chicago: University of Chicago Press.

Lehmer, Derrick N. 1910. *Factor Table for the First Ten Millions*. Washington, D.C.: Carnegie Institution of Washington.

———. 1914. *List of Prime Numbers from 1 to 10,006,721*. Washington, D.C.: Carnegie Institution of Washington.

———. 1919–1920. Dickson's History of the Theory of Numbers. *Bulletin of the American Mathematical Society* 26, 125–132.

Parshall, Karen Hunger. 1983. In Pursuit of the Finite Division Algebra Theorem and Beyond: Joseph H. M. Wedderburn, Leonard E. Dickson, and Oswald Veblen. *Archives internationales d'histoire des sciences* 33, 274–299.

———. 1991. A Study in Group Theory: Leonard Eugene Dickson's Linear Groups. *The Mathematical Intelligencer* 13 (1), 7–11.

———. 1998. America's First School of Mathematical Research: James Joseph Sylvester at The Johns Hopkins University 1876-1883. *Archive for History of Exact Sciences* 38, 153–196.

Parshall, Karen Hunger, Rowe, David E. 1994. *The Emergence of an American Mathematical Research Community: J.J. Sylvester, Felix Klein, and E.H. Moore*. History of Mathematics 8. Providence: American Mathematical Society; London: London Mathematical Society.

Peirce, Benjamin. 1881. Linear Associative Algebra with Notes and Addenda by C. S. Peirce, son of the Author. *American Journal of Mathematics* 4, 97–229.

Rowe, David E. 2001. Looking Back on a Bestseller: Dirk Struik's *A Concise History of Mathematics*. *Notices of the American Mathematical Society* 6, 590–592.

Scharlau, Winfried. 1999. Emmy Noether's Contributions to the Theory of Algebras. In *The Heritage of Emmy Noether*, ed. M. Teicher, pp. 39–55. Israel Mathematical Conference Proceedings 12. Oxford: Oxford University Press.

———. 2000. On the History of the Algebraic Theory of Quadratic Forms. In *Quadratic forms and their applications*, ed. E. Bayer-Fluckiger, D. Lewis, A. A. Ranicki, pp. 229–259. Contemporary Mathematics 272. Providence: American Mathematical Society.

Shaw, James Byrnie. 1907. *Synopsis of Linear Associative Algebra*. Washington, D.C.: Carnegie Institution.

Siegmund-schultze, Reinhard. 1997. The Emancipation of Mathematical Research Publishing in the United States from German Dominance (1878–1945). *Historia Mathematica* 24, 135–166.

Smith, David Eugene, Ginsburg, Jekuthiel. 1934. A History of Mathematics in America Before 1900. Chicago: The Mathematical Association of America.

Part VIII

Gauss's Theorems in the Long Run: Three Case Studies

Jusqu'ici, pour amples que soient nos généralisations des résultats de Gauss, on ne peut dire que nous les ayons vraiment dépassés.

André Weil, L'avenir des mathématiques, 1947

VIII.1

Reduction Theory of Quadratic Forms: Towards *Räumliche Anschauung* in Minkowski's Early Work

Joachim Schwermer

Hermann Minkowski (1864–1909) is well known in mathematics for his formation of the so-called "geometry of numbers." From his first paper, "Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten," submitted to the Paris Academy of Sciences in 1882, to his last mathematical one, "Diskontinuitätsbereich für arithmetische Äquivalenz", in 1905, Minkowski focused on the arithmetical theory of quadratic forms in n variables. Since C. F. Gauss had given a complete treatment of the theory of binary quadratic forms in his *Disquisitiones Arithmeticae* in 1801, the generalization of his results to forms in n variables presented a major challenge to the mathematicians of the XIX$^{\text{th}}$ century. The contributions by Gotthold Eisenstein, Gustav Lejeune-Dirichlet, Charles Hermite and, in particular, the applications to number theory found in their work, served as substantial stimuli for Minkowski's own studies at the beginning of his career during the period 1880–1887. He knew about the strong relationship between quadratic forms and problems in arithmetic as revealed in the work of Fermat, Lagrange, Gauss, Eisenstein and others. Thus Minkowski immediately obtained, by use of the discoveries and methods embodied in his "geometry of numbers," deep results in various fields of number theory, for example, in questions of Diophantine approximation.

What was meant by "geometry of numbers"? The title of Minkowski's paper that Felix Klein read in 1893, at the Chicago Mathematical Congress, provides some insight: "Eigenschaften von ganzen Zahlen, die durch räumliche Anschauung erschlossen sind." Thus, it is essentially a question of using visual-geometric thinking for the uncovering of properties (and relations) of integers. In his lecture "Über Geometrie der Zahlen," delivered in Halle in 1891, Minkowski wrote:

> If one has orthogonal coordinates in the 3-space then the systems of three *integers* correspond to discrete points … The totality of all these points with integers as coordinates is called the three-dimensional lattice of integers; the title "*geometry of numbers*" embraces geometrical studies of the 3-dimensional lattice of integers … and the generalization of the result of these studies to spaces of arbitrary dimension. Of course, each assertion about the lattice of integers contains a purely arithmetical core. However the word "geometry" appears appropriate in view of the questions to which the geometrical interpretation leads and in view of the methods of investigation which are steadily directed through geometrical concepts.[1]

The main objectives of this paper are to describe how visual thinking appeared in Minkowski's early works at various critical points and to discuss briefly the previous contributions and points of view of others on which he relied, in particular those of Gauss. Minkowski's book *Geometrie der Zahlen* was announced in 1893, and finally published in 1896. Minkowski gave the main arguments for obtaining one fundamental theorem, the so-called lattice-point theorem, in a paper in 1891, embodied in an estimate for the minimum of a positive definite quadratic form. In fact, his ideas emerged much earlier. In tracing the development of Minkowski's thoughts about the geometry of numbers and its close relation to the reduction theory of quadratic forms, I will mostly draw on previously unknown archival material. It includes a draft of a manuscript, titled "On the theory of reduction of positive quadratic forms" and written in November 1883 in Berlin. This draft marks a significant step in the development of Minkowski's reduction theory. In addition, I will also rely on the manuscript "Über einige Anwendungen der Arithmetik in der Analysis," and a preliminary draft of it, both written for his *Probevorlesung* at the occasion of his Habilitation 1887 in Bonn.[2]

1. The Biographical and Institutional Background of Minkowski's Early Scientific Career

Hermann Minkowski was born on June 22, 1864 in Alexotas, Russia, now Lithuania. In 1872 his family moved to Prussia and settled in Königsberg, where Minkowski attended the *Altstädtische Gymnasium*. There he received a solid education based on the Prussian curricula which, at the time, stressed classical languages, German

[1] [Minkowski, 1892]: *Wenn man für den Raum rechtwinklige Koordinaten einführt, so entsprechen den Systemen von drei* ganzen *Zahlen diskrete Punkte, welche derart über den Raum verstreut liegen, daß sie eine gewisse Nähe in bezug auf jede beliebige Raumstelle erreichen. Den Inbegriff aller dieser Punkte mit lauter Koordinaten, die ganze Zahlen sind, nennt der Vortragende das dreidimensionale* Zahlengitter*; unter dem Titel* "Geometrie der Zahlen" *begreift er geometrische Studien über das dreidimensionale Zahlengitter und über das entsprechende Gebilde in der Ebene, und in weiterem Sinne auch die Ausdehnung der Ergebnisse solcher Studien auf Mannigfaltigkeiten beliebiger Ordnung. Natürlich besitzt jede Aussage über die Zahlengitter einen rein arithmetischen Kern. Das Wort "Geometrie" erscheint durchaus am Platze im Hinblick auf Fragestellungen, zu welchen die geometrische Anschauung verhilft, und auf Untersuchungsmethoden, welche fortwährend durch geometrische Begriffe ihre Richtung angewiesen erhalten.*

[2] These two manuscripts are published in [Schwermer 1991].

and French (two hours each per week in the *prima*), mathematics (four hours), physics (two hours), history and geography. Due to his teacher Dr. Louis Hübner, a former student at the Albertus-University of Königsberg and a member of its mathematico-physical seminar[3] Minkowski enjoyed an unusually high level of mathematics courses in his last years at the *Gymnasium*.[4] While still at school he followed a suggestion of Hübner to contact Heinrich Weber, ordinary professor in mathematics between 1875 and 1882 at the university of Königsberg.[5] Weber praised Minkowski to Richard Dedekind:

> I want to write to you … about a mathematical and specially number-theoretical genius on whom one has great hopes. It is a last-year pupil in a local *Gymnasium* who … has worked his way totally on his own impulse into higher analysis and number theory, which he has studied after the first edition of your Dirichlet's lectures. Now, he has the *Disquisitiones* on his agenda[6]

Minkowski graduated in April 1880 and went on to the Albertus-University, where he studied mathematics, principally with Weber, Woldemar Voigt[7] and the former student of Jacobi, Johann Georg Rosenhain (1816–1887). Since 1876, Weber

[3] In 1834 the physicist Franz Neumann (1798–1895) established together with Carl Gustav Jacobi the mathematico-physical seminar at the university of Königsberg. It was composed of a division for pure and applied mathematics (mechanics, physical astronomy) and a division for mathematical physics. As the first official seminar in Prussia to incorporate mathematical methods in physics instruction, this institution became the center of a school of mathematical (or theoretical) physics, see [Olesko 1991]. Jacobi directed the mathematical division from 1834 to 1844. His student Friedrich Julius Richelot succeeded him and oversaw the division until 1875. He was very much involved in the 1866 reform of Prussia's examination for secondary school teachers. At that time, mathematics played a central role in the curriculum, see [Schlote 1995].

[4] Details on Minkowski's years at the *Gymnasium* are given in [Strobl 1985].

[5] Heinrich Martin Weber, born on March 5, 1842 in Heidelberg, enrolled in 1860 at the University of Heidelberg where he attended lectures by Otto Hesse, Robert Bunsen and Gustav Robert Kirchhoff. In the years 1863–1865 he continued his studies at Königsberg. Upon his return to Heidelberg he completed his *Habilitation*, and worked there as *Privatdozent*, then extraordinary professor until 1870, when he accepted a call as ordinary professor at the Polytechnic in Zürich. In 1875, Weber moved to Königsberg as the successor of Richelot.

[6] This letter from Weber to Dedekind is published in [Strobl 1985], pp. 144–145: *Ich will Dir … von einem … mathematischen u. speziell zahlentheoretischen Genie schreiben, welches viel verspricht. Es ist ein Primaner eines hiesigen Gymnasiums, der … sich ganz aus eigenem Antrieb in die höhere Analysis und die Zahlentheorie eingearbeitet hat, die er nach der ersten Auflage Deiner Dirichlet-Vorlesungen studiert hat. Jetzt hat er die Disquisitiones vor.*

[7] Voigt graduated from the *Gymnasium* in Leipzig in 1867 and enrolled at the University of Leipzig to study mathematics and natural sciences, including physics and mineralogy. After the Franco-Prussian war, Voigt continued his studies at the university of Königsberg and defended his dissertation by March, 1874. He was Franz Neumann's last doctoral student. Voigt received his Habilitation at the university of Leipzig where he had worked as a secondary school teacher for one year. In 1875 he accepted the call

directed the mathematical division of the seminar, while Voigt oversaw the physical division. One of Minkowski's fellow students was David Hilbert,[8] and it has been in these seminars that their long and celebrated friendship began. Both attended the basic courses "Differentialrechnung" and "Determinantentheorie," the latter one given by Weber. Weber's mathematical expertise and his instruction shaped the personal development of Minkowski considerably. But at the beginning of the 1880s, the academic situation at the seminar changed: for some time Weber wished to move to another university, and he did so in 1883 – first, for one year, to the recently founded technical university in Berlin-Charlottenburg, then to the university of Marburg. Moreover, in August 1883, the director of the physical division of the seminar, Voigt, who had continued for eight years the program of physics instruction at Königsberg as introduced and shaped by Neumann, but had not got, contrary to his expectations, an ordinary professorship at the Albertus-University, accepted an offer from Göttingen and became professor for theoretical physics and director of the mathematico-physical institute.

Meanwhile, Minkowski was attracted by a problem posed in 1881 by the Académie des Sciences in Paris for the 1882 *Grand Prix des Sciences Mathematiques*. The problem concerned the theory of the decomposition of integers as a sum of five squares. In 1847, Eisenstein[9] had announced without proof results on the number of representations of a given integer as a sum of five squares of integers. On May 29, 1882, Minkowski submitted a manuscript (written in German) to the Academy. Extending Gauss's theory on genera of binary quadratic forms, elaborated in the *Disquisitiones Arithmeticae*, Minkowski generalized the notion of genus to the case of quadratic forms with a higher number of variables. He constructed in fact a quite general theory of quadratic forms in n variables with integral coefficients, mainly focussing on orders and genera of such forms, their close relationship with one another, and possible characterizations by means of sets of certain invariants. Eisenstein's results then turned out to be easy consequences of Minkowski's far-reaching results on representations of positive definite quadratic forms with n variables by a quadratic form with a higher number of variables.

Despite the well-known turmoil around this prize,[10] the paper submitted to the Academy and the award of the prize made the young Minkowski, 17 years old at the time, a major promising figure in mathematics. He, however, still had to finish his scientific education.

as extraordinary professor of theoretical physics at Königsberg. Soon thereafter he took over Neumann's lectures in theoretical physics and set up his own mathematical-physical laboratory. Voigt's position at Königsberg until he accepted an offer from Göttingen in 1883 is discussed in detail in [Olesko, 1991], pp. 436–438.

[8] Hilbert, born on January 22, 1862, graduated in 1879 at the Wilhelms-Gymnasium in Königsberg.

[9] See Dossier "Grand Prix des Sciences Mathématiques 1882" (séance du 5 juin 1882), Archives de l'Académie des Sciences, Paris, and [Eisenstein 1847].

[10] For further details see [Strobl 1985], [Schwermer 1991], [Serre 1993].

In the winter semester 1882–1883, Minkowski enrolled at the University of Berlin where he attended lectures by Leopold Kronecker and Karl Weierstrass. After three semesters, he returned to Königsberg where he finally received his doctorate on July 30, 1885. In the fall 1883, Ferdinand Lindemann (1852–1939) had come to Königsberg as the successor of Weber. At his side, the young Adolf Hurwitz (1859–1919) worked as an extraordinary professor.[11] These two played a central role in the scientific and personal development of Minkowski and Hilbert in the following years. First, there were the lectures, as recommended to the students by the directors of the mathematico-physical seminar,[12] covering the foundations and more advanced material in analysis, the theory of functions, algebra, number theory, geometry and mathematical physics. Second, Lindemann launched a weekly mathematical colloquium which offered a forum for talks and scientific exchange at the research level. The topics included results of the participants and profound surveys of the work of others in mathematics and mathematical physics. In many ways, this colloquium was a social mechanism that transmitted more than mathematical results. For example, the friendship forged between Hilbert and Minkowski three years earlier expanded to include Hurwitz. Initially, Hurwitz served more as a mentor to Hilbert and Minkowski, but ultimately he turned into a friend.

In the fall of 1886, Minkowski wrote two very substantial papers, [Minkowski 1887a] and [Minkowski 1887b], on finite groups of linear transformations with integral coefficients, and, on February 26, 1887, he asked the Philosophical Faculty of the University of Bonn for admission to the *Habilitation*, submitting these two papers as *Habilitationsschrift*. On the same day, Minkowski proposed as one out of three possible topics for his *Probevorlesung* the theme "Über einige Anwendungen der Arithmetik in der Analysis." This talk, given on March 15, 1887, marked a decisive turning point in Minkowski's approach to the theory of quadratic forms. The ideas presented there were at the heart of Minkowski's geometrical thinking.

One line of Minkowski's research dates back to Dirichlet's discovery of a formula for the number of classes of integral binary forms of a given discriminant. The proof of this class number formula required deep analytic methods. In generalising this formula to forms with a higher number of variables, Eisenstein, Smith and later Minkowski had to encounter additional complications, in particular, that two genera of the same determinant need not contain the same number of classes. This theme already played a role in Minkowski's paper of 1883, and occupied the central position in his 1885 thesis. Minkowski also pursued the study of the theory of reduction for positive definite quadratic forms, a topic to which we will return. It is closely related to the problem of determining the precise bound for the minimum of a quadratic

[11] Hurwitz began his studies in 1877 at the Technical University in Munich, studied later in Berlin and Leipzig where he received his doctorate under the direction of Klein. His thesis "Grundlagen einer indepedenten Theorie der elliptischen Modulfunktionen und Theorie der Multiplikator–Gleichungen erster Stufe," published in *Mathematische Annalen* in 1881 pertained to geometry, number theory and the theory of functions as well. Hurwitz completed his *Habilitation* in Göttingen in 1882.

[12] Lindemann directed the mathematical division of the seminar, while Paul Volkmann, a student of Neumann, oversaw the physical division.

form. The geometric interpretation of the arithmetical objects involved in this circle of ideas ultimately led Minkowski to his geometry of numbers.

2. Reduction Theory of Quadratic Forms

2.1. Joseph Louis Lagrange

Diophantine analysis pertains, in general terms, to the study of the solvability of polynomial equations in integers or, alternatively, in rationals. This subject has a long tradition. The treatise by Dickson on the history of the theory of numbers, published in three volumes between 1919 and 1923, gives an account of the early results in this field. In the XVIII$^{\text{th}}$ and early XIX$^{\text{th}}$ centuries, the interest was mainly in rational solutions. However, it had been an important issue for Fermat to state the distinction between rational and integral solutions, which is discussed as well at the beginning of the *Disquisitiones Arithmeticae*. Initially, investigations of particular Diophantine equations involved methods of a more ad-hoc nature. Only in relatively recent times have more coherent theories emerged.

The arithmetic theory of quadratic forms is a central part of this field. Fermat and Euler had studied the nature of integral solutions of equations $f(x, y) = ax^2+by^2 = m$, where a, b, m are integers, in specific cases. It was the particular question regarding whether a given integer m can be represented by the quadratic form f (i. e. do there exist integers x, y so that $f(x, y) = m$?) which played a decisive role in the formation of the theory. Joseph-Louis Lagrange (1736–1813) unified these various investigations of particular forms in the systematic work "Recherches d'Arithmetique," [Lagrange 1773–1775]. There he laid the foundations of the theory of binary quadratic forms, that is, expressions of the form, $f(x, y) = ax^2 + bxy + cy^2$ with integral coefficients a, b, c and variables x, y. His work hinged on the observation that forms which can be transformed into one another by a substitution of the form $X = px+qy$, $Y = rx+sy$, where p, q, r, s are integers and $ps-rq = 1$ or $ps - rq = -1$, represent the same numbers. After Gauss, in particular, two such forms f and g are said to be equivalent.[13]

Lagrange highlighted the important role of the quantity $-b^2 + 4ac$, attached to a binary quadratic form f – we now consider the negative of this quantity, the discriminant $D(f)$.[14] A substitution of the form given above does not alter this quantity, that is, equivalent binary quadratic forms have the same discriminant.

[13] This relation is of course reflexive, symmetric and transitive, and an integral solution for the equation $f(x, y) = m$ gives rise to one for $g(X, Y) = m$ and vice versa.

[14] This term is related to the determinant $\Delta(f)$ by $D(f) = -4\Delta(f)$, which was the quantity privileged par Gauss. Plainly $D(f) \equiv 0 \mod 4$ if b is even and $D(f) \equiv 1 \mod 4$ if b is odd. The relation $4af(x, y) = (2ax + by)^2 - D(f)y^2$ implies that the values taken by f are all of the same sign or zero if $D(f) < 0$; accordingly f is called positive or negative definite. If $D(f) > 0$ then f takes values of both signs; in this case f is called indefinite. Like many of our authors, in the following we suppose that D is not a square and D does not equal zero. Note that a form f with $D(f)$ a square splits into a product of two linear factors.

More importantly, Lagrange observed that a given form can be transformed by a finite sequence of substitutions in an equivalent form f for which

$$|b| \leq |a| \qquad |b| \leq |c|.$$

Consequently there are only finitely many triples (a, b, c) that satisfy these conditions and so that the expression $b^2 - 4ac$ takes a given value, the discriminant of f. For if $|a| \leq |c|$ (which we may suppose) then $|D| = |b^2 - 4ac| \geq 3|a|^2$. Thus the coefficients of f have to satisfy the conditions

$$|a| \leq \sqrt{\frac{|D|}{3}}, \ |b| \leq |a|, \ c = \frac{b^2 - D}{4a}.$$

A binary quadratic form for which the above conditions hold on a, b, c (i. e. $|b| \leq |a|$ and $|b| \leq |c|$) is now said to be reduced in the sense of Lagrange.

By a subtle constructive method Lagrange was able to select from the infinitely many forms which are equivalent to a given form at least one which is characterized in some intrinsic way. He proceeded to apply these concepts to obtain far reaching results in the problem of the representation of integers by binary quadratic forms. In addition to this new approach – which gave rise to what afterwards became known as reduction theory –, Lagrange also discussed the question of how to determine the minimum $m(f)$ of a given form f (i. e. the minimum absolute value taken by $f(x, y)$ for all integers x, y not both zero), [Lagrange 1774]. Using the theory of continued fractions, he developed a constructive solution. Adrien-Marie Legendre pointed out, in [Legendre 1830], that, in the case of positive definite binary quadratic forms, there is a close relation between this question and reduction theory. For a given form g there is always an equivalent reduced form f (i. e., one whose coefficients satisfy the relation $|b| \leq a \leq c$) so that the coefficient a coincides with the minimum $m(f) = m(g)$. This principle that the leading coefficient of a reduced form can be characterized by a minimum condition for all forms in the corresponding class proved decisive in the further stages of the reduction theory of quadratic forms for arbitrary many variables.

2.2. *Initial Stages of Geometric Thinking in the Work of Gauss and Dirichlet*

A major part of Gauss's *Disquisitiones Arithmeticae* pertains to the theory of binary quadratic forms, and arts. 171–175 contain a systematic treatment of this theory. Gauss introduced the notion of proper equivalence, for which two forms belong to the same class if there exists an integral unimodular substitution

$$X = px + qy, \quad Y = rx + sy, \quad ps - qr = 1,$$

relating them. This notion differs notably from the one used by Lagrange. However, an analoguous result in the case of positive definite binary quadratic forms is obtained: a given form can be transformed into a form $f(x, y) = ax^2 + bxy + cy^2$ for which either $-a < b \leq a < c$ or $0 \leq b \leq a = c$. A form for which one or the other of these condtions holds is what we nowadays call "reduced in the sense of Gauss."

There are only finitely many reduced forms with a given discriminant, and any two reduced forms are not properly equivalent.

In a similiar vein, Gauss began to develop in the *Disquisitiones Arithmeticae* a reduction theory for positive definite ternary forms. This approach was finally completed by Ludwig August Seeber in his 1831 treatise *Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen*, [Seeber 1831]. Again, Seeber defined reduction by a finite set of linear inequalities on the coefficients. In his extensive review of this work, [Gauss 1831], Gauss acknowledged the results obtained by Seeber, and supplied some simplified arguments or improvements. Gauss's concluding remarks in his review are of particular importance to the current study. There he discussed the interpretation of a positive definite binary or ternary quadratic form as a lattice in space.

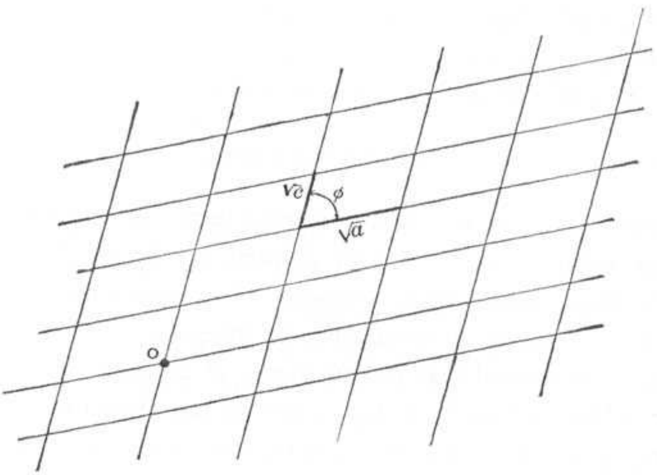


Fig. 13.

Fig. VIII.1A. Gauss's geometric representation of binary quadratic forms in Felix Klein's eighth lecture at Northwestern University, Evanston

Gauss suggested the following geometric construction: Given a positive definite binary quadratic form $f = ax^2+2bxy+cy^2$ the equation $\cos\alpha = b/\sqrt{ac}$ determines uniquely an acute or obtuse angle α so that one can attach a system of coordinates to f whose axes form the angle α. Then an arbitrary point in the plane has the coordinates $x\sqrt{a}$, $y\sqrt{c}$ with respect to this system. The form f gives the square of the distance of an arbitrary point to the origin. So far as the variables refer to integers the form f makes reference to a system of points which is given as the intersection of two families of equidistant parallel lines. In this way the plane is subdivided into parallelograms whose vertices just form this system of points. The determinant, that is, $ac - b^2$, coincides with the square of the area of each parallelogram.

Gauss then pointed out that such a given system of points can be subdivided into parallelograms in infinitely many ways. Thus, it refers to infinitely many forms as well. However, all these forms are equivalent, the area of a fundamental parallelepiped remains the same. In turn, equivalent forms give rise to the same system of points, but with reference to a different system of coordinates.

In the following, Gauss described this geometric interpretation in the case of ternary quadratic forms $ax^2+by^2+cz^2+2a'yz+2b'xz+2c'xy$. The determinant of such a form is given by the term $\Delta = abc + 2a'b'c' - bb'^2 - aa'^2 - cc'^2$. Concluding his review of Seeber's work, Gauss reinterpreted the relation $abc \leq 2\Delta$ between the coefficients of a reduced form f and its determinant, as conjectured by Seeber, in geometrical terms. Within this new set up, Gauss could give a simple proof for this estimate.

In current terminology this geometric interpretation can be described as follows: the coefficients of a given positive definite quadratic form in n variables, $f = \sum_{i,k} a_{ik}x_ix_k$, with $a_{ik} = a_{ki}$, give rise to a positive definite matrix $F = (a_{ik})$ which may be viewed as an element in the matrix algebra of $(n \times n)$- matrices with real entries. Then there exists a real matrix T so that F may be written as $F = T^tT$, that is, the symmetric bilinear form F on the real vectorspace $\mathbf{R^n}$ is identified with the usual Euclidean metric on this space, given by the identity matrix. The i-th column vector of T is denoted by t_i. We attach to f the lattice L in $\mathbf{R}^n$, defined as $\{\sum_i \alpha_i t_i | \alpha_i \in \mathbf{Z}\}$, spanned by the column vectors of T. Note that equivalent forms determine the same lattice but the basis vectors t_i are transformed by an integral linear transformation with determinant $+1$ into some other basis vectors for L. With respect to the canonical scalar product on Euclidean space one has the identities

$$(a_{ik}) = T^tT$$

$$a_{ii} = |t_i|^2,\ i = 1,\ldots,n\ ;\ a_{ik} = |t_i|\cdot|t_k|\cos\omega_{ik},\ i \neq k$$

where ω_{ik} denotes the angle between t_i and t_k. For a point $z = \sum \alpha_i t_i \in L$ in the lattice one has

$$|z|^2 = z \cdot z = f(\alpha_1, \ldots, \alpha_n),$$

that is, f gives the square of the distance of a lattice point to the origin. Note that in this geometric setting the minimum of f is given by the square of the minimal distance between two lattice points.

In giving this interpretation in geometrical terms in which Seeber's results should be looked at, Gauss stressed the view that this approach should lead to new far reaching methods and results. He also remarked that this type of reduction theory could be extended to forms whose coefficients are not necessarily integral ones:

> However, we should not omit the remark that, though originally a, b, c, a', b', c' represent integers, the major part of the theory of ternary forms … remains valid, independent of this assumption.[15]

[15] [Gauss 1831/1840], p. 319: *Wir dürfen jedoch die Bemerkung nicht übergehen, daß a, b, c, a', b', c' ganze Zahlen vorstellen, doch der größte Theil von der Lehre von den ternären Formen, und namentlich dasjenige was für jene Benutzung erforderlich ist, auch unabhängig von jener Voraussetzung gültig bleibt.*

This suggestion by Gauss to interprete ternary quadratic forms as lattices in space was taken up by Dirichlet in his paper "Über der Reduction der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen" which he presented to the Prussian Academy of Sciences in July 1848. Dirichlet provided a profound, systematic treatment of Seeber's results in completely geometric terms. He also unfolded a revisited form of reduction theory by working with lattices as geometric objects and with the corresponding notion of distance within the lattice in question. He obtained conditions of reduction on the coefficients by a principle of successive minima. More precisely, given a positive definite ternary form there is a corresponding geometrical object, namely, a system of points which is formed by the intersection of three families of equidistant parallel planes. In other words, the system of points is endowed with a subdivision given by a parallelepiped. Equivalent forms correspond to the same system of points but endowed with different subdivisions; again, the underlying parallelepipeds have the same content.

Finding conditions of reduction for the coefficients of a given form is then guided by a geometric argument. In the case of binary forms, Dirichlet showed that one can always find a subdivision so that the edges of the underlying parallelograms are not larger than its diagonals. A parallelogram with this property is called reduced. In the case of ternary forms, as Dirichlet proved, there is always a subdivision so that the faces of the underlying parallelepiped are reduced parallelograms and the edges are not larger then its diagonals. Minkowski later acknowledged, in [Minkowski 1893], that this work of Dirichlet proved decisive in his approach to the theory of quadratic forms.

2.3. Charles Hermite's Letters to Jacobi

For the development of his own work, Minkowski attached a similar important significance to the 1850 publication "Extraits de lettres de M. Ch. Hermite à M. Jacobi sur differents objets de la théorie des nombres," [Hermite 1850]. These letters stressed the remarkable programmatic shift that many of the properties of integers, or of the rational numbers, are most conveniently approached by methods which use irrational numbers, or again (in [Hermite 1851]) by methods which introduce continuous variables in the theory of numbers. Similarly, equations in integers may often be better examined in terms of inequalities. The following question, also mentioned by Minkowski at various occasions, may be viewed as exemplary of Hermite's approach relating a problem in Diophantine approximation to the arithmetic theory of quadratic forms.

Let a be an arbitrary real number, let δ be a positive parameter, and consider the binary quadratic form

$$(x - ay)^2 + \frac{y^2}{\delta}.$$

The determinant of this form is $1/\delta$. Hermite knew that for a given form f of determinant Δ there exists a constant γ independent of f such that the ratio of the minimum of f to the root of its determinant is bounded from above by γ; the best possible constant in this case is $2\sqrt{\frac{\Delta}{3}}$. Thus, applying this result to the particular form defined above, there are integers p and q so that

$$(p-aq)^2+\frac{q^2}{\delta}\leq\sqrt{\frac{4}{3\delta}}.$$

As δ increases from zero to infinity one obtains, by taking for a given δ integers p and q so that the corresponding form takes its precise minimum on these values, the set of convergents to a in its expansion as a continued fraction.

Applications of this type led Hermite to develop a reduction theory for quadratic forms in n variables, first published in his letters to Jacobi.[16] In his treatment, he followed very much the approach taken in the binary and ternary case in Gauss's *Disquisitiones Arithmeticae*, though a slight modification in the defining conditions for a reduced form had to be made. In the binary case the coefficients a and c of a reduced form $f=ax^2+bxy+cy^2$ can be characterized by the fact that a coincides with the (first) minimum of f, denoted by $\mu(f)$, and c coincides with the so-called second minimum, given as $minf(z)$ where z ranges over all lattice vectors $z\neq 0$ linearly independent of one, let us say z', for which $f(z')$ is the minimum $\mu(f)$. Due to the work of Seeber and Dirichlet, one could give a similar characterization in the ternary case but for larger n this procedure failed.[17] Hermite defined a reduced positive definite quadratic form with real coefficients in a recursive way making full use of a principle of successive minima. Within an equivalence class of positive definite quadratic forms a form $f=\sum a_{ik}x_ix_k$ is now said to be reduced in the sense of Hermite if f gives rise to the smallest system $(a_{11},a_{22},\dots,a_{nn})$ (that is, to the smallest value of $a_{11}g^{n-1}+a_{22}g^{n-2}+\cdots a_{nn}$ for sufficiently large positive g) in the n coefficients. Consequently, all reduced forms in the given class coincide in these coefficients. The coefficient a_{11} is characterized as the minimum of the form f. In the general case it is difficult to give a simple characterization of reduced forms in terms of the coefficients of the form. It should be noted that Hermite did not take into consideration the geometric interpretation of quadratic forms via lattices as introduced by Gauss and Dirichlet. However, this concept of reduction provided a way to select, from the infinitely many forms which are integrally equivalent to a given form, one which is characterized in some intrinsic way. Moreover, a form is equivalent to at most finitely many reduced forms.

An estimate for the ratio of the minimum of a definite quadratic form in n variables to the n-th root of its determinant by a constant depending only on n played a major role in Hermite's work on quadratic forms and, in particular, in its applications to various problems in number theory. Having repeated the well-known case $n=2$, Hermite stated and proved as one of his main results, [Hermite 1850], p. 263, that there is a constant c_n so that for a positive definite form f in n variables,

[16] These letters, and Hermite's programme, are discussed in C. Goldstein's chap. VI.1 in the present volume.

[17] The reason is that, in general, successive minimal vectors do not form a basis of the lattice in question. For a counter-example in the case $n=5$ we refer to [Van der Waerden 1956], sec. 7.

with determinant $\Delta(f)$, one has the estimate

$$\mu(f) \leq c_n \Delta(f)^{1/n}.$$

One may take as proved by Hermite that $c_n = (4/3)^{\frac{n-1}{2}}$. This is the best possible value for $n = 2$, as can be seen by considering the form $x^2 + 2xy + y^2$. Already in the case $n = 3$, the result by Seeber, as improved by Gauss, that the coefficients $a_{ii}(i = 1, 2, 3)$ of a reduced form satisfy the inequality $\prod_i a_{ii} < 2\Delta$ implied a sharper estimate. One has $\mu(f) \leq 2^{1/3}\Delta(f)^{1/3}$. This is a consequence of the estimate $abc \leq 2\Delta$ between the coefficients of a reduced form f and its determinant, because a is characterized as the minimum $\mu(f)$ and b, c as the successive minima.

In view of the many and diverse applications, for example, to questions of Diophantine approximation, the problem to determine the precise bound for the minimum of a quadratic form was a major issue in subsequent work. Even in cases of a small number of variables, this question gave rise to an extensive discussion of how the defining conditions for a reduced form could be refined. In 1874 Eduard Selling suggested a different approach to the reduction theory of binary and ternary quadratic forms, including the case of indefinite forms as well, see [Selling 1874]. He was familiar with Gauss's and Dirichlet's geometric ideas in this subject. Léon Charve extended the methods of Selling to the quaternary case in 1881.

Aleksandr N. Korkin and Egor I. Zolotarev, also, made crucial contributions, both theoretically and methodologically, with their publications in the *Mathematische Annalen*, [Korkin, Zolotarev 1872, 1873, 1874]: they gave a precise bound for the minimum in the quaternary case by reducing the question to the ternary case and, in their 1872 article, they introduced the notion of an extreme form, that is, one for which the ratio of the minimum of a positive definite quadratic form to the n-th root of its determinant takes the maximum value. They were also able to determine these forms in all cases $n \leq 5$. However, a detailed discussion of these results would lead us too far astray.

3. The Early Work of Minkowski in Reduction Theory

3.1. Minkowski and Hermite's Reduction Theory

In 1883 Minkowski published a short note, [Minkowski 1883], in which he took up Hermite's reduction theory for positive definite quadratic forms in n variables with real coefficients. Lagrange had given the conditions characterizing a reduced form for the case $n = 2$ and Seeber for the case $n = 3$: Minkowski stated a new result for quaternary forms.[18] He proved that a given form can be transformed by a finite sequence of unimodular substitutions into a reduced one. Moreover, a reduced form can be characterized by a finite number of linear inequalities in the coefficients.

In the second part of his paper "Ueber positive quadratische Formen," submitted in January 1885 to Crelle's Journal, he added to his previous results in the quaternary case a treatment of the case $n = 5$. He obtained an analogous characterization of a reduced form by means of a finite number of inequalities. As he pointed out,

[18] Léon Charve had also provided a reduction theory for such forms in 1881 and 1882.

> the more equality holds in the inequalities…, the more peculiar is a reduced form.[19]

This led him to introduce the notion of a "(primitive) Grenzform" and to establish these in the cases in question. These are closely related to the "formes extremes," introduced by Korkin and Zolotarev in 1872. Of particular interest is Minkowski's remark:

> These propositions, which for $n = 2$ and $n = 3$ express interesting properties of lattices in the plane or space, appear all the more remarkable the more they fail to hold for larger values of n.[20]

First, he was aware of the geometric interpretation of his results in terms of lattices. Second, it appears that Minkowski already had in mind that the notion of a reduced form in the sense of Hermite was not sufficient to characterize reduced n-ary forms for larger n by a finite number of linear inequalities in the coefficients.

3.2. An Unpublished Manuscript of Minkowski

In November 1883, while in Berlin, Minkowski wrote a draft of a manuscript which he titled "Zur Theorie der Reduction der wesentlich positiven quadratischen Formen."[21] On the one hand, here Minkowski layed the foundations for the results in the case $n = 5$ discussed above. On the other hand, the manuscript revealed the problems Minkowski had to face in his attempt to extend these results to the arbitrary case. In turn, Minkowski realized that the notion of a reduced form in the sense of Hermite was no longer adequate and, hence, required change.[22]

This unfinished manuscript consists of four chapters with a preceeding introduction. In the latter, Minkowski described the intended focus of this treatise:

> Hermite has shown which important conclusions one could draw from the knowledge of the precise bound for the minimum of a general positive quadratic form. To gain this knowledge a more detailed study of the reduction of positive forms in n variables appears necessary, however.
>
> Hermite has carried over the notion of a reduced form, put forward by Lagrange for the case of two variables, to the case of an arbitrary number of variables, and, particularly, the extension of this notion as given in his second letter to Jacobi, stands out by its great simplicity. In particular, the reduced forms set up there have the outstanding quality to be completely defined by a finite number of linear inequalities between the coefficients. In the following I intend, first, to give some theorems with reference to the reduced forms as set up by Hermite and, second, in particular, to show how one can deduce the determination of the precise bound for

[19] [Minkowski 1886]: *ist eine reduzierte Form umso eigenthümlicher, in je mehr von den Ungleichungen… das Gleichheitszeichen statt hat."*

[20] [Minkowski 1886]: *Diese Sätze, welche für* $n = 2$ *und* $n = 3$ *interessante Eigenschaften ebener und räumlicher Gitter ausdrücken, scheinen um so bemerkenswerter, als sie nicht mehr für grössere Werte des n gelten.*

[21] Manuscript, box IV, folder 3, in Notebooks H. Minkowski, unpaginated, ten boxes, Niels Bohr Library, American Institute of Physics, College Park, MD, USA.

[22] The content of this early manuscript and its significance for the development of Minkowski's reduction theory is discussed in detail in [Schwermer 2006].

> the minimum from the linear inequalities. At the same time the connection between the reduced forms of Hermite and the Gränzformen of Korkine and Zolotareff will become apparent.[23]

In chap. 1 of this manuscript, Minkowski considered positive definite quadratic forms f and proved that for a given bound there are only finitely many integral vectors x not equal to zero so that the value of f taken on x is smaller than the bound. As a consequence, he stated, one can find in a finite number of steps the smallest positive number N which can be represented by f, the so called minimum of f. Minkowski provided two different ways to prove these assertions. None of these is geometrical in nature.

In chap. 2, Minkowski introduced the usual notion of equivalence of forms in terms of integral substitutions with determinant one. In order to compare forms he introduced the following definition: A positive definite form $g = \sum b_{ik} y_i y_k$ stands next to a form $f = \sum a_{ik} x_i x_k$ if all the coefficients a_{hh} of f coincide with the corresponding coefficients b_{hh} of g. If this is not the case and if the first of the coefficients $a_{11}, a_{22}, \ldots, a_{nn}$ that does not coincide with the corresponding one of the coefficients b_{11}, b_{22}, ..., b_{nn} is a_{hh}, let us say for instance that a_{hh} is greater than b_{hh}, then f is said to stand above g, and g is said to stand below f, and that at the h-th entry. In what followed Minkowski provided a proof of the fact that in a given equivalence class (*Formenclasse* f) there are always a finite number of forms which stand below all other ones in the class. These are the reduced forms as introduced by Hermite.

The content of chap. 3 holds the essence of the development of Minkowski's theory of reduction, as it finally appeared in print in his paper "Diskontinuitätsbereich für arithmetische Äquivalenz," [Minkowski 1905]. There, Minkowski's considerations make it quite clear how he was led later on to his notion of a reduced form. His definition was slightly simpler than the one given by Hermite, and, as it turned out, if a form f was reduced in the sense of Hermite it was also reduced in the sense of Minkowski. The remarkable shift in the defining conditions for a given form f to be reduced in the sense of Minkowski appeared in chap. 3 as an observation

[23] *Hermite hat gezeigt, welche wichtigen Folgerungen man aus der Kenntnis der präzisen Gränze für das Minimum einer allgemeinen positiven quadratischen Form ziehen könnte. Um zu dieser Kenntnis zu gelangen, scheint jedoch ein eingehenderes Studium der Reduction der positiven Formen von n Variablen erforderlich. Hermite hat den von Lagrange für den Fall zweier Variablen aufgestellten Begriff einer reducierten Form, auf den Fall einer beliebigen Variablenzahl übertragen, und es zeichnet sich namentlich die in seinem zweiten Brief an Jacobi gegebene Erweiterung dieses Begriffs durch ihre grosse Einfacheit aus. Namentlich besitzen die daselbst aufgestellten reducierten Formen die hervorragende Eigenschaft durch eine endliche Anzahl linearer Ungleichungen zwischen den Coefficienten völlig definiert zu sein. Im Folgenden beabsichtige ich zunächst einige Theoreme in Bezug auf die von Hermite aufgestellten reducierten Formen zu geben, und dann namentlich zu zeigen, in welcher Weise die Bestimmung der präzisen Gränze für das Minimum aus den linearen Ungleichungen zu erschliessen ist. Hierbei wird zugleich der Zusammenhang zwischen den reducierten Formen von Hermite und den Gränzformen von Korkine und Zolotareff ersichtlich werden.*

about a reduced form in the sense of Hermite. If a reduced form $f = \sum \alpha_{ik} x_i x_k$ is transformed under an integral substitution[24]

$$S) \qquad x_i = \sum_{i=1}^{n} s_i^k y_k,$$

so that the coefficients s_i^k satisfy the equations

$$\sum_{1}^{n} \alpha_{ik} s_i^t s_k^t = \alpha_{tt} \ , \ t = 1, 2, \ldots, h-1,$$

then at the same time the inequality

$$T) \qquad \sum_{1}^{n} \alpha_{ik} s_i^h s_k^h \geq \alpha_{hh}$$

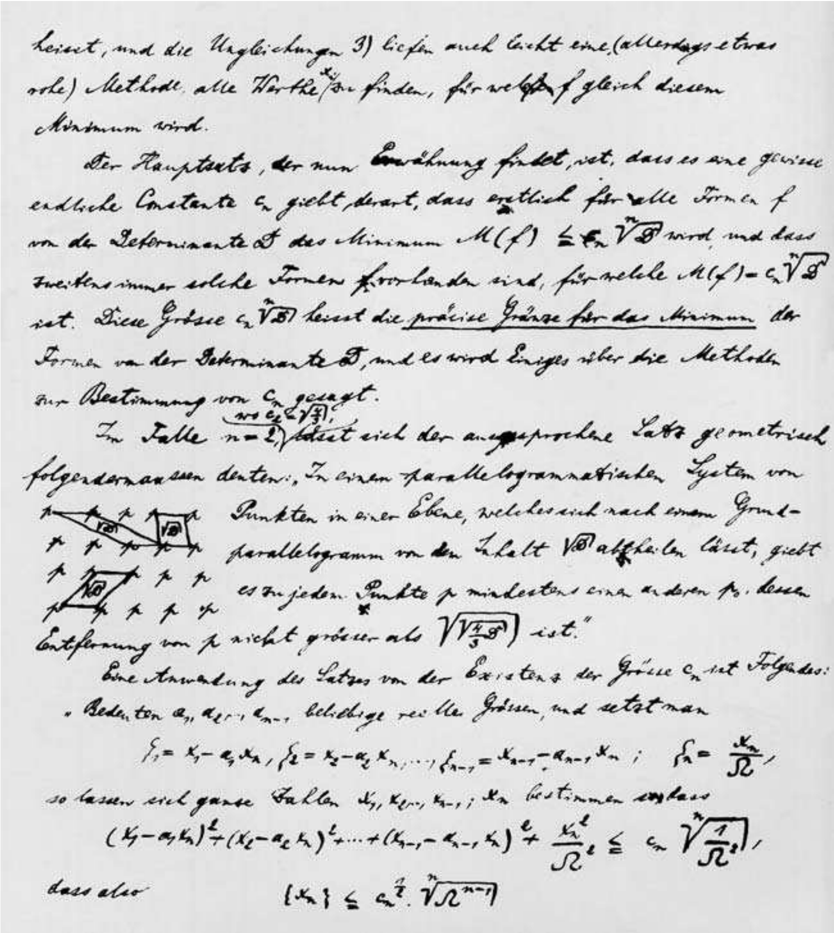
has to be valid. Otherwise, the new form obtained by this transformation would fall below f. Thus, any arbitrary substitution $S)$ of determinant 1 gives rise to certain restrictions on the coefficients of a reduced form. For Minkowski, the task at hand was to approach these inequalities by means of a finite set of substitutions so that all other ones are consequences of these. He then began to consider the following special substitutions: if out of n integers $s_1, s_2, \ldots, s_n$, the $n-k+1$ last ones $s_k, s_{k+1}, \ldots, s_n$ do not have a common divisor different from one, then there is a substitution of determinant 1 whose first $k-1$ columns coincide with the ones of the identity matrix and whose k-h column is formed by the integers $s_1, s_2, \ldots, s_n$. A substitution of this type does not alter the coefficients $\alpha_{11}, \alpha_{22}, \ldots, \alpha_{k-1,k-1}$ of a reduced form, and one obtains the inequality

$$U) \qquad \sum_{1}^{n} \alpha_{ik} s_i s_k \geq \alpha_{kk}.$$

If one compares the inequalities $U)$ with the content of §4 in 1905 Minkowski's paper, especially sec. 1, one immediately notices the similarity in approach. In his draft of 1883, however, Minkowski did not use these inequalites to formulate a new definition of a reduced form.[25] Though, the latter part of chap. 3 comprises a lengthy and very involved treatment of how a finite set T of inequalities can be extracted out of the set given by the inequalities $U)$ so that the validity of $T)$ implies the validity of all of them. Minkowski completed this task in the cases $n \leq 5$. Consequently, he obtained a characterization of a reduced form in the sense of Hermite by a finite set

[24] Here and in what follows we use Minkowski's original write up.

[25] The first manuscipt I am aware of and in which this new definition is given is an unpublished one written in 1897 in Zürich. One might view this latter manuscript as an incomplete draft preceding the publication "Diskontinuitätsbereich für arithmetische Äquivalenz" in 1905. For details we refer to [Schwermer 2006].



$\sqrt{D}$
$\sqrt{D}$
$\sqrt{D}$

heisst, und die Ungleichungen 3) liefern auch leicht eine (allerdings etwas rohe) Methode, alle Werthe x_i zu finden, für welche f gleich diesem Minimum wird.

Der Hauptsatz, der nun Erwähnung findet, ist, dass es eine gewisse endliche Constante c_n giebt, derart, dass erstlich für alle Formen f von der Determinante D das Minimum $M(f) \leq c_n \sqrt[n]{D}$ wird, und dass zweitens immer solche Formen vorhanden sind, für welche $M(f) = c_n \sqrt[n]{D}$ ist. Diese Grösse $c_n \sqrt[n]{D}$ heisst die präcise Gränze für das Minimum der Formen von der Determinante D, und es wird Einiges über die Methoden zur Bestimmung von c_n gesagt.

Im Falle $n = 2$, (wo $c_2 = \sqrt{\frac{4}{3}}$), lässt sich der ausgesprochene Satz geometrisch folgendermaassen deuten: „In einem parallelogrammatischen System von Punkten in einer Ebene, welches sich nach einem Grundparallelogramm von dem Inhalt $\sqrt{D}$ abtheilen lässt, giebt es zu jedem Punkte p mindestens einen anderen p_0, dessen Entfernung von p nicht grösser als $\sqrt{\sqrt{\frac{4}{3}D}}$ ist."

Eine Anwendung des Satzes von der Existenz der Grösse c_n ist Folgendes:

„Bedeuten $a_1, a_2, \dots, a_{n-1}$ beliebige reelle Grössen, und setzt man

$$\xi_1 = x_1 - a_1 x_n,\ \xi_2 = x_2 - a_2 x_n, \dots, \xi_{n-1} = x_{n-1} - a_{n-1} x_n;\quad \xi_n = \frac{x_n}{\Omega},$$

so lassen sich ganze Zahlen $x_1, x_2, \dots, x_{n-1}; x_n$ bestimmen, so dass

$$(x_1 - a_1 x_n)^2 + (x_2 - a_2 x_n)^2 + \dots + (x_{n-1} - a_{n-1} x_n)^2 + \frac{x_n^2}{\Omega^2} \leq c_n \sqrt[n]{\frac{1}{\Omega^2}},$$

dass also

$$\{x_n\} \leq c_n^{\frac{1}{2}} \cdot \sqrt[n]{\Omega^{n-1}}$$

Fig. VIII.1B. Talk by Hermann Minkowski, May 20, 1884
From the exposé written by himself in the colloquium book, University of Königsberg
(Courtesy[26] of Foundation Otto Volk,
Institute of Mathematics, University of Würzburg, Germany)

[26] I would like to thank Prof. Dr. H.-J. Vollrath, who kindly helped me to obtain the scan of this illustration.

of linear inequalities in the coefficients. Minkowski gave an explicit calculation for the cases $n < 5$ in chap. 4 but did not fully treat the $n = 5$ case. Minkowski stated the result in this case without further proof in a published paper [Minkowski 1886], where he also included the previously known cases.

In fact, Minkowski already mentioned Korkin and Zolotarev's papers his unfinished 1883 manuscript; here, at an early stage, Minkowski realized that the question of how to determine the precise bound for the minimum in the general case is closely related to a refinement of Hermite's reduction theory. Geometrical concepts had not directed his methods of investigation in this manuscript of 1883. However, the reinterpretation of forms as geometrical objects as well as a methodological shift became increasingly important already in the following year.

In his talk in the mathematical colloquium at Königsberg, given on May 20, 1884, Minkowski discussed this question regarding the minimum of a positive definite quadratic form. As his main result he stated the existence of such a constant c_n as alluded to above. Then he considered various methods to determine a precise bound. Remarkably, Minkowski discussed the geometrical significance of this precise bound in the case $n = 2$ as a result about the existence of a shortest vector in the lattice attached to the quadratic form in question. This point of view unfolded in the following years as an essential ingredient in Minkowski's work.

4. *Räumliche Anschauung* in the Early Work of Minkowski

4.1. Minkowski's Lecture "Über einige Anwendungen der Arithmetik in der Analysis"

As part of the requirements for his *Habilitation* Minkowski had to give a lecture, officially called *Probevorlesung*, to the members of the division for mathematics and natural sciences of the philosophical faculty at the university of Bonn. A *Colloquium*, that is, a discussion about the subjects of the talk, had to follow. On March 15, 1887, Minkowski lectured on the theme "Über einige Anwendungen der Arithmetik in der Analysis."[27] Following the manuscript of his lecture, he started with:

> The applications of arithmetic I want to talk about concern the problem to measure a given entity by means of rational numbers. This is a task of fundamental importance in analysis.[28]

In what followed Minkowski gave numerous examples which led him to consider this kind of subject. In particular, he referred to the problem of approximating a real number a by rational numbers x/y, already discussed by Hermite. Following his approach, Minkowski translated this question into the problem of minimizing the quadratic form $(x - ay)^2 + (ty)^2$. He viewed this as an approximate solution of

[27] Minkowski's *Habilitation* is discussed and documented in detail in [Schwermer 1991], one also finds there the manuscript of his *Probevorlesung* and the minutes of the corresponding faculty meeting.

[28] *Die Anwendungen der Arithmetik, von welchen ich sprechen will, betreffen die Aufgabe, irgendwie gegebene Grössen durch rationale Zahlen zu messen. Es ist das eine Aufgabe von fundamentaler Bedeutung in der Analysis.*

the system $x - ay = 0, \quad ty = 0$, where a is the given number and t is a small number assigning a weight to the condition $y = 0$. In order to have some systematic treatment of forms as described, he set up a more general framework. Consider three linear forms $\xi, \ \eta, \ \zeta$ depending on the variables x, y, z which only take integral values. The basic problem is to solve the equations $\xi = 0, \ \eta = 0, \ \zeta = 0$ in integers. Of course, the trivial solution $x = y = z = 0$ is not of interest, so one has to look for a solution such that the "equation" holds as an approximation. To make this precise, one has to establish in which sense one solution is better than another. Minkowski discussed this question from both a probabilistic and an analytic point of view. More importantly, he pointed out that the geometric interpretation of the linear forms $\xi, \ \eta, \zeta$ as orthogonal coordinates in space leads as well (and even more naturally) to a study of the form $\xi^2 + \eta^2 + \zeta^2$ because its square root measures the distance of a solution to the trivial solution. This term, expressed in the variables x, y, z, is a quadratic form. Minkowski continued in describing how one attaches the corresponding lattice to a given positive definite quadratic form. In discussing the minimal distance between lattice points he arrived at the following:

> For example, if one imagines an impenetrable ball centered at each lattice point of diameter equal to the minimal distance between [lattice] points, … these balls, which include exactly one lattice point, would touch one another in the directions of the lines connecting two points with minimal distance but they would not intersect one another, and they would still leave between one another some space without lattice points. Therefore, a portion of the space which is equal to such a ball with respect to its volume would, on average, not account for a full lattice point. However, a portion equal to the content of an elementary parallelepiped accounts for exactly one point. Hence the volume of a ball whose diameter is equal to the minimal distance between lattice points, that is, $\pi/6$ times third power of this distance, has to be smaller than the volume of an elementary parallelepiped. Thus, the distance is always smaller than the product of a constant and the third root of the volume of the elementary parallelepiped.[29]

A few lines later, he stated

> Of course, the same [statement] is valid for lattices in any number of dimensions,

[29] *Denkt man sich z. B. um jeden Gitterpunkt als Centrum eine undurchdringliche Kugel von einem Durchmesser gleich der Entfernung zweier nächster Punkte, so wird diese Entfernung überhaupt nicht kleiner werden können. Diese Kugeln, welche je einen Gitterpunkt einschliessen würden, würden sich in den Richtungen der Verbindungslinien zweier nächster Punkte berühren, sie thäten sich aber niemals schneiden, und würden zwischen sich noch einen von Gitterpunkten freien lassen. Auf einen Theil des Raumes, welcher an Inhalt einer solchen Kugel gleich wäre, würde also im Durchschnitt nicht ein voller Gitterpunkt zu rechnen sein. Nun kommt aber auf einen Raumtheil gleich dem Inhalt eines Elementarparallelepipedons genau ein Punkt. Also muss der Inhalt einer Kugel, deren Durchmesser gleich der Entfernung zweier nächster Punkte im Gitter ist, d. i.* $\pi/6$ *mal der dritten Potenz dieser Entfernung, kleiner sein als der Inhalt eines Elementarparallelepipedums, also bleibt diese Entfernung selbst stets kleiner als das Product aus einer Constanten und der dritten Wurzel aus dem Inhalt des Elementarparallelepipedums.*

> and it is the expression of an important quality of positive quadratic forms as it was first proved in general by Hermite but in a much more troublesome way.[30]

That is, Minkowski referred to the general statement that the volume of a ball K centered at a lattice point, and of diameter equal to the minimal distance $\mu(f)$ of points in the given lattice $L(f)$ attached to a positive definite quadratic form f in n variables is smaller than or equal to the volume of $L(f)$. Writing out this relation it reads as

$$\text{vol }(K) = \omega_n(\frac{1}{2}\mu(f))^n \leq \text{ vol }(L(f))$$

where ω_n denotes the volume of the unit ball. This leads to the estimate

$$\mu(f) \leq 4\omega_n^{-2/n} \sqrt[n]{\Delta(f)}.$$

It was a remarkable step on the part of Minkowski to use the concept of volume in conjunction with the geometric interpretation of positive definite quadratic forms as lattices in space.

4.2. Towards Arithmetic

With regard to the procedures for a *Habilitation* in Bonn in 1887, Minkowski's *Probevorlesung* had to be a mathematical lecture by content but, simultaneously, the audience consisted out of the members of the division for mathematics and natural sciences of the philosophical faculty, only a few of whom were close to mathematics proper. Thus, Minkowski confined himself to describe some leading principles in the arithmetic theory of quadratic forms, supplemented by some applications in analysis. He unfolded a geometric treatment of these arithmetically defined objects. The improved estimate for the minimum of a positive quadratic form exemplified the strength of this methodological shift. Thus, the content of the lecture marked a decisive turning point in Minkowski's approach to the theory of quadratic forms. His method of investigation was led by some kind of spatial intuition, that is, what Minkowski called, *Räumliche Anschauung*. Later on, Minkowski extended the line of argument as given in the *Probevorlesung* by replacing the balls centered at each lattice point by arbitrary symmetric convex bodies, i. e., he finally confined his considerations to the relevant properties of the ball he had to use in the previous proof. The argument, however, forms the core of the lattice point theorem. It was this simple geometric idea that led to fundamental results such as, for example, his bound for the discriminant of an algebraic number field in number theory in later years.

[30] *Dasselbe gilt natürlich für Gitter in jeder Anzahl von Dimensionen, und ist der Ausdruck einer wichtigen Eigenschaft der positiven quadratischen Formen, welche allgemein zuerst von Hermite, aber auf weit umständlicherem Wege bewiesen ist.*

5. Conclusion

The suggestion made by Gauss in 1831 and pursued by Dirichlet in his 1848 paper on ternary forms to interprete an integral quadratic form as

> a system of points put in order by parallelepipeds, that is, as the intersection of three systems of equidistant parallel planes[31]

in space ultimately proved decisive in Minkowski's approach to the theory of quadratic forms.

In Minkowski's early papers on reduction theory, the geometric point of view became increasingly apparent in his interpretation of the results obtained in an arithmetical mode as results about lattices in space. It was a decisive step that this approach evolved into a direct treatment of the arithmetically defined objects, [that is, the quadratic forms,] in the geometric framework. In this way Minkowski changed a question about the minimum of a quadratic form into one about the minimal distance of lattice points. In his 1887 *Probevorlesung*, required for his *Habilitation* at the University of Bonn, Minkowski introduced the concept of volume into his analysis and gave a convincing example of how these ideas led to a new result on the minimum of a positive definite quadratic form, thus considerably enhancing the understanding of the question.

However, if we look beyond our chosen time frame, 1880 to 1887, in Minkowski's work, the theory of reduction remained as a major challenge for him. In 1905, with his celebrated "Diskontinuitätsbereich für arithmetische Äquivalenz," he completed his investigations on the arithmetic equivalence of positive definite quadratic forms with real coefficients. Ironically, he succeeded in doing so only by recourse to the more arithmetic methods already at hand in his very early work. Thus, the final solution of the problem of reduction eluded his purely geometric approach. We now know that this was not due to an inadequacy of such methods but rather to an oversight on his part. As was shown by Ludwig Bieberbach and Isaai Schur in 1928 and later further explained in work of Kurt Mahler and Robert Remak, the geometric methods as developed by Minkowski can completely solve the problem.[32] Thus, Minkowski's great achievement "Diskontinuitätsbereich für arithmetische Äquivalenz" contains an element of failure. Due to the success and to the geometric applicability of his results, as illustrated in the succeeding chapters of this publication, the mixed nature of their genesis was easily and often overlooked at that time.

[31] [Gauss 1831/1840], p. 319: *System parallelpipedisch geordneter, d. i. durch die Durchschnitte dreier Systeme paralleler äquidistanter Ebenen sich ergebender Puncte.*

[32] Taking into account the subsequent work in the theory of reduction in the 1930's and 1940's van der Waerden gives a complete treatment, based on geometric methods, of the main results of Minkowski's 1905 publication, [van der Waerden 1956].

References

DIRICHLET, Johann Peter Gustav LEJEUNE-. 1848. Über die Reduktion der positiven quadratischen Formen mit drei unbestimmten ganzen Zahlen. *Bericht über die Verhandlungen der Königlichen Preussischen Akademie der Wissenschaften*, 285–288. Repr. in *Werke*, ed. L. Kronecker, L. Fuchs, vol. 2, pp. 21–26. Berlin: Reimer, 1897; repr. New York: Chelsea, 1969.

———. 1850. Über die Reduction der positiven quadratischen Formen in drei unbestimmten ganzen Zahlen. *Journal für die reine und angewandte Mathematik* 40, 209–227. Repr. in *Werke*, ed. L. Kronecker, L. Fuchs, vol. 2, pp. 27–48. Berlin: Reimer, 1897; repr. New York: Chelsea, 1969.

EISENSTEIN, Gotthold. 1847. Note sur la représentation d'un nombre par la somme de cinq carrés. *Journal für die reine und angewandte Mathematik* 35, 368. Repr. in *Mathematische Werke*, vol. 2, p. 505. New York: Chelsea, 1975.

GAUSS, Carl Friedrich. 1831. Recension der "Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen von Ludwig August Seeber." *Göttingische Gelehrte Anzeigen*, July 9, 1065ff. Repr. *Journal für die reine und angewandte Mathematik* 20 (1840), 312–320. Repr. in *Werke*, vol. 2, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, pp. 188–196. Göttingen: Universitäts-Druckerei, 1863; 2nd augm. ed., 1876.

HERMITE, Charles. 1850. Extraits de lettres de M. Ch. Hermite à M. Jacobi sur différents objets de la théorie des nombres. *Journal für die reine und angewandte Mathematik* 40, 261–315. Repr. in *Œuvres*, ed. E. Picard, vol. 1, pp. 100–163. Paris: Gauthier-Villars, 1905.

———. 1851. Sur l'introduction des variables continues dans la theorie des nombres. *Journal für die reine und angewandte Mathematik* 41, 191–216. Repr. in *Œuvres*, ed. E. Picard, vol. 1, pp. 164–192. Paris: Gauthier-Villars, 1905.

KORKIN, Aleksandr N. and ZOLOTAREV, Egor. 1872. Sur les formes quadratiques positives quaternaires. *Mathematische Annalen* 5, 581–583.

———. 1873. Sur les formes quadratiques. *Mathematische Annalen* 6, 366–389.

———. 1874. Sur les formes quadratiques positives. *Mathematische Annalen* 11, 242–292.

LAGRANGE, Joseph-Louis. 1773–1775. Recherches d'Arithmétique. *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-Lettres de Berlin*, 1st part. 1773, 2nd part. 1775. Repr. in *Œuvres*, ed. J.-A. Serret, G. Darboux, vol. 3, pp. 693–795. Paris: Gauthier-Villars, 1869. Repr. Hildesheim, New York: Georg Olms, 1973.

———. 1774. Additions à l'analyse indeterminée. In *Eléments d'algèbre par M. Leonard Euler, trasuits de l'allemand avec des notes et des additions*, vol. 2, pp. 369–664. Lyon: Bryset (an III). Repr. in L. Euler, *Opera Omnia*, Series prima: opera mathematica, vol. 1, *Vollständige Anleitung zur Algebra mit den Zusätzen von J.-L. Lagrange*, ed. H. Weber, pp. 499–651. Leipzig, Berlin: Teubner, 1911.

LEGENDRE, Adrien-Marie. 1830. *Théorie des nombres.* 3rd ed. 2 vols. Paris: Firmin-Didot.

MINKOWSKI, Hermann. 1882. Grundlagen für eine Theorie der quadratischen Formen mit ganzzahligen Koeffizienten. French transl., Mémoire sur la théorie des formes quadratiques. *Mémoires présentés par divers savants à l'Académie des sciences* 2nd ser. 29 (1887), n°2, 180 pp. Repr. in [Minkowski 1911], vol. 1, pp. 3–144.

———. 1883. Sur la réduction des formes quadratiques positives quaternaires. *Comptes rendus de l'Académie des Sciences* 96, 1205–1210. Repr. in [Minkowski 1911], vol. 1, pp. 145–148.

———. 1886. Über positive quadratische Formen. *Journal für die reine und angewandte Mathematik* 99, 1–9. Repr. in [Minkowski 1911], vol. 1, pp. 149–156.

———. 1887a. Über den arithmetischen Begriff der Äquivalenz und über die endlichen Gruppen linearer ganzzahliger Substitutionen. *Journal für die reine und angewandte Mathematik* 100, 449–458. Repr. in [Minkowski 1911], vol. 1, pp. 203–211.

———. 1887b. Zur Theorie der positiven quadratischen Formen. *Journal für die reine und angewandte Mathematik* 101, 196–202. Repr. in [Minkowski 1911], vol. 1, pp. 212–218.

———. 1892. Über Geometrie der Zahlen. Jahresbericht der Deutschen Mathematiker-Vereinigung 1, 64–65. Repr. in [Minkowski 1911], vol. 1, pp. 264-265).

———. 1893. Anzeige zur Geometrie der Zahlen. *Mitteilungen von B. G. Teubner* 7. Leipzig, Berlin: Teubner.

———. 1905. Diskontinuitätsbereich für arithmetische Äquivalenz. *Journal für die reine und angewandte Mathematik* 129, 220–279. Repr. in [Minkowski 1911], vol. 2, pp. 53–100.

———. 1911. *Gesammelte Abhandlungen*, ed. D. Hilbert, coll. A. Speiser, H. Weyl. 2 vols. Leipzig, Berlin: Teubner. Repr. in 1 vol., New York: Chelsea, 1967.

OLESKO, Kathryn. 1991. *Physics as a Calling. Discipline and Practice in the Königsberg Seminar for Physics*. Ithaca and London: Cornell University Press.

SCHLOTE, Karl-Heinz. 1995. Die Königsberger Schule. In *Die Albertus Universität zu Königsberg und ihre Professoren*, ed. D. Rauschning, D. v. Nerée, pp. 499–508. Berlin: Duncker, Humblot.

SCHWERMER, Joachim. 1991. Räumliche Anschauung und Minima positiv definiter quadratischer Formen: Zur Habilitation von Hermann Minkowski 1887 in Bonn. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 93, 49–105.

———. 2006. On Minkowski's reduction theory for positive forms. Forthcoming.

SEEBER, Ludwig August. 1831. *Untersuchungen über die Eigenschaften der positiven ternären quadratischen Formen*. Freiburg: Wagner.

SELLING, Eduard. 1874. Über die binären und ternären quadratischen Formen. *Journal für die reine und angewandte Mathematik* 77, 169–229. French rev. transl., *Journal de mathématiques pures et appliquées* 3th ser. 3 (1877), 43–60, 153–206.

SERRE, Jean-Pierre. 1993. Smith, Minkowski et l'Académie des sciences. *Gazette des mathématiciens* 56, 3–9.

STROBL, Walter. 1985. Aus den wissenschaftlichen Anfängen Hermann Minkowskis. *Historia Mathematica* 12, 142–156.

VAN DER WAERDEN, Bartel Leendert. 1956. Die Reduktionstheorie der positiven quadratischen Formen. *Acta Mathematica* 96, 265–294. Repr. in *Studien zur Theorie der quadratischen Formen*, eds. B. L. van der Waerden, H. Gross, pp. 17–44. Basel: Birkhäuser, 1968.

VIII.2

Gauss Sums

Samuel James Patterson

The subject of this chapter is the determination of the sign of (quadratic) Gauss sums. The sums considered by Gauss are of the form

$$\sum_{j=0}^{n-1} \exp\Big(2\pi \mathrm{i} \frac{j^2}{n}\Big).$$

This determination of the sign, or rather of the argument, of this sum represents one of Gauss's most remarkable achievements. He discovered the underlying phenomenon experimentally while he was completing his work on the *Disquisitiones Arithmeticae*, shortly before it was finally published. He only discovered a formal proof some years later. This theorem and its ramifications have continued to fascinate over the last two hundred years – partly because of its intrinsic beauty and significance and partly because it goes considerably beyond what one should expect from class-field theory and the general theory of cyclotomic fields. There have been many very different proofs and many generalizations. Here we shall be concerned mainly with the proofs; a comprehensive survey of the generalizations would be too great a task to undertake within the confines of the present chapter. It should be remarked at this point that if n is square-free and odd then

$$\sum_{j=0}^{n-1} \exp\Big(2\pi i \frac{j^2}{n}\Big) = \sum_{x \pmod{n}} \Big(\frac{x}{n}\Big) \exp\big(2\pi \mathrm{i} \frac{x}{n}\big)$$

and therefore sums of the form $\sum\limits_{x \pmod{n}} \chi(x) \exp\big(2\pi \mathrm{i} \frac{x}{n}\big)$, where χ is a Dirichlet character to the modulus n, are also often called Gauss sums, as are their local and finite-field analogues. This multiple use of the designation has led to some confusion.

1. Gauss and Gauss Sums

The determination of the sign of the Gauss sums, in the case of a prime modulus, is stated – with remarkable confidence – by Carl Friedrich Gauss at the end of art. 356 of the *Disquisitiones Arithmeticae*. We know from his mathematical diary that he discovered this result in the middle of May, 1801 and stated it there for general moduli. Specifically Gauss wrote:

> A fifth method of proving the fundamental theorem has presented itself thanks to a most elegant theorem from the division of the circle, namely[1]
>
> $$\begin{array}{lccccccc} \sum & \left.\begin{matrix}\sin\\ \cos\end{matrix}\right\} \frac{nn}{a}\mathcal{P} & = & \begin{matrix}+\sqrt{a}\\ +\sqrt{a}\end{matrix}\Bigg| & \begin{matrix}0\\ +\sqrt{a}\end{matrix}\Bigg| & \begin{matrix}0\\ 0\end{matrix}\Bigg| & \begin{matrix}+\sqrt{a}\\ 0\end{matrix}\Bigg| & \\ \text{according as} & a & \equiv & 0 & 1 & 2 & 3 & (\text{mod. } 4) \end{array}$$
>
> where for n are to be substituted all numbers from 0 to $a - 1$.

Note that Gauss saw this theorem in the first place as another (fifth) proof of the law of quadratic reciprocity. Again, through the diary we know that he found the first *proof* of his 1801 entry only on August 30, 1805. Specifically:

> The proof of the most beautiful theorem mentioned above, May 1801, which we had been seeking for 4 years and more with all efforts, we have at last completed. *Comment[ationes] rec[entiores], I* [2]

The reference is to [Gauss 1811]; this only appeared in 1811 but it is not clear when it was written. Presumably this reference (and the underlining of this entry) were added later. Three entries of the diary intervening between the two entries quoted above deal with computational astronomy and entry 122 explains (for whom?) that the years 1802 to 1804 were spent doing astronomical calculations. Gauss wrote to Wilhelm Olbers about his proof on September 3, 1805. Let us quote the first half of this letter in full :

> I hope that it is only your too many duties, and not sickness or anything else unplesant, which account for the fact that I have not been made happy by a letter from you in such a long time. My recent occupations were also not such that they would have provided anything particular to communicate to the geometer, nor did events provide anything of interest for the sympathetic friend. Through various circumstances – partly through several letters from Le Blanc in Paris who studies my *Disquisitiones Arithmeticae* with true passion, has completely familiarised himself with them, and shared quite a few nice comments about them with me; partly because of the presence of a friend who is also studying that work and often asks me for advice – and partly also because of a sort of tedium, or at least fatigue from the dead, mechanical

[1] [Gauss 1796–1814], entry 118; our translation of: *Methodus quinta theorema fundamentale demonstrandi se obtulit, adiumento theorematis elegantissimi theoriae sectionis circuli, puta …*

[2] [Gauss 1796–1814], entry 123; our translation of: *Demonstratio theorematis venustissimi supra 1801 Mai. commemorati quam per 4 annos et ultra omni contentione quaesiveramus, tandem perfecimus. Comment rec. I.*

> computations, I have been seduced to take a break from it for once and take up again my beloved arithmetical investigations. You may recall from our conversations in Bremen, in particular on that beautiful afternoon which we spent on the *Vahr*, that I have had for some time already a fair number of investigations, if not in my drawer, at least in my head, which would provide sufficient material for a second volume of the *Disquisitiones Arithmeticae*, and which – at least according to my own judgement – are just as remarkable as those contained in the first volume. But you may also recall my complaints about a theorem, which is partly interesting in itself, and partly serves as a foundation or keystone for a substantial part of those investigations, and which I have known for more than two years, but which confouded all my attempts to find an adequate proof. This theorem is already hinted at in the *Disquisitiones Arithmeticae*, p. 636,[3] or more precisely, only a special case of it, namely the one where n is a prime number, to which the others could be reduced. What is written there between *Quaecunque igitur radix etc.* and *valde sunt memoribilia*, is rigorously proved there, but what follows, i.e., the determination of the sign, is exactly what has tortured me all the time. This shortcoming spoiled everything else that I found; and hardly a week passed during the last four years where I have not made this or that vain attempt to untie that knot – especially vigorously during recent times. But all this brooding and searching was in vain, sadly I had to put the pen down again. Finally, a few days ago, it has been achieved - but not by my cumbersome search, rather through God's good grace, I am tempted to say. As the lightning strikes the riddle was solved; I myself would be unable to point to a guiding thread between what I knew before, what I had used in my last attempts, and what made it work. Curiously enough the solution now appears to me to be easier than many other things that have not detained me as many days as this one years, and surely noone whom I will once explain the material will get an idea of the tight spot into which this problem had locked me for so long. Now I cannot resist to occupy myself with writing up and elaborating on this material. However, my astronomical work should not be completely neglected all the same.[4]

Gauss's literary skill in this letter is abundantly clear. I would like to make a few comments about it:

Concerning the readers of the *Disquisitiones Arithmeticae* mentioned in the letter, the "Le Blanc" to whom Gauss refers was Sophie Germain. For more details about the exchange of letters between Gauss and Sophie Germain see [Leibrock 2001]. The "friend" in Braunschweig remains unclear. Although his identification is not that important it is of some interest as the number of people who studied the D.A. in detail in the years immediately following its publication – especially in Germany – was small.

(*The main text continues on page 511.)*

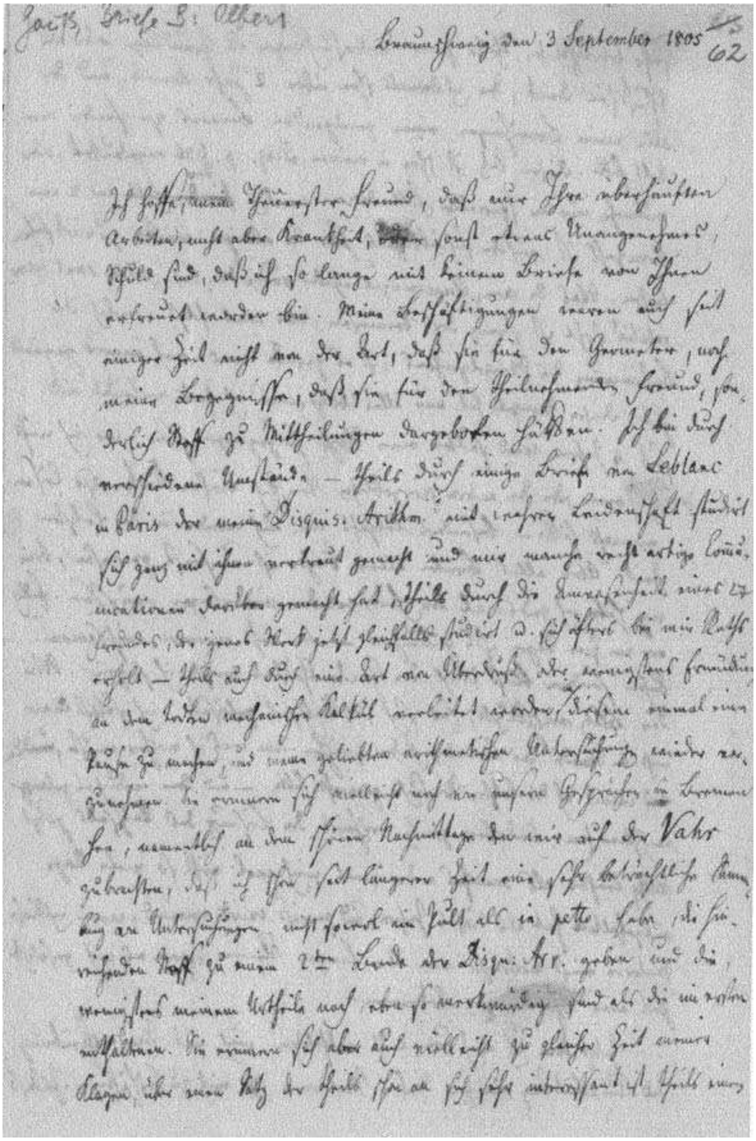
[3] Towards the end of art. 356.

[4] Our translation. The original of this part of the letter is reproduced and transcribed on the following pages. The whole letter is published in [Gauss & Olbers 1900–1909], vol. 1, *Brief* 133, pp. 267–270. After the passage quoted here, Gauss goes over to an astronomical theme, which he also deals with in a letter to Bessel with the same date, and which he asks Olbers to give to Bessel.

Transcription of the first half of Gauss's letter to Olbers, September 3, 1805

Ich hoffe, mein theuerster Freund, daß nur Ihre überhäuften Arbeiten, nicht aber Krankheit, oder sonst etwas Unangenehmes, Schuld sind, daß ich so lange mit keinem Briefe von Ihnen erfreut worden bin. Meine Beschäftigungen waren auch seit einiger Zeit nicht von der Art, daß sie für den Geometer, noch meine Begegnisse, daß sie für den theilnehmenden Freund, sonderlich Stoff zu Mittheilungen dargeboten hätten. Ich bin durch verschiedene Umstände – theils durch einige Briefe von Le Blanc in Paris, der meine Disq. Arithm. mit wahrer Leidenschaft studirt, sich ganz mit ihnen vertraut gemacht und mir manche recht artige Communicationen darüber gemacht hat, theils durch die Anwesenheit eines Freundes, der jenes Werk jetzt gleichfalls studirt u[nd] sich öfters bei mir Raths erholt – theils auch durch eine Art von Überdruß oder wenigstens Ermüdung an dem todten mechanischen Kalkül verleitet worden, in diesem einmal eine Pause zu machen, und meine geliebten arithmetischen Untersuchungen wieder vorzunehmen. Sie erinnern sich vielleicht noch von unsern Gesprächen in Bremen her, namentlich an dem schönen Nachmittage den wir auf der Vahr zubrachten, daß ich schon seit längerer Zeit eine sehr beträchtliche Sammlung von Untersuchungen nicht sowohl im Pult als in petto habe, die hinreichenden Stoff zu einem 2$^{\text{ten}}$ Bande der Disq. Arr. geben und die, wenigstens meinem Urtheile nach, eben so merkwürdig sind als die im ersten enthaltenen. Sie erinnern sich aber auch vielleicht zu gleicher Zeit meiner Klagen, über einen Satz der 1|2 *theils schon an sich sehr interessant ist, theils einem | sehr beträchtlichen Theile jener Untersuchungen als Grundlage oder als Schlußstein dient, den ich damals schon über 2 Jahr kannte, und der alle meine Bemühungen einen genügenden Beweis zu finden, vereitelt hatte. Dieser Satz ist schon in meinen Disq. p. 636 angedeutet, oder vielmehr nur ein specieller Fall davon, nemlich der wo n eine Primzahl ist, auf den sich übrigens hier die übrigen würden zurückführen lassen. Was da von "Quaecunque igitur radix etc." bis "valde sunt memoribilia" steht ist streng dort bewiesen, aber was folgt nemlich die Bestimmung des Wurzelzeichens, ist es gerade was mich immer gequält hat. Dieser Mangel hat mir alles übrige, was ich fand, verleidet und seit 4 Jahren wird selten eine Woche hingegangen sein, wo ich nicht [den] einen oder den andren vergeblichen Versuch diesen Knoten zu lösen gemacht hätte – besonders lebhaft nun auch wieder in der letzten Zeit. Aber alles Brüten alles Suchen ist umsonst gewesen, traurig habe ich jedesmal die Feder wieder niederlegen müssen. Endlich vor ein paar Tagen ists gelungen – aber nicht meinem mühsamen Suchen sondern bloß durch die Gnade Gottes möchte ich sagen. Wie der Blitz einschlägt, hat sich das Räthsel gelöset : ich selbst wäre nicht im Stande den leitenden Faden zwischen dem was ich vorher wußte, dem womit ich die letzten Versuche gemacht hatte – und dem wodurch es gelang nachzuweisen. Sonderbar genug erscheint die Lösung des Räthsels jetzt leichter als manches andere, was mich wohl nicht so viele Tage aufgehalten hat als dieses Jahre, und gewiß wird niemand, wenn ich die Materie einst vortrage von der langem Klemme, worin es mich gesetzt hat, eine Ahndung bekommen.*

Jetzt kann ich mich nun nicht enthalten, mich mit Niederschreibung und Ausarbeitung einiger dieser Materien mit zu beschäftigen. Indeß sollen meine astronomischen Arbeiten darüber nicht ganz vernachlässigt werden.

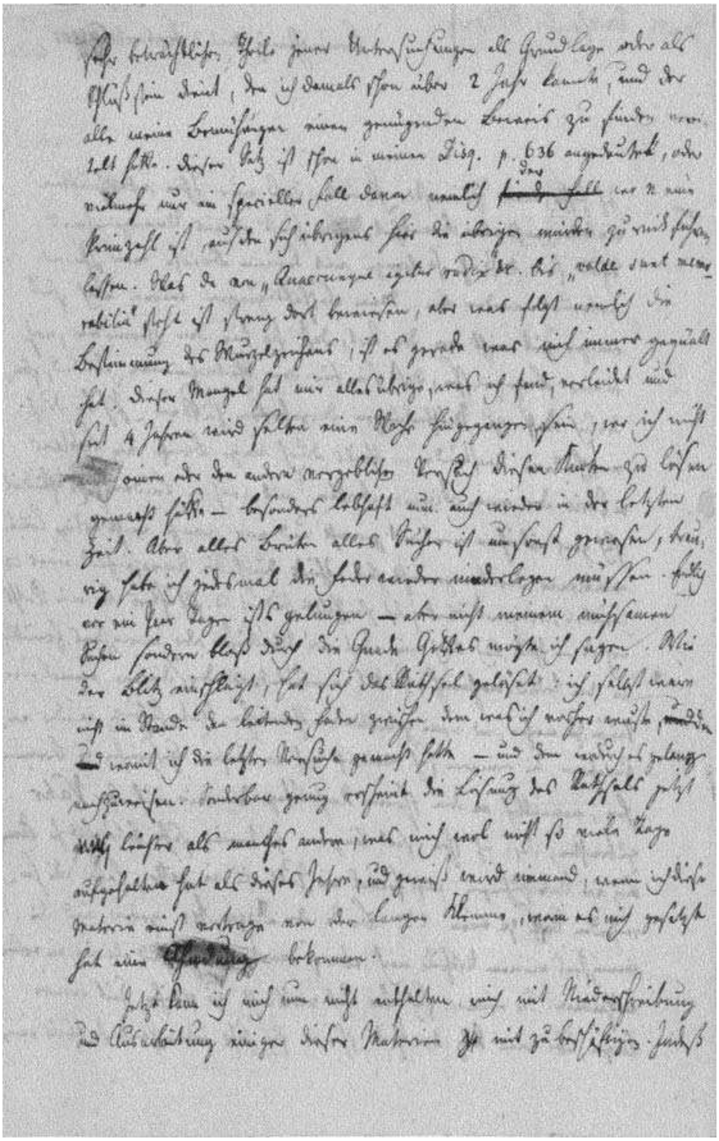


Gauß, Briefe B: Olbers

Braunschweig den 3 September 1805 62

Ich hoffe, mein theuerster Freund, daß nur Ihre überhäuften Arbeiten, nicht aber Krankheit, ~~oder~~ sonst etwas Unangenehmes, Schuld sind, daß ich so lange mit keinem Briefe von Ihnen erfreuet worden bin. Meine Beschäftigungen waren auch seit einiger Zeit nicht von der Art, daß sie für den Geometer, noch meine Begegnisse, daß sie für den theilnehmenden Freund, sonderlich Stoff zu Mittheilungen dargeboten hätten. Ich bin durch verschiedene Umstände — theils durch einige Briefe von Leblanc in Paris der meine Disquis. Arithm. mit wahrer Leidenschaft studirt sich ganz mit ihnen vertraut gemacht und mir manche recht artige Communicationen darüber gemacht hat, theils durch die Anwesenheit eines 27 Fremden, der jenes Werk jetzt gleichfalls studirt u. sich öfters bei mir Raths erholt — theils auch durch eine Art von Überdruß oder wenigstens Ermüdung an den bisher mechanischen Kalkül verleitet worden, diesem einmal eine Pause zu machen, und meine geliebten arithmetischen Untersuchungen wieder vorzunehmen. Sie erinnern sich vielleicht noch von unsern Gesprächen in Bremen her, namentlich an den schönen Nachmittage den wir auf der Vahr zubrachten, daß ich schon seit längerer Zeit eine sehr beträchtliche Sammlung an Untersuchungen nicht sowol im Pult als in petto habe, die hinreichenden Stoff zu einem 2ten Bande der Disqu: Ar. geben und die wenigstens meinem Urtheile nach eben so merkwürdig sind als die im ersten enthalten. Sie erinnern sich aber auch vielleicht zu gleicher Zeit meiner Klagen über einen Satz der theils schon an sich sehr interessant ist, theils einen

Fig. VIII.2A. The first page of Gauss's letter to Olbers, front. (Courtesy of NSUB Göttingen)



sehr beträchtlichen Theile jener Untersuchungen als Grundlage oder als Schlussstein dient, den ich damals schon über 2 Jahre kannte, und der alle meine Bemühungen einen genügenden Beweis zu finden vereitelt hatte. Dieser Satz ist schon in meinen Disq. p. 636 angedeutet, oder vielmehr nur ein specieller Fall davon nemlich ~~[illegible]~~ der Fall wo n eine Primzahl ist, woraus sich übrigens für die übrigen wieder zurückschließen lassen. Was da am „Quaecunque igitur radix &c. bis „valde sunt memorabilia" steht ist streng dort bewiesen, aber was fehlt nemlich die Bestimmung des Wurzelzeichens, ist es gerade was mich immer gequält hat. Dieser Mangel hat mir alles übrige, was ich fand, verleidet und seit 4 Jahren wird selten eine Woche hingegangen sein, wo ich nicht einen oder den andern vergeblichen Versuch diesen Knoten zu lösen gemacht hätte – besonders lebhaft nun auch wieder in der letzten Zeit. Aber alles Brüten alles Suchen ist umsonst gewesen, traurig habe ich jedesmal die Feder wieder niederlegen müssen. Endlich vor ein paar Tagen ists gelungen – aber nicht meinem mühsamen Suchen sondern bloß durch die Gnade Gottes möchte ich sagen. Wie der Blitz einschlägt, hat sich das Räthsel gelöset; ich selbst wäre nicht im Stande den leitenden Faden zwischen dem was ich vorher wußte, ~~[illegible]~~ dem womit ich die letzten Versuche gemacht hatte – und dem wodurch es gelang nachzuweisen. Sonderbar genug erscheint die Lösung des Räthsels jetzt leichter als manches andere, was mich wol nicht so viele Tage aufgehalten hat als dieses Jahre, und gewiß wird niemand, wenn ich diese Materie einst vortrage, von der langen Klemme, worin es mich gesetzt hat eine Ahndung bekommen.

Jetzt kann ich mich nun nicht enthalten, mich mit Niederschreibung und Ausarbeitung einiger dieser Materien itzt mit zu beschäftigen. Jedoch

Fig. VIII.2B. The first page of Gauss's letter to Olbers, back. (Courtesy of NSUB Göttingen)

The proof that Gauss found *was* easy; it is very much in the Euler tradition, especially Euler's work on theta functions.[5] Skill in this area is not common today, but it was for contemporaries of Gauss. More precisely, the proof is based on a q-analogue of the consequence of the binomial theorem $\sum_{j=0}^{n}(-1)^j\binom{n}{j} = 0$. For odd n, one has

$$(1-q)(1-q^3)\ldots(1-q^{n-2}) = 1 - \frac{(1-q^{n-1})}{(1-q)} + \frac{(1-q^{n-1})(1-q^{n-2})}{(1-q)(1-q^2)} - \cdots$$

which can be proved by a modification of the techniques used in working with combinatorial identities. From this it follows that if ζ is an n^{th} root of unity then, with $q = \zeta$, one obtains

$$\begin{aligned}(1-\zeta)(1-\zeta^3)\ldots(1-\zeta^{n-2}) &= 1 - \frac{(1-\zeta^{n-1})}{(1-\zeta)} + \frac{(1-\zeta^{n-1})(1-\zeta^{n-2})}{(1-\zeta)(1-\zeta^2)}\cdots\\ &= \sum_{j=0}^{n-1} \zeta^{-\frac{1}{2}j(j+1)}.\end{aligned}$$

If we take ζ to be $\exp(2\pi i/n)$, or better, $\exp(8\pi i/n)$, then the product is easily transformed into a multiple of a product of sines whose argument is easy to determine. From this Gauss's theorem follows easily.

The fact that the search for a proof *tortured* Gauss is perhaps a reflection that he had been so confident in the *Disquisitiones Arithmeticae* – he was honour-bound to find a proof, especially when others were making progress in studying the D.A. and could soon be asking questions. The part of the D.A. – Section 7 – which treats cyclotomy was studied with great interest, especially in France. The proof was, however, only published in 1811, and was, in fact, only taken up by others more than twenty years later.

Finally I would like to point out that this letter shows Gauss working on his image.[6] He naturally does so within the ethos of the time. One important element which marked those years was the aftermath of the sort of veneration of genius which had been a trademark of German literature and philosophy since the 1770s, but which underwent significant changes in the new postrevolutionary cultural and political reality. Some of these changes crystallized around the self-legitimizing heroic figure of Napoleon. Johann Wolfgang von Goethe, for instance, noted in his diary on August 8, 1806 that he had been musing about "new titles for Napoleon," about "subjective princes," and that he was able to interpret "Napoleon's deeds and practices" as a vindication of Fichte's theory.[7] The same kind of interpretation of Napoleon as a paradigm for autonomous, charismatic creativity underlied the original

[5] See [Euler 1748], Cap. XVI, *De partitione numerorum*, [Euler 1783a] and [Euler 1783b].

[6] Kurt R. Biermann has observed this in a different context in [Biermann 1991].

[7] See [Schmidt 1985], p. 451.

dedication of Ludwig van Beethoven's Eroica Symphony to Bonaparte in 1804.[8]

But Napoleon's genius may not have been on Gauss's mind when he wrote the letter to Olbers.[9] Gauss's favourite German novelist, the bestselling Jean Paul,[10] had published between 1800 and 1803 his monumental novel *Titan* of which an important aspect is the balance of romantic genius and reality.[11] In his 1804 theoretical treatise "Vorschule der Ästhetik" he sees the decisive quality of true (literary) genius as the successful combination of subconscious instinct with superior talent. When describing this subconscious element, Jean Paul appears to be very close indeed to Gauss's description of his discovery (in Jean Paul's text preceding the following quote, there is also a reference to God somewhat similar to Gauss's letter):

> The instinct is the sense of the future; it is blind, but only as the ear is blind to light, and the eye deaf to sound. It signifies and contains its object in the same way as the cause contains the effect. If the secret were open to us as to how a given cause contains the effect in itself, despite the fact that the effect follows the cause in time, then we would also understand how the instinct claims, determines and knows its object and yet does without it.[12]

There was no reaction in print to Gauss's work [Gauss 1811] until about 1835 when Peter Gustav Lejeune-Dirichlet introduced his new, Fourier-theoretic methods. After this, by 1850 almost all of the general methods of proof had been found although over the 150 years since then many variants have been given. The main later innovation was the method of Hecke and I shall turn to this later. A second very novel proof is due to Issai Schur – see below.

2. Dirichlet and Poisson Summation

The first general method is Dirichlet's – see [Dirichlet 1835], [Dirichlet 1839–40]. It is perhaps worthy of note that Harold Davenport remarked:

[8] See [Grove 1896], pp. 54–55. Cf. [George 1998]. For later, strongly contrasting views on this theme, we mention in passing Lev Tolstoi's considerations in *War and Peace* (1865–1868) and Thomas Carlyle's *Lectures on Heroes, Hero-Worship, and the Heroic in History* (1840).

[9] The letter was written about three weeks before Napoleon's troops crossed the Rhine and more than a year before their advance would directly affect Gauss's life, first in Braunschweig, then in Göttingen.

[10] "Jean Paul" was the pen name of Johann Paul Friedrich Richter (1763–1825). Gauss occasionally quoted romantic, witty, or sobering lines from various works of Jean Paul in letters and in conversation.

[11] See [Schmidt 1985], pp. 433–446.

[12] See Jean Paul, *Vorschule der Ästhetik*, 3rd *Programm*, § 13: *Der Instinkt … ist der Sinn der Zukunft; er ist blind, aber nur, wie das Ohr blind ist gegen Licht und das Auge taub gegen Schall. Er bedeutet und enthält seinen Gegenstand ebenso wie die Wirkung die Ursache; und wär' uns das Geheimnis aufgetan, wie die mit der gegebenen Ursache notwendig ganz und gar zugleich gegebene Wirkung doch in der Zeit erst der Ursache nachfolget, so verständen wir auch, wie der Instinkt zugleich seinen Gegenstand fodert, bestimmt, kennt und doch entbehrt.*

> The method used by Dirichlet in 1835 to evaluate G is probably the most satisfactory of all that are known. It is based on Poisson's Summation Formula, and it has the advantage that once the proof has been embarked upon, no special ingenuity is called for.[13]

Yet, this proof is the one that is least often reproduced; as far as I know, apart from Davenport, Martin Neil Huxley is the only writer to use it.[14]

Dirichlet's proof is as follows. We begin by proving a version of the Poisson Summation Formula. Let f be of bounded variation on $[0, 1]$. Then Dirichlet's Theorem on the representability of functions of bounded variation by their Fourier series yields

$$\frac{1}{2}\big(f(0+) + f(1-)\big) = \lim_{N\to\infty} \sum_{j=-N}^{N} \int_0^1 f(x)e^{-2\pi \mathrm{i} jx}\,\mathrm{d}x$$

Summing this over the intervals $[j, j+1]$ with $0 \le j < k$ gives Dirichlet's version of the Poisson Summation Formula for a continuous function of bounded variation on $[0, k]$:

$$\begin{aligned}\frac{1}{2}f(0) + f(1) + f(2) + \cdots + f(k-1) + \frac{1}{2}f(k)\\ = \lim_{N\to\infty} \sum_{j=-N}^{N} \int_0^k f(x)e^{-2\pi \mathrm{i} jx}\,\mathrm{d}x\end{aligned}$$

Now take $f(x) = \exp(2\pi \mathrm{i} x^2/k)$. The left-hand side is the Gauss sum whereas the right-hand side is

$$\begin{aligned}&= \lim_{N\to\infty} \sum_{j=-N}^{N} \int_0^k \exp(2\pi \mathrm{i}(x^2/k - jx))\mathrm{d}x\\ &= \lim_{N\to\infty} \sum_{j=-N}^{N} \int_0^k \exp\Big(\frac{2\pi \mathrm{i}(x - jk/2)^2}{k}\Big)\mathrm{d}x \ \exp\Big(\frac{2\pi \mathrm{i} j^2 k}{4}\Big).\end{aligned}$$

We now separate the sum into those terms where j is odd and those where it is even. We find:

$$\begin{aligned}\lim_{N\to\infty} \sum_{j=-N,\ \text{even}}^{N} \Big\{\int_0^k \exp(\frac{-2\pi \mathrm{i}(x - jk/2)^2}{k})\mathrm{d}x \exp(\frac{2\pi \mathrm{i} j^2 k}{4})\\ + i^{-k} \int_0^k \exp(\frac{2\pi \mathrm{i}(x - \frac{k}{2} - \frac{j-1}{2}k)^2}{k})\mathrm{d}x \ \exp(-\frac{2\pi \mathrm{i} j^2 k}{4})\Big\}\\ = \sqrt{k}(1 + \mathrm{i}^{-k}) \int_{-\infty}^{\infty} \exp(2\pi \mathrm{i} x^2)\mathrm{d}x.\end{aligned}$$

[13] See [Davenport 1967], p. 14.

[14] See [Huxley 1996], § 5.4.

From $k = 1$ we get

$$\int_{-\infty}^{\infty} \exp(2\pi \mathrm{i} x^2)\mathrm{d}x = \frac{1+\mathrm{i}}{2}.$$

From this Gauss's theorem follows at once, and we have also evaluated the improper integral $\int_{-\infty}^{\infty} \exp(2\pi \mathrm{i} x^2)\mathrm{d}x$.

Note that the proof of the Poisson Summation Formula is not the usual one which is based on the Fourier synthesis of the periodic function $\sum_{n\in\mathbf{Z}} f(n+x)$ and was the method used by Siméon-Denis Poisson [Poisson 1827].[15] In fact, this method could have been used here again in conjunction with Dirichlet's theorem to give an alternative proof. It is worth noting here that Poisson had developed a theory of the representability of periodic functions by their Fourier series based on the use of the Poisson kernel and the summation method $\lim_{y<1, y\to 1} \sum_{n\in\mathbf{Z}} \hat{f}(n) y^{|n|} \exp(2\pi \mathrm{i} nx)$. This is valid for continuous functions. If the sum $\sum_{n\in\mathbf{Z}} \hat{f}(n) \exp(2\pi \mathrm{i} nx)$ converges then, by Abel's theorem,[16] the limit coincides with this sum. Although Abel's paper is almost contemporary with those of Poisson, Abel was interested in the hypergeometric function and made no mention of any application to Fourier series.

The same method was applied by Mathias Schaar and Angelo Genocchi to $\exp(2\pi \mathrm{i} px^2/q)$ to prove the reciprocity formula for Gauss sums, [Schaar 1848], [Genocchi 1852] and [Genocci 1854]. This formula states that, for p and q relatively prime positive integers one of which is even, one has

$$\frac{1}{\sqrt{q}} \sum_{j=0}^{q-1} \exp\Big(\pi \mathrm{i} \frac{pj^2}{q}\Big) = \exp\Big(\frac{\pi \mathrm{i}}{4}\Big) \frac{1}{\sqrt{p}} \sum_{k=0}^{p-1} \exp\Big(-\pi \mathrm{i} \frac{qk^2}{p}\Big).$$

This beautiful formula generalizes that of Gauss and yields the law of quadratic reciprocity as well. For this one only has to observe that, if p and q are odd primes, then an elementary transformation shows that

$$\sum_{j=0}^{q-1} \exp\Big(-\pi \mathrm{i} \frac{pj^2}{q}\Big) = \Big(\frac{-2p}{q}\Big) \sum_{j=0}^{q-1} \exp\Big(2\pi \mathrm{i} \frac{j^2}{q}\Big)$$

from which the assertion easily follows.

The standard argument that one uses today to prove this is the following. Let p and q be distinct odd primes; we shall consider the Gauss sum

$$\sum_{j=0}^{pq} \exp\Big(2\pi \mathrm{i} \frac{j^2}{pq}\Big).$$

[15] I would like to take this opportunity to thank Catherine Goldstein for her generous help obtaining copies of Poisson's rather extensive papers. These are regrettably not easily accessible, although their importance in the development of analysis is manifest.

[16] See [Abel 1826], Theorem IV.

In this we set $j = pj_1 + qj_2$; by the Chinese Remainder Theorem the set of such j will run through a set of residues (mod pq) if j_1 runs through a set of residues (mod q) and j_2 through a set of residues (mod p). If we replace j^2 by $(pj_1+qj_2)^2 = p^2j_1^2 + 2pqj_1j_2 + q^2j_2^2$ and then one finds that the sum above is equal to

$$\sum_{j_1=0}^{q} \exp\Big(2\pi\mathrm{i}\frac{pj_1^2}{q}\Big) \sum_{j_2=0}^{p} \exp\Big(2\pi\mathrm{i}\frac{qj_2^2}{p}\Big).$$

The first of these sums is

$$\Big(\frac{p}{q}\Big) \sum_{j_1=0}^{q} \exp\Big(2\pi\mathrm{i}\frac{j_1^2}{q}\Big)$$

as was used in the previous paragraph. The second is given by the analogous expression. Thus

$$\sum_{j=0}^{pq} \exp\Big(2\pi\mathrm{i}\frac{j^2}{pq}\Big) = \Big(\frac{p}{q}\Big)\Big(\frac{q}{p}\Big) \sum_{j_1=0}^{q} \exp\Big(2\pi\mathrm{i}\frac{j_1^2}{q}\Big) \sum_{j_2=0}^{p} \exp\Big(2\pi\mathrm{i}\frac{j_2^2}{p}\Big).$$

If we substitute Gauss's evaluation for the three Gauss sums here we obtain the law of quadratic reciprocity. Presumably Gauss's argument was similar.

A more modern and more precise formulation of these relationships is due to André Weil: Let (e_p) be a non-trivial character on the adèle ring $\mathbf{Q}_{\mathbf{A}}$ of $\mathbf{Q}$, which is trivial on $\mathbf{Q}$. Then Weil's formula states that the Hilbert symbol at p – either a prime or ∞, i.e., representing the archimedean completion $\mathbf{R}$ of $\mathbf{Q}$ – satisfies

$$(x, y)_p = \frac{\gamma_p(xy)\gamma_p(1)}{\gamma_p(x)\gamma_p(y)} \tag{$*$}$$

where

$$\gamma_p(x) = \int_{\mathbf{Q}_p} e_p(x \cdot u^2)\mathrm{d}u,$$

(an improper integral) and, with a self-dual additive measure on the adèles, one has for $x \in \mathbf{Q}$ the product formula

$$\prod_p \gamma_p(x) = 1,$$

where the product is over all primes and ∞. The Hilbert-Furtwängler form of the reciprocity law is

$$\prod_p (x, y)_p = 1$$

which therefore follows immediately.

One of the major preoccupations around 1840–1860 was the generalization of the quadratic reciprocity law. Since the Hilbert symbol of order n is skew–symmetric it follows that for $n > 2$ there is no analogue to (*). The recognition that this was so was chiefly due to Eisenstein – see [Eisenstein 1850a]. Before this paper, Kummer had tried to formulate a version of the general reciprocity law in terms of "ideal numbers," i.e., ideals. For this to make sense he was forced to restrict his attention to the case of regular cyclotomic fields, that is, fields where the class number is coprime to n. In this, n was usually taken to be prime. Eisenstein recognised that this was not natural but that one could define a Legendre symbol $\left(\frac{A}{B}\right)$ of order n by copying the classical definition from the quadratic case. It is possible for B to be an ideal but not A. For the symbol to be well defined, B has to be coprime to n and A and B have to be coprime to one another. In [Eisenstein 1850a], Eisenstein posits a reciprocity law of the form

$$\left(\frac{A}{B}\right) = (A, B) \left(\frac{B}{A}\right)$$

under the assumption that A is also coprime to n. Here (A, B) should depend only on A, B modulo some power of n. By an argument using congruences and special choices of the A, B he shows that (A, B) is completely determined should the reciprocity law hold in this form.[17]

Although the notation used by Eisenstein is very similar to that used by Hilbert, this is probably a coincidence as Hilbert came to introduce the symbol named after him by a rather different line of argument. It apparently developed while he was writing the *Zahlbericht* [Hilbert 1897] where it is introduced in § 64 while he is discussing the theory of genera in quadratic fields. The product formula appears as a lemma (*Hilfssatz 14*) in [Hilbert 1897], § 69. It seems clear that Hilbert had not yet recognised the fundamental nature of his product formula; this he emphasises in [Hilbert 1899]. In [Hilbert 1897] he also introduced an analogue of the quadratic Hilbert symbol in the case of cyclotomic fields.[18] This is based on Kummer's approach to the general reciprocity law[19] ; Hilbert, like Kummer, proves it when n is a regular prime. At the end of [Hilbert 1897], § 161, Hilbert notes the relationship to Eisenstein's approach.

Once Hilbert had formulated the general reciprocity law in a general context, one of his students, Philipp Furtwängler[20] (1869–1940), took up the challenge of proving it. This he did in a series of papers over a long period[21] in which he removed the condition that n should be regular; n remained a prime, with 2 permitted. These papers use the methods developed by Kummer, Hilbert and Heinrich Weber and are

[17] This argument is repeated in [Cassels, Fröhlich 1967] as Exercises 2.12 and 2.13, pp. 353–354.

[18] See [Hilbert 1897], § 148.

[19] See [Kummer 1859].

[20] In fact, Furtwängler was formally a student of Felix Klein, but worked along the lines of Hilbert's *Zahlbericht*.

[21] See [Furtwängler 1902], [Furtwängler 1909], [Furtwängler 1912], [Furtwängler 1913], and [Furtwängler 1928].

fairly technical. They do make use of the Hilbert symbol as introduced in [Hilbert 1897]. These papers became obsolete with the development of the new class–field theory in the 1920s by Emil Artin, Helmut Hasse, and others, for it was easy to deduce them from Artin's Reciprocity Law. The fact that this form of the reciprocity law was introduced by Hilbert and was proved in a large number of cases by himself and Furtwängler seems, at least to the author, to justify the designation Hilbert-Furtwängler Reciprocity Law.

A number of variants of the proofs using Gauss sums indicated above were found by about 1850. Thus both Victor Amédée Lebesgue [Lebesgue 1840] and Ferdinand Gotthold Max Eisenstein[22] gave very elegant derivations of Gauss's q-formula. On the other hand Augustin Louis Cauchy gave in [Cauchy 1840] a quite different proof of the identity

$$\sum_{j=0}^{n-1} \zeta^{j^2} = \left(\frac{-2}{n}\right) \prod_{k=1}^{(n-1)/2} (\zeta^k - \zeta^{-k}) \tag{$\dagger$}$$

where n is odd and ζ is a primitive n^{th} root of unity. This is essentially equivalent to the formula derived by Gauss. Cauchy's proof consists essentially in showing that the quotient of the two sides is a root of unity in $\mathbf{Z}[\zeta]$ and then, at least when n is a prime, using a congruence argument to show that this root of unity is in fact 1. More or less the same proof was published by Leopold Kronecker in [Kronecker 1856].

A very interesting and suggestive proof of (†) was given by Issai Schur [Schur 1921]. He interpreted the left–hand side of the formula as the trace of the Fourier transformation over a finite field and investigated the matrix of this transformation. The eigenvalues are fourth roots of 1; the determinant is a Vandermonde determinant which gives enough information to determine the multiplicities.

Later, as complex analysis developed, it was possible to replace Fourier theory by complex analytic methods. This was first done by Leopold Kronecker [Kronecker 1889] but there were many variants found later. In particular Louis Joel Mordell developed these ideas[23] and they were taken up again by George Neville Watson in his work on Ramanujan's Mock Theta Functions.[24]

Likewise, real-analytic proofs were found, the best-known being Theodor Esterman's [Estermann 1945], but Edmund Landau's version in [Landau 1928] is both interesting and earlier. Gauss's formula is also a consequence (for almost all n) of the Euler-Maclaurin Summation Formula, or of van der Corput's Summation Formula, i.e., an approximate version of the Poisson Summation Formula with a truncated sum over the Fourier transform – see [Lehmer 1976], although this was presumably known earlier.[25] Although it may be pushing the point a bit, one can regard these analytic proofs as being variations on Dirichlet's theme.

[22] In [Eisenstein 1844a], [Eisenstein 1844b], [Eisenstein 1844c], and esp. [Eisenstein 1844f].

[23] See [Mordell 1918] and [Mordell 1933].

[24] See [Watson 1936] and [Watson 1937].

[25] A lengthy bibliography of the proofs of Gauss's theorem, with more emphasis on the more recent ones than here, is given in [Berndt, Evans, Williams 1998].

3. Theta Functions

The theory of quadratic Gauss sums runs parallel to the theory of theta functions especially in terms of the techniques used. However, the theory of theta functions, especially the transformations under the modular group, can be used to determine the Gauss sums. This was first discovered by Cauchy, [Cauchy 1840], the same paper where his proof of Gauss's theorem based on a congruence argument appeared. A little later Carl Gustav Jacob Jacobi [Jacobi 1848] indicated vaguely what form the general transformation law should have; the multiplier system has a Jacobi symbol as one of its major components. This was formulated precisely and proved by Charles Hermite in [Hermite 1858]. This emphasizes the relationship between the reciprocity formula for Gauss sums and the transformation theory for the theta functions. Many proofs have been given. Particularly noteworthy is that of Heinrich Weber in [Weber 1908], § 38, which is group-theoretic. Although it did not have any immediate influence the same idea was rediscovered by Tomio Kubota in 1964.[26] This can be combined with more modern techniques in the theory of automorphic functions to investigate Gauss sums of higher order. Elaborating on this would, unfortunately, take us too far afield.

In the attempts to discover and to prove a general reciprocity law in the 1840s, Gotthold Eisenstein used Gauss sums in a very sophisticated fashion.[27] It appears that the experience gained in these works was his major motivation for formulating the "general" reciprocity law [Eisenstein 1850a], that is, the Hilbert-Furtwängler reciprocity law. The Gauss sums that he used were, in contradistinction to Gauss and Ernst Eduard Kummer, those of the form

$$\sum_{x \pmod{n}} \chi(x) \ \exp\Bigl(2\pi \mathrm{i}\frac{x}{n}\Bigr),$$

but defined over the ring of integers of a cyclotomic field and where χ is a suitable Legendre-Jacobi symbol of higher order.[28] These sums are the basis of Eisenstein's reciprocity law, namely that

$$\Bigl(\frac{A}{B}\Bigr) = \Bigl(\frac{B}{A}\Bigr)$$

when either A or B is a rational integer.[29] It turns out that, as Eisenstein discovered, first in various special cases in 1844,[30] and then in the case of cyclotomic fields of

[26] See [Kubota 1966b]. This was first indicated by Kubota in [Kubota 1966a].

[27] See [Eisenstein 1844a], [Eisenstein 1844d], [Eisenstein 1844e], [Eisenstein 1844g], [Eisenstein 1844h], and [Eisenstein 1850b].

[28] The description is a little anachronistic as the theory of algebraic numbers was just beginning to develop at this time. The notion of a character is generally introduced through artifice (for us) of the index with respect to a primitive root.

[29] See [Eisenstein 1850b].

[30] See [Eisenstein 1844c], [Eisenstein 1844d], [Eisenstein 1844e], [Eisenstein 1844g], and [Eisenstein 1844h].

prime order in [Eisenstein 1850b], certain powers of the Gauss sums can be given explicitly.

This was rediscovered by André Weil in 1952 in a more general setting, and extended by him further in 1974.[31] In the course of this, one needs some p-adic theory of Gauss sums, which is to say that one determines both the powers of those prime ideals dividing the Gauss sums and certain congruences that they satisfy. This was pioneered first by Jacobi and then by Eisenstein in increasing generality.[32] It was given in a general form by Ludwig Stickelberger in [Stickelberger 1890]. Gauss's investigations in the same direction were not published in his lifetime and for this reason we shall not consider them further.

Cauchy's "p-adic" proof of Gauss's formula led John William Scott Cassels to propose a kind of formula for cubic Gauss sums in terms of elliptic functions.[33] This, and a biquadratic analogue, were proved by Charles Russell Matthews.[34] In terms of individual Gauss sums, little more is known at the moment; to find a more general analogue remains a most challenging problem.

In the 1840s, Kummer proposed, rather tentatively, a statistical distribution of cubic Gauss sums.[35] This proposal turned out to be false in its original form; in the case considered by Kummer this was proved by David Roger Heath-Brown and the author, and in general by the author.[36] These results can be understood as asserting that there is no formula analogous to that of Gauss for Gauss sums of order greater than 2.

4. Hecke's Approach

Around 1900 the theory of the Riemann ζ-function was well-developed – the prime number theorem had been proved and the basis of the determination of the properties of the $L(s, \chi)$ had been laid by Hurwitz in 1882, although one sees, for example in Edmund Landau's *Handbuch*, that the proof still was considered difficult in 1909.[37] In algebraic number theory, and especially in class-field theory, a number of further ζ- and L-functions had been introduced – for example Dedekind's ζ-function of a number field dates to 1871[38] – the ideas are already implicit in Kummer's paper [Kummer 1859] where Kummer cites Dirichlet.[39] Moreover the relationship between $\lim_{s\to 1}(s-1)\zeta_k(s)$ and the class-number of the number field k was known; this was the main motivation behind its introduction. Moreover, one had studied various

[31] See [Weil 1952] and [Weil 1974d].

[32] See [Jacobi 1827], and the papers [Eisenstein 1844c], [Eisenstein 1844d], [Eisenstein 1844e], [Eisenstein 1844g], [Eisenstein 1844h], and [Eisenstein 1850b].

[33] See [Cassels 1970], [Cassels 1977].

[34] See [Matthews 1979a] and [Matthews 1979b].

[35] See [Kummer 1842] and [Kummer 1846].

[36] See [Heath-Brown, Patterson, 1979] and [Patterson 1987].

[37] See [Landau 1909], § 103, § 124.

[38] See [Dirichlet 1871], Supplement X, § 167 ff.

[39] See [Kummer 1859], p. 138, and, perhaps more to the point, [Kummer 1850], introduction.

L-functions of the type $L_k(s,\chi)$, where

$$\chi(\mathfrak{a}) = \left(\frac{\delta}{N_{k/k_0}(\mathfrak{a})}\right)_n ;$$

again such L-series also go back at least to Kummer's paper. One also knew that $L_{\mathbf{Q}}(s,\chi)$, $\chi = (\frac{D}{\cdot})$, is essentially an L-function of the type considered by Hurwitz. But if we now look at Hilbert's 8th problem what we see is rather curious:

> But of no lesser interest, and perhaps even broader consequences, seems to me to be the task of transferring the results obtained about the distribution of rational prime numbers, to the theory of the distribution of prime ideals in a given algbraic number field k – a task which amounts to studying the function associated to the field
>
> $$\zeta_k(s) = \sum \frac{1}{n(\mathfrak{j})^s},$$
>
> where the sum extends over all ideals $\mathfrak{j}$ of the given number field k, and $n(\mathfrak{j})$ denotes the norm of the ideal $\mathfrak{j}$. [40]

Thus Hilbert stresses that the Dedekind ζ-functions could be important, but he *does not* conjecture that they have analytic continuation. One can only read into his formulation that he had at the back of his mind that this might be the case, but he was not prepared to stick his neck out. From a present-day perspective this seems strange; it appears that there was a barrier that had to be overcome. Also the Artin Hypothesis on the analytic properties of Artin L-functions and Hasse's question about the properties of the global L-function of an elliptic curve have so shaped our thinking that we can hardly imagine not putting such questions at the centre of our considerations. It is, however, helpful to realize that, at that time, one apparently felt that whereas the Riemann ζ-function is arithmetically significant, its construction appeared to be analytic and so its analytic properties seemed natural. The Dedekind ζ-function was arithmetic in its definition and so its analytic properties were not considered natural. It is the experience of the last hundred years that leads us to be confident of the analytic properties of such arithmetic functions.

Curiously it was Landau, just three years after Hilbert's Paris lecture, who proved that the Dedekind ζ-function has an analytic continuation into a narrow strip,[41] and he used methods which Hilbert had used in his paper on relative quadratic extensions.[42]

[40] See [Hilbert 1900], pp. 309–310, the discussion of the 8th problem, *8. Primzahlprobleme*: *… Aber nicht von geringerem Interesse und vielleicht noch größerer Tragweite, erscheint mir die Aufgabe, die für die Verteilung der rationalen Primzahlen gewonnenen Resultate auf die Theorie der Verteilung der Primideale in einem gegebenen Zahlkörper k zu übertragen – eine Aufgabe, die auf das Studium der dem Zahlkörper zugehörigen Funktion* $\zeta_k(s) = \sum \frac{1}{n(\mathfrak{j})^s}$ *hinausläuft, wo die Summe über alle Ideale* $\mathfrak{j}$ *des gegebenen Zahlkörpers k zu erstrecken ist, und* $n(\mathfrak{j})$ *die Norm des Ideals* $\mathfrak{j}$ *bedeutet.*

[41] See [Landau 1903a], p. 81.

[42] See [Hilbert 1899], *Satz 31*; see also [Weber 1896], § 194.

For Landau, in contrast to Hilbert, the methods of complex function theory were entirely natural; he used his result in [Landau 1903b] to prove the prime ideal theorem, and later developed the method to deal with characters of the class group in [Landau 1907].

Ten years after this, Erich Hecke proved the analytic properties of the Dedekind ζ-function.[43] As one now sees he used a generalization of the known proofs, sharpening the technique used by Landau. The method also immediately extends to the analogues of Dirichlet L-series. Hecke [Hecke 1917] observed moreover that his results implied that the relation (for an abelian extension K/k of number fields, and all characters χ on the Galois group of K/k)

$$\zeta_K(s) = \zeta_k(s) \prod_{\chi \neq 1} L_k(s, \chi)$$

which one can prove for almost all Euler factors directly, has to be true for all factors. Then he remarked that, if one looks at the root number $W_k(\chi)$ appearing in the functional equation, and K/k is quadratic, the functional equation yields

$$W_K(\omega \circ N) = \prod W_k(\omega \cdot \chi),$$

where ω is a *Grössencharakter* for k. The case of a quadratic extension implies the determination of the sign of the quadratic Gauss sum – and its generalization to algebraic number fields.

This line of argument can be considered as a deduction of Gauss's theorem from the law of quadratic reciprocity, and this is what is novel about it. Hecke took this up in his book *Algebraische Zahlen* [Hecke 1923] and used it to prove a beautiful theorem on the different of k, namely that the class of the absolute different in the ideal class group is a square. This theorem – an analogue of the fact that the Euler characteristic of a Riemann surface is even – is the crowning moment (*coronidis loco*) in both Hecke's book[44] and André Weil's *Basic Number Theory*.[45] The same idea also leads to the Davenport-Hasse theorems [Davenport, Hasse 1935]. The idea has been in the modern theory of automorphic forms to deduce that a statement which has been proved at almost all places of an **A**-field is in fact valid at all places. This beautiful technique reflects the marvellous way in which the places of a number-field are intimately bound up with one another, as one already sees in Gauss's theorem.

In considering Gauss' theorem one is impressed over and over again with how fecund it has been. Although at first sight his theorem about Gauss sums may seem to be little more than a curiosity, what we have seen is that it has been at the root of several important developments in number theory over the last 200 years and that it has continued to inspire the leading practitioners of this part of mathematics.

[43] Hecke refers no more than necessary to Landau; there is one obscurely formulated footnote. This is hard to understand, for five years earlier in the CV attached to his dissertation he had thanked "Herr Professor Landau, to whom I owe a large part of my mathematical education." (*Herrn Professor Landau, dem ich einen großen Teil meiner mathematischen Ausbildung verdanke.*) See [Hecke 1910], p. 58.

[44] See [Hecke 1923], § 63, *Satz 176.*

[45] See [Weil 1967], chap. XIII, § 12, Theorem 13.

References

Abel, Niels Henrik. 1826. Untersuchung über die Reihe $1+\frac{1}{m}x+\frac{m.m-1}{2}x^2+\frac{m.m-1.m-2}{2.3}x^3+\cdots$. *Journal für die reine und angewandte Mathematik* 1, 331–339. French version: Recherches sur la série $1+\frac{1}{m}x+\frac{m.m-1}{2}x^2+\frac{m.m-1.m-2}{2.3}x^3+\cdots$. Repr. *Œuvres complètes*, vol. I, ed. L. Sylow, S. Lie, pp. 219–250. Christiana: Grondahl, 1881; repr. New York, London: Johnson, 1965. Amended German transl.: ed. A. Wangerin. Ostwalds Klassiker der exakten Wissenschaften 71. Leipzig: Wilhelm Engelmann, 1895.

Berndt, Bruce C., Evans, Ronald J., Williams, Kenneth S. 1998. *Gauss and Jacobi Sums.* Canadian Mathematical Society Series of Monographs and Advanced Texts. New York: John Wiley.

Biermann, Kurt R. 1991. Wandlungen unseres Gaußbildes, *Mitteilungen der Gauß-Gesellschaft Göttingen* 28, 3–13.

Cassels, John William Scott. 1970. On Kummer sums. *Proceedings of the London Mathematical Society* (3) 21, 19–27.

———. 1977. Trigonometric sums and elliptic functions. In *Algebraic Number Theory (Kyoto International Symposium, Research Institute for Mathematical Sciences, University of Kyoto, Kyoto 1976)*, ed. S. Iyanaga, pp. 1–7. Tokyo: Japanese Society for the Promotion of Science.

Cassels, John William Scott, Fröhlich, Albrecht (eds.). 1967. *Algebraic Number Theory. Proceedings of a Conference in Brighton, UK, 1965.* London, New York: Academic Press.

Cauchy, Augustin Louis. 1840. Méthode simple et nouvelle pour la détermination complète des sommes alternées formées avec les racines primitives des équations binômes. *Journal de mathématiques pures et appliquées* 5, 154–168.

Davenport, Harold. 1967. *Multiplicative Number Theory*. Chicago: Markham Publishing Company.

Davenport, Harold, Hasse, Helmut. 1935. Die Nullstellen der Kongruenzzetafunktionen in gewissen zyklischen Fällen. *Journal für die reine und angewandte Mathematik* 172, 151–182.

Dirichlet, Johann Peter Gustav Lejeune-. 1835. Über eine neue Anwendung bestimmter Integrale auf die Summation endlicher oder unendlicher Reihen. *Abhandlungen der Königlich preussischen Akademie der Wissenschaften* 1835, 391–407. Repr. in [Dirichlet 1899], pp. 239–256. Condensed French transl. *Journal für die reine und angewandte Mathematik* 17 (1837), 57–67. Repr. in [Dirichlet 1889], pp. 259–270.

———. 1839–1840. Reserches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. *Journal für die reine und angewandte Mathematik* 19, 324–369; 21, 1–12 and 134–155. Repr. in [Dirichlet 1889], pp. 411–496.

———. 1871. *Vorlesungen über Zahlentheorie*, ed. with supplements R. Dedekind. 2nd ed. Braunschweig: Vieweg.

———. 1889. *Werke*, vol. 1, ed. L. Kronecker. Berlin: G. Reimer.

Eisenstein, Gotthold. 1844a. Über eine merkwürdige identische Gleichung. *Journal für die reine und angewandte Mathematik* 27, 105–106. Repr. in [Eisenstein 1975], vol. I, pp. 26–27.

———. 1844b. Transformations remarquables de quelques séries. *Journal für die reine und angewandte Mathematik* 27, 193-197; 28, 36–40. Partially repr. in *Nouvelles Annales de Mathématiques* 8 (1849), 341–343. Repr. in [Eisenstein 1975], vol. 1, pp. 35–44.

———. 1844c. Beiträge zur Kreistheilung. *Journal für die reine und angewandte Mathematik* 27, 269–278. Repr. in [Eisenstein 1975], vol. 1, pp. 45–54.

———. 1844d. Beweis des Reciprocitätssatzes für die cubischen Reste in der Theorie der aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. *Journal für die reine und angewandte Mathematik* 27, 289–310. Repr. in [Eisenstein 1975], vol. 1, pp. 59–80.

———. 1844e. Nachtrag zum cubischen Reciprocitätssatze für die aus dritten Wurzeln der Einheit zusammengesetzten complexen Zahlen. Criterien des cubischen Characters der Zahl 3 und ihrer Theiler. *Journal für die reine und angewandte Mathematik* 28, 28–35. Repr. in [Eisenstein 1975], vol. 1, pp. 81–88.

———. 1844f. Neuer Beweis und Verallgemeinerung des Binomischen Lehrsatzes. *Journal für die reine und angewandte Mathematik* 28, 44–48. French transl. in *Nouvelles Annales de Mathématiques* 8 (1849), 344–347. Repr. in [Eisenstein 1975], vol. 1, pp. 117–121.

———. 1844g. Lois de réciprocité. *Journal für die reine und angewandte Mathematik* 28, 53–67. Repr. in [Eisenstein 1975], vol. 1, pp. 126–140.

———. 1844h. Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste. *Journal für die reine und angewandte Mathematik* 28, 223–245. Repr. in [Eisenstein 1975], vol. 1, pp. 141–163.

———. 1850a. Über ein einfaches Mittel zur Auffindung der höheren Reciprocitätsgesetze und der mit ihnen zu verbindenden Ergänzungssätze. *Journal für die reine und angewandte Mathematik* 39, 351–364. Repr. in [Eisenstein 1975], vol. 2, pp. 623–636.

———. 1850b. Beweis der allgemeinsten Reciprocitätsgesetze zwischen reellen und complexen Zahlen. *Bericht über die zur Bekanntmachung geeigneten Verhandlungen der Königlich Preussischen Akademie der Wissenschaften zu Berlin*,189–198. Repr. in [Eisenstein 1975], vol. 2, pp. 712–721.

———. 1975. *Mathematische Werke*, 2 vols. New York: Chelsea.

ESTERMANN, Theodor. 1945. On the sign of the Gaussian sum. *Journal of the London Mathematical Society* 20, 66–67.

EULER, Leonard. 1748. *Introductio in analysin infinitorum*. Lausanne: Marc-Michel Bousquet. Repr. in *Opera Omnia*, ed. A. Krazer, F. Rudio, Series 1, vol. 8. Leipzig, Berlin: Teubner, 1922.

———. 1783a. Evoluto producti infini $(1-x)(1-xx)(1-x^3)(1-x^4)(1-x^5)(1-x^6)$ etc. in seriem simplicam. *Acta AcademiæScientarum Imperialis Petropolitanæ* 1780 (1783), 47–55. Repr. in *Opera Omnia*, ed. A. Krazer, F. Rudio, P. Stäckel, Series 1, vol. 3, pp. 472–479. Leipzig, Berlin: Teubner, 1917.

———. 1783b. De mirabilibus propriatetibus numerorum pentagonalium. *Acta Academiæ Scientiarum Imperialis Petropolitanæ* 1780 (1783), 56–75. Repr. in *Opera Omnia*, ed. A. Krazer, F. Rudio, P. Stäckel, Series 1, vol. 3, pp. 480–496. Leipzig, Berlin: Teubner, 1917.

FURTWÄNGLER, Philipp. 1902. Über die Reziprozitätsgesetze zwischen ℓ^{ten} Potenzresten, wenn ℓ eine ungerade Primzahl bedeutet. *Abhandlungen der Königlichen Gesellschaft der Wissenschaften, Göttingen* 2, Nr. 3, 1–82. Repr. in *Mathematische Annalen* 58 (1904), 1–50.

———. 1909. Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlekörpern, I. *Mathematische Annalen* 67, 1–31.

———. 1912. Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlenkörpern, II. *Mathematische Annalen* 72, 346–386.

———. 1913. Reziprozitätsgesetze für Potenzreste mit Primzahlexponenten in algebraischen Zahlenkörpern, III. *Mathematische Annalen* 74, 413–429.

———. 1928. Über die Reziprozitätsgesetze für ungerade Primzahlexponenten. *Mathematische Annalen* 98, 539–543.

GAUSS, Carl Friedrich. 1796–1814. Mathematical Diary. Original manuscript in Latin: Handschriftenabteilung Niedersächsische Staats- und Universitätsbibliothek Göttingen, Cod. Ms. Gauss Math. 48 Cim. Ed. (Latin with German annotations): Abdruck des Tagebuchs (Notizenjournals), *Werke*, X.1, pp. 483–575. Leipzig: Teubner, 1917. French annotated transl. P. Eymard, J.-P. Lafon: Le journal mathématique de Gauss. *Revue d'histoire des sciences et de leurs applications* 9 (1956), 21–51. English commented transl. J. Gray: A commentary on Gauss's mathematical diary, 1796-1814, with an English translation. *Expositiones Mathematicae* 2 (1984), 97–130. Rep. in [Dunnington 2004], pp. 409-505. German transl. E. Schuhmann, with a historical introduction by K.-R. Biermann, and annotations by H. Wußing und O. Neumann: *Mathematisches Tagebuch 1796–1814*. 5th ed. Ostwalds Klassiker der exakten Wissenschaften 256. Leipzig: Akademische Verlagsgesellschaft Geest & Portig; Frankfurt am Main, Thun: Harri Deutsch, 2005.

———. 1811. Summatio quarumdam serierum singularium. *Commentationes societatis regiae scientiarum Gottingensis recentiores* 1. Repr. in *Werke*, vol. II, *Höhere Arithmetik*, ed. Königliche Gesellschaft der Wissenschaften zu Göttingen, pp. 9–45, 155–158. Göttingen: Universitäts-Druckerei. 2nd augm. ed., 1876.

GAUSS & OLBERS. 1900–1909. *Briefwechsel zwischen Olbers und Gauß*, ed. C. Schilling, I. Kramer. *Wilhelm Olbers, sein Leben und seine Werke*, ed. C. Schilling, vol. 2. Berlin: J. Springer. Repr. in C. F. Gauss, *Werke. Ergänzungsreihe* 4. 2 vols. Hildesheim: G. Olms, 1976.

GENOCCHI, Angelo. 1852. Sulla formula summatoria di Eulero, et sulla teoria di residui quadratici. *Annali delle scienze matematiche e fisiche, Roma* 8, 402–436.

———. 1854. Note sur la théorie des residues quadratiques. *Mémoires couronnés et mémoires des savants étrangers, Académie royale des sciences, des lettres et des beaux-arts de Belgique* 25, 1–54.

GEORGE, Christopher T. 1998. The Eroica Riddle: Did Napoleon remain Beethoven's "Hero"? *Napoleonic Scholarship: The Journal of the International Napoleonic Society*, vol. I No. 2; http://www.napoleon-series.org/ins/scholarship98/c_eroica.html.

GROVE, Sir George. 1896. *Beethoven and his Nine Symphonies*. London: Novello & Co. Repr. New York: Dover, 1962.

HEATH-BROWN, David Rodney (Roger), PATTERSON, Samuel James. 1979. The distribution of Kummer sums at prime arguments, *Journal für die reine und angewandte Mathematik* 310, 111–130.

HECKE, Erich. 1910. *Zur Theorie der Modulfunktionen von zwei Variabeln und ihre Anwendungen auf die Zahlentheorie.* Dissertation Göttingen. Repr.: Höhere Modulfunktionen und ihre Anwendungen auf die Zahlentheorie. *Mathematische Annalen* 71 (1912), 1–37. Repr. in [Hecke 1970], pp. 21–58

———. 1917a. Über die Zetafunktionen beliebiger algebraischer Zahlkörper. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse* 1917, 77–89. Repr. in [Hecke 1970], pp. 159–171.

———. 1917b. Über eine neue Anwendung der Zetafunktionen auf die Arithmetik der Zahlkörper. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse* 1917, 90–95. Repr. in [Hecke 1970], pp. 172–177.

———. 1923. Vorlesungen über die Theorie der algebraischen Zahlen. Leipzig: Teubner.

———. 1970. *Mathematische Werke*, ed. B. Schoeneberg. 2nd ed. Göttingen: Vandenhoeck.

HERMITE, Charles. 1858. Sur quelquels formules relatives à la theorie des fonctions elliptiques. *Journal de mathématiques pures et appliquées* 2nd ser. 3, 26–36. Repr. in *Œuvres*, ed. E. Picard, vol. 1, pp. 487–496. Paris: Gauthier-Villars, 1905.

HILBERT, David. 1897. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4 (“1894–1895”), 177–546 + Vorwort 1–xviii. Repr. in [Hilbert 1932], pp. 63–363. Engl. transl. I. Adamson, *The Theory of Algebraic Number Fields*, introd. F. Lemmermeyer, N. Schappacher. New York: Springer, 1998.

———. 1899. Über die Theorie der relativquadratischen Zahlkörper, *Mathematische Annalen* 51, 1–127. Repr. in [Hilbert 1932], pp. 370–509.

———. 1900. Mathematische Probleme. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse* 1900 Heft 3, 253–297. Repr. *Archiv für Mathematik und Physik* (3) 1 (1901), 44–63 and 213–237. Repr. in [Hilbert 1935], pp. 290–329.

———1932. *Gesammelte Abhandlungen*, vol. I: *Zahlentheorie*. Berlin: Springer, 1932. 2nd ed., 1970.

———. 1935. *Gesammelte Abhandlungen*, vol. III: *Analysis, Grundlagen der Mathematik, Physik, Verschiedenes, Lebensgeschichte*. Berlin: Springer, 1935. 2nd ed., 1970.

HURWITZ, Adolf. 1882. Einige Eigenschaften der Dirichletschen Functionen $F(s) = \sum \left(\frac{D}{n}\right) \frac{1}{n^s}$, die bei der Bestimmung der Classenanzahlen binärer quadratischer Formen auftreten. *Zeitschrift für Mathematik und Physik* 27, 86–101.

HUXLEY, Martin Neil. 1996. *Area, Lattice Points and Exponential Sums.* London Mathematical Society Monographs, New Series 13. Oxford, New York: Oxford University Press.

JACOBI, Carl Gustav Jacob. 1827. De residuis cubicis commentatio numerosa. *Journal reine und angewandte Mathematik* 2, 66–69. Repr. in *Gesammelte Werke*, vol. VI, ed. K. Weierstrass, pp. 233–237. Berlin: G. Reimer, 1891.

———. 1848. Über die Differentialgleichung, welcher die Reihen $1 \pm 2q + 2q^4 \pm 2q^9 +$ etc., $2\sqrt[4]{q} + 2\sqrt[4]{q^9} + 2\sqrt[4]{q^{25}} +$ etc. Genüge leisten. *Journal für die reine und angewandte Mathematik* 36, 97–112. French transl. in *Journal de mathématiques pures et appliquées* 14 (1849), 181–200. Repr. in *Gesammelte Werke*, vol. II, ed. K. Weierstrass, pp. 171–190. Berlin: G. Reimer, 1882.

———. 1827. De residuis cubicis commentatio numerosa. *Journal für die reine und angewandte Mathematik* 2, 66–69.

KRONECKER, Leopold. 1856. Sur une formule de Gauss. *Journal de mathématiques pures et appliquées* (2) 1, 392–395. Repr. in [Kronecker 1929], pp. 173–175.

———. 1889. Summirung der Gauss'schen Reihen $\sum\limits_{h=0}^{h=n-1} e^{\frac{2h^2\pi i}{n}}$. *Journal für die reine und angewandte Mathematik* 105, 267–268. Repr. in [Kronecker 1929], pp. 297–300.

———. 1929. *Werke*, vol. IV, ed. K. Hensel. Leipzig: Teubner.

KUBOTA, Tomio. 1966a. Modular forms for Picard groups. In *Algebraische Zahlentheorie, Bericht einer Tagung in Oberwolfach 6.–12. Sept. 1964*, ed. H. Hasse, P. Roquette, pp. 143–153. Mannheim: Bibliographisches Institut.

———. 1966b. Ein arithmetischer Satz über eine Matrizengruppe. *Journal für die reine und angewandte Mathematik* 222, 55–57.

KUMMER, Ernst Eduard. 1842. Eine Aufgabe betreffend die Theorie der cubischen Reste. *Journal für die reine und angewandte Mathematik* 23, 285–286. Repr. in [Kummer 1975], pp. 143–144.

———. 1846. De residuis cubicis disquistiones nonnullae analyticae. *Journal für die reine und angewandte Mathematik* 32, 341–359. Repr. in [Kummer 1975], pp. 145–163.

———. 1850. Bestimmung der Anzahl nicht äquivalenter Classen für die aus λten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben. *Journal für die reine und angewandte Mathematik* 40, 93–116. Repr. in [Kummer 1975], pp. 299–322.

———. 1859. Über die allgemeinen Reciprocitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. *Mathematische Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin* 1859, 19–159. Repr. in [Kummer 1975], pp. 690–839.

———. 1975. *Collected Papers*, ed. A. Weil, vol. 1, *Contributions to Number Theory*. Berlin, Heidelberg etc.: Springer.

LANDAU, Edmund. 1909. *Handbuch der Lehre von der Verteilung der Primzahlen*. Leipzig: Teubner.

———. 1903a. Ueber die zu einem Zahlkörper gehörige Zetafunction und die Ausdehnung der Tschebyschefschen Primzahlentheorie auf das Problem der Verteilung der Primideale, *Journal für die reine und angewandte Mathematik* 125, 64–188. Repr. in *Collected Works*, ed. L. Mirsky, I.J. Schoeneberg, W. Schwarz, H. Wefelscheid, vol. 1, pp. 201–326. Essen: Thales, 1985.

———. 1903b. Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes. *Mathematische Annalen* 56, 645–670. Repr. in *Collected Works*, ed. L. Mirsky, I.J. Schoeneberg, W. Schwarz, H. Wefelscheid, vol. 1, pp. 327–352. Essen: Thales, 1985.

———. 1907. Über die Verteilung der Primideale in den Idealklassen eines algebraischen Zahlkörpers, *Mathematische Annalen* 63, 145–204. Repr. in *Collected Works*, ed. L. Mirsky, I.J. Schoeneberg, W. Schwarz, H. Wefelscheid, vol. 3, pp. 181–240. Essen: Thales, 1986.

———. 1928. Über das Vorzeichen der Gaußschen Summe. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse* 1928, 19–20. Repr. in *Collected Works*, ed. P.T. Bateman, L. Mirsky, H.L. Montgomery, W. Schaal, I.J. Schoeneberg, W. Schwarz, H. Wefelscheid, vol. 9, pp. 39–40. Essen: Thales, n. d.

Lebesgue, Victor Amédée. 1840. Sommation de quelques séries. *Journal de mathématiques pures et appliquées* 1st ser. 5, 42–71.

Lehmer, Derrick Henry. 1976. Incomplete Gauss sums. *Mathematika* 23, 125–135.

Leibrock, Gerd. 2001. Meine Freundin Sophie – Carl Friedrich Gauß' Brieffreundschaft mit Sophie Germain. *Mitteilungen der Gauß-Gesellschaft Göttingen* 38, 17–28.

Matthews, Charles R. 1979a. Gauss sums and elliptic functions, I. The Kummer sum. *Inventiones Mathematicae* 52, 163–185.

———. 1979b. Gauss sums and elliptic functions, II. The quartic sum. *Inventiones Mathematicae* 54, 23–52.

Mordell, Louis Joel. 1918. On a simple summation of the series $\sum_{s=0}^{n-1} e^{2s^2\pi i/n}$. *Messenger of Mathematics* 48, 54–56.

———. 1933. The definite integral $\int_{\infty}^{-\infty} \frac{e^{ax^2+bx}}{e^{cx}+d}\,dx$ and the analytic theory of numbers. *Acta Mathematica* 61, 323–360.

Patterson, Samuel James. 1987. The distribution of general Gauss sums and similar arithmetic functions at prime arguments. *Proceedings of the London Mathmeatical Society* 3rd ser. 54, 193–215.

Poisson, Siméon-Denis. 1823. Suite du Mémoire sur les intégrales définies et sur la sommation des séries. *Journal de l'École Royale Polytechnique* 12, 404–509.

———. 1827. Mémoire sur le calcul numérique des intégrales définies. *Mémoires de l'Académie Royale des Sciences de l'Institut de France* 6, 571–602.

Schaar, Mathias. 1848. Mémoires sur les intégrales Eulériennes et sur la convergence d'une certaine classe de séries. *Mémoires couronnés et mémoires des savants étrangers, Académie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique* 22, 1–16.

Schilling, Carl. 1900. Wilhelm Olbers: Sein Leben und seine Werke. Vol. II, 1. Berlin, Heidelberg: Springer.

Schmidt, Jochen. 1985. *Die Geschichte des Genie-Gedankens 1750–1945. Band I: Von der Aufklärung bis zum Idealismus.* Darmstadt: Wissenschaftliche Buchgesellschaft.

Schur, Issai. 1921. Über die Gaußschen Summen. *Nachrichten von der Gesellschaft der Wissenschaften zu Göttingen. Mathematisch-physikalische Klasse* 1921, 147–153.

Stickelberger, Ludwig. 1890. Über eine Verallgemeinerung der Kreistheilung. *Mathematische Annalen* 37, 321–367.

Watson, George Neville. 1936. The final problem: an account of the mock theta functions. *Journal of the London Mathematical Society* 11, 55–80.

———. 1937. The mock theta functions (II). *Proceedings of the London Mathematical Society* 2nd ser. 42, 274–304.

Weber, Heinrich. 1896. *Lehrbuch der Algebra*, vol. 2. Braunschweig: Vieweg. 2nd ed., 1899.

———. 1908. *Lehrbuch der Algebra*, vol. 3. Braunschweig: Vieweg.

Weil, André. 1952. Jacobi sums as "Grössencharaktere." *Transactions of the American Mathematical Society* 73, 487–495. Repr. in [Weil 1979], vol. 2, pp. 63–71.

———. 1967. *Basic Number Theory.* Die Grundlehren der Mathematischen Wissenschaften 144. Berlin, Heidelberg, New York: Springer.

———. 1974c. La cyclotomie jadis et naguère. *Séminaire Bourbaki* 452. Repr. *Enseignement Mathématique* 20, 247–263. Repr. in [Weil 1979], vol. 3, pp. 311–327.

———. 1974d. Sommes de Jacobi et caractères de Hecke. *Nachrichten der Akademie der Wissenschaften in Göttingen. II. Mathematisch-Physikalische Klasse* 1974 no. 1, 1–14. Repr. in [Weil 1979], vol. 3, pp. 329–342.

———. 1979. *Œuvres – Collected Papers*. Cor. 2nd pr. 3 vols. Berlin, Heidelberg, New York: Springer.

VIII.3

The Development of the Principal Genus Theorem

FRANZ LEMMERMEYER

Genus theory today belongs to algebraic number theory and deals with a certain part of the ideal class group of a number field that is more easily accessible than the rest. Historically, the importance of genus theory stems from the fact that it was the essential algebraic ingredient in the derivation of the classical reciprocity laws, from Gauss's second proof, via Kummer's contributions, all the way to Takagi's reciprocity law for p-th power residues.

The central theorem in genus theory is the principal genus theorem.[1] Here, we shall outline the development of the principal genus theorem from its conception by Gauss in the context of binary quadratic forms – with hindsight, traces of genus theory can already be found in the work of Euler on quadratic forms and idoneal numbers – to its modern formulation within the framework of class field theory.

Gauss formulated the theorem in the *Disquisitiones Arithmeticae*, but only in passing: after observing in art. 247 that duplicated classes of binary quadratic forms lie in the principal genus, the converse, i.e., the principal genus theorem, is alluded to for the first time in art. 261:

> … if therefore all classes of the principal genus can be obtained from the duplication of some class (and the fact that this is always so will be proved in the sequel), …[2]

The actual statement of the result in art. 286 of the D.A. is then presented in the form of a problem:

[1] The name "principal genus theorem" (*Hauptgeschlechtssatz*) was apparently coined by Helmut Hasse in [Hasse 1927], Ia, § 19, pp. 120–128, and then quickly adopted by mathematicians around Emmy Noether.

[2] D.A. art. 261: *si itaque omnes classes generis principalis ex duplicatione alicuius classis provenire possunt (quod revera semper locum habere in sequentibus demonstrabitur).*

> Problem. Given a binary form $F = (A, B, C)$ of determinant D belonging to the principal genus: to find a binary form f from whose duplication we get the form F.[3]

This way of presenting the result does not imply any lack of emphasis on Gauss's part. In fact, he wrote about the result and a few of its consequences:

> Unless we are strongly mistaken, these theorems have to be counted among the most beautiful in the theory of binary forms, particularly because, despite their extreme simplicity, they are so recondite that their rigorous demonstration cannot be built without the help of so many other investigations.[4]

Gauss's theory of quadratic forms was generalized in several completely different directions: the theory of n-ary quadratic forms over fields;[5] the arithmetic of algebraic tori;[6] the theory of forms of higher degree,[7] in particular cubic forms;[8] finally the theory of quadratic and, later, general algebraic number fields.

This chapter deals with genus theory of quadratic forms (from Euler to Dirichlet-Dedekind) in sections 1 to 3. From § 4, we shall focus on genus theory of number fields.[9] In this setting, the principal genus theorem for abelian extensions $k/\mathbf{Q}$ describes the splitting of prime ideals of k in the genus field k_{gen} of k which, by definition, is the maximal unramified extension of k that is abelian over $\mathbf{Q}$. In § 8 and § 9 below we explain the relationship between genus theory and higher reciprocity laws. The class field theoretic setting will be developed starting in § 10. The paper ends with a discussion of the Galois cohomological connection introduced by Emmy Noether.

[3] D.A., art. 286. Problema. *Proposita forma binaria $F = (A, B, C)$ determinantis D ad genus principale pertinente: invenire formam binariam f, e cuius duplicatione illa oriatur.*

[4] Our translation of D.A., art. 287: *Haecce theoremata, ni vehementer fallimur, ad pulcherrima in theoria formarum binarium sunt referenda, eo magis quod licet summa simplicitate gaudeant, tamen tam recondita sint ut ipsarum demonstrationem rigorosam absque tot aliarum disquisitionum subsidio condere non liceat.*

[5] See for instance [Jones 1950], [Lam 1973], and [O'Meara 1963] for n-ary forms, and [Buell 1989] for the binary case. A very readable presentation of Gauss's results close to the original is given in [Venkov 1970].

[6] See [Shyr 1975], [Shyr 1979] for a presentation of Gauss's theory in this language, and [Ono 1985] for a derivation of the principal genus theorem using results from Shyr's thesis.

[7] Recently, Manjul Bhargava developed a theory of composition for a variety of forms. See [Bhargava 2004] and [Belabas 2005].

[8] Let us just mention: (i) Eisenstein's results [Eisenstein 1844], cf. the modern treatment in [Hoffman, Morales 2000] via composition of cubic forms à la Kneser; (ii) Manin's viewpoint of obstructions to the local-global principle – see [Manin 1972] and [Skorobogatov 2001].

[9] For a related survey with an emphasis on the quadratic case, but sketching generalizations of the genus concept, e.g. in group theory, see [Frei 1979].

1. Prehistory: Euler, Lagrange, and Legendre

There are hardly any elements of genus theory in the mathematical literature prior to Gauss's *Disquisitiones Arithmeticae*. What one does find, in particular in Leonhard Euler's work, are results and conjectures that would later on be explained by genus theory.

One such conjecture was developed between Christian Goldbach and Leonhard Euler; on March 12, 1753, Goldbach wrote to Euler that if p is a prime of the form $4dm + 1$, then p can be represented as $p = da^2 + b^2$. Euler replied on March 23/April 3:

> I have noticed this very theorem quite some time ago, and I am just as convinced of its truth as if I had proof of it.[10]

He then gave the examples

$$\begin{array}{llcccl} p & = 4 \cdot 1m + 1 & \Rightarrow & p & = & aa + bb \\ p & = 4 \cdot 2m + 1 & \Rightarrow & p & = & 2aa + bb \\ p & = 4 \cdot 3m + 1 & \Rightarrow & p & = & 3aa + bb \\ p & = 4 \cdot 5m + 1 & \Rightarrow & p & = & 5aa + bb \qquad etc. \end{array}$$

and remarked that he could prove the first claim, but not the rest.[11] Euler then went on to observe that the conjecture is only true in general when a and b are allowed to be rational numbers, and gives the example $89 = 4 \cdot 22 + 1$, which can be written as $89 = 11(\frac{5}{2})^2 + (\frac{9}{2})^2$ but not in the form $11a^2 + b^2$ with integers a, b. Thus, he says, the theorem has to be formulated like this:

Conjecture 1. If $4n + 1$ is a prime number, and d is a divisor of this n, then that number $4n+1$ is certainly of the form $daa+bb$, if not in integers, then in fractions.[12]

Euler also studied the prime divisors of a given binary quadratic form x^2+ny^2,[13] and observed that those not dividing $4n$ are contained in half of the possible prime residue classes modulo $4n$.[14] Now, as Euler knew and used in his proof of the cubic case of Fermat's Last Theorem, odd primes dividing $x^2 + ny^2$ can be represented by the same quadratic form if $n = 3$, and he also knew that this property failed

[10] See [Euler & Goldbach 1965], Letters 166 and 167: *Ich habe auch eben diesen Satz schon längst bemerket und bin von der Wahrheit desselben so überzeugt, als wann ich davon eine Demonstration hätte.*

[11] Later he found a proof for the case $p = 3a^2 + b^2$; the other two cases mentioned here were first proved by Lagrange.

[12] *Si* $4n + 1$ *sit numerus primus, et d divisor ipsius n, tum iste numerus* $4n + 1$ *certo in hac forma daa + bb continentur, si non in integris, saltem in fractis.*

[13] In what follows, we shall always talk about proper divisors of quadratic forms, that is, we assume that $p \mid x^2 + ny^2$ with $\gcd(x, y) = 1$.

[14] In [Euler 1785], p. 210, this is formulated by saying that primes (except $p = 2, 5$) dividing $x^2 + 5y^2$ have the form $10i \pm 1$, $10i \pm 3$, where the plus sign holds when i is even, and the minus sign when i is odd.

for $n = 5$. He then saw that the primes $p \equiv 1, 9 \bmod 20$ could be represented[15] as $p = x^2 + 5y^2$ with $x, y \in \mathbf{N}$, whereas $p \equiv 3, 7 \bmod 20$ could be written as $2x^2 + 2xy + 3y^2$ with $x, y \in \mathbf{Z}$. His first guess was that this would generalize as follows: the residue classes containing prime divisors of x^2+ny^2 could be associated uniquely with a reduced quadratic form of the same discriminant as $x^2 + ny^2$. For example, the reduced forms associated to $F = x^2 + 30y^2$ are the forms D satisfying $D = F, 2D = F, 3D = F$ and $5D = F$, where $2D = F$ refers to $D = 2r^2 + 15s^2$, $3D = F$ to $3r^2 + 10s^2$, and $5D = F$ to $D = 5r^2 + 6s^2$. All of these forms have different classes of divisors.

But as Euler found out,[16] the number $n = 39$ provides a counterexample because it has "three kinds of divisors":

$$1) \quad D = F, \qquad 2) \quad 3D = F, \qquad 3) \quad 5D = F.$$

The three kinds of divisors are $D = F = r^2+39s^2$; $D = 3r^2+13s^2$ (note that $3D = (3r)^2 + 39s^2$, which explains Euler's notation $3D = F$); and $D = 5r^2 + 2rs + 8s^2$. Euler then observed that the divisors of the first and the second class share the same residue classes modulo 156; the prime $61 = 3 \cdot 4^2 + 13 \cdot 1^2$ belonging to the second class can be represented rationally by the first form since $61 = (\frac{25}{4})^2 + 39(\frac{3}{4})^2$.

One of the results in which Euler came close to genus theory is related to a conjecture of his that was shown to be false by Joseph-Louis Lagrange; it appears in [Euler 1764]. In his comments on Euler's *Algebra*, Lagrange writes:

> M. Euler, in an excellent Memoir printed in vol. IX of the *New Commentaries of Petersburg*, finds by induction this rule for determining the solvability of every equation of the form
> $$x^2 - Ay^2 = B,$$
> where B is a prime number: the equation must be possible whenever B has the form $4An + r^2$, or $4An + r^2 - A$.[17]

For example, $-11 = 4 \cdot 3 \cdot (-1) + 1^2$, and $-11 = 1^2 - 3 \cdot 2^2$. Similarly, $-2 = 4 \cdot 3 \cdot (-2) + 5^2 - 3$ and $-2 = 1^2 - 3 \cdot 1^2$. Euler's main motivation for this conjecture was numerical data, even though he also had a proof that $p = x^2 - ay^2$ implies $p = 4an + r^2$ or $p = 4an + r^2 - a$.[18]

But Euler's conjecture is not correct; Lagrange pointed out the following counterexample: the equation $x^2 - 79y^2 = 101$ is not solvable in integers, although

[15] At this stage, he had already studied Lagrange's theory of reduction of binary quadratic forms.

[16] See [Euler 1785], p. 192.

[17] See [Lagrange 1774/1877], p. 156–157: *Euler, dans un excellent Mémoire imprimé dans le tome IX des* Nouveaux Commentaires de Pétersbourg, *trouve par induction cette règle, pour juger la résolubilité de toute equation de la forme $x^2 - Ay^2 = B$, lorsque B est un nombre premier; c'est que l'équation doit être possible toutes les fois que B sera de la forme* $4An + r^2$, *ou* $4An + r^2 - A$.

[18] He wrote $x = 2at + r$, $y = 2q + s$, and found that $p = x^2 - ay^2 = 4am + r^2 - as^2$ for some $m \in \mathbf{Z}$. If s is even, then $-as^2$ has the form $4am'$, and if s is odd, one finds $-as^2 = -4am'' - a$. This proves the claim.

$101 = 4An + r^2 - A$ with $A = 79$, $n = -4$ and $r = 38$. Whether Euler ever heard about Lagrange's counterexample is not clear.

At any rate, the following amendment of conjecture 1 suggests itself, which we shall see below to be equivalent to Gauss's principal genus theorem:

Conjecture 2. If p not dividing $4a$ is a prime of the form $4an + r^2$ or $4an + r^2 - a$, then one has $p = x^2 - ay^2$ for rational numbers x, y.

Historical appraisals of Euler's achievements on this topic range from the wholesale claim that the concept of genera is due to Euler,[19] via a more moderate picture of Euler as a provider of resources for Gauss's theory, all the way to André Weil who called Euler's papers on idoneal numbers "ill coordinated with one another" and complained about the "confused and defective ... formulations and proofs" in them.[20] Most of all, one must not forget that Euler only had isolated results on (divisors of) numbers represented by quadratic forms, which were subsequently subsumed under a few general theorems (reciprocity, class group, principal genus theorem) of Gauss's theory of quadratic forms.

As is well-known, Joseph-Louis Lagrange introduced reduction and equivalence into the theory of binary quadratic forms. Focusing on which numbers a given form represents, he discovered that an invertible linear change of variables with integer coefficients in the form does not affect the result – he did not fix the sign of the determinant of the transforming substitution, contrarily to Gauss later. In this way he obtained results like the following: *If a prime p properly divides a number of the form x^2+5y^2, then p is represented by one of the forms x^2+5y^2 or $2x^2 \pm 2xy + 3y^2$.* Now, primes represented by $x^2 + 5y^2$ clearly are congruent to 1, 9 mod 20, those represented by $2x^2 \pm 2xy + 3y^2$ are 3, 7 mod 20. Lagrange established the converse a little later.[21] Lagrange derived analogous results for forms $x^2 - ny^2$ and integers n with $|n| \leq 12$, but failed to obtain a general result.

It was left to Adrien-Marie Legendre to complete these investigations by attaching residue classes (actually linear forms such as $20n + 1$, $20n + 9$, which he called *diviseurs linéaires*) to Lagrange's equivalence classes of quadratic forms of discriminant $-4n$ (which he called *diviseurs quadratiques* of $x^2 - ny^2$).[22] Legendre also touched upon the composition of forms and the representation of binary quadratic forms by sums of three squares, a technique that would later reappear, in a more general perspective, in Gauss's D.A. in the proof of the principal genus theorem.[23]

[19] See [Antropov 1989a,b], and [Antropov 1995]. However, Euler's usage of the term *genus* is not compatible with Antropov's reading of it.

[20] See [Weil 1984], p. 224. For a historical survey of these papers of Euler see [Steinig 1966].

[21] The first part of the work alluded to is [Lagrange 1773], the sequel is [Lagrange 1775].

[22] See [Legendre 1830], Art. 212, for the 4 *diviseurs quadratiques* of $x^2 - 39y^2$ and the 6 *diviseurs linéaires* corresponding to each of them. Cf. the later comment in [Dirichlet 1839], p. 424: *Les formes différentes qui correspondent au déterminant quelconque D, sont divisées par M.* GAUSS *en genres, qui sont analogues à ce que* LEGENDRE *appelle groupes des diviseurs quadratiques.*

[23] See [Weil 1984], p. 313.

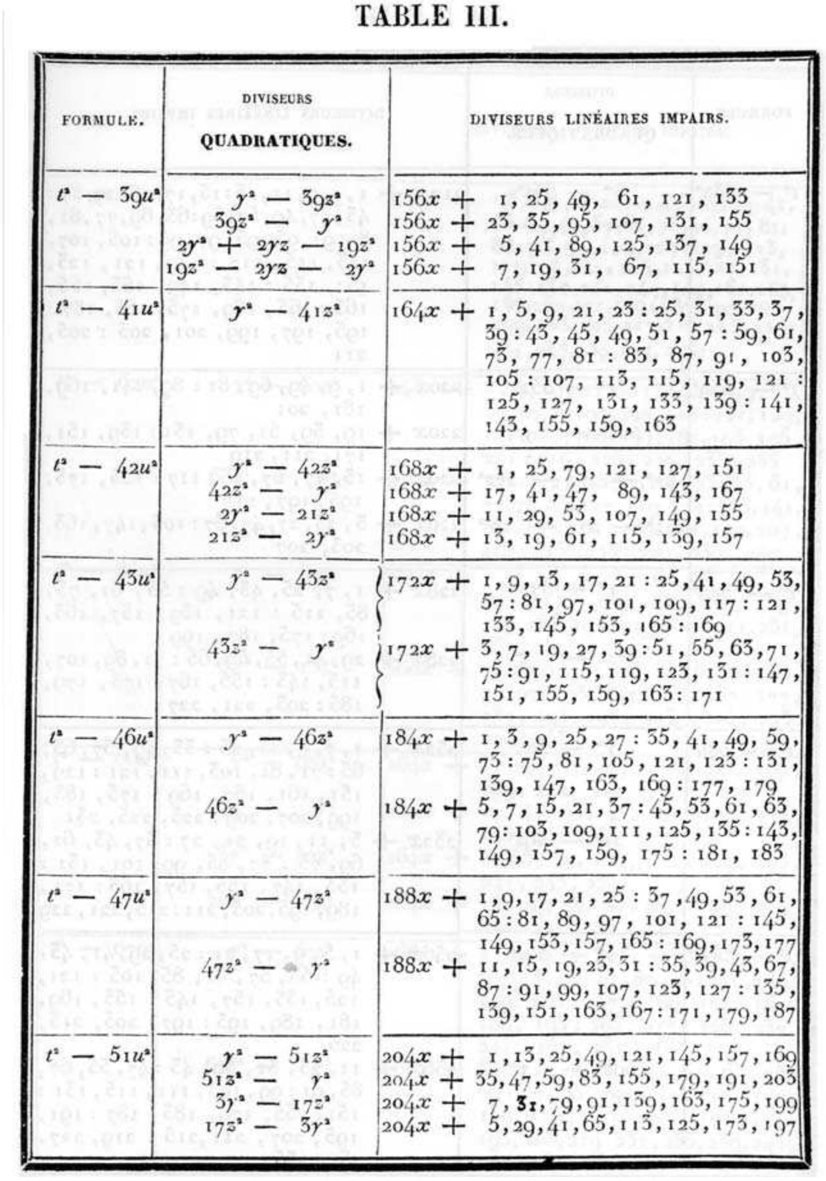


TABLE III.

FORMULE.	DIVISEURS QUADRATIQUES.	DIVISEURS LINÉAIRES IMPAIRS.
$t^2 - 39u^2$	$y^2 - 39z^2$	$156x +$ 1, 25, 49, 61, 121, 133
	$39z^2 - y^2$	$156x +$ 23, 35, 95, 107, 131, 155
	$2y^2 + 2yz - 19z^2$	$156x +$ 5, 41, 89, 125, 137, 149
	$19z^2 - 2yz - 2y^2$	$156x +$ 7, 19, 31, 67, 115, 151
$t^2 - 41u^2$	$y^2 - 41z^2$	$164x +$ 1, 5, 9, 21, 23 : 25, 31, 33, 37, 39 : 43, 45, 49, 51, 57 : 59, 61, 73, 77, 81 : 83, 87, 91, 103, 105 : 107, 113, 115, 119, 121 : 125, 127, 131, 133, 139 : 141, 143, 155, 159, 163
$t^2 - 42u^2$	$y^2 - 42z^2$	$168x +$ 1, 25, 79, 121, 127, 151
	$42z^2 - y^2$	$168x +$ 17, 41, 47, 89, 143, 167
	$2y^2 - 21z^2$	$168x +$ 11, 29, 53, 107, 149, 155
	$21z^2 - 2y^2$	$168x +$ 13, 19, 61, 115, 139, 157
$t^2 - 43u^2$	$y^2 - 43z^2$	$172x +$ 1, 9, 13, 17, 21 : 25, 41, 49, 53, 57 : 81, 97, 101, 109, 117 : 121, 133, 145, 153, 165 : 169
	$43z^2 - y^2$	$172x +$ 3, 7, 19, 27, 39 : 51, 55, 63, 71, 75 : 91, 115, 119, 123, 131 : 147, 151, 155, 159, 163 : 171
$t^2 - 46u^2$	$y^2 - 46z^2$	$184x +$ 1, 3, 9, 25, 27 : 35, 41, 49, 59, 73 : 75, 81, 105, 121, 123 : 131, 139, 147, 163, 169 : 177, 179
	$46z^2 - y^2$	$184x +$ 5, 7, 15, 21, 37 : 45, 53, 61, 63, 79 : 103, 109, 111, 125, 135 : 143, 149, 157, 159, 175 : 181, 183
$t^2 - 47u^2$	$y^2 - 47z^2$	$188x +$ 1, 9, 17, 21, 25 : 37, 49, 53, 61, 65 : 81, 89, 97, 101, 121 : 145, 149, 153, 157, 165 : 169, 173, 177
	$47z^2 - y^2$	$188x +$ 11, 15, 19, 23, 31 : 35, 39, 43, 67, 87 : 91, 99, 107, 123, 127 : 135, 139, 151, 163, 167 : 171, 179, 187
$t^2 - 51u^2$	$y^2 - 51z^2$	$204x +$ 1, 13, 25, 49, 121, 145, 157, 169
	$51z^2 - y^2$	$204x +$ 35, 47, 59, 83, 155, 179, 191, 203
	$3y^2 - 17z^2$	$204x +$ 7, 31, 79, 91, 139, 163, 175, 199
	$17z^2 - 3y^2$	$204x +$ 5, 29, 41, 65, 113, 125, 173, 197

Fig. VIII.3A. Table of linear and quadratic divisors (extract)
A.-M. Legendre's *Théorie des nombres*, vol. 1, 1830

2. Gauss's *Disquisitiones Arithmeticae*

We briefly recall Gauss's definitions in sec. 5 of the *Disquisitiones*. A binary quadratic form $F(x, y) = ax^2 + 2bxy + cy^2$ is also denoted by (a, b, c). The *determinant* of F is $D = b^2 - ac$. An integer n is said to be *represented* by F if there exist integers x, y such that $n = F(x, y)$. A form (a, b, c) is *ambiguous* if $a \mid 2b$, and *primitive* if $\gcd(a, b, c) = 1$.

The following theorem, proved in art. 229 of the D.A., is the basis for the definition of the genus of a binary quadratic form:

> If F is a primitive form of determinant D, p a prime number dividing D, then the numbers not divisible by p that can be represented by F agree in that they are either all quadratic residues of p, or all nonresidues.[24]

For $p = 2$ the claim is correct but trivial. If $4 \mid D$, however, then the numbers represented by f are all $\equiv 1 \bmod 4$, or all $\equiv 3 \bmod 4$. Similarly, if $8 \mid D$, the numbers lie in exactly one of the four residue classes $1, 3, 5$ or $7 \bmod 8$. For odd primes *not* dividing the discriminant, Gauss observes in the same art. 229:

> If it were necessary for our purposes, we could easily show that numbers representable by the form F have no such fixed relationship to a prime number that does not divide D.[25]

The only exception occurs for the residue classes modulo 4 and 8 of representable odd numbers in the case where D is odd:

I. If $D \equiv 3 \bmod 4$, then odd n that can be represented by F are either all $1 \bmod 4$ or all $3 \bmod 4$.
II. If $D \equiv 2 \bmod 8$, then odd n that can be represented by F are either all $\pm 1 \bmod 8$ or all $\pm 3 \bmod 8$.
III. If $D \equiv 6 \bmod 8$, then odd n that can be represented by F are either all $1, 3 \bmod 8$ or all $5, 7 \bmod 8$.

Gauss uses these observations in D.A., art. 230, to define the *(total) character* of a primitive binary quadratic form. For example, to the quadratic form $(7, 0, 23)$ of determinant $-7\cdot 23 = -161 \equiv 3 \bmod 4$ he attaches the total character $1, 4$; $R7$; $N23$ because the integers represented by $7x^2 + 23y^2$ are $\equiv 1 \bmod 4$, quadratic residues modulo 7, and quadratic nonresidues modulo 23. Gauss observes that if (a, b, c) is a primitive quadratic form, then a prime p dividing $b^2 - ac$ does not divide $\gcd(a, c)$, so the character of primitive forms can be determined from the integers a and c, which of course are both represented by (a, b, c). Finally he remarks that forms

[24] Our translation of D.A., art. 229: Theorema. *Si F forma primitiva determinantis D, p numerus primus ipsum D metiens: tum numeri per p non divisibiles qui per formam F repraesentari possunt in eo convenient, ut vel omnes sint residua quadratica ipsius p, vel omnes non residua.*

[25] D.A., art. 229: *Ceterum, si ad propositum praesens necessarium esset, facile demonstrare possemus, numeros per formam F repraesentabiles ad nullum numerum primum qui ipsum D non metiatur, talem relationem fixam habere, sed promiscue tum residua tum non-residua numeri cuiusuis primi ipsum D non metientis per formam F repraesentari posse.*

in the same class have the same total character, so the notion of character passes to classes of forms. A *genus*[26] of quadratic forms is then defined to consist of all classes with the same total character. The *principal genus* is the genus containing the principal class, i.e., the class containing the form $(1, 0, -D)$ of determinant D.

In art. 261 of the D.A., Gauss proves the *first inequality* of genus theory: at least half of all possible total characters do not occur. In art. 262, the quadratic reciprocity law is deduced from this first inequality.

After having studied the representations of binary quadratic forms by ternary forms, Gauss returns to binary quadratic forms in art. 286, and now proves the principal genus theorem quoted in our introduction. This immediately implies the *second inequality* of genus theory in art. 287: at least half of all possible total characters do in fact occur. Finally, in art. 303, Gauss characterizes Euler's idoneal numbers using genus theory. One of the key ingredients of genus theory is the determination of the number of the so-called *ambiguous classes*[27] in arts. 257–259 of the D.A.

A word on terminology may be in order: In his 1932–1933 Marburg lectures on Class Field Theory, Helmut Hasse wrote: "The term *ambig*, whose usage in this connection is somewhat unfortunate, is due to Gauss."[28] Gauss, however, had of course written in Latin and called an "ambiguous" quadratic form *forma anceps*. From Dedekind we learn:

> When giving his lectures, Dirichlet always used the word *forma anceps*, which I have kept when I prepared the first edition (1863); in the second and third editions (1871, 1879), … I called them *ambige Formen* following Kummer, who used this notation in a related area.[29]

[26] This terminology, which fits in with the *orders* and *classes* of quadratic forms that Gauss defines in arts. 234–256 of the D.A., is obviously inspired by biology. Carl von Linné (1707–1778) had classified the living organisms into kingdoms (plants, animals), classes, orders, genera, and species. Ernst Eduard Kummer would use the German *Gattung* for Gauss's latin *genus*, but in the long run the translation *Geschlecht* prevailed in Germany.

[27] Gauss called a class of forms *anceps* if it was "opposite to itself" (D.A., art. 224: *classes sibi ipsis oppositae*), in other words, if its order in the class group divides 2.

[28] See [Hasse 1967], p. 158: *Die in diesem Zusammenhang nicht sehr glückliche Bezeichnung "ambig" stammt von Gauss.* Hasse apparently worked from Maser's German translation of the D.A. which does have *ambig*. Clarke in his English translation of the D.A. used "ambiguous," whereas I. Adamson used "ambig" in his English translation of Hilbert's *Zahlbericht*.

[29] See [Dirichlet 1863/1894], p. 139: *Im mündlichen Vortrage gebrauchte Dirichlet immer die Bezeichnung* forma anceps*, welche ich auch bei der Ausarbeitung der ersten Auflage (1863) beibehalten habe; in der zweiten und dritten Auflage (1871, 1879), wo diese Formen und die ihnen entsprechenden Formen-Classen häufiger auftraten (*§§ *152, 153), habe ich sie im Anschluss an die von Kummer (Monatsber. d. Berliner Akad. vom 18. Februar 1858) auf einem verwandten Gebiete benutzte Bezeichnung* ambige Formen *genannt.* As a matter of fact, A.C.M. Poullet-Delisle in his 1807 French translation of the D.A., already used *classe ambiguë*; Kummer may have got his term from there.

In the fourth edition (1894), Dedekind replaced *ambig* by "twosided" (*zweiseitig*), i.e., the German translation of *anceps*.

Gauss used his theory of *ternary quadratic forms* to prove the principal genus theorem, but also to derive Legendre's theorem,[30] as well as the celebrated 3-squares theorem to the effect that every positive integer not of the form $4^a(8b+7)$ can be written as a sum of three squares. Friedrich Arndt first, and later Dedekind and Paul Mansion[31] realized that Legendre's theorem is sufficient for proving the principal genus theorem. This simplified genus theory considerably[32] – see [Lemmermeyer 2000], chap. 2.[33]

3. Dirichlet and Dedekind

Johann Peter Gustav Lejeune-Dirichlet is said[34] to have never put Gauss's *Disquisitiones Arithmeticae* on the bookshelf, but to have always kept the copy on his desk and taken it along even on journeys. He is well-known for having simplified Gauss's exposition (sometimes by restricting to a special case), thereby making the D.A. accessible to a wider circle of mathematicians. In [Dirichlet 1839], he replaced Gauss's notation aRp, aNp for quadratic (non)residues by Legendre's symbol $\left(\frac{a}{p}\right) = \pm 1$, thus giving Gauss's characters the now familiar look. But his main contribution in this paper was an analytic proof of the second inequality of genus theory.[35]

Dirichlet's results were added as supplement IV and X of Dedekind's edition of Dirichlet's Lectures. Thus in § 122 of [Dirichlet 1863/1894] an integer λ is defined by

$$\lambda = \#\{\text{odd primes dividing } D\} + \begin{cases} 0 & \text{if } D \equiv 1 \bmod 4 \\ 2 & \text{if } D \equiv 0 \bmod 8 \\ 1 & \text{otherwise,} \end{cases}$$

and in § 123 the first inequality of genus theory is proved: $g \leq 2^{\lambda-1}$. In § 125, Dedekind gives Dirichlet's analytic proof of the existence of these genera, i.e., the

[30] To the effect that the equation $ax^2 + by^2 + cz^2 = 0$ has a nontrivial solution in integers if and only if the coefficients do not have the same sign, and $-bc$, $-ca$, and $-ab$ are squares modulo a, b, and c, respectively.

[31] See [Arndt 1859], [Dirichlet 1863/1894], and [Mansion 1896].

[32] Note, however, that Gauss's proof was constructive, while those based on Legendre's theorem are not.

[33] Legendre's theorem does not seem to imply the 3-squares theorem. In [Deuring 1935], VII, § 9, a beautiful proof is sketched which uses the theory of quaternion algebras – see also [Weil 1984], III, App. II, pp. 292–294. In 1927, Venkov used Gauss's theory of ternary quadratic forms to give an arithmetic proof of Dirichlet's class number formula for negative discriminants $-m$ in which m is the sum of three squares – see [Venkov 1970]. Shanks [Shanks 1971a] used binary quadratic forms to develop his clever factorization algorithm SQUFOF (short for SQUare FOrm Factorization) and Gauss's theory of ternary quadratic forms for an algorithm to compute the 2-class group of complex quadratic number fields – see [Shanks 1971b].

[34] See [Reichardt 1963], p. 14. [Editors' note: see also chaps. I.1 and II.2 above].

[35] Cf. [Zagier 1981] for a modern exposition of it.

second inequality of genus theory:

> The number of existing genera is $2^{\lambda-1}$, and all these genera contain equally many classes of forms.[36]

He also remarks that the second inequality follows immediately from Dirichlet's theorem on the infinitude of primes in arithmetic progressions.

Dedekind returned to the genus theory of binary quadratic forms in his supplement X: § 153 gives the first inequality, § 154 the quadratic reciprocity law, and in § 155 he observes that the second inequality of genus theory (the existence of half of all the possible genera) is essentially identical with the principal genus theorem: "Every class of the principal genus arises from duplication." He then adds:

> It is impossible for us to go here into communicating the proof which Gauss has based on the theory of ternary quadratic forms. But since this deep theorem is the most beautiful conclusion of the theory of composition, we cannot abstain from deriving this result without the use of Dirichlet's principles, in a second way, which will at the same time form the basis for other important investigations.[37]

This new proof begins by showing that the following statement is equivalent to the principal genus theorem:

> If (A, B, C) is a form in the principal genus of determinant D, then the equation $Az^2 + 2Bzy + Cy^2 = x^2$ has solutions in integers z, y, x such that x is coprime to $2D$.[38]

In § 158, Dedekind gives a proof of the principal genus theorem based on Legendre's theorem, referring to [Arndt 1859] for a first proof of this kind.

4. David Hilbert

Although Dedekind introduced ideals and maximal orders in number fields, he did not translate genus theory into his new language. David Hilbert on the other hand worked on the arithmetic of quadratic extensions of $\mathbf{Q}(i)$ even before his report on algebraic number fields [Hilbert 1897]. His goal then was to

> extend the theory of Dirichlet's biquadratic number field in a purely arithmetic way to the same level that the theory of quadratic number fields has had since Gauss,

[36] See [Dirichlet 1863/1871], p. 324: *Die Anzahl der wirklich existierenden Geschlechter ist gleich* $2^{\lambda-1}$*, und alle diese Geschlechter enthalten gleich viele Formenklassen.*

[37] See [Dirichlet 1863/1871], p. 407: *Wir können hier unmöglich darauf eingehen, den Beweis mitzutheilen, welchen Gauss auf die Theorie der ternären quadratischen Formen gestützt hat; da dieses tiefe Theorem aber den schönsten Abschluss der Lehre von der Composition bildet, so können wir es uns nicht versagen, dasselbe auch ohne Hülfe der Dirichlet'schen Principien auf einem zweiten Wege abzuleiten, der zugleich die Grundlage für andere wichtige Untersuchungen bildet.*

[38] See [Dirichlet 1863/1894], § 155, p. 408: *Ist* (A, B, C) *eine Form des Hauptgeschlechtes der Determinante D, so ist die Gleichung* $Az^2 + 2Bzy + Cy^2 = x^2$ *stets lösbar in ganzen Zahlen* z, y, x*, deren letzte relative Primzahl zu* $2D$ *ist.*

and the main tool for achieving this goal was, according to Hilbert, the notion of genera of ideal classes.[39]

Let $\mathbf{Z}[i]$ denote the ring of Gaussian integers, and let $\delta \in \mathbf{Z}[i]$ be a squarefree nonsquare. Hilbert considers the quadratic extension $K = \mathbf{Q}(\sqrt{\delta}\,)$ of $k = \mathbf{Q}(i)$, computes integral bases, and determines the decomposition of primes. For the definition of the genus, Hilbert then introduces the prototype of his norm residue symbol. For $\sigma \in k$ and λ a prime divisor different from $(1+i)$ of the discriminant of K/k, Hilbert writes $\sigma = \alpha\nu$ as a product of a relative norm ν and some $\alpha \in \mathbf{Z}[i]$ not divisible by λ, and puts

$$\left[\frac{\sigma}{\lambda : \delta}\right] = \left[\frac{\alpha}{\lambda}\right],$$

where $[\frac{\cdot}{\cdot}]$ is the quadratic residue symbol in $\mathbf{Z}[i]$. (The definition for $\lambda = 1 + i$ is slightly more involved.)

Then Hilbert defines the character system of an ideal $\mathfrak{a}$ in $\mathcal{O}_K$ as the system of signs

$$\left[\frac{\sigma}{\lambda_1 : \delta}\right], \ldots, \left[\frac{\sigma}{\lambda_s : \delta}\right],$$

where $\lambda_1, \ldots, \lambda_s$ denote the ramified primes. The character system of ideals only depends on their ideal class, and classes with the same character system are then said to be in the same genus. The principal genus is the set of ideal classes whose character system is trivial. The principal genus theorem is then formulated thus:

> Each ideal class in the principal genus is the square of some ideal class.[40]

Hilbert went on to determine the number of genera, derived the quadratic reciprocity law, and finally gave an arithmetic proof of the class number formula for $\mathbf{Q}(i, \sqrt{m}\,)$ and $m \in \mathbf{Z}$. He apparently had not yet realized that his symbols $\left[\frac{\sigma}{\lambda:\delta}\right]$ were norm residue symbols, nor that the quadratic reciprocity law could be expressed via a product formula for them.

He took these steps in the third section of his *Zahlbericht* [Hilbert 1897] dealing with the theory of quadratic number fields. There he called an integer n a norm residue[41] at p in $\mathbf{Q}(\sqrt{m}\,)$ if m is a square or if for all $k \geq 1$ there exist integers $x, y \in \mathbf{Z}$ such that $n \equiv x^2 - my^2 \bmod p^k$.

[39] The complete quotation from the introduction of [Hilbert 1894] reads: *Die vorliegende Abhandlung hat das Ziel, die Theorie des Dirichletschen biquadratischen Zahlkörpers auf rein arithmetischem Weg bis zu demjenigen Standpunkt zu fördern, auf welchem sich die Theorie der quadratischen Körper bereits seit* Gauss *befindet. Es ist hierzu vor allem die Einführung des Geschlechtsbegriffs sowie eine Untersuchung derjenigen Einteilung aller Idealklassen notwendig, welche sich auf den Geschlechtsbegriff gründet.*

[40] See [Hilbert 1894], § 4: *Eine jede Idealklasse des Hauptgeschlechtes ist gleich dem Quadrat einer Idealklasse.*

[41] I will adopt the following convention: an element is a norm residue *modulo* $\mathfrak{a}$ if it is congruent to a norm modulo $\mathfrak{a}$, and a norm residue *at* $\mathfrak{p}$ if it is congruent to norms modulo every power $\mathfrak{p}^k$.

Then he defined the norm residue symbol by

$$\left(\frac{n\,,\,m}{p}\right) = \begin{cases} +1 & \text{if } m \text{ is a norm residue at } p \text{ in } \mathbf{Q}(\sqrt{m}\,) \\ -1 & \text{otherwise.} \end{cases}$$

Hilbert used the norm residue symbol to define characters on ideal classes and defined the principal genus to consist of those ideal classes with trivial character system. In [Hilbert 1897], § 68, he employed ambiguous ideals and his famous *Satz 90* to prove that quadratic number fields with exactly one ramified prime have odd class number. The quadratic reciprocity law is deduced from this in § 69, and the version for quadratic number fields of the principal genus theorem in § 72, including an acknowledgement of the *Disquisitiones Arithmeticae*:

> In a quadratic number field, each class of the principal genus is the square of a class [Gauss (1)].[42]

Hilbert's proof uses a reduction technique reminiscent of Lagrange; the solvability of the norm equation $n = x^2 - my^2$ for $x, y \in \mathbf{Q}$ is equivalent to the fact that the ternary quadratic form $x^2 - my^2 - nz^2$ nontrivially represents 0 in integers. Hilbert explicitly referred to Lagrange when he stated :

> If n, m denote two rational integers, of which m is not a square, and which for any prime w satisfy the condition $\left(\frac{n\,,\,m}{w}\right) = +1$, then n is the norm of an integral or fractional number α of the field $k(\sqrt{m}\,)$.[43]

Note in passing that this is a special case of Hasse's Norm Theorem, according to which elements that are local norms everywhere (with respect to a cyclic extension) are global norms. The ambiguous class number formula (*Satz 108*, § 77) follows, and finally Hilbert gives a second proof of the principal genus theorem using Dirichlet's analytic techniques, in § 82.

With Hilbert's 1897 *Zahlbericht*, the translation of Gauss's genus theory of binary quadratic forms into the corresponding theory of quadratic extensions was complete. Distinctive features of Hilbert's presentation are the central role of the ambiguous class number formula, the introduction of norm residue symbols, and the corresponding formulation of the reciprocity law as a product formula. Although Hilbert saw that the norm residue symbol for the infinite rational prime[44] would simplify the presentation, he chose not to use it. But these symbols could no longer be avoided when he replaced the rational numbers by arbitrary base fields k in his article [Hilbert 1898] on class field theory in the quadratic case.

[42] [Hilbert 1897], § 71, *Satz 103: In einem quadratischen Körper ist jede Klasse des Hauptgeschlechts stets gleich dem Quadrat einer Klasse* [Gauss (1)].

[43] [Hilbert 1897], § 71, *Satz 102: Wenn n, m zwei ganze rationale Zahlen bedeuten, von denen m keine Quadratzahl ist, und die für jede beliebige Primzahl w die Bedingung* $(\frac{n\,,\,m}{w}) = +1$ *erfüllen, so ist die Zahl n stets gleich der Norm einer ganzen oder gebrochenen Zahl α des Körpers $k(\sqrt{m}\,)$.* Here $k(\sqrt{m}\,)$ denotes the quadratic number field k one gets by adjoining $\sqrt{m}$ to the field of rational numbers.

[44] See [Hilbert 1897], § 70; Hilbert wrote it as $(\frac{n,m}{-1})$.

5. Heinrich Weber

In the third volume of his algebra [Weber 1908], § 108, Heinrich Weber gave an account of genus theory that shows Hilbert's influence: Even though Weber did not include the theory of the quadratic Hilbert symbol, he did realize the importance of the concept of norm residues.

For a modulus $m \in \mathbf{N}$ and a natural number S divisible by m, Weber formed the multiplicative group Z of rational numbers $\frac{a}{b}$ relatively prime to S, that is, $a, b \in \mathbf{Z}$ and $\gcd(a, S) = \gcd(b, S) = 1$. The kernel of the natural map $Z \to (\mathbf{Z}/m\mathbf{Z})^\times$ is the group M of all elements of Z that are congruent to 1 mod m, and Weber observed that $(Z : M) = \phi(m)$.

Now let $\mathcal{O}$ denote an order of a quadratic number field k (Weber wrote Q instead of $\mathcal{O}$) such that the prime factors of the conductor of $\mathcal{O}$ divide S; in particular, the discriminant Δ of $\mathcal{O}$ is only divisible by primes dividing S. The set of integers $a \in \mathbf{Z}$ for which there is an $\omega \in \mathcal{O}$ with $N\omega \equiv a \bmod m$ form a subgroup A of Z containing M, namely, the group of norm residues modulo m of $\mathcal{O}$. To simplify the presentation, let $A\{m\}$ denote this group of norm residues modulo m. Weber in [Weber 1908], § 107, observed that if $m = m_1 m_2$ with $\gcd(m_1, m_2) = 1$, then $(Z : A\{m\}) = (Z : A\{m_1\})(Z : A\{m_2\})$, thereby reducing the computation of the index $(Z : A\{m\})$ to the case of prime powers m. In the following section § 108, he proved that

$$(Z : A\{p^t\}) = \begin{cases} 1 & \text{if } p \text{ does not divide } \Delta \\ 2 & \text{if } p \text{ divides } \Delta \end{cases}$$

for an odd prime p, and

$$(Z : A\{2^t\}) = \begin{cases} 1 & \text{if } \Delta \equiv 1 \bmod 4,\ \ \Delta \equiv 4, 20 \bmod 32, \\ 2 & \text{if } \Delta \equiv 8, 12, 16, 24, 28 \bmod 32, \\ 4 & \text{if } \Delta \equiv 0 \bmod 32. \end{cases}$$

If r is a norm residue modulo m for any modulus m prime to r, Weber called r an *absolute norm residue*; the set of all such $r \in Z$ forms a group R.[45] As a consequence of his index computations above, Weber obtained $(Z : R) = 2^\lambda$, where λ is the number of *discriminant divisors* of Δ. Here a divisor δ of Δ is called a *discriminant divisor* if both δ and Δ/δ are discriminants.

In [Weber 1908], § 109, the genus of an ideal is defined to be the set of all ideals $\mathfrak{a}$ coprime to Δ whose norms $N\mathfrak{a}$ are in the same coset of Z/R. Weber observes that equivalent ideals have the same genus. The principal genus is the group of all ideals relatively prime to Δ such that $N\mathfrak{a} \in R$. He shows that the existence of primes that are quadratic nonresidues modulo Δ implies that the number g of genera satisfies the inequality $g \le \frac{1}{2}(Z : R)$, and that the existence of such primes is equivalent to the quadratic reciprocity law. The fact that this inequality is in fact an equality is proved in § 113 of [Weber 1908] with the help of Dirichlet's analytic methods.

The local nature of the index calculations is much more visible in Weber's treatment than in Hilbert's. Weber's index formulas are closely related to Gauss's observation in the second passage from art. 229 of the D.A. quoted in § 2 above.

[45] See [Weber 1908], §§ 108–109.

6. Erich Hecke

Erich Hecke's *Vorlesungen über die Theorie der algebraischen Zahlen* [Hecke 1923] contains a masterful exposition of algebraic number theory including the genus theory of (the maximal orders of) quadratic fields. Shortly after the publication of this textbook, during the reformulation of class field theory in the 1930s, genus theory would be thrust into the background, as local methods gradually replaced it in the foundation of class field theory.

Hecke's presentation of genus theory in quadratic fields k with discriminant d combined known features with novel ones. First, Hecke used class groups in the strict sense. Already Hilbert had seen that this simplified the exposition of genus theory because some of the statements "can be expressed in a simpler way by using the new notions."[46] Second, Hecke used Weber's index computation for norm residues, but restricted his attention right from the start to norm residues modulo d. Third, Hecke gave a new and very simple definition of genera: two ideals $\mathfrak{a}$ and $\mathfrak{b}$ coprime to d are said to belong to the same genus if there exists an $\alpha \in k^\times$ such that $N\mathfrak{a} = N\mathfrak{b} \cdot N(\alpha)$; note that $N(\alpha) > 0$.

As a corollary of genus theory and the index calculations Hecke finally obtained the following characterizations:[47]

Proposition. Let k be a quadratic number field with discriminant d. An ideal $\mathfrak{a}$ coprime to d is in the principal genus if and only if one of the following equivalent conditions is satisfied:

(1) $\mathfrak{a}$ is equivalent in the strict sense to the square of some ideal $\mathfrak{b}$.
(2) $(\frac{N\mathfrak{a},d}{p}) = +1$ for all primes $p \mid d$.
(3) $N\mathfrak{a} = N(\alpha)$ for some $\alpha \in k^\times$.
(4) $N\mathfrak{a} \equiv N(\alpha) \bmod d$ for some $\alpha \in k^\times$.

Hecke, not surprisingly, proved the existence of genera analytically:

> The fact that the number g of genera is $= 2^{t-1}$ can be proved most conveniently by using transcendental methods.[48]

After the statement of his *Fundamentalsatz über die Geschlechter*, Hecke remarks that "Gauss was the first to discover this theorem and gave a purely arithmetic proof of it."[49]

[46] See [Hilbert 1897], § 83–84. The quote is from the end of §84: ... *und einige [dieser Tatsachen] erhalten bei Verwendung der neuen Begriffe sogar noch einen einfacheren Ausdruck.*

[47] This result summarizes parts of Theorems 138–141 and 145 in [Hecke 1923].

[48] See [Hecke 1923], § 48, paragraph preceding *Satz 144*: *Die Tatsache, daß die Anzahl der Geschlechter g genau* $= 2^{t-1}$ *ist, wird nun am bequemsten mit Benutzung transzendenter Methoden ... bewiesen.*

[49] See [Hecke 1923], § 48, remark following *Satz 145*: *Gauss hat diesen Satz zuerst gefunden und für ihn einen rein arithmetischen Beweis gegeben.*

7. Euler's Conjecture Revisited

In this section we will show that the modified Euler Conjecture 2 of § 1 above follows from genus theory. Assume that n is a positive squarefree integer and that $p \equiv 1 \bmod 4n$ is prime. Then $\left(\frac{p}{p_i}\right) = +1$ for all primes $p_i \mid n$, which by quadratic reciprocity implies $\left(\frac{d_i}{p}\right) = \left(\frac{p_i}{p}\right) = +1$, where d_i are the prime discriminants[50] dividing the discriminant d of $\mathbf{Q}(\sqrt{n}\,)$. Applying the following proposition with $a = -n$ then proves the Goldbach-Euler conjecture for squarefree n:

Proposition. Let a be a squarefree integer $\neq 1$, $k = \mathbf{Q}(\sqrt{a}\,)$ a quadratic number field with discriminant d, and $p > 0$ a prime not dividing d. Then the following conditions are equivalent:

(i) there exist $x, y \in \mathbf{Q}$ with $p = x^2 - ay^2$;

(ii) we have $\left(\frac{d_i}{p}\right) = 1$ for all prime discriminants d_i dividing the discriminant of k;

(iii) we have $p\mathcal{O}_k = \mathfrak{p}\mathfrak{p}'$, and $\mathfrak{p}$ is equivalent (in the strict sense) to the square of an ideal in $\mathcal{O}_k$.

Proof. Condition (i) says that the norm of a prime ideal $\mathfrak{p}$ above p is the norm of an element, which by Hecke's Proposition (see § 6 above) implies that $\mathfrak{p}$ is in the principal genus, i.e., (iii). Similarly, if p does not divide d, then the Legendre symbols $\left(\frac{d_i}{p}\right)$ essentially coincide with the Hilbert symbols $(\frac{p,d}{p_i})$, where p_i is the unique prime dividing d_i, and this time we see that $\mathfrak{p}$ is in the principal genus by part (2) of Hecke's Proposition. Finally, (iii) $\Rightarrow$ (i) is proved by taking norms.

Looking at Lagrange's counterexample to Euler's original conjecture in the light of Hecke's genus theory, observe that 79 is the smallest natural number a such that the class group of $\mathbf{Q}(\sqrt{a}\,)$ is strictly larger than the genus class group.

The above proposition shows in fact the *equivalence* of the amended Conjecture 2 of § 1 with the Principal Genus Theorem, in view of the following obervation whose proof is a simple exercise using the quadratic reciprocity law:

Let $a \neq 1$ be a squarefree integer, $k = \mathbf{Q}(\sqrt{a}\,)$ a quadratic number field with discriminant d, and $p > 0$ a prime not dividing d. Then the following conditions are equivalent:

1. There exist $n, r \in \mathbf{Z}$ such that $p = 4an + r^2$ or $p = 4an + r^2 - a$.
2. We have $(d_i/p) = 1$ for all prime discriminants d_i dividing d.

To the best of my knowledge, this equivalence has never been noticed before.[51] In his preface to Euler's *Opera Omnia*, Karl Rudolf Fueter remarks[52] that Euler's observation in [Euler 1775] to the effect that only half of all possible prime residue classes mod $4n$ may yield prime factors of $x^2 + ny^2$, is equivalent to Gauss's result that at most half of all possible genera exist. Gauss himself had remarked in art. 151 of the D.A. that there was a gap in Euler's proof. H.M. Edwards has observed:

[50] A prime discriminant is a discriminant of a quadratic number field that is a prime power.

[51] Not by Lagrange (who disproved Euler's conjecture), nor by Legendre (who proved a result on $ax^2 + by^2 + cz^2$, which contains criteria for the solvability of $-c = aX^2 + bY^2$ in rational numbers as a special case), nor apparently anywhere else in the literature.

[52] See [Fueter 1941], p. xiii.

"The case $D = 79$ is one that Gauss frequently uses as an example,"[53] and has gone on to suggest that Gauss's interest in this discriminant may have been sparked by Lagrange's counterexample to Euler's conjecture.

8. Ernst Eduard Kummer

Kummer's motivation for creating a genus theory for Kummer extensions over $\mathbf{Q}(\zeta)$, where ζ is a primitive ℓ-th root of unity and ℓ an odd prime number, was his quest for a proof of the reciprocity law for ℓ-th powers: call an $\alpha \in \mathbf{Z}[\zeta]$ *primary* if α is congruent to a nonzero integer modulo $(1-\zeta)^2$ and if $\alpha\overline{\alpha}$ is congruent to an integer modulo ℓ. Given two primary, coprime integers $\alpha, \beta \in \mathbf{Z}[\zeta]$, Kummer had conjectured the reciprocity law $\left(\frac{\alpha}{\beta}\right) = \left(\frac{\beta}{\alpha}\right)$ for the ℓ-th power residue symbol. When all other methods of proof had failed (in particular cyclotomic methods via Gauss and Jacobi sums), he turned to Gauss's genus theory.

Let us write $\lambda = 1 - \zeta$, and $\mathfrak{l} = (\lambda)$ for the prime ideal[54] in $k = \mathbf{Q}(\zeta)$ above ℓ. Let M denote the set of all $\alpha \in k^\times$ coprime to $\mathfrak{l}$. Assume that $\alpha \in \mathbf{Z}[\zeta]$ satisfies $\alpha \equiv 1 \bmod \lambda$, and write it as $\alpha = f(\zeta)$ for some polynomial $f \in \mathbf{Z}[X]$; evaluate the r-th derivative of $\log f(e^v)$ with respect to v at $v = 0$, and call the result $\mathcal{L}^r(\alpha)$.[55] For $1 \le r \le \ell - 2$, the resulting integer modulo ℓ does not depend on the choice of f; with a little bit more care it can be shown that a similar procedure gives a well defined result even for $r = \ell - 1$. We will not follow here Kummer's *tour de force* to set up his formalism, but only give the conclusion.[56]

Put $K = \mathbf{Q}(\zeta_\ell)$, fix an integer $\mu \in \mathbf{Z}[\zeta_\ell]$ and consider the Kummer extension $L = K(\sqrt[\ell]{\mu})$. Kummer's "integers in w" were elements of $\mathcal{O}[w]$, where $w = \sqrt[\ell]{\mu}$ and $\mathcal{O} = \mathbf{Z}[\zeta_\ell]$; observe that $\mathcal{O}[w] \ne \mathcal{O}_L$ in general even when μ is squarefree. He introduced integers $z_j = (1-\zeta)(1-\mu)/(1-w\zeta^j) \in \mathcal{O}[w]$ as well as the ring $\mathcal{O}_z = \mathcal{O}[z_0, z_1, \ldots, z_{\ell-1}]$ and observed that $\ell\mathcal{O}[w] \subseteq \mathcal{O}_z \subseteq \mathcal{O}[w]$. Assume that $\mathfrak{p}$ is a prime ideal in $\mathbf{Z}[\zeta]$ and let h denote the class number. Then $\mathfrak{p}^h = (\pi)$, and we can try to define $\mathcal{L}^r(\mathfrak{p})$ by the equation $h\mathcal{L}^r(\mathfrak{p}) = \mathcal{L}^r(\pi)$. Unfortunately, the values of $\mathcal{L}^r(\pi)$ depend on the choice of π in general. But not always: since it turns out that $\mathcal{L}^{2r+1}(\varepsilon_j) = 0$ for all real units ε_j and all $0 \le r \le \rho = \frac{1}{2}(\ell - 1)$, and since moreover $\mathcal{L}^{2r+1}(\zeta) = 0$ for all $1 \le r \le \rho$, the quantity $\mathcal{L}^{2r+1}(\mathfrak{p}) = \frac{1}{h}\mathcal{L}^{2r+1}(\pi)$ is well defined.

This allowed Kummer to define characters $\chi_3, \chi_5, \ldots, \chi_{\ell-2}$ on the group of ideals in $\mathcal{O}_z$ which are prime to $\ell \cdot \operatorname{disc}(L/K)$ by putting

$$\chi_{2r+1}(\mathfrak{P}) = \zeta^{\mathcal{L}^{2r+1}(N_{L/K}\mathfrak{P})}, \quad \text{to which he added} \quad \chi_{\ell-1}(\mathfrak{P}) = \zeta^{\frac{1-N\mathfrak{P}}{\ell}}.$$

[53] See [Edwards 1977], p. 274; Edwards explicitly mentions D.A., arts. 185, 186, 187, 195, 196, 198, 205, 223 as examples.

[54] For Kummer: the "ideal prime number."

[55] Kummer wrote $\frac{d_0^r \log f(e^v)}{dv^r}$ instead.

[56] Kummer's work on reciprocity laws is spread out over several papers; the main articles are [Kummer 1850], [Kummer 1859], and [Kummer 1861]. As noticed by Takagi and Hasse, Kummer's differential logarithms can be neatly described algebraically. A detailed exposition will be given in the forthcoming [Lemmermeyer 2007].

Now let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ denote the primes different from (λ) that are ramified in L/K. For each such prime Kummer defined a character $\psi_j(\mathfrak{p})$ as follows: $\mathfrak{p} = N_{L/K}\mathfrak{P}$ is an ideal in $\mathbf{Z}[\zeta]$, $\mathfrak{p}^h = (\pi)$ is principal, and if we insist on taking π primary, then the symbol $\left(\frac{\pi}{\mathfrak{p}_j}\right)$ only depends on $\mathfrak{P}$. We put

$$\psi_j(\mathfrak{P}) = \left(\frac{N_{L/K}\mathfrak{P}}{\mathfrak{p}_j}\right) := \left(\frac{\pi}{\mathfrak{p}_j}\right)^{h^*},$$

where h^* is an integer such that $h^*h \equiv 1 \bmod \ell$.

In total there are now $\rho + t$ characters, and these can be shown[57] to depend only on the ideal class of $\mathfrak{P}$. The ideal classes with trivial characters form a subgroup C^z_{gen} in $\text{Cl}^z(L)$, the class group of the order $\mathcal{O}_z$, and C^z_{gen} is called the principal genus. The quotient group $\text{Cl}^z_{\text{gen}}(L/K) = \text{Cl}^z(L)/C^z_{\text{gen}}$ is called the genus class group, and the main problem of determining its order is solved by invoking ambiguous ideal classes:

> The number of existing genera is not greater than the number of all essentially different nonequivalent ambiguous classes.[58]

In forty pages,[59] Kummer then showed that there are exactly $\ell^{\rho+t-1}$ ambiguous ideal classes. This is quite striking, because the usual ambiguous class number formulas all contain a unit index as a factor. It is Kummer's peculiar choice of the order he is working in which eliminates this index; by working in an order with a nontrivial conductor Kummer is actually able to simplify genus theory considerably. But as the number of pages shows, he had to work hard nonetheless.

The upshot is the first inequality of genus theory in Kummer's setting: there are at most $\ell^{\rho+t-1}$ genera.[60] Kummer noted, however, that this is not good enough to prove the reciprocity law: imitating Gauss's second proof only gives a distinction between ℓ-th power residues and nonresidues, that is, a statement to the effect that $\left(\frac{\alpha}{\beta}\right)_\ell = 1$ for primary $\alpha, \beta \in \mathbf{Z}[\zeta_\ell]$ if and only if $\left(\frac{\beta}{\alpha}\right)_\ell = 1$. Kummer closed this gap by proving the second inequality in some special cases. To this end, he effectively studied norm residues modulo powers of $(1-\zeta)$ in the Kummer extensions $\mathbf{Q}(\zeta, \sqrt[\ell]{\mu})/\mathbf{Q}(\zeta)$. His first result ([Kummer 1859], p. 805) was that if $\alpha \in \mathbf{Z}[\zeta]$ is a norm from $\mathcal{O}_w$, then

$$\mathcal{L}^1(\alpha)\mathcal{L}^{\ell-1}(\mu) + \mathcal{L}^2(\alpha)\mathcal{L}^{\ell-2}(\mu) + \mathcal{L}^{\ell-1}(\alpha)\mathcal{L}^1(\mu) \equiv 0 \bmod \ell. \qquad (*)$$

This means that a certain element of $\mathbf{F}_p$ vanishes if α is a norm from $\mathcal{O}_w$. Hilbert later realized that the left hand side is just the additively written norm residue symbol

[57] See [Kummer 1859], p. 748.

[58] See [Kummer 1859], p. 751: *Die Anzahl aller wirklich vorhandenen Gattungen ist nicht größer, als die Anzahl aller wesentlich verschiedenen, nicht äquivalenten ambigen Klassen.*

[59] See [Kummer 1859], pp. 752–796.

[60] See [Kummer 1859], p. 796, statement (V). Kummer writes λ instead of our ℓ.

at the prime $\mathfrak{p}$ above p. In [Kummer 1859], p. 808, Kummer showed that condition $(*)$ is equivalent to

$$\Big(\frac{\varepsilon}{\mu}\Big) = \Big(\frac{\eta}{\alpha}\Big),$$

where ε and η are units such that $\varepsilon\alpha$ and $\eta\mu$ are primary.

The first special case was obtained on p. 811 of [Kummer 1859]: if $t = 1$, and if the ramified prime ideal has a special property, then there are exactly ℓ^{ρ} genera. On p. 817, he derived a similar result for certain Kummer extensions with exactly two ramified primes. This turned out to be sufficient for proving the reciprocity laws, but before Kummer did so, he applied these reciprocity laws to derive the general principal genus theorem:

> The number of existing genera in the theory of ideal numbers in z is equal to the ℓ-th part of all total characters.[61]

9. Hilbert and the Kummer Field

Hilbert's *Zahlbericht* [Hilbert 1897] consists of five parts: the foundations of ideal theory, Galois theory, quadratic number fields, cyclotomic fields, and Kummer extensions. The first four parts are still considered to be standard topics in any introduction to algebraic number theory. The fifth part, clearly the most difficult section of the *Zahlbericht*, did not make it into any textbook and was soon superseded by the work of Furtwängler and Takagi. Yet it is this chapter that I regard to be the *Zahlbericht*'s main claim to fame: it reflects Hilbert's struggle with digesting Kummer's work, with finding a good definition of the norm residue symbol, and with incorporating Kummer's special results on genus theory of Kummer extensions into a theory which is on a par with the genus theory of binary quadratic forms in sec. 5 of Gauss's *Disquisitiones Arithmeticae*.

The quadratic norm residue symbol $(\frac{n\,,m}{p})$ is defined to be $+1$ if m is a square or if n is congruent modulo every power of p to the norm of a suitable integer from $\mathbf{Q}(\sqrt{m}\,)$, and $(\frac{n\,,m}{p}) = -1$ otherwise. This Hilbert symbol can be expressed using generalized Legendre symbols; in [Hilbert 1899], § 9, *Satz 13*, Hilbert derived the formula

$$\Big(\frac{\nu,\mu}{\mathfrak{p}}\Big) = \Big(\frac{(-1)^{ab}\rho\sigma}{\mathfrak{p}}\Big)$$

for primes $\mathfrak{p}$ not dividing 2 in number fields k, where $\mathfrak{p}^a \parallel \mu$, $\mathfrak{p}^b \parallel \nu$, and $\nu^a\mu^{-b} = \rho\sigma^{-1}$ for integers $\rho, \sigma \in \mathcal{O}_k$ coprime to $\mathfrak{p}$.

To define the ℓ-th power norm residue symbol for odd primes ℓ, Hilbert proceeded the other way around. Let $v_{\mathfrak{p}}$ be the discrete valuation associated to the prime ideal $\mathfrak{p}$. Writing $\nu^{v_{\mathfrak{p}}(\mu)}\mu^{-v_{\mathfrak{p}}(\nu)} = \rho\sigma^{-1}$ with integers $\rho, \sigma \in \mathcal{O}_k$ such that $v_{\mathfrak{p}}(\rho) = v_{\mathfrak{p}}(\sigma) = 0$, he defined for prime ideals $\mathfrak{p}$ not dividing ℓ:

$$\Big(\frac{\nu,\mu}{\mathfrak{p}}\Big)_\ell = \Big(\frac{\rho}{\mathfrak{p}}\Big)_\ell\Big(\frac{\sigma}{\mathfrak{p}}\Big)_\ell^{-1}.$$

[61] See [Kummer 1859], p. 825: *Die Anzahl der wirklich vorhandenen Gattungen der idealen Zahlen in z ist genau gleich dem ℓ-ten Theile aller Gesamtcharaktere.*

The definition of the norm residue symbol for prime ideals $\mathfrak{p} \mid \ell$ is much more involved; in his *Zahlbericht*, Hilbert only considered the case $k = \mathbf{Q}(\zeta_\ell)$ and used Kummer's differential logarithms in the case $\ell \geq 3$: for $\mu \equiv \nu \equiv 1 \bmod \ell$, he put (compare Kummer's result $(*)$ above)

$$\Big(\frac{\nu,\mu}{\mathfrak{l}}\Big)_\ell = \zeta^S \text{ with } S = \mathcal{L}^1(\nu)\mathcal{L}^{\ell-1}(\mu) - \mathcal{L}^2(\nu)\mathcal{L}^{\ell-2}(\mu) \pm \cdots - \mathcal{L}^{\ell-1}(\nu)\mathcal{L}^1(\mu),$$

and then extended it to μ, ν coprime to ℓ by

$$\Big(\frac{\nu,\mu}{\mathfrak{l}}\Big)_\ell = \Big(\frac{\nu^{\ell-1},\mu^{\ell-1}}{\mathfrak{l}}\Big)_\ell.$$

Hilbert's genus theory then went as follows.[62] Let $k = \mathbf{Q}(\zeta_\ell)$, and assume that the class number h of k is not divisible by ℓ. Consider the Kummer extension $K = k(\sqrt[\ell]{\mu}\,)$. Let $\mathfrak{p}_1, \ldots, \mathfrak{p}_t$ denote the primes that are ramified in K/k (including infinite ramified primes, if $\ell = 2$). For each ideal $\mathfrak{a}$ in $\mathcal{O}_k$, write $N_{K/k}\mathfrak{a}^h = \alpha\mathcal{O}_k$; the map

$$\alpha \mapsto X(\alpha) = \Big\{\Big(\frac{\alpha,\mu}{\mathfrak{p}_1}\Big), \ldots, \Big(\frac{\alpha,\mu}{\mathfrak{p}_t}\Big)\Big\}$$

induces a homomorphism $\psi : \mathrm{Cl}(K) \to \mathbf{F}_\ell{}^t/X(E_k)$ by mapping an ideal class $[\mathfrak{a}]$ to $X(\alpha)^{h^*}X(E_k)$, where h^* is an integer such that $h^*h \equiv 1 \bmod \ell$. Its kernel $C_{\mathrm{gen}} = \ker\psi$ is called the principal genus, and the quotient group $\mathrm{Cl}_{\mathrm{gen}}(K) = \mathrm{Cl}(K)/C_{\mathrm{gen}}$ the genus class group of K.

In [Hilbert 1897], *Satz 150*, Hilbert generalized Gauss's work by proving that the index of norm residues modulo $\mathfrak{p}^e$ in the group of all numbers coprime to $\mathfrak{p}$ is 1 if $\mathfrak{p}$ is unramified, and equal to ℓ if $\mathfrak{p} \neq \mathfrak{l}$ is ramified or if $\mathfrak{p} = \mathfrak{l}$ and $e > \ell$. In the following *Satz 151*, Hilbert showed that his symbol defined in terms of power residue symbols actually is a norm residue symbol. Following Gauss, Hilbert first[63] derived the inequality $g \leq a$ between the number of genera and ambiguous ideal classes, then[64] proved the reciprocity law $\prod_v(\frac{a,b}{v}) = 1$ for the ℓ-th power Hilbert symbol and regular primes ℓ, and finally[65] obtained the second inequality $g \geq a$. This result is then used for proving the principal genus theorem:

> Every class of the principal genus in a regular Kummer field K is the product of the $1-S$-th symbolic power of an ideal class and of a class containing ideals of the cyclotomic field $k(\zeta)$.[66]

[62] We rewrite it slightly using the concept of quotient group which Hilbert avoids.

[63] See [Hilbert 1897], *Hilfssatz 34*.

[64] See [Hilbert 1897], § 160.

[65] See [Hilbert 1897], *Satz 164*.

[66] See [Hilbert 1897], *Satz 166: ... jede Klasse des Hauptgeschlechtes in einem regulären Kummerschen Körper K ist gleich dem Produkt aus der* $1-S$*-ten symbolischen Potenz einer Klasse und einer solchen Klasse, welche Ideale des Kreiskörpers* $k(\zeta)$ *enthält.*

This implies the familiar equality $C_{\text{gen}} = \text{Cl}(K)^{1-\sigma}$ if we work with ℓ-class groups. *Satz 167* finally shows that numbers in k that are norm residues at every prime $\mathfrak{p}$ actually are norms from K, and Hilbert concluded this section with the following remark, which blissfully passes over the difference between the Gaussian language of quadratic forms and its translation into algebraic number theory:

> Thus we have succeeded in transferring all those properties to the regular Kummer field that have been stated and proved for the quadratic number field already by Gauss.[67]

10. Philipp Furtwängler

In Philipp Furtwängler's construction of Hilbert class fields, the following Principal Genus Theorem played a major role:[68]

Theorem. Let L/K be a cyclic unramified extension, σ a generator of the Galois group $\text{Gal}(L/K)$, and let $N : \text{Cl}(L) \to \text{Cl}(K)$ be the norm map on the ideal class groups. Then $\ker N = \text{Cl}(L)^{1-\sigma}$.

To a cohomologically trained eye, this looks deceptively like the vanishing of $H^{-1}(G, \text{Cl}(L))$, but it is not. Indeed, one has $H^{-1}(G, \text{Cl}(L)) \neq 0$ in general. The point is that there is a difference between the relative norm $N_{L/K} : \text{Cl}(L) \longrightarrow \text{Cl}(K)$ and the algebraic norm

$$\nu_{L/K} = 1 + \sigma + \sigma^2 + \cdots + \sigma^{(L:K)-1} : \text{Cl}(L) \longrightarrow \text{Cl}(L).$$

The connection between them is $\nu = j \circ N$, where $j : \text{Cl}(K) \longrightarrow \text{Cl}(L)$ is the transfer of ideal classes. This means that Furtwängler's principal genus theorem cannot be translated easily into the cohomological language; ideal classes may capitulate. Furtwängler used his principal genus theorem in [Furtwängler 1916] to study the capitulation of ideals in Hilbert 2-class fields of number fields with 2-class group isomorphic to $(2, 2)$. Furtwängler also proved that, for cyclic extensions L/K of prime degree, an element $\alpha \in K^\times$ is a norm from L if and only if it is a norm residue modulo the conductor $\mathfrak{f}$ of L/K.[69]

[67] See [Hilbert 1897], § 165, last sentence: *Damit ist es dann gelungen, alle diejenigen Eigenschaften auf den regulären Kummerschen Körper zu übertragen, welche für den quadratischen Körper bereits von* Gauss *aufgestellt und bewiesen worden sind.* For connections between genus theory and reciprocity laws see also [Skolem 1928].

[68] Hilbert's version of the Principal Genus Theorem discussed above characterizes $\text{Cl}(L)^{1-\sigma}$ for cyclic extensions K/k of degree ℓ in cases where the ℓ-class number of the base field K is trivial. Furtwängler's result, which is *Satz 1* of [Furtwängler 1906], characterizes the group $\text{Cl}(L)^{1-\sigma}$ for unramified cyclic extensions L/K, in which the class number of the base field is necessarily divisible by ℓ.

[69] We will mention below the cohomological interpretation of this result in terms of the idèle class group. Because of this interpretation, Kubota credited Furtwängler with the "fully idèle-theoretic" result in the case of Kummer extensions of prime degree – see [Kubota 1989]. In the same paper, Kubota showed that the second inequality of class field theory

11. Teiji Takagi and Helmut Hasse

In this section, we assume some familiarity with class field theory in its classical formulation. Let L/K be an extension of number fields and $\mathfrak{m}$ a modulus in K. Let $P^1\{\mathfrak{m}\}$ denote the set of principal ideals (α) in K with $\alpha \equiv 1 \bmod \mathfrak{m}$, let $D_K\{\mathfrak{m}\}$ denote the group of ideals in K coprime to $\mathfrak{m}$, and let $D_L\{\mathfrak{m}\}$ denote the corresponding object for L. Then we call $H_{L/K}\{\mathfrak{m}\} = N_{L/K} D_L\{\mathfrak{m}\} \cdot P^1\{\mathfrak{m}\}$ the ideal group defined mod $\mathfrak{m}$ associated to L/K.

In the special case where $\mathfrak{m}$ is an integral ideal, such groups had been studied by Heinrich Weber. In their theory of the Hilbert class field, Hilbert and Furtwängler defined infinite primes, and Takagi combined these two notions to create his class field theory.

Takagi called L a class field of K for the ideal group $H_{L/K}\{\mathfrak{m}\}$ if $(D_K\{\mathfrak{m}\} : H_{L/K}\{\mathfrak{m}\}) = (L : K)$. In order to show that abelian extensions are class fields, this equality has to be proved, and the proof is done in two steps. The *first inequality* $(D_K\{\mathfrak{m}\} : H_{L/K}\{\mathfrak{m}\}) \leq (L : K)$ holds for any finite extension L/K and any modulus $\mathfrak{m}$ and can be proved rather easily using analytic techniques. The *second inequality* says that $(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) \geq (L : K)$ for any cyclic extension L/K of prime degree ℓ, and where $\mathfrak{f}$ is the conductor of L/K, that is, the ideal such that the relative discriminant of L/K is $\mathfrak{f}^{\ell-1}$.

In his 1932–1933 Marburg lectures on class field theory, Helmut Hasse put the proof of the second inequality into historical perspective by mentioning the role of Gauss's work:

> We now are aiming at the proof of the inverse theorem. The considerations of this section, which will be needed to achieve this, are generalizations of Gauss's famous investigations in the genus theory of quadratic forms in the D.A.[70]

The relative discriminant of a cyclic extension L/K of prime degree ℓ equals $\mathfrak{f}^{\ell-1}$, for some ideal $\mathfrak{f}$ in $\mathcal{O}_K$, called the conductor of L/K. Takagi's definition of genera in L/K is based on a connection between the class group $\mathrm{Cl}(L)$ and some ray class group Cl_K^ν defined modulo $\mathfrak{f}$: given a class $c = [\mathfrak{A}] \in \mathrm{Cl}(L)$, we can form the ray class $[N_{L/K}\mathfrak{A}]$ in the group Cl_K^ν of ideals modulo norm residues, that is, in the group $D_K\{\mathfrak{f}\}$ of ideals coprime to $\mathfrak{f}$ modulo the group $P_K^\nu\{\mathfrak{f}\}$ of principal ideals generated by norm residues modulo the conductor $\mathfrak{f}$; if $\mathfrak{A} = \lambda\mathfrak{B}$ for some $\lambda \in L^\times$, then the ray classes generated by $N_{L/k}\mathfrak{A}$ and $N_{L/k}\mathfrak{B}$ coincide since $N_{L/K}\lambda \in P_K^\nu\{\mathfrak{f}\}$.

The image of the norm map $N_{L/K} : \mathrm{Cl}(L) \longrightarrow \mathrm{Cl}_K^\nu$ is $H_{L/K}\{\mathfrak{f}\}/P_K^\nu\{\mathfrak{f}\}$, and thus involves the ideal group associated with L/K. The kernel of the norm map is called the principal genus C_{gen}; it is the group of all ideal classes $c = [\mathfrak{A}] \in \mathrm{Cl}(L)$

is essentially a corollary of two of Furtwängler's results: the product formula for the Hilbert symbol (i.e., the reciprocity law), and the principal genus theorem mentioned above.

[70] See [Hasse 1967], p. 151: *Wir gehen jetzt auf den Beweis des Umkehrsatzes aus. Die dazu erforderlichen Überlegungen des laufenden Paragraphen bilden die Verallgemeinerung der berühmten Gaussschen Untersuchungen über die Theorie der Geschlechter quadratischer Formen aus seinen Disquisitiones Arithmeticae.*

such that $N_{L/K}\mathfrak{A} = (\alpha)$ for norm residues $\alpha \in K^\times$ (i.e., α is coprime to $\mathfrak{f}$ and a norm residue at every prime ideal). This gives the exact sequence

$$1 \longrightarrow C_{\text{gen}} \longrightarrow \text{Cl}(L) \xrightarrow{N} H_{L/K}\{\mathfrak{f}\}/P_K^\nu\{\mathfrak{f}\} \longrightarrow 1. \qquad (**)$$

Thus computing the number of genera $g = (\text{Cl}(L) : C_{\text{gen}})$ will help us in getting information about the order of the ideal class group associated to L/K. We will show that $g = a$, where a denotes the number of ambiguous ideal classes in L. In fact, C_{gen} clearly contains the group $\text{Cl}(L)^{1-\sigma}$, where σ is a generator of $\text{Gal}(L/K)$. This shows that

$$a = (\text{Cl}(L) : \text{Cl}(L)^{1-\sigma}) \geq (\text{Cl}(L) : C_{\text{gen}}) = g,$$

that is, the first inequality of genus theory. Its left hand side can be evaluated explicitly; the ambiguous class number formula says that

$$a = h_K \cdot \frac{\prod e(\mathfrak{p})}{(L : K)(E : E_\nu)},$$

where $h_K = \#\text{Cl}(K)$ is the class number of K, $e(\mathfrak{p})$ is the ramification index of a prime ideal $\mathfrak{p}$ in L/K, the product is over all (ramified) primes in K including the infinite primes, E is the unit group of K, and E_ν its subgroup of units that are norm residues modulo $\mathfrak{f}$.

To prove the second inequality of genus theory: $g \geq a$, we use the exact sequence $(**)$ and get

$$(\text{Cl}(L) : C_{\text{gen}}) = (N\text{Cl}(L) : 1) = (H_{L/K}\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\}) = \frac{(D_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\})}{(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\})}.$$

The index in the denominator satisfies $(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) \leq \ell$ by the first inequality. The index in the numerator is the product of $h_K = (D_K\{\mathfrak{f}\} : P_K\{\mathfrak{f}\})$, the class number of K, by the index $(P_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\})$. This index can be computed explicitly:

$$(P_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\}) = (E_\nu : E \cap NL^\times) \cdot \frac{\prod e(\mathfrak{p})}{(E : E_\nu)}.$$

Therefore $(D_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\}) = (E_\nu : E \cap NL^\times) \cdot a\ell \geq a\ell$, and we have equalities throughout in the sequence of inequalities

$$a \geq (\text{Cl}(L) : C_{\text{gen}}) = g = \frac{(D_K\{\mathfrak{f}\} : P_K^\nu\{\mathfrak{f}\})}{(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\})} \geq a.$$

Thus $(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) = \ell$, and *cyclic extensions are class fields.* Next we get the

Principal Genus Theorem.[71] $C_{\text{gen}} = \text{Cl}(L)^{1-\sigma}$.

[71] If L/K is unramified, then $C_{\text{gen}} = \text{Cl}(L)[N]$ coincides with the kernel of the norm map $\text{Cl}(L) \longrightarrow \text{Cl}(K)$, and the principal genus theorem becomes the Theorem of § 10 above.

Finally, we also obtain the *norm theorem for units*: $(E_\nu : E \cap NL^\times) = 1$, i.e., each unit that is a norm residue modulo the conductor is the norm of some element of $L^\times$.

Takagi derived the norm theorem – to the effect that in cyclic extensions norm residues modulo the conductor are actual norms – from the principal genus theorem. In his *Klassenkörperbericht* [Hasse 1927], Hasse reproduced Takagi's proof of the second inequality with only minor modifications. But in his 1932 Marburg lectures [Hasse 1967], he established the second inequality

$$(D_K\{\mathfrak{f}\} : H_{L/K}\{\mathfrak{f}\}) \geq (L : K) \qquad (***)$$

directly by a different route. The main advantage of this arrangement of proof is that it is valid for finite cyclic extensions of arbitrary degree. Furthermore, the full norm theorem is a consequence of equality in $(***)$, and the new proof does not use the first inequality. This last fact would later allow Claude Chevalley to give an arithmetic proof of class field theory by proving the second inequality first and then deriving the first inequality without analytic means.

At some point in the computation of $(***)$, the index (norm residues modulo conductor : norms) is written as the product of (units that are norm residues : norms of units) and (ideal classes of the principal genus : $(1-\sigma)$-th powers of ideal classes). In this way, Hasse's norm theorem – which follows by comparing $(***)$ with the first inequality – contains the principal genus theorem.

Recall that ideal classes in L are mapped by the norm to ray classes modulo $\mathfrak{f}$ in K. The question arises whether more generally ray classes in L can be linked to ray classes in K. This was established by Hasse's General principal genus theorem.[72] In order to state it for a cyclic extension of prime degree L/K with Galois group generated by σ, one needs, for a given modulus $\mathfrak{m}$ in K, a σ-invariant modulus $\mathfrak{M}$ in L dividing $\mathfrak{m}$ such that for $\beta \in L^\times$ coprime to $\mathfrak{M}$ we have $N_{L/K}(\beta) \equiv 1 \bmod \mathfrak{m}$ if and only if $\beta \equiv \alpha^{1-\sigma} \bmod \mathfrak{M}$. Using this, Hasse defined the principal genus $\overline{H_1}$ mod $\mathfrak{M}$ in L to be the group of ray classes modulo $\mathfrak{M}$ whose relative norms land in the ray modulo $\mathfrak{m}$ in K. With this notation the General Principal Genus Theorem states that *the principal genus* $\overline{H_1}$ *coincides with the group of* $(1-\sigma)$*-th powers of ray classes mod* $\mathfrak{M}$ *in* L.[73]

12. Nikolai Grigorievich Čebotarev and Arnold Scholz

The generalization of genus theory from cyclic to arbitrary normal extensions was mainly the work of Nikolai Grigorievich Čebotarev and Arnold Scholz.[74]

Let L/K be a normal extension. The maximal unramified extension of L of the form LF, where F/K is abelian, is called the genus class field L_{gen} of L with respect to K; the maximal unramified extension which is central over K is called the central class field and is denoted by L_{cen}.

According to Scholz, these definitions are contained in [Čebotarev 1929]; the characterization of the genus and central class fields in terms of class groups is due

[72] See [Hasse 1927], pp. 304–310.

[73] This was further generalized by Herbrand – see [Herbrand 1932].

[74] See [Čebotarev 1929] and [Scholz 1940].

to Scholz, who used the following theorem to generalize Hasse's norm theorem – everywhere local norms are global norms – to all extensions whose Galois groups have trivial Schur multiplier:[75]

Theorem. Let L/K be a normal extension of number fields, let H_0 denote the elements of $K^\times$ that are norm residues, and put $N_0 = N_{L/K}L^\times$. Next, let H and N denote the group of ideals in L whose norms land in the groups of principal ideals generated by elements of H_0 and N_0 respectively.[76] Then the class field associated to the ideal group H is the genus class field L_{gen}, and the class field associated to N is the central class field L_{cen}. In particular, Scholz's number knot H_0/N_0 is isomorphic to the Galois group of $L_{\text{cen}}/L_{\text{gen}}$.

Being an unramified abelian extension of L, L_{gen} corresponds to some quotient $\text{Cl}(K)/C_{\text{gen}}$ of the class group of K. This group C_{gen} is called the *principal genus*. For cyclic extensions L/K, it satisfies $C_{\text{gen}} = \text{Cl}(L)^{1-\sigma}$, for σ a generator of $\text{Gal}(L/K)$.

The following theorem – called the *classical principal genus theorem* in [Fröhlich 1983], pp. 18–19 – connects the modern definition of the principal genus with the classical one by Takagi:

Theorem. Let L/K be a cyclic extension, and σ a generator of $\text{Gal}(L/K)$. Then $[\mathfrak{a}] \in C_{\text{gen}}$ if and only if $N_{L/K}\mathfrak{a} = (\alpha)$, where $\alpha \in K^\times$ is a norm residue at all ramified primes in L/K.

This form of genus theory was used by various number theorists; among the many contributions, let us refer to [Hasse 1951], [Leopoldt 1953], [Gold 1975], [Stark 1976] (this generalization of genus theory lacks an analogue of Gauss's principal genus theorem), [Gurak 1977], and [Razar 1977].

13. Emmy Noether

In 1932, Emmy Noether was invited to deliver a lecture at the International Congress of Mathematicians in Zürich. She devoted this lecture to two new illustrations of the usefulness of the then flourishing theory of algebras:[77]

> I would like to report today on this relevance of the noncommutative for the commutative; more precisely, I would like to trace this phenomenon in detail for two classical questions which go back to Gauss: the Principal Genus Theorem and the closely related Norm Theorem. These questions have changed again and again in the course of time: with Gauss they appear as the conclusion of his theory of quadratic forms; then they play an essential part in characterizing relatively cyclic and abelian number fields, and they can finally be stated as theorems on automorphisms and on

[75] Cf. Jehne's more modern presentation and generalization in [Jehne 1979].

[76] Observe that H is the principal genus in the sense of Takagi.

[77] The footnotes in [Noether 1932] give a vivid impression of the activity of the theory of algebras at the time. In [Noether 1932], § 4, the Norm Theorem is related to the Brauer-Hasse-Noether Theorem. Cf. [Fenster, Schwermer 2005], and [Hasse & Noether 2006].

the splitting of algebras. It is this latter formulation which yields a transfer of these theorems to arbitrary relatively abelian number fields.[78]

The noncommutative algebras are thus presented by Emmy Noether as the stepping stone to generalize arithmetic theorems from cyclic to abelian extensions. To generalize the Principal Genus Theorem, she therefore starts with crossed products.[79]

Let K be a field and L/K a separable extension of degree n with Galois group G. The crossed product of L and G is an algebra A together with injections $L \hookrightarrow A$ and $G \hookrightarrow A$ such that all automorphisms of L become inner automorphisms of A. As an L-vector space, A is generated by basis elements $u_{\sigma_1}, \ldots, u_{\sigma_n}$ corresponding to the group elements σ_i : $A = u_{\sigma_1}L \oplus \cdots \oplus u_{\sigma_n}L$. It is required that $z^\sigma = u_\sigma^{-1} z u_\sigma$ hold for every $z \in L$. This defines a *factor system* $(a_{\sigma,\tau})$ in $L^\times$ by the formulae $u_\sigma u_\tau = u_{\sigma\tau} a_{\sigma,\tau}$, and associativity of multiplication gives the cocycle relation $a_{\sigma\tau,\rho} a_{\sigma,\tau}^\rho = a_{\sigma,\tau\rho} a_{\tau,\rho}$. The product

$$\sum u_\sigma b_\sigma \cdot \sum u_\tau c_\tau = \sum u_\sigma u_\tau b_\sigma^\tau c_\tau$$

makes A into a simple normal algebra over K which is denoted by $A = (a_{\sigma,\tau}, L, G)$. Different factor systems $a_{\sigma,\tau}$ and $\overline{a}_{\sigma,\tau}$ generate isomorphic algebras if there are $c_\sigma \in L^\times$ such that $\overline{a}_{\sigma,\tau} = a_{\sigma,\tau} c_\sigma^\tau c_\tau / c_{\sigma\tau}$. The cosets $u_\sigma L^\times$ define a group extension $G^\times$ of G by $L^\times$.

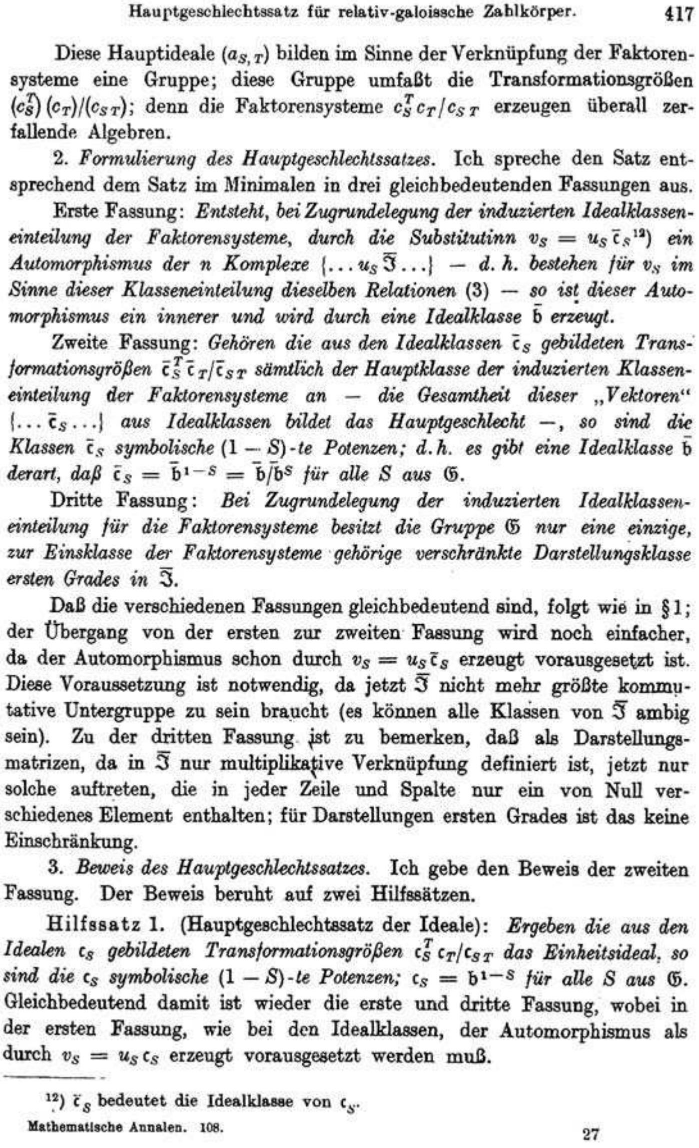
Emmy Noether published a detailed account of her Principal Genus Theorem in [Noether 1933]. The first result there, which she called the *Hauptgeschlechtssatz im Minimalen*, i.e., Minimal Principal Genus Theorem, was formulated, for a finite Galois extension L/K with Galois group G, in three equivalent variants:[80]

1. Every group automorphism of $G^\times$ whose restriction to $L^\times$ is the identity is inner, and is generated by an element of $L^\times$.
2. If $c_\sigma^\tau c_\tau / c_{\sigma\tau} = 1$ for all σ, $\tau \in G$, then there exists $b \in L^\times$ such that $c_\sigma = b^{1-\sigma}$ for all $\sigma \in G$.

[78] See [Noether 1932], § 1: *Über diese Bedeutung des Nichtkommutativen für das Kommutative möchte ich heute berichten: und zwar will ich das im einzelnen verfolgen an zwei klassischen, auf Gauss zurückgehenden Fragestellungen, dem Hauptgeschlechtssatz und dem eng damit verbundenen Normensatz. Diese Fragestellungen haben sich im Laufe der Zeit immer wieder gewandelt: bei Gauss treten sie auf als Abschluss seiner Theorie der quadratischen Formen; dann spielen sie eine wesentliche Rolle bei der Charakterisierung der relativ zyklischen und abelschen Zahlkörper durch die Klassenkörpertheorie, und schliesslich lassen sie sich aussprechen als Sätze über Automorphismen und über das Zerfallen von Algebren, und diese letztere Formulierung gibt dann zugleich eine Übertragung der Sätze auf beliebige relativ galoissche Zahlkörper.*

[79] Cf. [Noether 1932], § 3; except for the letters used to denote Galois automorphisms, our notations are the same as Noether's. More technical details are given in the preprint version http://www.math.uiuc.edu/Algebraic-Number-Theory/0354/ of this chapter, and will be published elsewhere.

[80] See [Noether 1933], p. 414-415. This article was already announced in her Zürich talk, and was submitted on October 27, 1932.



Hauptgeschlechtssatz für relativ-galoissche Zahlkörper. 417

Diese Hauptideale $(a_{S,T})$ bilden im Sinne der Verknüpfung der Faktorensysteme eine Gruppe; diese Gruppe umfaßt die Transformationsgrößen $(c_S^T)(c_T)/(c_{ST})$; denn die Faktorensysteme $c_S^T c_T / c_{ST}$ erzeugen überall zerfallende Algebren.

2. *Formulierung des Hauptgeschlechtssatzes.* Ich spreche den Satz entsprechend dem Satz im Minimalen in drei gleichbedeutenden Fassungen aus.

Erste Fassung: *Entsteht, bei Zugrundelegung der induzierten Idealklasseneinteilung der Faktorensysteme, durch die Substitutinn* $v_S = u_S \bar{\mathfrak{c}}_S$[12]) *ein Automorphismus der n Komplexe* $\{\ldots u_S \overline{\mathfrak{J}} \ldots\}$ — *d. h. bestehen für* v_S *im Sinne dieser Klasseneinteilung dieselben Relationen* (3) — *so ist dieser Automorphismus ein innerer und wird durch eine Idealklasse* $\bar{\mathfrak{b}}$ *erzeugt.*

Zweite Fassung: *Gehören die aus den Idealklassen* $\bar{\mathfrak{c}}_S$ *gebildeten Transformationsgrößen* $\bar{\mathfrak{c}}_S^T \bar{\mathfrak{c}}_T / \bar{\mathfrak{c}}_{ST}$ *sämtlich der Hauptklasse der induzierten Klasseneinteilung der Faktorensysteme an — die Gesamtheit dieser „Vektoren"* $\{\ldots \bar{\mathfrak{c}}_S \ldots\}$ *aus Idealklassen bildet das Hauptgeschlecht —, so sind die Klassen* $\bar{\mathfrak{c}}_S$ *symbolische* $(1-S)$*-te Potenzen; d. h. es gibt eine Idealklasse* $\bar{\mathfrak{b}}$ *derart, daß* $\bar{\mathfrak{c}}_S = \bar{\mathfrak{b}}^{1-S} = \bar{\mathfrak{b}}/\bar{\mathfrak{b}}^S$ *für alle S aus* $\mathfrak{G}$.

Dritte Fassung: *Bei Zugrundelegung der induzierten Idealklasseneinteilung für die Faktorensysteme besitzt die Gruppe* $\mathfrak{G}$ *nur eine einzige, zur Einsklasse der Faktorensysteme gehörige verschränkte Darstellungsklasse ersten Grades in* $\overline{\mathfrak{J}}$.

Daß die verschiedenen Fassungen gleichbedeutend sind, folgt wie in § 1; der Übergang von der ersten zur zweiten Fassung wird noch einfacher, da der Automorphismus schon durch $v_S = u_S \bar{\mathfrak{c}}_S$ erzeugt vorausgesetzt ist. Diese Voraussetzung ist notwendig, da jetzt $\overline{\mathfrak{J}}$ nicht mehr größte kommutative Untergruppe zu sein braucht (es können alle Klassen von $\overline{\mathfrak{J}}$ ambig sein). Zu der dritten Fassung ist zu bemerken, daß als Darstellungsmatrizen, da in $\overline{\mathfrak{J}}$ nur multiplikative Verknüpfung definiert ist, jetzt nur solche auftreten, die in jeder Zeile und Spalte nur ein von Null verschiedenes Element enthalten; für Darstellungen ersten Grades ist das keine Einschränkung.

3. *Beweis des Hauptgeschlechtssatzes.* Ich gebe den Beweis der zweiten Fassung. Der Beweis beruht auf zwei Hilfssätzen.

Hilfssatz 1. (Hauptgeschlechtssatz der Ideale): *Ergeben die aus den Idealen* $\mathfrak{c}_S$ *gebildeten Transformationsgrößen* $\mathfrak{c}_S^T \mathfrak{c}_T / \mathfrak{c}_{ST}$ *das Einheitsideal, so sind die* $\mathfrak{c}_S$ *symbolische* $(1-S)$*-te Potenzen;* $\mathfrak{c}_S = \mathfrak{b}^{1-S}$ *für alle S aus* $\mathfrak{G}$. Gleichbedeutend damit ist wieder die erste und dritte Fassung, wobei in der ersten Fassung, wie bei den Idealklassen, der Automorphismus als durch $v_S = u_S \mathfrak{c}_S$ erzeugt vorausgesetzt werden muß.

[12]) $\bar{\mathfrak{c}}_S$ bedeutet die Idealklasse von $\mathfrak{c}_S$.

Mathematische Annalen. 108. 27

Fig. VIII.3B. The Principal Genus Theorem According to Emmy Noether [Noether 1933], p. 417.

3. The group G has a unique crossed representation class of the first degree associated to the trivial factor system.

Here (in 3.) a representation $u_\sigma \mapsto C_\sigma$ is called a crossed representation for the factor system $a_{\sigma,\tau}$ if $C_\sigma^\tau C_\tau = C_{\sigma\tau} a_{\sigma,\tau}$. Two crossed representations $u_\sigma \mapsto C_\sigma$ and $u_\sigma \mapsto D_\sigma$ for $a_{\sigma,\tau}$ belong to the same class if $C_\sigma = B^{-\sigma} D_\sigma B$.

In the slightly more modern language of Galois cohomology groups, version 2. of the minimal principal genus theorem claims that $H^1(G, L^\times) = 0$. This is Speiser's generalization of Hilbert's *Satz 90* of [Hilbert 1897], from cyclic to arbitrary finite Galois extensions.

In § 2 of [Noether 1933], Noether considered what we may call an *ideal factor system* of a Galois extension L/K with Galois group $\mathrm{Gal}(L/K) = \{\sigma, \tau, \dots\}$, i.e., a system of n^2 ideals $\mathfrak{a}_{\sigma,\tau}$ of L satisfying the cocycle relations

$$\mathfrak{a}_{\sigma,\tau\rho}\mathfrak{a}_{\tau,\rho} = \mathfrak{a}_{\sigma\tau,\rho}\mathfrak{a}_{\sigma,\tau}^{\rho}.$$

Given n ideals $\mathfrak{c}_\sigma$, one obtains the so-called *transformation system* $\mathfrak{a}_{\sigma,\tau} = \frac{\mathfrak{c}_\sigma^\tau \mathfrak{c}_\tau}{\mathfrak{c}_{\sigma\tau}}$.

Ideal factor systems form a group C, and the transformation systems form a subgroup B of C. In analogy to the group of norm residues modulo the conductor, Noether defines the principal class of ideal factor systems as consisting of systems $\mathfrak{a}_{\sigma,\tau}$ with the following property: there exists a factor system $a_{\sigma,\tau}$ in $L^\times$ such that (1) $\mathfrak{a}_{\sigma,\tau} = (a_{\sigma,\tau})$, and (2) $a_{\sigma,\tau}$ determines an algebra $\mathfrak{A} = (L, a)$ which splits at every ramified place $\mathfrak{p}$ of L/K. With this notation, we have version 2. of

Emmy Noether's Principal Genus Theorem.[81] If the transformation system $\mathfrak{c}_\sigma^\tau \mathfrak{c}_\tau \mathfrak{c}_{\sigma\tau}^{-1}$ is in the principal class, then there is an ideal class $[\mathfrak{b}]$ such that $[\mathfrak{c}_\sigma] = [\mathfrak{b}]^{1-\sigma}$ for all $\sigma \in \mathrm{Gal}(L/K)$.

Noether's proof of this result follows easily from two lemmas, of which the second[82] is a variant of the Brauer-Hasse-Noether theorem on the local characterization of the splitting of semi-simple algebras, whereas the first one is Noether's Principal Genus Theorem for Ideals.[83] In terms of Galois cohomology of the normal extension of number fields L/K with Galois group G, writing D_L for the group of fractional ideals in L, the latter theorem amounts to the statement that $H^1(G, D_L) = 0$.

Noether's formulation of the principal genus theorem was apparently not very influential, but there have been a few articles picking up her ideas; we mention [Terada 1952], [Terada 1953], [Kunihishi, Takahashi 1953], as well as [Tannaka 1958]. Let us briefly sketch here two modern reformulations of Noether's Theorems. Peter Roquette has proposed[84] the following translation of Noether's results into the language of Galois cohomology of idèles.

[81] For all three versions 1.–3. and their equivalence, see [Noether 1933], p. 417.

[82] See [Noether 1933], *Hilfssatz 2*, p. 418.

[83] See [Noether 1933], *Hilfssatz 1*, p. 417, for the statement in terms of transformation systems. Noether gives a direct four line proof of this *Hilfssatz 1* due to Emil Artin.

[84] In an email to the author dated June 14, 2001.

We fix a normal extension L/K of number fields with Galois group $G = \mathrm{Gal}(L/K)$. All our cohomology groups will be formed with G, so we write simply $H^q(M)$ for $H^q(G, M)$. Let S be the set of primes of L ramified in L/K. Let $H^2_S(L^\times)$ denote the subgroup of $H^2(L^\times)$ whose elements split at all primes in S; in other words, $H^2_S(L^\times)$ is the kernel of the natural map $H^2(L^\times) \longrightarrow H^2\big(\prod_{w\in S} L_w^\times\big)$ induced by $L^\times \longrightarrow \prod_{w\in S} L_w^\times$.

The exact sequence $1 \longrightarrow E_L \longrightarrow L^\times \longrightarrow P_L \longrightarrow 1$, where P_L denotes the group of principal ideals and E_L the units in L, yields a map $H^2_S(L^\times) \longrightarrow H^2(P_L)$ whose image we denote simply by H_S.

The sequence $1 \longrightarrow P_L \longrightarrow D_L \longrightarrow \mathrm{Cl}_L \longrightarrow 1$ defining the ideal class group of L gives us the following exact sequence whose first term is 0 in view of Noether's Principal Genus Theorem for Ideals:

$$0 = H^1(D_L) \longrightarrow H^1(\mathrm{Cl}_L) \longrightarrow H^2(P_L) \longrightarrow H^2(D_L).$$

This identifies $H^1(\mathrm{Cl}_L)$ with a subgroup of $H^2(P_L)$, and we can formulate:

Noether's Principal Genus Theorem. $H_S \cap H^1(\mathrm{Cl}) = 0$.

To see the connection with Noether's original formulation, observe that a transformation system $\mathfrak{c}_\sigma$ of ideals is a cocycle of the ideal class group and therefore defines an element $c_\sigma \in H^1(\mathrm{Cl}_L)$ if $[\mathfrak{c}_\sigma]^\tau[\mathfrak{c}_\tau] = [\mathfrak{c}_{\sigma\tau}]$ (this is the first condition of the system $\mathfrak{c}_\sigma$ being in the principal class). The requirement that $c_\sigma = [\mathfrak{c}_\sigma] = [\mathfrak{b}]^{1-\sigma}$ says that the cocycle is a coboundary. Thus $H^1(\mathrm{Cl}_L) = 1$. However, this is only true if the second condition is also satisfied; this condition requires that $\mathfrak{c}_\sigma^\tau \mathfrak{c}_\tau \mathfrak{c}_{\sigma\tau}^{-1} = (a_{\sigma,\tau})$ for a factor system $a_{\sigma,\tau} \in H^2(L^\times)$ whose associated algebra splits at every place $\mathfrak{p}$ that is ramified in L/K. In our language, the element $c_\sigma \in H^1(\mathrm{Cl}_L)$ defines a factor set of principal ideals in $H^2(P_L)$ under the connecting homomorphism; if this factor system actually comes from an element $a_{\sigma,\tau} \in H^2(L^\times)$ whose associated algebra splits at the ramified primes – i.e., if $a_{\sigma,\tau} \in H^2_S(L^\times)$ – then Noether's principal genus theorem claims that the element c_σ is trivial.

Albrecht Fröhlich's article [Fröhlich 1983] contains a cohomological interpretation of Noether's principal genus theorem that differs slightly from Roquette's. Let $J_L' \simeq \prod_{w\in S} L_w^\times$ denote idèles having entries 1 outside of S. The projection from all idèles $J_L \longrightarrow J_L'$ and the inclusion $L^\times \longrightarrow J_L$ give rise to maps $\pi_1 : H^2(J_L) \longrightarrow H^2(J_L')$ and $\iota : H^2(L^\times) \longrightarrow H^2(J_L)$ such that $\ker \pi_1 \circ \iota = H^2_S(L^\times)$. Fröhlich defines maps $\psi : H^2(L^\times) \longrightarrow H^2(P_L)$ and $\phi : H^2(P_L) \longrightarrow H^2(D_L)$ such that $\psi(\ker \pi_1 \circ \iota) = H_S$. The injectivity of $H^2_S(L^\times) \longrightarrow H^2(D_L)$ then amounts to $\ker \pi_1 \circ \iota \cap \ker \phi \circ \psi = 0$, and Fröhlich's version of Noether's theorem reads:

Theorem. The following composition of maps is injective:

$$H^1(\mathrm{Cl}_L) \longrightarrow H^2(P_L) \longrightarrow H^2(P_L)/\psi(\ker \pi_1 \circ \iota).$$

In other words, the induced map $H^1(\mathrm{Cl}_L) \longrightarrow H^2(P_L)/H_S$ is injective. This is, of course, equivalent to the statement that $H_S \cap H^1(\mathrm{Cl}_L) = 0$ in $H^2(P_L)$.

We conclude our survey of the development of the principal genus theorem with Emmy Noether's peculiar acknowledgement of Gauss's *Disquisitiones Arithmeticae*:

> Incidentally, in preparation for my Zürich lecture I have read Gauss, for once. It has been said that a halfway educated mathematician knows Gauss's principal genus theorem, but only exceptional people know the principal genus theorem of class field theory. I don't know if that's true – my knowledge went the other way around – but in any case I learned a lot from Gauss about how to view things; above all, that it is good to place the verification of the fact that the classes determined by factor systems are ray classes, at the end; for the transition from my version to Gauss's can be done independently of this, and directly, and it is not before the specialization to class field theory that the conductor is needed. What I am doing is the generalization of the definition of genera via characters.[85]

Acknowledgements

I would like to thank Peter Roquette for explaining the content of Noether's paper to me.

References

Antropov, Alexander A. 1989. On the history of the concept of genus of binary quadratic form (in Russian). *Istoriya i Metodologiya Estestvennykh Nauk* 36, 17–27.

———. 1989. Partitioning of forms by genus and the reciprocity law in L. Euler's work (in Russian). *Voprosy Istorii Estestvoznaniya i Tekhniki* 1, 56–57.

———. 1995. On Euler's partition of forms into genera. *Historia Mathematica* 22, 188–193.

Arndt, Friedrich. 1859. Ueber die Anzahl der Genera der quadratischen Formen. *Journal für die reine und angewandte Mathematik* 56, 72–78.

Belabas, Karim. 2005. Paramétrisation de structures algébriques et densité de discriminants (d'après Bhargava). In *Séminaire Bourbaki. Vol. 2003–2004*, exposé 935, pp. 267-299. Astérisque 299. Paris: Société mathématique de France.

Bhargava, Manjul. 2004. Higher Composition Laws I, II. *Annals of Mathematics* 159, 217–250, 865–886.

Buell, Duncan A. 1989. *Binary Quadratic Forms*. Berlin, Heideberg, New York : Springer.

[85] See [Hasse & Nother 2006]: *Im übrigen habe ich anläßlich der Ausarbeitung meines Züricher Vortrags einmal Gauss gelesen. Es wurde behauptet, daß ein halbwegs gebildeter Mathematiker den Gaussschen Hauptgeschlechtssatz kennt, aber nur Ausnahmemenschen den der Klassenkörpertheorie. Ob das stimmt, weiß ich nicht – meine Kenntnisse gingen in umgekehrter Reihenfolge – aber jedenfalls habe ich in bezug auf Auffassung allerhand von Gauss gelernt; vor allem daß es gut ist den Nachweis, daß die durch Faktorensysteme bestimmte Klasseneinteilung eine Strahlkl.-Einteilung ist, an den Schluß zu stellen; der Übergang meiner Fassung zu der Gaussschen geht nämlich unabhängig davon direkt, erst die Spezialisierung auf die Klassenkörpertheorie braucht den Führer. Was ich mache, ist die Verallgemeinerung der Definition der Geschlechter durch Charaktere.* Noether's letter to Hasse of November 25, 1932 (see [Hasse & Nother 2006]) shows that she had plans to further work out her theory. She died, however, in 1935 without ever returning to the topic.

Čebotarev, Nikolai Grigorievich. 1929. Zur Gruppentheorie des Klassenkörpers. *Journal für die reine und angewandte Mathematik* 161, 179–193.

Deuring, Max. 1935. *Algebren.* Ergebnisse der Mathematik und ihrer Grenzgebiete 41. Berlin, Heidelberg : Springer.

Dirichlet, Johann Peter Gustav Lejeune-. 1863. *Vorlesungen über Zahlentheorie*, ed. R. Dedekind. 1st ed. 2nd ed., 1871. 3rd ed., 1879. 4th ed., 1894. Braunschweig: Vieweg.

———. 1839. Recherches sur diverses applications de l'analyse infinitésimale à la théorie des nombres. *Journal für die reine und angewandte Mathematik* 19, 324–369. Repr. in *Werke*, ed. L. Kronecker, vol. 1, pp. 411–496. Berlin: G. Reimer, 1889.

Edwards, Harold M. 1977. *Fermat's Last Theorem.* Berlin, Heidelberg, New York: Springer.

Eisenstein, Gotthold. 1844. Théorèmes sur les formes cubiques et solution d'une équation du quatrième degré indeterminée. *Journal für die reine und angewandte Mathematik* 27, 75–79. Repr. in *Mathematische Werke* vol. 1, pp. 1–5. New York: Chelsea, 1975.

Euler, Leonhard. 1764. De resolutione formularum quadraticarum indeterminatarum per numeros integros. *Novi Commentarii academiae scientiarum imperialis Petropolitanae* 9 (1762–1763), 3–33. Repr. in [Euler 1915], pp. 576–602.

———. 1783. Novae demonstrationes circa divisores numerorum formae xx+nyy, (E 610), Nov. 20, 1775. *Nova Acta Academiae Scientiarum Imperialis Petropolitanae* 1, 47–74. Repr. in [Euler 1941], pp. 197–220.

———. 1785. De insigni promotione scientiae numerorum, (E 598), Oct. 26, 1775. In *Opuscula analytica* 2, pp. 275–314. St. Petersburg: Typis Academiae Imperialis Scientiarum. Repr. in [Euler 1941], pp. 163–196.

———. 1915. *Opera Omnia*, ed. R. Fueter, vol. I_2. Leipzig, Berlin: Teubner.

———. 1941. *Opera Omnia*, ed. R. Fueter, vol. I_4. Leipzig, Berlin: Teubner.

Euler & Goldbach. 1965. *Briefwechsel 1729–1764, von Leonhard Euler und Christian Goldbach*, ed. A.P. Yuškevič, E. Winter. Berlin: Akademie-Verlag.

Fenster, Della D., Schwermer, Joachim. 2005. A Delicate Collaboration: Adrian Albert and Helmut Hasse and the Principal Theorem in Division Algebras in the early 1930's. *Archive for History of Exact Sciences* 59, 349–379.

Frei, Günter. 1979. On the development of the genus of quadratic forms. *Annales des Sciences Mathématiques du Québec* 3, 5–62.

Fröhlich, Albrecht. 1981. Algebraic Number Theory. In *Emmy Noether. A Tribute to her Life and Work*, ed. J.W. Brewer, M.K. Smith, pp. 157–163. New York, Basel: Marcel Dekker.

Fueter, Rudolf. 1941. Vorwort des Herausgebers. In [Euler 1941], pp. vii–xxx.

Furtwängler, Philipp. 1906. Eine charakteristische Eigenschaft des Klassenkörpers, Erste Mitteilung. *Göttinger Nachrichten*, 417–434.

———. 1916. Über das Verhalten der Ideale des Grundkörpers im Klassenkörper, *Monatshefte für Mathematik* 27, 1–15.

Gold, Robert. 1975. Genera in Abelian extensions. *Proceedings of the American Mathematical Society* 47, 25–28.

Gurak, Stanley J. 1977. Ideal-theoretic characterization of the relative genus field, *Journal für die reine und angewandte Mathematik* 296, 119–124.

HASSE, Helmut. 1927. Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper. Teil Ia, Beweise zu I. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 36, 233–311. Repr. (as book) Würzburg, Wien: Physica-Verlag, 3rd ed., 1970.

———. 1951. Zur Geschlechtertheorie in quadratischen Zahlkörpern. *Journal of the Mathematical Society of Japan* 3, 45–51.

———. 1967. *Vorlesungen über Klassenkörpertheorie*. Würzburg, Wien: Physica-Verlag.

HASSE & NOETHER. 2006. *Helmut Hasse – Emmy Noether. Die Korrespondenz 1925 – 1935*, ed. F. Lemmermeyer, P. Roquette. Göttingen: Universitätsverlag.

HECKE, Erich. 1923. *Vorlesungen über die Theorie der algebraischen Zahlen*. Leipzig: Teubner. Repr. New York: Chelsea, 1948, 1970. Engl. tr. G.U. Brauer, J.R. Goldman, R. Kotzen. Heidelberg, New York: Springer-Verlag, 1981.

HERBRAND, Jacques. 1932. Sur les théorèmes du genre principal et des idéaux principaux. *Abhandlungen aus dem Mathematischen Seminar der Universität Hamburg* 3, 84–92.

HILBERT, David. 1894. Über den Dirichletschen biquadratischen Zahlkörper. *Mathematische Annalen* 45, 309–340. Repr. in [Hilbert 1932], pp. 24–52.

———. 1897. Die Theorie der algebraischen Zahlkörper. *Jahresbericht der Deutschen Mathematiker-Vereinigung* 4 (“1894–1895”), 177–546 + Vorwort 1–xviii. Repr. in [Hilbert 1932], pp. 63–363. Eng. tr. by I. Adamson, *The Theory of Algebraic Number Fields*, introd. F. Lemmermeyer, N. Schappacher. New York: Springer, 1998.

———. 1889. Über die Theorie der relativ-Abelschen Zahlkörper. *Nachrichten der Königlichen Gesellschaft der Wissenschaften zu Göttingen*, 370–399. Repr. modified *Acta Mathematica* 26 (1902), 99–132. Repr. in [Hilbert 1932], pp. 483–509.

———. 1899. Über die Theorie des relativquadratischen Zahlkörpers. *Mathematische Annalen* 51, 1–127. Repr. in [Hilbert 1932], pp. 370–482.

———. 1932. *Gesammelte Abhandlungen*, vol. 1. Berlin: Springer. 2nd ed., 1970.

HOFFMAN, J. William, MORALES, Jorge. 2000. Arithmetic of binary cubic forms. *Enseignement Mathématique* 2nd ser. 46, 61–94.

JEHNE, Wolfram. 1979. On knots in algebraic number theory. *Journal für die reine und angewandte Mathematik* 311–312, 215–254.

JONES, Burton W. 1950. *The Arithmetic Theory of Quadratic Forms*. New York : John Wiley & Sons.

KRONECKER, Leopold. 1864. Über den Gebrauch der Dirichletschen Methoden in der Theorie der quadratischen Formen. *Monatsberichte der Königlich Preussischen Akademie der Wissenschaften zu Berlin*, 285–303. Repr. in *Werke*, vol. IV, ed. K. Hensel, pp. 227–244. Leipzig: Teubner, 1929.

KUBOTA, Tomio. 1989. Remarks on the theorems of Takagi and Furtwängler. In *Algebraic Number Theory, in honor of K. Iwasawa. Proceedings of the Workshop “Iwasawa Theory and Special Values of L-Functions,” Berkeley, CA, 1987*, ed. J. Coates, R. Greenberg, B. Mazur, I. Satake, pp. 267–270. Advanced Studies in Pure Mathematics 17. Boston, etc.: Academic Press and Tokyo : Kinokuniya.

KUMMER, Ernst Eduard. 1850. Allgemeine Reziprozitätsgesetze für beliebig hohe Potenzreste. *Monatsberichte der Königlich Preußischen Akademie der Wissenschaften zu Berlin*, 154–165. Repr. in [Kummer 1975], pp. 345–357.

———. 1859. Über die allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. *Mathematische Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin*, 19–159. Repr. in [Kummer 1975], pp. 699–839.

———. 1861. Zwei neue Beweise der allgemeinen Reziprozitätsgesetze unter den Resten und Nichtresten der Potenzen, deren Grad eine Primzahl ist. *Mathematische Abhandlungen der Königlichen Akademie der Wissenschaften zu Berlin*, 81–122. Repr. *Journal für die reine und angewandte Mathematik* 100 (1887), 10–50. Repr. in [Kummer 1975], pp. 842–882.

———. 1975. *Collected Papers*, ed. A. Weil. vol. 1, *Contributions to Number Theory*. Berlin, Heidelberg etc.: Springer.

Kuniyoshi, Hideo, Takahashi, Shuichi. 1953. On the principal genus theorem. *Tohoku Mathematical Journal* 5, 128–131.

Lagrange, Joseph-Louis. 1773. Recherches d'arithmétique. *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-lettres de Berlin, année 1773* (1775), 265–312. Repr. in *Œuvres*, ed. J.-A Serret, vol. III, pp. 695–758. Paris: Gauthier-Villars, 1869; repr. Hildesheim, New York: Georg Olms, 1973.

———. 1774. *Additions aux Eléments d'Algèbre d'Euler*. Lyon: Bruyset, Paris: Desaint. Repr. in *Œuvres* ed. J.A. Serret, vol. VII, pp. 5–182. Paris: Gauthier-Villars, 1877; repr. Hildesheim, New York: Olms 1973.

———. 1775. Suite de recherches d'arithmétique. *Nouveaux Mémoires de l'Académie royale des Sciences et Belles-lettres de Berlin, année 1775* (1777), 323–356. Repr. in *Œuvres*, ed. J.-A Serret, vol. III, pp. 759–795. Paris: Gauthier-Villars, 1869; Hildesheim/New York: Georg Olms, 1973.

Lam, Tsit-Yuen. 1973. *The Algebraic Theory of Quadratic Forms*. Reading: W.A. Benjamin. 2nd ed., 1980.

Legendre, Adrien-Marie. 1830. *Théorie des nombres*. 3rd ed. 2 vols. Paris: Didot.

Lemmermeyer, Franz. 2000. *Reciprocity Laws. From Euler to Eisenstein*. Berlin, Heidelberg, New York: Springer-Verlag.

———. 2007. *Reciprocity Laws. From Kummer to Hilbert*. In preparation.

Leopoldt, Heinrich Wolfgang. 1953. Zur Geschlechtertheorie in abelschen Zahlkörpern. *Mathematische Nachrichten* 9, 351–362.

Manin, Yuri. 1972. *Kubicheskie formy: algebra, geometriya, aritmetika. (Cubic Forms: algebra, geometry, arithmetic.)* Moscow: Nauka. Engl. tr. M. Hazewinkel. Amsterdam: North-Holland, 1986.

Mansion, Paul. 1896. Rapport. *Bulletin de l'Academie Royale des Sciences, des Lettres et des Beaux-Arts de Belgique* 3rd ser. 30, 189–193.

Noether, Emmy. 1932. Hyperkomplexe Systeme in ihren Beziehungen zur kommutativen Algebra und zur Zahlentheorie. In *Verhandlungen des Internationalen Mathematiker-Kongresses Zürich 1932*, ed. W. Saxer, vol. I, pp. 189–194. Zürich: Orell-Füssli 1932. Repr. in *Gesammelte Abhandlungen – Collected Papers*, ed. N. Jacobson, pp. 636–641. Berlin, etc.: Springer, 1983.

———. 1933. Der Hauptgeschlechtssatz für relativ-galoissche Zahlkörper. *Mathematische Annalen* 108, 411–419. Repr. in *Gesammelte Abhandlungen – Collected Papers*, ed. N. Jacobson, pp. 670–678. Berlin, etc.: Springer, 1983.

Ono, Takashi. 1985. A generalization of Gauss's theorem on the genera of quadratic forms. *Proceedings Japan Academy. Series A, Mathematical Sciences* 61, 109–111.

Razar, Michael J. 1977. Central and genus class field and the Hasse norm theorem. *Compositio Mathematica* 35, 281–298.

Reichardt Hans. 1963. Über Dirichlet's zahlentheoretische Arbeiten. In *Bericht von der Dirichlet-Tagung*, ed. H. Reichardt, pp. 13–21. Berlin: Akademie-Verlag.

Scholz, Arnold. 1940. Totale Normenreste, die keine Normen sind, als Erzeuger nicht-abelscher Körpererweiterungen. 2. *Journal für die reine und angewandte Mathematik* 182, 217–234.

Shanks, Daniel. 1971a. Class number, a theory of factorization, and genera. In *1969 Number Theory Institute*, ed. D.J. Lewis, pp. 415–440. Proceedings of Symposia in Pure Mathematics 20. Providence: American Mathematical Society.

———. 1971b. Gauss's ternary form reduction and the 2-Sylow subgroup. *Mathematics of Computation* 25, 837–853; Corrigendum 32 (1978), 1328–1329.

Shyr, Jih Min. 1975. On relative class numbers of certain quadratic extensions. *Bulletin of the American Mathematical Society* 81, 500–502.

———. 1979. Class numbers of binary quadratic forms over algebraic number fields. *Journal für die reine und angewandte Mathematik* 307/308, 353–364.

Skolem, Thoralf. 1928. Geschlechter und Reziprozitätsgesetze. *Norsk matematisk Forenings skrifter* 1$^{\text{st}}$ ser. 18, 38pp.

Skorobogatov, Alexei. 2001. *Torsors and Rational Points*. Cambridge: Cambridge University Press.

Stark, Harold M. 1976. The genus theory of number fields. *Communications on Pure and Applied Mathematics* 29, 805–811.

Steinig, John. 1966. On Euler's idoneal numbers. *Elemente der Mathematik* 21, 73–88.

Tannaka, Tadao. 1958. A generalized principal ideal theorem and a proof of a conjecture of Deuring. *Annals of Mathematics* 67, 574–589.

Taussky, Olga. 1983. Some non-commutative methods in algebraic number theory. In *Emmy Noether in Bryn Mawr*, ed. B. Srinivasan, J. Sally, pp. 47–57. New York, Berlin: Springer-Verlag.

Terada, Fumiyuki. 1952. On the principal genus theorem concerning the Abelian extensions. *Tohoku Mathematical Journal* 4, 141–152.

———. 1953. A note on the principal genus theorem. *Tohoku Mathematical Journal* 5, 211–213.

Venkov, Boris Alekseevič. 1970. *Elementary Number Theory*. Transl. from Russian by H. Alderson. Groningen: Wolters-Noordhoff.

Weber, Heinrich. 1908. *Lehrbuch der Algebra*, vol. 3. Braunschweig: Vieweg. Repr. New York: Chelsea, 1961.

Weil, André. 1984. *Number Theory. An Approach through History from Hammurapi to Legendre*. Basel, Boston: Birkhäuser.

Zagier, Don. 1981. *Zetafunktionen und quadratische Körper. Eine Einführung in die höhere Zahlentheorie*. Berlin, Heidelberg, New York: Springer-Verlag.

Table of Illustrations

Index

Except if discussed in some detail, secondary sources and passing references to mathematical literature past 1950 are generally not included in this index.

Authors' addresses

Reinhard Bölling. Universität Potsdam, Institut für Mathematik. Postfach 60 15 53.
14415 Potsdam, Germany.
boelling@rz.uni-potsdam.de

Jacqueline Boniface. Université de Nice - Sophia Antipolis, U.F.R. Lettres, Arts et Sciences humaines, Département de Philosophie. 98, boulevard Édouard Herriot, B.P. 3209. 06204 Nice Cedex, France.
jacqueline.boniface@wanadoo.fr

Aldo Brigaglia. Universita di Palermo, Dipartimento di Matematica ed Applicazioni.
Via Archirafi 34. 90100 Palermo, Italy.
brig@math.unipa.it

Anne-Marie Décaillot. Université René Descartes, MAP5, UFR de Mathématiques et Informatique. 45, rue des Saints-Pères. 75270 Paris Cedex, France.
decaillot@math-info.univ-paris5.fr

Harold M. Edwards. New York University, Courant Institute of Mathematical Sciences. 251 Mercer Street. New York, NY 10012, USA.
hme1@scires.acf.nyu.edu

Della Fenster. University of Richmond, Department of Mathematics and Computer Science. Richmond, VA 23173, USA.
dfenster@richmond.edu

José Ferreirós Domínguez. Universidad de Sevilla, Departamento de Filosofía y Lógica. C/ Camilo José Cela, s/n. 41018 Sevilla, Spain.
josef@us.es

Günther Frei. Lützelstrasse 36. 8634 Hombrechtikon, Switzerland.
g.frei@active.ch

Catherine Goldstein. Histoire des sciences mathématiques, Institut de mathématiques de Jussieu. 175, rue du Chevaleret. 75013 Paris, France.
cgolds@math.jussieu.fr

Christian Houzel. 11, rue Monticelli. 75014 Paris, France.
Houzel@vjf.cnrs.fr

Franz Lemmermeyer. Bilkent University, Department of Mathematics. Bilkent.
06800 Ankara, Turkey.
franz@fen.bilkent.edu.tr

Olaf Neumann. Friedrich-Schiller-Universität, Mathematisches Institut. Ernst Abbe Platz 2. 07740 Jena, Germany.
neumann@minet.uni-jena.de

Samuel J. Patterson. Georg-August-Universität, Mathematisches Institut. Bunsenstr. 3-5. 37073 Göttingen, Germany.
sjp@uni-math.gwdg.de

Birgit Petri. Technische Universität Darmstadt, Fachbereich Mathematik. Schlossgartenstrasse 7. 64289 Darmstadt, Germany.
petri@mathematik.tu-darmstadt.de

Paola Piazza. Via delle Fornaci 19/A. 57128 Livorno, Italy.
p.piazza@tin.it

Herbert Pieper. Berlin-Brandenburgische Akademie der Wissenschaften, Alexander-von-Humboldt-Forschungsstelle. Jägerstrae 22/23. 10117 Berlin, Germany.
pieper@bbaw.de

Norbert Schappacher. Université Louis Pasteur, IRMA, 7, rue René Descartes. 67084 Strasbourg cedex, France.
schappa@math.u-strasbg.fr

Joachim Schwermer. Universität Wien, Fakultät für Mathematik. Nordbergstrasse 15. 1090 Wien, Austria.
Joachim.Schwermer@univie.ac.at