Part 1. Factorization

0. Introduction.

Fermat's Last Theorem

Fermat numbers $F_n = 2^{2^n} + 1$ mistakenly thought to be prime:

$$F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65537$$

are prime but

$F_5 = 4\ 294\ 967\ 297$ is divisible by 641 – calculated by Euler

Euler's conjecture: no nth power is a sum of fewer than n nth powers. Counterexamples:
(1964) by computer search $144^5 = 27^5 + 84^5 + 110^5 + 135^5$,
(1987) by using elliptic curves arithmetic $20615673^4 = 2682440^4 + 15365639^4 + 18796760^4$.

The Goldbach conjecture (1742) – verified up to 100 000.

Twin prime numbers conjecture.

Odd perfect numbers query.

Riemann hypothesis.

1. Divisibility in $\mathbb{Z}$.

$d \in \mathbb{Z}, a|b, a|c \Rightarrow a|(b+c), a|db$. Denote $I_a = \{b \in \mathbb{Z} : a|b\}$.

Call a subset I of $\mathbb{Z}$ an ideal if

(1) $b, c \in I \Rightarrow b + c \in I$;

(2) $b \in I, d \in \mathbb{Z} \Rightarrow db \in I$.

So I_a is an ideal.

Every non-zero ideal I of $\mathbb{Z}$ is equal to some I_a. Indeed, let a be the minimal positive element of I and let $b \in I$. Then $b = ca + q$ with $q, c \in \mathbb{Z}$, $0 \leqslant q < a$ (division algorithm). Since $q = b + (-c)a$ belongs to I by (1) and (2), it is zero. Hence all elements of I are divisible by a. On the other hand, all numbers divisible by a belong to I by property (2). Thus $I = I_a$.

The number a is called a generator of I, I is called a principal ideal. There are two choices for a generator of a non-zero ideal: a or $-a$.

For non-zero a, b the property $a|b$ (b is divisible by a, a divides b) is equivalent to the property $I_a \supset I_b$ (I_b is contained in I_a, I_a contains I_b). From arithmetic point of view instead of working with numbers we can work with ideals.

Put $(a) = a\mathbb{Z} = I_a$ is $a \neq 0$, $(0) = 0A = \{0\}$.

Diagramme of ideals of $\mathbb{Z}$.

For two ideal I and J define

$$I \cap J = \{a : a \in I, a \in J\}, \qquad I + J = \{a + b : a \in I, b \in J\}.$$

Then $I \cap J$ and $I + J$ are ideals.

$e =$ LCM(a, b) is the positive generator of $I_a \cap I_b$. Indeed, $I_e \subset I_a, I_b$, so $I_e \subset I_a \cap I_b$. If $I_a \cap I_b = I_c$, then $a|c, b|c$, so $e|c$ and $I_a \cap I_b \subset I_e$. Thus, $I_e = I_a \cap I_b$.

$d =$ GCD(a, b) is the positive generator of $I_a + I_b$. Indeed, if $I_f = I_a + I_b$, then $f|a, b$, so $f|d$ and $I_f \supset I_d$. On the other hand, $I_d \supset I_a, I_b$, so $I_d \supset I_a + I_b$. Thus, $I_d = I_a + I_b$.

Linear representation of GCD. If $d = \mathrm{GCD}(a, b)$, then there are $m, n \in \mathbb{Z}$ such that $d = ma + nb$.

Recall that a, b are relatively prime if their GCD is 1. Hence a, b are relatively prime iff $I_a + I_b = \mathbb{Z}$ iff there are $m, n \in \mathbb{Z}$ such that $ma + nb = 1$.

Denote by IJ the ideal generated by $ab : a \in I, b \in J$. Then $I_a I_b = I_{ab}$. We get $I_a I_b = (I_a \cap I_b)(I_a + I_b) = I_e I_d$.

Prime numbers (in $\mathbb{Z}$): those divisible by exactly four different numbers. Usually one considers positive prime numbers. If c is not divisible by a prime number p, then p, c are relatively prime.

An ideal I is called prime if it doesn't contain 1 and for every a, b whenever $ab \in I$ at least one of a, b is in I.

A number p is prime iff the ideal I_p is prime. Indeed, let p be prime. If $ab \in I_p$, then $p|ab$. If $p \not| a$, then a, p are relatively prime, so there are $m, n \in \mathbb{Z}$ such that $ma + np = 1$. Then p divides $mab + npb = b$. So I_p is a prime ideal. If I_p is prime, and $p = rq$, then $rq \in I_p$, so $r \in I_p$ or $q \in I_p$. In the first case $p|r$ and $r = \pm p$, in the second case $p|q$ and $q = \pm p$, so p is prime.

Units in $\mathbb{Z}$: $1, -1$. An ideal I_a is improper (coincides with $\mathbb{Z}$) iff a is a unit.

Factorization. Every non-zero integer is a product of a unit and positive powers of positive prime numbers; the prime numbers and their powers are uniquely determined.

Indeed, if a isn't prime, then $a = a_1 a_2$ where $|a_1|, |a_2| < |a|$. Apply induction on $|\quad|$.

Thus, every proper non-zero ideal of $\mathbb{Z}$ is the product of prime ideals.

2. Euclidean domains.

A ring A is called an integral domain if for every $a, b \in A$

$$ab = 0 \Rightarrow a \in A \quad \text{or} \quad b \in A.$$

For example, $\mathbb{Z}$, any field F, the polynomial ring $F[X]$ over a field F are integral domains.

A ring A is called an Euclidean domain (ED) if A is an integral domain and there is a function $\lambda\colon A \setminus \{0\} \to \{0, 1, 2, \dots\}$, such that for every $a \in A$ and every non-zero $b \in A$ there are $c, q \in A$ such that

$$a = bc + q \quad \text{and} \quad \text{either } q = 0 \text{ or } \lambda(q) < \lambda(b)$$

(the division algorithm).

For example $\mathbb{Z}$ is an ED, just set $\lambda(a) = |a|$ and use the usual division algorithm.

The ring $F[X]$ is an ED with respect to $\lambda(f(X)) = \deg(f)$.

Another important example of an ED is the ring of Gaussian integers $\mathbb{Z}[i]$ which consists of $a + bi$, $a, b \in \mathbb{Z}$. It is a commutative ring with unity. Since $\mathbb{Z}[i] \subset \mathbb{C}$, it is an integral domain. Define $\lambda\colon \mathbb{Z}[i] \to \{0, 1, 2, \dots\}$ by $\lambda(a + bi) = |a + bi|^2 = a^2 + b^2$. Clearly, $\lambda((a + bi)(c + di)) = \lambda(a + bi)\lambda(c + di)$. For $\alpha = a + bi$ and $\beta = c + di \neq 0$ consider

$$\alpha/\beta = (a + bi)/(c + di) = (a + bi)(c - di)/(c^2 + d^2) = m + ni$$

with rational m, n. Let e, f be integers which satisfy the property $|m - e|, |n - f| \leqslant 1/2$. Put $\gamma = m + ni$ and $\delta = \alpha - \beta\gamma$.

We claim that $\lambda(\delta) < \lambda(\beta)$. Indeed,

$$\lambda(\delta) = |\alpha - \beta\gamma|^2 = |\beta|^2 |\alpha/\beta - \gamma|^2 = \lambda(\beta)|\alpha/\beta - \gamma|^2$$

and $|\alpha/\beta - \gamma|^2 = (m - e)^2 + (n - f)^2 \leqslant (1/2)^2 + (1/2)^2 < 1$, thus $\lambda(\delta) < \lambda(\beta)$.

In the same way as in section 1 we define ideals of a ring A. A principal ideal $(a) = aA$ is an ideal generated by one element.

In general denote by $(a_1, \dots, a_n)$ the ideal generated by the elements $a_1, \dots, a_n$, ie $\{c_1a_1 + \dots + c_na_n : c_i \in A\}$. Then $(a_1, \dots, a_n) = (a_1) + \dots + (a_n) = a_1A + \dots + a_nA$.

For ideals I, J of A define

$$I \cap J = \{a \in J, a \in J\}, \quad , I + J = \{a + b : a \in I, b \in J\}, \quad IJ = \{\sum_{k=1}^{n} a_k b_k\}.$$

Note that the ideal IJ is generated by all elements ab with $a \in I, b \in J$.

A ring A is called a <u>principal ideal ring</u> (PID) if it is an integral domain and every ideal of A is principal.

$\mathbb{Z}$ is a PID. EXAMPLE of non-PID: $\mathbb{Z}[X]$. Indeed, the ideal generated by 2 and X isn't principal (a polynomial dividing simultaneously 2 and X, is ± 1, the ideal generated by ± 1 is different from $(2, X)$).

THEOREM. *Every Euclidean domain is a principal ideal domain.*

Proof. Let I be a non-zero ideal of A. Consider $\min\{\lambda(a) : a \in I \setminus \{0\}\}$. Clearly it is achieved on some element b of I. We claim that $I = (b)$. Since $(b) \subset I$, we need to check the inverse inclusion. Let a be an element of I. Write $a = bc + q$. Note that $q = a + b(-c)$ belongs to I. If $\lambda(q) < \lambda(b)$, then we would get a contradiction with the definition of b. Thus, $q = 0$ and $a \in (b)$, so $I \subset (b)$.

As a corollary we deduce that every ideal of $K[X]$ is principal. Since $\mathbb{Z}[X]$ isn't a PID, it isn't an ED.

Therefore the ring of Gaussian integers $\mathbb{Z}[i]$ is an ED and a PID.

3. Divisibility in integral domains.

Let A be an integral domain. Let $a, b \in A$ and $b \neq 0$. We write $b|a$ (b divides a) if there is $c \in A$ such that $a = bc$, or equivalently, $a \in (b)$, or equivalently $(a) \subset (b)$. b is called a divisor of a.

If $b|a, d|c$, then $(bd)|(ac)$.

An element $u \in A$ is called a <u>unit</u> of A if $u|1$, or equivalently, there is $v \in A$ such that $uv = 1$. Note that $v = u^{-1}$ is then a unit of A.

u is a unit iff $(u) = A$.

For two units $v, u \in A$ the product uv is a unit, since $(uv)|1$.

The group of units of A is denoted by $U(A)$.

EXAMPLES: $U(\mathbb{Z}) = \{1, -1\}, \quad U(\mathbb{Q}) = \mathbb{Q}^* = \mathbb{Q} \setminus \{0\}, \quad U(\mathbb{Z}[i]) = \{1, -1, i, -i\}$.

Two non-zero elements $a, b \in A$ are said to be associated $a \sim b$ if there is a unit $u \in A$ such that $a = bu$.

$a \sim b$ iff $(a) = (b)$, so the map

$$A \setminus \{0\}/\sim \to \text{principal ideals of } A, \qquad a \to (a)$$

is injective.

Properties: $a \sim a; \quad a \sim b \Rightarrow b \sim a; \quad a \sim b, b \sim c \Rightarrow a \sim c.$

$a \sim 1$ iff $(a) = A$ iff $a \in U(A)$.

An element $d \in A$ is called a GCD of non-zero a, b if $d|a, d|b$ and every common divisor c of a, b divides d. There are rings where for some a, b their GCD doesn't exist! If GCD(a, b) exists, then it is defined up to a unit.

Non-zero elements a, b are called relatively prime if every common divisor of them is a unit.

If $d =$GCD(a, b) exists, then $a/d, b/d$ are relatively prime.

A non-zero element $p \in A \setminus U(A)$ is called irreducible (primitive) if any divisor of p is either a unit or is associated with p.

Properties of irreducible elements:

(1) if $p = ab$ then either $a \sim p$ or $b \sim p$;

(2) if $p = ab$ and $a \in (p)$, then $a \sim p, b \sim 1$;

(3) if p divides an irreducible element q, then $p \sim q$;

(4) for every $a \in A$ which isn't divisible by p GCD(a, p) exists and is a unit.

PROBLEM: *to factorize elements of A into a product of irreducible elements.*

4. PID is a unique factorization domain.

Let A be a PID.

LEMMA 1. *Every two non-zero elements a, b in A have a GCD.*

Proof. Consider the ideal (a, b). It is principal, so there is $d \in A$ such that $(d) = (a) + (b)$. Let $d = a\alpha + b\beta$ with appropriate $\alpha, \beta \in A$. Since $(d) \supset (a)$, $(d) \supset (b)$ we get $d|a, d|b$. If $c|a, c|b$, then $c|(a\alpha + b\beta)$, so $c|d$.

In particular, a, b are relatively prime iff $(a, b) = A$.

LEMMA 2. *Let a, b be relatively prime and let $b|ac$. Then $b|c$.*

Proof. Since $(a, b) = A$, there are $\alpha, \beta \in A$ such that $a\alpha + b\beta = 1$. Then $(ac)\alpha + b(c\beta) = c$ is divisible by b.

Recall that a proper ideal I of A is called prime if whenever $ab \in I$ either a or b belongs to I. A proper ideal I is called maximal if it isn't contained in any strictly larger proper ideal of A. In other words, every ideal J between I and A coincides with either I or A.

Every maximal ideal I is prime: if $a \notin I$, then consider the ideal $aA + I$. It is strictly larger than I, so $aA + I = A$. Then $1 = ae + c$ with $e \in A$, $c \in I$. So if $ab \in I$, then $b = abe + bc \in I$.

In general, a prime ideal isn't necessarily maximal. In principal ideal domains non-zero prime ideals are maximal as the following lemma shows.

LEMMA 3. *Let A be a PID. Let p be a non-zero element of A The following conditions are equivalent*

(1) *p is irreducible;*

(2) *the ideal (p) is prime;*

(3) *for every nonzero $a, b \in A$ if p divides ab then p divides either a or b;*

(4) *the ideal (p) is maximal.*

Proof. (1)⇒(2): Let p be irreducible. Then (p) is a proper ideal, since p isn't a unit. Let $ab \in (p)$. If $a \notin (p)$ then by property (4) of irreducible elements GCD(a, p) is a unit. Hence there are $\alpha, \beta \in A$ such that $\alpha a + \beta p = 1$. Multiplying by b we deduce that $\alpha ab + \beta pb = b$ is divisible by p, i.e. $b \in (p)$. Thus, (p) is prime.

(2)⇒(3): Let (p) be prime. If p divides ab, then $ab \in (p)$, so either $a \in (p)$ (and p divides a) or $b \in (p)$ (and p divides b).

(3)⇒(4): if (p) is contained in an ideal of A, say (a), then $p = ab$ for some $b \in A$. Then either p divides a (and since a divides p we deduce $a \sim p$, $(a) = (p)$) or p divides b (and then $b \sim p$, $a \sim 1$, $(a) = (1) = A$).

(4)⇒(1): Let $a|p$. Then $(p) \subset (a)$. Since (p) is maximal, either $(a) = (p)$ (and $a \sim p$) or $(a) = A$ (and a is a unit).

REMARK. By induction, if p is irreducible and $p|a_1 \dots a_n$, then p divides one of a_i.

A ring A is called a unique factorization domain if every non-zero element a of A is a product $up_1 \dots p_n$ of a unit u and irreducible elements $p_1, \dots, p_n$ and if $a = vq_1 \dots q_m$ is another factorization, then $m = n$ and up to permutation $p_1 \sim q_1, \dots, p_n \sim q_n$.

THEOREM. *Every principal ideal domain is a unique factorization domain.*

Proof. Existence:

Let a be a non-zero element of A which isn't a unit. Then the ideal (a) is proper. Consider all ideals of A which contain (a). Let (p) be a maximal ideal containing (a). Then p is irreducible by Lemma 3 and $p|a$. Put $a = pa_1$. Since p isn't a unit, the ideal (a_1) strictly includes (a).

If a_1 isn't a unit, then find an irreducible element p_1 and factorization $a_1 = p_1 a_2$ and so on. Assume that each subsequent a_n isn't a unit. Put $a_0 = a$. Then we get an infinite chain of ideals $(a_0) \subset (a_1) \subset (a_2) \subset \dots$ with strict inclusions. Consider the set I which consists of finite linear combinations with coefficients from A of a_n, ie

$$I = \left\{ \sum c_k a_k : \text{only finitely many } c_k \text{ are different from zero} \right\}.$$

I is an ideal which contains every (a_n). Let $I = (b)$. Then b is a finite sum $\sum_{k=0}^{l} e_k a_k$, $e_k \in A$. Note that $a_l | a_k$ for $k \leqslant l$, so $a_l | b$, ie $(b) \subset (a_l)$. Thus, $(b) = (a_l)$. Then $(b) = (a_l) \subset (a_{l+i}) \subset (b)$ for $i \geqslant 1$, and therefore $(a_l) = (a_{l+i})$ for $i \geqslant 1$, a contradiction.

Thus, a_n is a unit for some n. Then $a = a_n p p_1 \dots p_{n-1}$ is a required factorization of a.

Uniqueness:

If $a = up_1 \dots p_n = vq_1 \dots q_m$, then p_1 divides $vq_1 \dots q_m$, so by Remark p_1 divides one of q_i. Without loss of generality assume that p_1 divides q_1. However, q_1 is irreducible, so p_1 is associated with q_1, $q_1 = p_1 w$. Now $a/p_1 = up_2 \dots p_n = vwq_2 \dots q_m$. Continue and deduce that $m = n$ and up to a permutation $p_2 \sim q_2, \dots, p_n \sim q_n$.

5. Euclidean algorithm.

Let A be an ED. Given elements $a, b \in A$, $b \neq 0$ make a repeated application of the division algorithm

$a = bq_1 + r_1$, $r_1 \neq 0, \lambda(r_1) < \lambda(b)$,

$b = r_1 q_2 + r_2$, $r_2 \neq 0, \lambda(r_2) < \lambda(r_1)$,

...

$r_{n-1} = r_n q_{n+1} + r_{n+1}$, $r_{n+1} \neq 0, \lambda(r_{n+1}) < \lambda(r_n)$,

$r_n = r_{n+1} q_{n+2}$.

Claim: $r_{n+1} = \text{GCD}(a, b)$.

Proof: $r_{n+1} | r_n \Rightarrow r_{n+1} | r_{n-1} \Rightarrow \dots \Rightarrow r_{n+1} | b \Rightarrow r_{n+1} | a$.

If $c|a, c|b$, then $c|r_1 \Rightarrow \dots \Rightarrow c|r_{n+1}$.

COROLLARY 1. Linear representation of GCD in Euclidean domains: start with $r_{n+1} = r_{n-1} - r_n q_{n+1}$, then substitute $r_n = r_{n-2} - r_{n-1}q_n$, so $r_{n+1} = r_{n-1} - (r_{n-2} - r_{n-1}q_n)q_{n+1} = r_{n-1}(1 + q_n q_{n+1}) - r_{n-2}q_{n+1}$ and continue, eventually getting $r_{n+1} = \alpha a + \beta b$ with $\alpha, \beta \in A$.

COROLLARY 2. Linear equations over ED: to solve an equation $aX + bY = c$ first find $d =$GCD$(a, b) = \alpha a + \beta b$ using the Euclidean algorithm. If $d \not| c$, the equation doesn't have solutions. If $d|c$, then $x_0 = (c/d)\alpha, y_0 = (c/d)\beta$ is a solution and all solutions are given by $x = x_0 + tb/d, y = y_0 - ta/d$ where t runs over A.

Proof: if $ax+by = c$, then $a(x-x_0) = -b(y-y_0)$. Since A is a PID and $a/d, b/d$ are relatively prime, from Lemma 1 of the previous section and the equality $(a/d)(x - x_0) = -(b/d)(y - y_0)$ we deduce that $x - x_0$ is divisible by b/d. Put $x - x_0 = (b/d)t$, then $y = y_0 - ta/d$. Clearly $x = x_0 + tb/d, y = y_0 - ta/d$ is a solution.

Part 2. Congruences

Still all rings are commutative with unity.

1. The quotient ring.

Definition. Let I be an ideal of a ring A. For an element $a \in A$ the set

$$a + I = \{a + i : i \in I\}$$

is called a coset of I in A; the element a is called a representative of the coset $a + I$. Sometimes the coset $a + I$ is denoted by $\overline{a}$.

Note that if $a - b \in I$, then

$$a + I = \{a + i : i \in I\} = \{a + (b - a + i) : i \in I\} = b + I.$$

Define an equivalence relation: $a \sim b$ if $a - b \in I$. Then cosets of I in A are precisely equivalence classes of this relation.

Denote the set of all cosets of I in A by A/I.

Definition. For two cosets $a + I$ and $b + I$ define

$$(a + I) + (b + I) = (a + b) + I, \quad (a + I)(b + I) = ab + I.$$

Let's check correctness of this definition, Let $a' + I = a + I$ and $b' + I = b + I$, then $(a'+I)+(b'+I) = (a'+b')+I = (a+b)+I$, since $(a'+b')-(a = b) = a'-a+b'-b \in I+I \subset I$; and $(a' + I)(b' + I) = a'b' + I = ab + I$, since $a'b' - ab = a'(b' - b) + b(a - a') \in I + I \subset I$. Thus, the sum and the product of two cosets doesn't depend on the choice of representatives.

Now one can show that all axioms of a commutative ring are satisfied for the set of all cosets with respect to the addition and multiplication defined above. For example,

$$((a+I)+(b+I))(c+I) = (a+b+I)(c+I) = (a+b)c+I = ac+I+bc+I = (a+I)(c+I)+(b+I)(c+I).$$

The unity of A/I is the coset $1 + I$, the zero of A/I is the coset $I = 0 + I$.

The ring A/I is called the quotient (factor) ring of A modulo I.

EXAMPLE. Let n be a non-zero integer. If $n = \pm 1$, then the ideal $n\mathbb{Z}$ coincides with $\mathbb{Z}$ and $\mathbb{Z}/n\mathbb{Z}$ consists of one element zero. If n isn't a unit of $\mathbb{Z}$, then first notice that $n\mathbb{Z} = -n\mathbb{Z}$. So we can assume $n > 1$. The ring $\mathbb{Z}/n\mathbb{Z}$ consists of n cosets

$$\overline{0} = 0 + n\mathbb{Z} = n\mathbb{Z}, \overline{1} = 1 + n\mathbb{Z}, \ldots, \overline{n-1} = (n-1) + n\mathbb{Z}.$$

The sum of $\overline{a}$ and $\overline{b}$ is $\overline{a+b} = \overline{c}$ where c is the remainder of $a + b$ modulo n; the product of $\overline{a}$ and $\overline{b}$ is $\overline{ab} = \overline{d}$ where d is the remainder of ab modulo n.

LEMMA. *A proper ideal I is prime iff the quotient ring A/I is an integral domain. A proper ideal I is maximal iff the quotient ring A/I is a field.*

Proof. Let I be prime. Let $ab + I = (a + I)(b + I) = 0 + I = I$. It means that $ab \in I$. Hence either $a \in I$ and so $a + I = 0 + I$, or $b \in I$ and so $b + I = 0 + I$. Thus, A/I is an integral domain.

Let A/I be an integral domain. If $ab \in I$, then $(a + I)(b + I) = ab + I = I = 0 + I$, so either $a + I = 0 + I$ or $b + I = 0 + I$. In the first case $a \in I$, in the second case $b \in I$. Thus, I is a prime ideal.

Let I be maximal. If $a+I \neq 0+I = I$, then $a \notin I$. Hence the ideal $(a)+I$ is strictly larger than I, so $(a)+I = A$. Therefore there is $b \in A$, $c \in I$ such that $ab+c = 1$. We deduce that $(a+I)(b+I) = (1-c)+I = 1+I$. So the coset $a+I$ is invertible in A/I. Thus, every non-zero coset is invertible in A/I, i.e. A/I is a field.

Let A/I be a field. Assume that $I \subset J$ for an ideal J of A. Let $a \in J \setminus I$. Then the coset $a+I$ is invertible in A/I, so there is $b+I$ such that $(a+I)(b+I) = ab+I = 1+I$. In other words, $1 \in (a)+I \subset J$. Hence $J = A$ and I is maximal.

EXAMPLE. The ring $\mathbb{Z}/n\mathbb{Z}$ is a field iff $n\mathbb{Z}$ is a prime ideal of $\mathbb{Z}$ iff n is prime. Thus, we have prime fields

$$\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}, \quad \mathbb{F}_3 = \mathbb{Z}/3\mathbb{Z}, \ldots, \quad \mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}, \ldots$$

The finite field $\mathbb{F}_p$ consists of p elements $\overline{0}, \ldots, \overline{p-1}$.

The quotient ring $\mathbb{Z}/n\mathbb{Z}$ isn't a field if n isn't prime. Moreover, $\mathbb{Z}/n\mathbb{Z}$ isn't an integral domain if $n = n_1 n_2$, $1 < n_1, n_2 < n$, isn't prime: $\overline{n_1 n_2} = \overline{n} = \overline{0}$, $\overline{n_1}, \overline{n_2} \neq \overline{0}$.

Definition. For two rings A and B the map

$$f\colon A \to B$$

is called a ring homomorphism if for every $a_1, a_2 \in A$

$$f(a_1+a_2) = f(a_1)+f(a_2), \quad f(a_1 a_2) = f(a_1)f(a_2)$$

and $f(1_A) = 1_B$ where 1_A is the unity of A, 1_B is the unity of B.

EXAMPLES:

1) If A is a subring of B, then the map $g\colon A \to B$ is a ring homomorphism.

2) If I is a proper ideal of A, then the map $h\colon A \to A/I$, $a \to a+I$ is a ring homomorphism.

The kernel of f denoted by $\ker(f)$ is the set $\{a \in A : f(a) = 0\}$.

The kernel of f is $\{0\}$ iff f is injective.

The image of f denoted by $\mathrm{im}(f)$ is the set $\{b \in B$: there is $a \in A$ such that $b = f(a)\}$. So $\mathrm{im}(f) = f(A)$.

$\mathrm{im}(f) = B$ iff f is surjective.

EXAMPLES:

in 1) $\ker(g) = \{0\}, \mathrm{im}(g) = A$; in 2) $\ker(h) = I, \mathrm{im}(h) = A/I$.

Two rings are called isomorphic if there is a ring homomorphism between them which is bijective.

LEMMA. *The kernel* $\ker(f)$ *is an ideal of* A*; the image* $\mathrm{im}(f)$ *is a subring of* B.

Proof. Let $a, b \in \ker(f)$. Then $f(a+b) = f(a)+f(b) = 0$, so $a+b \in \ker(f)$. If $c \in A$, then $f(ac) = f(a)f(c) = 0$, so $ac \in \ker(f)$. Thus, $\ker(f)$ is an ideal of A.

Let $b = f(a)$ and $d = f(c)$. Then $b-d = f(a-c), bd = f(ac), 1_B = f(1_A)$, so $\mathrm{im}(f)$ is a subring of B.

THEOREM. *Homomorphic image* $\mathrm{im}(f)$ *is isomorphic to the quotient ring* $A/\ker(f)$.

Proof. Define a map $f'\colon A/\ker(f) \to \mathrm{im}(f)$ by the rule $f'(a+\ker(f)) = f(a)$. Then f' is a ring homomorphism and f' is surjective. If $f'(a+\ker(f)) = 0$, then $f(a) = 0$, so $a \in \ker(f)$ and $a+\ker(f) = 0+\ker(f)$. Thus, f' is injective. We deduce that f' is the required isomorphism.

In other words every ring homomorphism $f\colon A \to B$ is the composition if $h\colon A \to A/I$, the isomorphism $A/I \to f(A)$ and the imbedding $g\colon f(A) \to B$.

2. The product of rings and Chinese remainder theorem.

Definition. For two rings A, B define their product $A \times B$ as the set of all pairs (a, b) with addition $(a, b) + (c, d) = (a + c, b + d)$ and multiplication $(a, b)(c, d) = (ac, bd)$. Hence $A \times B$ is a commutative ring with unity $(1, 1)$ and zero $(0, 0)$.

Similarly define the product of several rings.

CHINESE REMAINDER THEOREM. *Let $n_1, \dots, n_k$ be integers > 1 such that every two n_i, n_j are relatively prime for $i \neq j$. Denote $n = n_1 \dots n_k$. Then the quotient ring $\mathbb{Z}/n\mathbb{Z}$ is isomorphic to the product of the quotient rings $\mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}$.*

Proof. Consider a map

$$f: \mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \dots \times \mathbb{Z}/n_k\mathbb{Z}, \quad a \to (a + n_1\mathbb{Z}, \dots, a + n_k\mathbb{Z}).$$

It is a ring homomorphism, since $f(1) = 1$,

$$\begin{aligned} f(a + b) &= (a + b + n_1\mathbb{Z}, \dots, a + b + n_k\mathbb{Z}) \\ &= (a + n_1\mathbb{Z}, \dots, a + n_k\mathbb{Z}) + (b + n_1\mathbb{Z}, \dots, b + n_k\mathbb{Z}) = f(a) + f(b) \end{aligned}$$

and similarly $f(ab) = f(a)f(b)$. Its kernel consists of $a \in \mathbb{Z}$ for which $a + n_1\mathbb{Z} = n_1\mathbb{Z}, \dots,$ $a + n_k\mathbb{Z} = n_k\mathbb{Z}$, i.e. $a \in n_1\mathbb{Z}, \dots, \in n_k\mathbb{Z}$, i.e. $n_1|a, \dots, n_k|a$. Since the prime divisors of n_i are distinct, we deduce that $n|a$. Conversely, if $n|a$, then $f(a) = 0$. Thus, $\ker(f) = n\mathbb{Z}$.

Now let's prove f is surjective. Let $(a_1 + n_1\mathbb{Z}, \dots, a_k + n_k\mathbb{Z})$ be an element of $\mathbb{Z}/n_1\mathbb{Z} \times \dots \times$ $\mathbb{Z}/n_k\mathbb{Z}$. Since n_i and n/n_i are relatively prime for every $i = 1, \dots, k$ we deduce that there are b_i, c_i such that

$$b_i n_i + c_i n/n_i = 1.$$

Consider

$$a = \sum_{i=1}^{m} a_i c_i n/n_i = a_1 c_1 n/n_1 + \dots + a_k c_k n/n_k.$$

The number n_1 divides n/n_2, ... , n/n_k, hence $a - a_1 c_1 n/n_1$ is divisible by n_1. Since $c_1 n/n_1 = 1 - b_1 n_1$, we deduce that

$$a + n_1\mathbb{Z} = a_1 c_1 n/n_1 + n_1\mathbb{Z} = a_1(1 - b_1 n_1) + n_1\mathbb{Z} = a_1 + n_1\mathbb{Z}.$$

Similarly $a + n_i\mathbb{Z} = a_i + n_i\mathbb{Z}$, so we conclude that $f(a) = (a_1 + n_1\mathbb{Z}, \dots, a_k + n_k\mathbb{Z})$, so f is surjective. It remains to apply the theorem of the previous section to complete the proof.

So now we can characterize the finite quotient ring $\mathbb{Z}/p_1^{m_1} \dots p_k^{m_k}\mathbb{Z}$ as being isomorphic to the product of rings $\mathbb{Z}/p_i^{n_i}\mathbb{Z}$, $i = 1, \dots, k$.

3. The Euler function and group of units of $\mathbb{Z}/n\mathbb{Z}$.

Definition. The Euler function $\varphi: \{0, 1, 2, \dots\} \to \{1, 2, \dots\}$ is defined as $\varphi(0) = \varphi(1) = 1$, and

$$\varphi(n) = \#U(\mathbb{Z}/n\mathbb{Z})$$

for $n > 1$.

EXAMPLE. $\varphi(p^a) = p^a - p^{a-1} = p^{a-1}(p - 1)$ for $a > 1$.

Note that $\overline{n} \in U(\mathbb{Z}/p^a\mathbb{Z})$ iff n is relatively prime to p. Indeed, if n is relatively prime to p, then n is relatively prime to p^a, so there are integers m, l such that $nm + p^a l = 1$. Then $\overline{nm} = \overline{1}$ and

$\overline{n} \in U(\mathbb{Z}/p^a\mathbb{Z})$. Conversely, if $\overline{n} \in U(\mathbb{Z}/p^a\mathbb{Z})$, then there is $m \in \mathbb{Z}$ such that $\overline{nm} = \overline{1}$, so $nm - 1$ is divisible by p^a. If p divided n, then p would divide $nm - (nm - 1) = 1$, a contradiction.

So

$$U(\mathbb{Z}/p^a\mathbb{Z}) = \{\overline{n} : 0 \leqslant n \leqslant p^a - 1,\ n \text{ relatively prime to } p\}$$

and hence $\varphi(p^a) = p^a - p^{a-1}$.

THEOREM.

(1) $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$ *for two relatively prime numbers* n_1 *and* n_2;

(2) $\varphi(n) = n\prod(1 - 1/p_i)$ *where* p_i *are all distinct prime divisors of* n.

(3) $\sum_{0<d|n} \varphi(d) = n$.

Proof. (1) From the Chinese remainder theorem we deduce that $U(\mathbb{Z}/n_1 n_2\mathbb{Z})$ is isomorphic to $U(\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z})$. The latter is the group of all pairs (x, y) such that there is a pair (x', y') with $(x, y)(x', y') = (xx', yy') = (1, 1)$, i.e. $x \in U(\mathbb{Z}/n_1\mathbb{Z})$ and $y \in U(\mathbb{Z}/n_2\mathbb{Z})$. So $U(\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}) = U(\mathbb{Z}/n_1\mathbb{Z}) \times U(\mathbb{Z}/n_2\mathbb{Z})$. Thus, $\varphi(n_1 n_2) = \varphi(n_1)\varphi(n_2)$.

(2) Now if $n = p_1^{m_1} \dots n_k^{m_k}$, then

$$\varphi(n) = \varphi(p_1^{m_1}) \dots \varphi(p_k^{m_k}) = p_1^{m_1}(1 - 1/p_1) \dots p_k^{m_k}(1 - 1/p_k) = n\prod(1 - 1/p_i).$$

(3) First, for $n = p^a$ and prime p we get

$$\sum_{0<d|n} \varphi(d) = \sum_{0\leqslant i\leqslant a} \varphi(p^i) = 1 + \sum_{1\leqslant i\leqslant a} (p^i - p^{i-1}) = p^a.$$

Now prove the equality by induction on n. We need to consider only non-powers of primes. If $n = n_1 n_2$ with relatively prime $n_1 < n$ and $n_2 < n$, then $d|n \Rightarrow d = d_1 d_2$ with $d_1|n_1, d_2|n_2$ and

$$\sum_{0<d|n} \varphi(d) = \sum_{0<d_1|n_1} \varphi(d_1) \sum_{0<d_2|n_2} \varphi(d_2) = n_1 n_2 = n.$$

THREE THEOREMS.

(Euler's theorem) *for every unit* $\overline{a}$ *of* $\mathbb{Z}/n\mathbb{Z}$

$$\overline{a}^{\varphi(n)} = \overline{1}.$$

(Fermat's small theorem) *for every* $\overline{a} \neq \overline{0}$ *of* $\mathbb{Z}/p\mathbb{Z}$

$$\overline{a}^{p-1} = \overline{1}.$$

(Wilson's theorem) *for every prime* p

$$(p - 1)! = -1 \quad \text{in } \mathbb{Z}/p\mathbb{Z}.$$

Proof. (1) Since the group $U(\mathbb{Z}/n\mathbb{Z})$ has order $\varphi(n)$ we deduce that $\overline{a}^{\varphi(n)} = \overline{1}$ for every $\overline{a} \in U(\mathbb{Z}/n\mathbb{Z})$.

(2) follows from (1), since $\varphi(p) = p - 1$.

(3) By (2) the polynomial $X^p - X$ has exactly p roots in the field $\mathbb{Z}/p\mathbb{Z}$, so it can be factorized over $\mathbb{Z}/p\mathbb{Z}$ into the product

$$X^p - X = X(X-1)\dots(X-(p-1)).$$

The coefficient of X at the LHS is -1 and the coefficient of X at the RHS is $(-1)(-2)\dots(-p+1) = (-1)^{p-1}(p-1)! = (p-1)!$, since $(-1)^{p-1} = 1$ if $p = 2$ and $(-1)^{p-1} = 1$ if $p > 2$. Thus, $(p-1)! = -1$ in $\mathbb{Z}/p\mathbb{Z}$.

THEOREM. *For a prime p the group $U(\mathbb{Z}/p\mathbb{Z})$ is cyclic* .

Proof. If n divides $p-1$, say $p-1 = nm$, then

$$X^{p-1} - 1 = (X^n - 1)(X^{n(m-1)} + X^{n(m-2)} + \dots + 1).$$

The polynomials of the RHS has no more than n and $n(m-1) = p-1-n$ roots in the field $\mathbb{Z}/p\mathbb{Z}$. However, the polynomial $X^{p-1} - 1$ has exactly $p-1$ distinct roots in $\mathbb{Z}/p\mathbb{Z}$, so the polynomial $X^n - 1$ has exactly n distinct root in the field $\mathbb{Z}/p\mathbb{Z}$.

For $d > 0$ let

$$\psi(d) = \#\{\overline{a} \in \mathbb{Z}/p\mathbb{Z} \text{ of order } d\}.$$

Then for $n|(p-1)$ we get $\sum_{0<d|n} \psi(d) = n$. Clearly $\psi(1) = \varphi(1) = 1$. Assume that $\psi(d) = \varphi(d)$ for $d|n, d < n$. Then

$$\psi(n) = n - \left(\sum_{0<d|n, d<n} \psi(d)\right) = n - \left(\sum_{0<d|n, d<n} \varphi(d)\right) = \varphi(n).$$

Thus, $\psi(p-1) = \varphi(p-1) > 0$ and there is an element of order $p-1$ in the group $U(\mathbb{Z}/p\mathbb{Z})$. It generates it.

4. Linear congruences.

Traditionally the equality of two cosets $a + n\mathbb{Z} = b + n\mathbb{Z}$ is written down as a congruence $a \equiv b \mod n$. In other words, $a \equiv b \mod n$ iff n divides $a - b$.

We easily deduce the following properties of congruences:

$a \equiv a \mod n$; $a \equiv b \mod n \Rightarrow b \equiv a \mod n$; $a \equiv b \mod n, b \equiv c \mod n \Rightarrow a \equiv c \mod n$; $a \equiv b \mod n \Rightarrow ad \equiv bd \mod n$ for $d \in \mathbb{Z}$; $a \equiv b \mod n, c \equiv d \mod n \Rightarrow a+c \equiv b+d \mod n, ac \equiv bd \mod n$.

Our nearest aim is to discuss linear congruences.

A linear congruence is $ax \equiv b \mod n$. Using Corollary 2 in the last section of Part 1, we can solve it.

THEOREM. *Let $d = \mathrm{GCD}(a, n)$. If $d \not| b$, then the linear congruence $ax \equiv b \mod n$ has no solutions. If $d|b$, then the linear congruence $ax \equiv b \mod n$ has d distinct solutions $x_0, x_0 + n/d, \dots, x_0 + n(d-1)/d \mod n$ where (x_0, y_0) is a solution if the linear equation $ax - ny = b$.*

Proof.

First rewrite the congruence as $n|(ax - b)$, or $ax - b = ny$ with some $y \in \mathbb{Z}$, or as a linear equation $ax - ny = b$.

Now from Part 1 we know that to solve the linear equation we should first find

$$d = \mathrm{GCD}(a, -n) = \mathrm{GCD}(a, n).$$

If d doesn't divide b, then the equation doesn't have solutions and so the congruence doesn't have solutions. If d divides b, then there is a solution (x_0, y_0) of the equation and all solutions are given by $x = x_0 - tn/d, y = y_0 - ta/d$ where t runs over $\mathbb{Z}$. So solutions of the congruence are given by $x \equiv x_0 - tn/d \mod n$, i.e. $x \equiv x_0, x_0 + n/d, \ldots, x_0 + n(d-1)/d \mod n$.

The Chinese Remainder Theorem can be read off as the statement on solutions of a system of linear congruences: Let $n_1, \ldots, n_k$ be integers > 1 such that every two n_i, n_j are relatively prime for $i \neq j$. Denote $n = n_1 \ldots n_k$. Then for every integers $a_1, \ldots, a_k$ the system of linear congruences

$$x \equiv a_1 \mod n_1, \quad \ldots, \quad x \equiv a_k \mod n_k$$

has a solution a which is uniquely determined modulo n.

We can provide an interpretation of other results of section 2 in terms of congruences. Note that $\overline{a} \in \mathbb{Z}/n\mathbb{Z}$ is a unit iff a is relatively prime to n. Indeed, if $\overline{a}\overline{b} = \overline{1}$, then $ab \equiv 1 \mod n$, so n divides $ab - 1$ and hence a is relatively prime to n. If a is relatively prime to n, then by the preceding theorem the linear equation $ax \equiv 1 \mod n$ has a solution, say $b \mod n$. Then $\overline{a}\overline{b} = \overline{1}$ and $\overline{a}$ is a unit of $\mathbb{Z}/n\mathbb{Z}$.

Thus, the Euler function can be defined as

$$\varphi(n) = \#\{1 \leqslant a \leqslant n : \mathrm{GCD}(a, n) = 1\}.$$

This function is a so called multiplicative function:

$$\varphi(nm) = \varphi(n)\varphi(m) \quad \text{if } \mathrm{GCD}(n, m) = 1.$$

Euler's theorem can be stated in its classical form as

$$a^{\varphi(n)} \equiv 1 \mod n \quad \text{for } a \text{ relatively prime to } n.$$

Wilson's theorem says that

$$(p-1)! \equiv -1 \mod p.$$

The theorem on the cyclicity of $U(\mathbb{Z}/p\mathbb{Z})$ means that there is an integer a such that its powers $1 = a^0, a, a^2, \ldots, a^{p-2}$ have distinct non-zero remainders modulo p. Such an a is called a primitive root modulo p.

5. Quadratic congruences.

Definition. Let $p > 2$ be a prime. An integer a not divisible by p is called a quadratic residue modulo p (q.r.) if the congruence $X^2 \equiv a \mod p$ is soluble, or equivalently, $\overline{a}$ is a square in $\mathbb{Z}/p\mathbb{Z}$. An integer a not divisible by p is called a quadratic non-residue modulo p (q.nr.) if the conguence $X^2 \equiv a \mod p$ isn't soluble. For an odd prime p the Legendre symbol $\left(\frac{a}{p}\right)$ is defined as 0 if $p|a$, 1 if a is a q.r. modulo p and -1 if a is a q.nr. modulo p.

LEMMA. *Let i, j be in $\{-1, 0, 1\}$. Let p be an odd prime. Then $i \equiv j \mod p$ implies $i = j$.*

Proof. Since p divides $i - j$ and $|i - j| \leqslant 2$ we deduce that $i - j = 0$.

PROPOSITION. Let $p > 2$ be a prime. Then

(1) *The number of q.r. modulo p is equal to the number of q.nr. modulo p and is equal to $(p-1)/2$;*

(2) $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \mod p$;

(3) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$;

(4) $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$.

Proof. (1) Let g be a primitive root modulo p. Every even power of g is a q.r. modulo p and every q.r. is a root of the polynomial $X^{(p-1)/2} - 1$, since

$$(\overline{h}^2)^{(p-1)/2} = \overline{h}^{p-1} = \overline{1}.$$

Therefore they are all roots of the polynomial $X^{(p-1)/2} - 1$ (which has no more than $(p-1)/2$ roots). Every non-zero element of $\mathbb{Z}/p\mathbb{Z}$ is root of $X^{p-1} - 1 = (X^{(p-1)/2} - 1)(X^{(p-1)/2} + 1)$, so odd powers of $\overline{g}$ are roots of $X^{(p-1)/2} + 1$. Hence the polynomial $X^{(p-1)/2} + 1$ has exactly $(p-1)/2$ roots which are odd powers of $\overline{g}$. None of them is a quadratic residue, since those are roots of the polynomial $X^{(p-1)/2} - 1$. Thus, the set of quadratic residues modulo p coincides with the set of even powers of $\overline{g}$ and coincides with the set of roots of the polynomial $X^{(p-1)/2} - 1$; the set of quadratic non-residues modulo p coincides with the set of odd powers of $\overline{g}$ and coincides with the set of roots of the polynomial $X^{(p-1)/2} + 1$. Therefore we get (1). Since, in addition, $a^{(p-1)/2} \equiv 0 \mod p$ iff p divides a iff $\left(\frac{a}{p}\right) = 0$, we deduce (2).

(3) Both $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$ and $\left(\frac{ab}{p}\right)$ are congruent modulo p to $(ab)^{(p-1)/2}$, so by Lemma

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right).$$

(4) Follows from (3) and the lemma.

COROLLARY. -1 is a q.r. modulo p iff $p \equiv 1 \mod 4$.

EXAMPLE 1. There are infinitely many primes congruent to 1 modulo 4.

Indeed, if $p_1, \ldots, p_m$ are such primes, then there is a prime number p which divides $4(p_1 \ldots p_m)^2 + 1$. Then $-1 \equiv (2p_1 \ldots p_m)^2 \mod p$, so -1 is a q.r. modulo p, hence $p \equiv 1 \mod 4$ and distinct from $p_1, \ldots, p_m$.

EXAMPLE 2. If a prime odd number divides $a^2 + b^2$, then
either p divides both a and b and then p^2 divides $a^2 + b^2$
or $p \equiv 1 \mod 4$.

Indeed, if $p|a$, then $p|b$, so $p^2|(a^2 + b^2)$. If a, b are not divisible by p, then find c such that $ac \equiv 1 \mod p$. Then $(bc)^2 \equiv -(ac)^2 \equiv -1 \mod p$, so $p \equiv 1 \mod 4$.

LEMMA. *Let p be an odd positive prime and let $q \geqslant 2$ be a prime different from p. Let $S = \{2, 4, \ldots, p-1\}$. Define*

$$r_a = qa - p[qa/p].$$

Then

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{a \in S} r_a} = (-1)^{\sum_{a \in S} [qa/p]}.$$

Proof. First, $r_a \neq 0$, since q and a is relatively prime to p and so is qa.

Now, $(-1)^{r_a} r_a \equiv r_a \mod p$ if r_a is even between 1 and p and $(-1)^{r_a} r_a \equiv p - r_a \mod p$ is even between 1 and p if r_a is odd. On the other hand, if $(-1)^{r_a} r_a \equiv (-1)^{r_b} r_b \mod p$ for $a, b \in S$,

then $qa \equiv \pm qb \mod p$, so $q(a \pm b)$ is divisible by p and hence $a \equiv \pm b \mod p$; for elements in S that implies $a = b$.

Thus, in $\mathbb{Z}/p\mathbb{Z}$ we get

$$\{\overline{(-1)^{r_a} r_a} : a \in S\} = \{\overline{a} : a \in S\}.$$

We deduce that

$$\prod_{a \in S} (-1)^{r_a} r_a \equiv \prod_{a \in S} a \mod p.$$

Calculate

$$q^{(p-1)/2} \prod_{a \in S} a = \prod_{a \in S} (qa) \equiv \prod_{a \in S} r_a$$
$$\equiv (-1)^{\sum_{a \in S} r_a} \prod_{a \in S} a \mod p.$$

Since $\prod_{a \in S} a$ is relatively prime to p, we conclude that

$$\left(\frac{q}{p}\right) \equiv q^{(p-1)/2} \equiv (-1)^{\sum_{a \in S} r_a} \mod p$$

and from the first lemma of this section that

$$\left(\frac{q}{p}\right) = (-1)^{\sum_{a \in S} r_a}.$$

Finally,

$$0 \equiv \sum_{a \in S} qa = \sum_{a \in S} (p[qa/p] + r_a) = p \sum_{a \in S} [qa/p] + \sum_{a \in S} r_a \mod 2,$$

so $\sum_{a \in S} r_a \equiv \sum_{a \in S} [qa/p] \mod 2$ and $(-1)^{\sum_{a \in S} r_a} = (-1)^{\sum_{a \in S} [qa/p]}$.

THEOREM (Gauss quadratic reciprocity law) *For $p \neq q$ odd positive primes*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{(p-1)(q-1)/4}, \quad \left(\frac{2}{p}\right) = (-1)^{(p^2-1)/8}.$$

Proof. Let $O = (0,0), A = (p,q), B = (p,0), E = (p/2,0), F = (p/2, q/2), G = (p/2, q), H = (0, q/2)$. Note that there are no integer points inside OA and EF. Then $\sum_{a \in S} [qa/p]$ is the number n of integer points with even x-coordinate inside the triangle OAB. It is equal to the sum of the number n_1 of integer points with even x-coordinate inside the triangle OEF and the number n_2 of integer points with even x-coordinate inside $EBAF$. For every even integer b the number of integer points $\{(b,y) : 0 < y < q\}$ is equal to $q-1$, so $n_2 \equiv n_3 \mod 2$ where n_3 is the number of integer points with even x-coordinate inside FAG. The map $(x,y) \to (p-x, q-y)$ transforms integer points with even x-coordinate inside FAG into integer points with odd x-coordinate inside OEF. Thus, $n \equiv n_1 + n_4 \mod 2$ where n_4 is the number of integer points with odd x-coordinate inside OEF.

Thus, $\left(\frac{p}{q}\right) = (-1)^m$ where m is just the number of integer points inside OEF.

Similarly, $\left(\frac{q}{p}\right) = (-1)^l$ where l is the number of integer points inside OHF.

So $m + l$ is the number of integer points inside OEFH which is equal to $(p-1)/2 \times (q-1)/2$.

To prove the second equality consider $\sum_{a \in S} [2a/p] = \sum_{(p+1)/2 \leqslant a \leqslant p-1} 1$ which is easy to show is even if $p \equiv \pm 1 \mod 8$ and odd is $p \equiv \pm 3 \mod 8$.

EXAMPLE. Is 37 a q.r. modulo 83?

Calculate

$$\left(\frac{37}{83}\right) = (-1)^{(37-1)(83-1)/4}\left(\frac{83}{37}\right) = \left(\frac{83}{37}\right) = \left(\frac{9}{37}\right)\left(\frac{3}{37}\right)^2 = 1,$$

so it is. Then the congruence $x^2 \equiv 37 \mod 83$ has at least one solution, say $a \mod 83$, the second is $-a \mod 83$ and $-a \not\equiv a \mod 83$ since $a \not\equiv 0 \mod 83$. Since $\mathbb{Z}/83\mathbb{Z}$ is a field, the congruence has exactly two distinct solutions modulo 83.

Definition. Let $m > 1$ be an odd integer. An integer n relatively prime to m is said to be a q.r. (q.nr.) modulo m if $\overline{n}$ is (is not) a square in $\mathbb{Z}/m\mathbb{Z}$. If $m = p_1 \dots p_s$ is the factorization of m into the product of odd primes, define the Jacobi symbol

$$\left(\frac{n}{m}\right) = \left(\frac{n}{p_1}\right) \dots \left(\frac{n}{p_s}\right).$$

If n is a q.r. modulo p_i for $1 \leqslant i \leqslant s$, then $\left(\frac{n}{m}\right) = 1$. However $\left(\frac{n}{m}\right) = 1$ doesn't imply that n is a q.r. modulo m: $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, though 2 isn't a q.r. modulo 15.

If $\left(\frac{n}{m}\right) = -1$, then n isn't a q.r. modulo at least one of p_i, hence it is a q.nr. modulo m.

From the definition we deduce the following properties of the Jacobi symbol:

(1)

$$n_1 \equiv n_2 \mod m \Rightarrow \left(\frac{n_1}{m}\right) = \left(\frac{n_2}{m}\right)$$

(2)

$$\left(\frac{n_1 n_2}{m}\right) = \left(\frac{n_1}{m}\right)\left(\frac{n_2}{m}\right), \left(\frac{n}{m_1 m_2}\right) = \left(\frac{n}{m_1}\right)\left(\frac{n}{m_2}\right).$$

PROPOSITION. *Let $m, n > 1$ be relatively prime odd integers. Then*

$$\left(\frac{-1}{m}\right) = (-1)^{(m-1)/2}, \quad \left(\frac{2}{m}\right) = (-1)^{m^2-1)/8}, \quad \left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = (-1)^{(n-1)(m-1)/4}.$$

Proof. For odd integers a, b use the congruences

$$(a-1)/2 + (b-1)/2 \equiv (ab-1)/2 \mod 2, \quad (a^2-1)/8 + (b^2-1)/8 \equiv (a^2b^2-1)/8 \mod 2$$

and deduce that

$$\sum (p_i - 1)/2 \equiv (\prod p_i - 1)/2 \mod 2, \quad \sum (p_i^2 - 1)/8 \equiv (\prod p_i^2 - 1)/8 \mod 2.$$

Then, apply the QRL. For example, if $m = \prod p_i, n = \prod q_j$, then

$$\left(\frac{n}{m}\right)\left(\frac{m}{n}\right) = \prod \left(\frac{q_j}{p_i}\right)\left(\frac{p_i}{q_j}\right) = \prod (-1)^{(p_i-1)(q_j-1)/4} = (-1)^{(n-1)(m-1)/4}.$$

EXAMPLE. Is 161 a q.r. modulo 577?

Calculate

$$\left(\frac{161}{577}\right) = \left(\frac{577}{161}\right) = \left(\frac{94}{161}\right) = \left(\frac{2}{161}\right)\left(\frac{47}{161}\right) = (1)\left(\frac{47}{161}\right) =$$
$$\left(\frac{20}{47}\right) = \left(\frac{2^2 \cdot 5}{47}\right) = \left(\frac{5}{47}\right) = \left(\frac{47}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

so 161 isn't a q.r. modulo 577.

Part 3. Gaussian integers and applications

1. Sums of two squares.

PROPOSITION. *Let p be a prime number > 2 congruent to 1 modulo 4. Then there are positive integers a, b such that $p = a^2 + b^2$.*

Proof. Due to the last section of the previous chapter there is an integer c such that $c^2 \equiv -1 \mod p$. Let $\sqrt{p} \in (k, k+1)$. The set

$$S = \{x + yc : 0 \leqslant x \leqslant k, 0 \leqslant y \leqslant k\}$$

consists of $(k+1)^2 > p$ elements, so two of them, say $x_1 + y_1 c$ and $x_2 + y_2 c$ with $(x_1, y_1) \neq (x_2, y_2)$ have the same remainder modulo p. Let $a = |x_1 - x_2|$ and $b = |y_1 - y_2|$. Then $a^2 \equiv b^2 c^2 \equiv -b^2 \mod p$ and $p|(a^2 + b^2)$. Note that $0 < a^2 + b^2 < p + p = 2p$, the latter inequality due to $a, b \leqslant k < \sqrt{p}$. Thus, $a^2 + b^2 = p$.

THEOREM. *Let*

$$n = \prod p^{m_p}$$

be the factorization of integer $n > 1$. Then n is a sum of two squares iff m_p is even for every $p \equiv 3 \mod 4$.

Proof. Let $n = a^2 + b^2$. For a prime $p \equiv 3 \mod 4$ which divides n we get $p|(a^2 + b^2)$ and so by Example 2 of the last section of the previous chapter p divides a and b. Write $a_1 = a/p, b_1 = b/p$ and deduce that $p^{m_p - 2}$ divides $a_1^2 + b_1^2$. If $m_p > 2$, repeat the previous argument. Thus, we deduce that m_p is even.

Conversely, for each prime $p \equiv 1 \mod 4$ and for $p = 2$ find integers a_p, b_p such that $p = a_p^2 + b_p^2$. Write $p^{m_p} = (p^{m_p/2})^2 + 0^2$ for $p \equiv 3 \mod 4$. Then

$$n = \prod_{p=2, p \equiv 1 \mod 4} (a_p^2 + b_p^2)^{m_p} \prod_{p \equiv 3 \mod 4} ((p^{m_p/2})^2 + 0^2).$$

Note that $(a^2 + b^2)(c^2 + d^2) = (ac - bd)^2 + (ad + bc)^2$. Thus, n is a sum of two squares.

2. Irreducible elements of $\mathbb{Z}[i]$.

LEMMA. *Every irreducible element π of $\mathbb{Z}[i]$ divides some integer prime p.*

Proof. Since $\mathbb{Z}[i]$ is a PID, the ideal $\pi\mathbb{Z}[i]$ is prime. Consider the ideal $I = \mathbb{Z} \cap \pi\mathbb{Z}[i]$ of $\mathbb{Z}$. It doesn't contain 1, since otherwise 1 belongs to $\pi\mathbb{Z}$, a contradiction. If $ab \in \mathbb{Z} \cap \pi\mathbb{Z}[i]$, then either $a \in \mathbb{Z}[i]$ or $b \in \mathbb{Z}[i]$, therefore either $a \in I$ or $b \in I$. Then $I = p\mathbb{Z}$ and $\pi|p$.

Thus, I is a non-zero prime ideal of $\mathbb{Z}$. Hence it is equal to $p\mathbb{Z}$ for a prime p. We conclude $p \in I \subset \pi\mathbb{Z}[i]$, so π divides p.

THEOREM. *For every prime $p \equiv 1 \mod 4$ let a_p, b_p be integers such that $a_p^2 + b_p^2 = p$. Then every irreducible element of $\mathbb{Z}[i]$ is associated to exactly one of the following:*

$$1 + i,$$

$$a_p + b_p i, a_p - b_p i, \quad \textit{for every positive prime } p \equiv 1 \mod 4,$$

$$\textit{positive primes } q \equiv 3 \mod 4.$$

Proof.

First, let's check that each of the listed Gaussian integers is irreducible. If π is one of them and $\pi = \pi_1 \pi_2$, then $|\pi|^2 = |\pi_1|^2 |\pi_2|^2$.

In the first and second case we deduce that $|\pi_1|^2 |\pi_2|^2$ is a prime, and then one of π_i is a unit and so π is irreducible.

In the third case $|\pi_1|^2 |\pi_2|^2 = q^2$ for a prime $q \equiv 3 \mod 4$. Note that $|\pi_i|^2$ is the sum of two squares. According to the previous section q isn't a sum of two squares, so one of $|\pi_i|^2$ is equal to 1 and so one of π_i is a unit. Thus, π is irreducible.

Second, let's check that the listed Gaussian integers are not associated to each other. Note that if $\alpha \sim \beta$ in $\mathbb{Z}[i]$, then $\alpha = \beta u$ for $u \in \mathbb{Z}[i]$ and $|\alpha|^2 = |\beta|^2$. The quotient $(1+i)/(1-i)$ is equal to i, so $1 + i \sim 1 - i$. The quotient $(a_p + b_p i)/(a_p - b_p i)$ for $p > 2$ is equal to $(a_p^2 + b_p^2)/p + 2a_p b_p i/p$. Since $2, a_p, b_p < p$, $2a_p b_p$ are relatively prime to p, $(a_p^2 + b_p^2)/p + 2a_p b_p i/p$ isn't a Gaussian integer. So $a_p + b_p i \not\sim a_p - b_p i$ for $p > 2$.

Third, let's check that every irreducible element π of $\mathbb{Z}[i]$ is associated to one of the listed elements. By the preceding lemma there is a prime p such that $p = \pi\alpha$ with appropriate $\alpha \in \mathbb{Z}[i]$. Then $p^2 = |\pi|^2 |\alpha|^2$, so $|\pi|^2$ divides p^2. Note than $|\pi|^2 \neq 1$, since only units of $\mathbb{Z}[i]$ have module 1. Thus, either (a) $|\pi|^2$ is a prime p or (b) $|\pi|^2$ is the square of a prime q.

If (a), then p as the sum of two squares is either 2 or $\equiv 1 \mod 4$ by the previous section. Put $a_2 = b_2 = 1$. So $\pi\overline{\pi} = p = (a_p + b_p i)(a_p - b_p i)$. Then π divides one of the two terms of the RHS, and since that one is irreducible by the first part of the proof, they are associated to each other.

If (b), then we first check that $q \equiv 3 \mod 4$. Clearly $q \neq 2$, since 4 isn't a sum of two squares. If q were congruent to 1 modulo 4, then by the previous section we would find integers a_q, b_q such that $q = a_q^2 + b_q^2$. Then similarly to the previous arguments π divides one of $a_q + b_q i, a_q - b_q i$. Hence $|\pi|^2$ divides $|a_q + b_q i|^2 = q$, a contradiction. Thus, $q \equiv 3 \mod 4$ and therefore it is irreducible in $\mathbb{Z}[i]$ by the first part of the proof. From $\pi\overline{\pi} = qq$ we conclude that π divides q, so it is associated with q.

EXAMPLE. Solve the Diophantine equation $Y^2 = X^3 - 1$.

Rewrite it as $X^3 = (Y+i)(Y-i)$. Let α be GCD$(Y+i, Y-i)$. Then α divides $Y+i-(Y-i) = 2i = (1+i)^2$. If α isn't a unit of $\mathbb{Z}[i]$, then $(1+i)|\alpha$, $2|2i = (1+i)^2|\alpha^2|(Y+i)(Y-i) = X^3$, so X is even and $Y^2 \equiv 8 - 1 = 7 \mod 8$. However, 7 isn't a square modulo 8. Thus, α is a unit and $Y + i, Y - i$ are relatively prime in $\mathbb{Z}[i]$.

Factorize $X = \prod u\pi_i^{n_i}$ into a product of a unit u and irreducible elements π_i of $\mathbb{Z}[i]$. Then $(Y + i)(Y - i) = \prod u^3 \pi_i^{3n_i}$. Since $Y + i$, $Y - i$ are relatively prime, each $\pi_i^{3n_i}$ divides only one of them. Thus, each of them as a product of some third powers $\pi_i^{3n_i}$ and a unit. Looking at four different possibilities for a unit in $\mathbb{Z}[i]$ we see that each of them is a third power. Thus, $Y + i$ is a third power and $Y - i$ is a third power in $\mathbb{Z}[i]$, So $Y + i = (a + bi)^3$ for $a, b \in \mathbb{Z}$. Comparing coefficients of i we get a simple equation $1 = b(3a^2 - b^2)$. Then $b = -1, a = 0$ and $X = 1, Y = 1$ is the only solution of the equation $Y^2 = X^3 - 1$.

3. Sums of four squares.

THEOREM. *Every positive integer is a some of four squares.*

Proof.

We will use the following equality

$$(a_1^2+a_2^2+a_3^2+a_4^2)(b_1^2+b_2^2+b_3^2+b_4^2)=c_1^2+c_2^2+c_3^2+c_4^2$$

where

$$c_1=a_1b_1+a_2b_2+a_3b_3+a_4b_4,\quad c_2=a_1b_2-a_2b_1+a_3b_4-a_4b_3$$
$$c_3=a_1b_3-a_3b_1+a_4b_2-a_2b_4,\quad c_4=a_1b_4-a_4b_1+a_2b_3-a_3b_2$$

To prove the theorem it suffices to show that every positive prime p is a sum of four squares. We can assume $p>2$.

Consider the set $A_1\subset\mathbb{Z}/p\mathbb{Z}$ consisting of zero and all quadratic residues modulo p and set $A_2=-\overline{1}-A_1\subset\mathbb{Z}/p\mathbb{Z}$. Each consists of $(p+1)/2$ elements, so their intersection is not empty. So there are $a,b\in\mathbb{Z}$ such that $a^2\equiv -1-b^2 \mod p$. Then $p|(1+a^2+b^2)$.

We have shown there are integers a_i such that p divides $a_1^2+\cdots+a_4^2>0$. By passing to remainders modulo p we can assume $|a_i|<p/2$ for all i. Then $a_1^2+\cdots+a_4^2=pm$ with $0<m<p$. Assume that $m>1$.

Let $b_i\equiv a_i \mod m$ and $|b_i|\leqslant m/2$. Then $b_1^2+\cdots+b_4^2=mr$ with $0\leqslant r\leqslant m$.

If $r=0$, then $b_i=0$ and $m|a_i$ for each i, so $mp=a_1^2+\cdots+a_4^2$ is divisible by m^2 and p is divisible by m which is between 1 and p, a contradiction. If $r=m$, then $m/2$ is an integer, $|b_i|=m/2$ and $m/2$ divides a_i for each i. Then $m^2/4$ divides $a_1^2+\cdots+a_4^2=pm$, so either $m=2$ or $m=4$. If $m=2$, then $a_i\equiv 1 \mod 2$, so $2p=a_1^2+\cdots+a_4^2\equiv 4 \mod 4$ and then p is divisible by 2, a contradiction. If $m=4$, then $a_i\equiv 2 \mod 4$, so $4p=a_1^2+\cdots+a_4^2\equiv 16 \mod 16$ and p is divisible by 4, a contradiction. Thus, $0<r<m$.

Then

$$m^2rp=(a_1^2+\cdots+a_4^2)(b_1^2+\cdots+b_4^2)=c_1^2+\cdots+c_4^2,$$

where c_i are given by the first equality of the proof. The formulas for c_i and the congruences $b_i\equiv a_i \mod m$ show that $c_1\equiv a_1^2+\cdots+a_4^2=pm\equiv 0 \mod m$, $c_2,c_3,c_4\equiv 0 \mod m$. Set $d_i=c_i/m\in\mathbb{Z}$. Then $d_1^2+\cdots+d_4^2=pr$.

Thus, we have descented from pm as a sum of four squares to pr with $r<m$ as a sum of four squares. Therefore we can reach the level p and so p is a sum of four squares.

Part 4. p-adic numbers

1. Norms on a field.

Definition Let F be a field. A map $|\ |: F \to [0, +\infty)$ is called a norm on F if it satisfies the following three properties:

$$|\alpha| = 0 \quad \text{iff} \quad \alpha = 0$$

$$|\alpha\beta| = |\alpha||\beta| \quad \text{for every } \alpha, \beta \in F$$

$$|\alpha + \beta| \leqslant |\alpha| + |\beta| \quad \text{for every } \alpha, \beta \in F.$$

We can deduce that $|1| = 1$ and $|-1||-1| = 1$, so $|-1| = 1$. Then $|-\alpha| = |-1||\alpha| = |\alpha|$.

EXAMPLES. 1) the trivial norm: $|\alpha| = 1$ for $\alpha \neq 0$, $|0| = 0$.

2) if $F = \mathbb{Q}, \mathbb{R}, \mathbb{C}$, then the module is a norm on F. We denote it by $|\ |_\infty$.

3) let p be a positive prime. Define a new norm on $\mathbb{Q}$ which is called the p-adic norm.

First, for a non-zero integer a put

$$v_p(a) = \min\{m \in \mathbb{Z} : p^m | a\} = \min\{m \in \mathbb{Z} : a \in p^m\mathbb{Z}\}.$$

Then $v_p(ab) = v_p(a) + v_p(b)$ and $v_p(a + b) \geqslant \min(v_p(a), v_p(b))$. For a non-zero rational $\alpha = a/b$ define

$$v_p(\alpha) = v_p(a) - v_p(b).$$

If $\alpha = c/d$, then $ad = bc$ and $v_p(a) + v_p(d) = v_p(b) + v_p(c)$, so $v_p(a) - v_p(b) = v_p(c) - v_p(d)$. Thus, $v_p: \mathbb{Q}^* \to \mathbb{Z}$ is a well defined map. It is called the p-adic valuation.

We get

$$v_p(\alpha\beta) = v_p(a/b \cdot e/f) = v_p(ae) - v_p(bf) = v_p(\alpha) + v_p(\beta)$$

and

$$v_p(\alpha + \beta) = v_p(a/b + e/f) = v_p((af + be)/(bf)) = v_p(af + be) - v_p(bf)$$
$$\geqslant \min(v_p(af) - v_p(bf), v_p(be) - v_p(bf)) = \min(v_p(a/b), v_p(e/f)) = \min(v_p(\alpha), v_p(\beta)).$$

Put

$$|\alpha|_p = \begin{cases} p^{-v_p(\alpha)}, & \text{if } \alpha \neq 0 \\ 0, & \text{if } \alpha = 0. \end{cases}$$

Thus closer $|\alpha|_p$ to zero, more is the power of p which divides α.

We then have the first and second property of a norm for $|\ |_p$. If $\alpha + \beta = 0$ or $\alpha = 0$ or $\beta = 0$, then

$$|\alpha + \beta|_p \leqslant \max(|\alpha|_p, |\beta|_p) \leqslant |\alpha|_p + |\beta|_p.$$

Otherwise,

$$|\alpha + \beta|_p = p^{-v_p(\alpha+\beta)} \leqslant \max(p^{-v_p(\alpha)}, p^{-v_p(\beta)}) = \max(|\alpha|_p, |\beta|_p) \leqslant |\alpha|_p + |\beta|_p.$$

Thus, $|\ |_p$ is a norm on $\mathbb{Q}$. It is called the p-adic norm on $\mathbb{Q}$.

Definition. A norm $|\ |$ on a field F is called non-Archimedean if it satisfies

$$|\alpha+\beta| \leqslant \max(|\alpha|,|\beta|) \quad \text{for every } \alpha,\beta \in F.$$

It is called Archimedean otherwise.

EXAMPLES: the trivial norm is a non-Archimedean norm, the module is an Archimedean norm, the p-adic norm on $\mathbb{Q}$ is non-Archimedean.

2. All norms on $\mathbb{Q}$.

Let P be the set of all positive primes and infinity.

THEOREM. *Let $|\ |$ be a non-trivial norm on $\mathbb{Q}$. Then there is $p \in P$ and a real $c>0$ such that*

$$|\ | = |\ |_p^c.$$

Proof.

Consider two possible cases.

1) $|n| \leqslant 1$ for every integer $n \geqslant 1$. Let p be the minimal positive integer, such that $|p|<1$. If $p=p_1p_2$ with positive integers p_1, p_2, then $|p|=|p_1||p_2|<1$, so either $p_1=1$ or $p_2=1$. Hence p is a prime. If $q \notin p\mathbb{Z}$, then p^s, q^s are relatively prime for every $s \geqslant 1$. Hence $ap^s+bq^s=1$ with some integers a, b and hence

$$1=|1| \leqslant |a||p^s|+|b||q^s| \leqslant |p^s|+|q^s|.$$

If $|q|<1$, then for sufficiently large s we would get $|q|^s, |p|^s < 1/2$ which contradicts the previous inequality. Thus, $|q|=1$ for every positive prime q different from p. Hence $|p'|=1$ for every integer p' relatively prime to p. Let $c>0$ be such that $|p|=p^{-c}$. Then for in integer $n=p^{v_p(n)}p'$ with p' relatively prime to p we get $|p'|=1$, $|n|_p=|p|^{v_p(n)}=p^{-v_p(n)c}=|n|_p^c$. Therefore $|\alpha|=|\alpha|_p^c$ for every $\alpha \in \mathbb{Q}$.

2) Let $|b|>1$ for some integer $b>1$. Then for every integer $a>1$ one can write $b=b_ka^k+b_{k-1}a^{k-1}+\cdots+b_0$ with $0 \leqslant b_i < a$, $b_k \neq 0$, $a^k \leqslant b$. Then

$$|b| \leqslant (|b_k|+|b_{k-1}|+\cdots+|b_0|)\ \max(1,|a|,\ldots,|a|^k).$$

Note that $k \leqslant \log_a b$, so if $|a|>1$, then $\max(1,|a|,\ldots,|a|^k)=|a|^k \leqslant |a|^{\log_a b}$. In addition, $|b_k|+|b_{k-1}|+\cdots+|b_0| \leqslant (k+1)\max(|0|,|1|,\ldots,|a-1|) \leqslant (\log_a b+1)d$ where $d=\max(|0|,|1|,\ldots,|a-1|)$. Therefore

$$|b| \leqslant (\log_a b+1)d\max(1,|a|^{\log_a b}).$$

Substituting b^m instead of b in the last inequality, we get

$$|b| \leqslant (m\log_a b+1)^{1/m} d^{1/m} \max(1,|a|^{\log_a b})$$

and

$$|b| \leqslant \max(1,|a|^{\log_a b}) \lim_{m\to+\infty}(m\log_a b+1)^{1/m} \lim_{m\to+\infty} d^{1/m}\max(1,|a|^{\log_a b}) = \max(1,|a|^{\log_a b}).$$

Hence $|a|>1$ and then $|b| \leqslant |a|^{\log_a b}$. Similarly we deduce that $|a| \leqslant |b|^{\log_b a}$. Thus, $|a|=|b|^{\log_b a}$ for every integer $a>1$. Let $c>0$ be such that $|b|=|b|_\infty^c$. Then $|a|=|a|_\infty^c$ for every integer

$a > 1$. The same equality holds for $a = 1, 0$ and negative integers, since $|-a| = |a|$. From multiplicativity of the norm we conclude that $|\alpha| = |\alpha|_\infty^c$ for every $\alpha \in \mathbb{Q}$.

All norm $|\ |_p$, $p \in P$ are linked together by the following remarkable property.

LEMMA.

$$\prod_{p \in P} |a|_p = 1 \quad \textit{for every } a \in \mathbb{Q}^*.$$

Proof. Each norm is multiplicative, so it is sufficient to check the equality for non-zero integers. Using factorization, it suffices to check the equality for a positive prime q. We get $|q|_q = q^{-1}$, $|q|_\infty = q$, $|q|_p = 1$ for $p \neq q$, and the formula follows.

3. p-adic numbers.

Recall that the field of real numbers $\mathbb{R}$ is the completion of $\mathbb{Q}$ with respect to the norm $|\ |_\infty$. In other words every real number α has a decimal representation and is expressed as $\alpha = \sum_{k \geqslant i} a_k 10^{-k}$ where $a_k \in \{0, \ldots, 9\}$. If we avoid decimal representations in which $a_k = 9$ for all $k \geqslant i'$, then every real number has a unique decimal representation. Note that $|10^{-k}|_\infty \to 0$ when $k \to +\infty$.

We can consider a completion of $\mathbb{Q}$ with respect to the p-adic norm.

Definition. The field of p-adic numbers $\mathbb{Q}_p$ is the completion of $\mathbb{Q}$ with respect to the p-adic norm $|\ |_p$. In other words, p-adic numbers are convergent (with respect to the p-adic norm) series $\sum_{k=i}^{+\infty} a_k p^k$, $a_k \in \mathbb{Z}$; addition and multiplication of power series as elements of the field $\mathbb{Q}_p$ is defined by the natural rule:

$$\sum_{k=i}^{+\infty} b_k p^k + \sum_{k=i}^{+\infty} b'_k p^k = \sum_{k=i}^{+\infty} (b_k + b'_k) p^k,$$

$$\Big(\sum_{k=i}^{+\infty} b_k p^k\Big) \times \Big(\sum_{k=i}^{+\infty} b'_k p^k\Big) = \sum_{k=i}^{+\infty} b''_k p^k, \quad \text{where } b''_k = \sum_l b_l b'_{k-l}.$$

So we have the field of 2-adic numbers $\mathbb{Q}_2$, 3-adic numbers $\mathbb{Q}_3$, ...

To justify the definition, consider an infinite series

$$\alpha = a_i p^i + a_{i+1} p^{i+1} + \cdots = \sum_{k=i}^{+\infty} a_k p^k, \quad a_k \in \mathbb{Z}$$

Its partial sums $\alpha_n = \sum_{k=i}^{n} a_k p^k$ satisfy the property for every $\varepsilon > 0$ there is N such that for all $n > m \geqslant N$

$$|\alpha_n - \alpha_m|_p \leqslant \varepsilon.$$

Indeed, just take N such that $p^{-N} < \varepsilon$. Then $|\alpha_n - \alpha_m|_p \leqslant |\sum_{k=m}^{n} a_k p^k|_p \leqslant p^{-N} < \varepsilon$. So, the partial sums α_n form a Cauchy sequence (α_n) of rational numbers with respect to $|\ |_p$. Therefore, by the definition of the completion its limit α exists as an element of $\mathbb{Q}_p$.

On the other hand, each element of $\mathbb{Q}_p$ is the limit of a Cauchy sequence (β_n) of rational numbers. It means that $|\beta_n - \beta_{n-1}|_p$ tends to zero, so for the rational number $a_n/b_n = \beta_n - \beta_{n-1}$ with relatively prime a_n and b_n we get $i_n = v_p(a_n/b_n) = v_p(a_n) - v_p(b_n) \to +\infty$. Moving all powers of p to the numerator, we can assume that b_n is relatively prime to p and $a_n = p^{i_n} a'_n$ with integer a'_n relatively prime to p. There are integers e, f such that $b_n e + pf = 1$ and we can rewrite a_n/b_n as $(a_n e)/(1 - pf)$. Note that $1/(1 - pf) = 1 + pf + p^2 f^2 + \ldots$ converges in $\mathbb{Q}_p$.

So $a_n/b_n = a_n e + pfa_n e + p^2 f^2 a_n e + \dots$. Similarly we can produce a power p expression for $a_{n-1}/b_{n-1}, \dots, a_0/b_0, \beta_0$. Then $\beta_n = \beta_0 + a_1/b_1 + \dots + a_n/b_n = \sum_{k=i}^{+\infty} b_k^{(n)} p^k$. Since i_n tends to $+\infty$, for a fixed k the coefficients $b_k^{(n)}$ stabilize $= b_k \in \mathbb{Z}$ for sufficiently large n. Thus, the limit of β_n in $\mathbb{Q}_p$ is equal to the convergent series $\sum_{k=i}^{+\infty} b_k p^k$.

We conclude that every p-adic number is a power series $\sum_{k=i}^{+\infty} b_k p^k$ with integer b_k.

Writing b_k in powers of p with coefficients in $S_p = \{0, 1, \dots, p-1\}$ we even can assume that the coefficients b_k belong to S_p. For instance, $-1 = p-1+(-1)p = p-1+(p-1)p+(-1)p^2 = \dots = \sum_{i \geqslant 0}(p-1)p^i$. Note that if $\sum_{k=i}^{+\infty} c_k p^k = \sum_{k=i}^{+\infty} c'_k p^k$ with $c_k, c'_k \in S_p$, then $\sum_{k=i}^{+\infty}(c_k - c'_k)p^k = 0$, so $(c_i - c'_i)p^i = \sum_{k=i+1}^{+\infty}(c_k - c'_k)p^k$. Then $(c_i - c'_i)p^i$ is divisible by p^{i+1} and hence $c_i - c'_i$ is divisible by p. Since $c_i, c'_i \in S_p$ we deduce that $c_i = c'_i$. Similarly, we show that $c_k = c'_k$ for all k. Thus, for a p-adic number α the expression $\alpha = \sum_{k=i}^{+\infty} c_k p^k$ with $c_k \in S_p$ is unique (without any restriction on the sequence of c_k contrary to the case of $\mathbb{R}$!).

So

$$\mathbb{Q}_p = \{\sum_{k=i}^{+\infty} c_k p^k : c_k \in S_p\}.$$

We can extend the p-adic valuation v_p to $\mathbb{Q}_p$ by the rule

$$v_p(\sum_{k=i}^{+\infty} c_k p^k) = i \quad \text{if } c_i \neq 0.$$

Then we get a non-Archimedean norm $|\ |_p : \mathbb{Q}_p \to [0, +\infty)$, $|\sum_{k=i}^{+\infty} c_k p^k| = p^{-i}$.

Similarly to the real analysis one can develop a so called p-adic analysis. It is simpler to study than the real analysis: for example a series $\sum_{k=0}^{+\infty} \alpha_k$, $\alpha_k \in \mathbb{Q}_p$ converges in $\mathbb{Q}_p$ iff $|\alpha_k|_p \to 0$ when $k \to +\infty$.

4. p-adic integers.

In the field of p-adic numbers $\mathbb{Q}_p$ we have an analogue of integers, which are called p-adic integers $\mathbb{Z}_p$. Those are

$$\begin{aligned}
\mathbb{Z}_p &= \{\alpha \in \mathbb{Q}_p : |\alpha|_p \leqslant 1\} \\
&= \{\alpha \in \mathbb{Q}_p^* : v_p(\alpha) \geqslant 0\} \cup \{0\} \\
&= \{\sum_{k=0}^{+\infty} c_k p^k : c_k \in S_p\} \\
&= \{\sum_{k=0}^{+\infty} a_k p^k : a_k \in \mathbb{Z}\}.
\end{aligned}$$

p-adic integers form a ring. Its group of units is

$$\begin{aligned}
U(\mathbb{Z}_p) &= \{\alpha \in \mathbb{Q}_p : |\alpha|_p = 1\} \\
&= \{\alpha \in \mathbb{Q}_p^* : v_p(\alpha) = 0\} \\
&= \{\sum_{k=0}^{+\infty} c_k p^k : c_k \in S_p, c_0 \neq 0\}.
\end{aligned}$$

Every element α of $\mathbb{Z}_p$ is a product of a non-negative power of p: $p^{v_p(\alpha)}$ and a unit ε. Every prime in $\mathbb{Z}$ which is relatively prime to p is a unit to $\mathbb{Z}_p$. Every irreducible element of $\mathbb{Z}_p$ is associated to p. So up to associativity there is exactly one irreducible element of $\mathbb{Z}_p$: p.

The ring $\mathbb{Z}_p$ is an ED with respect to the map $\lambda(a) = v_p(a) + 1$ for non-zero a and $\lambda(0) = 0$. Indeed, for non-zero $b \in \mathbb{Z}_p$ define $q, r \in \mathbb{Z}_p$ such that $a = bq + r$ by the rule: if $v_p(a) < v_p(b)$, then $q = 0, r = a$; if $v_p(a) \geqslant v_p(b)$, then $r = 0$ and $q = ab^{-1}$; note that $q \in \mathbb{Z}_p$, since $v_p(ab^{-1}) = v_p(a) - v_p(b) \geqslant 0$.

Thus, $\mathbb{Z}_p$ is an ED, a PID and a UFD. Factorization is $\mathbb{Z}_p$ is simple:

$$a = p^{v_p(a)}e, e \in U(\mathbb{Z}_p) \quad \text{for non-zero } a \in \mathbb{Z}_p.$$

Part 5. Distribution of primes

1. Zeta-function.

Recall that the harmonic series

$$1+\frac{1}{2}+\frac{1}{3}+\cdots=\sum_{n=1}^{\infty}\frac{1}{n}$$

diverges.

Euler introduced the zeta-function in 1737 as

$$\zeta(s)=\sum_{n=1}^{\infty}\frac{1}{n^s},\quad s\in\mathbb{R}.$$

Riemann considered this function for complex values of s.

LEMMA 1. *For every $\varepsilon>0$ zeta-function absolutely and uniformly converges in the half-plane $\mathrm{Re}(s)\geqslant 1+\varepsilon$. For $\mathrm{Re}(s)>1$*

$$\prod_p(1-p^{-s})^{-1}=\zeta(s)$$

where the product is taken over all positive primes.

Proof. Put $s=\sigma+i\tau$ for $\sigma,\tau\in\mathbb{R}$. Then $|n^{-s}|=|n^{-\sigma}||n^{-i\tau}|=|n^{-\sigma}|$ and

$$|\sum_{n=m}^{\infty}n^{-s}|\leqslant\sum_{n=m}^{\infty}n^{-\sigma}\leqslant\int_{m-1}^{\infty}x^{-\sigma}\,dx=(m-1)^{1-\sigma}/(\sigma-1)<1/((m-1)^{\varepsilon}\varepsilon)\to 0$$

when $m\to+\infty$. This proves the first statement.

Now

$$\prod_{p\leqslant m}(1-p^{-s})^{-1}=\prod_{p\leqslant m}(1+p^{-s}+p^{-2s}+\dots)=\sum_{n\leqslant m}n^{-s}+\Delta(m,s)$$

where $\Delta(m,s)$ as a sum of some n^{-s} with $n>m$ is $<\sum_{n>m}n^{-s}<1/(m^{\varepsilon}\varepsilon)\to 0$ when $m\to+\infty$.

Corollary. Zeta-function is analytic for $\mathrm{Re}(s)>1$.

Remark. Zeta-function can be analytically extended to the whole plane. It has a simple pole at $s=1$. It is analytic at all other complex points. It has zeros at $-2,-4,-6,\dots$ and there are no more zeros outside the critical strip $0\leqslant\mathrm{Re}(s)\leqslant 1$.

Riemann conjecture. All zeros of $\zeta(s)$ in the critical strip lie on the vertical line $\mathrm{Re}(s)=1/2$.

With the help of computers this is checked for 3 000 000 zeros of $\zeta(s)$.

In 1837 Dirichlet defined a modified zeta-function for real values of s. His definition involves characters modulo a prime m. Let χ be a homomorphism from the group of units of $\mathbb{Z}/m\mathbb{Z}$ to the multiplicative group of non-zero elements of $\mathbb{C}$, $\chi\colon U(\mathbb{Z}/m\mathbb{Z})\to\mathbb{C}^*$. Since the order of the first group is $m-1$, $\chi(\overline{n})$ is an $(m-1)$st complex root of 1. Both the group $U(\mathbb{Z}/m\mathbb{Z})$ and the group of $(m-1)$st roots of unity are cyclic. Let g be a generator of the first and h be a generator of the second. Then every character is uniquely determined by the image of g, i.e. by number i, $0\leqslant i<m-1$, such that $\chi(g)=h^i$. So there are exactly $m-1$ distinct characters modulo m.

The product of two characters is a character and from the previous description it follows that the characters modulo m form a cyclic group X_m of order $m-1$. The identity element of this group is the character χ_1 for which $\chi_1(g)=1$. One easy property of characters is given by

LEMMA 2.

$$\frac{1}{m-1}\sum_{\chi\in X}\chi(\overline{g}) = \begin{cases} 1, & \text{if } \overline{g}=\overline{1} \\ 0, & \text{otherwise.} \end{cases}$$

Proof.

$$\sum_{\chi\in X}\chi(\overline{1}) = \sum_{\chi\in X} 1 = m-1.$$

If $\overline{g}\neq\overline{1}$, then there is χ' such that $\chi'(\overline{g})\neq 1$. Note that $X = X\chi' = \{\chi\chi' : \chi\in X\}$. Hence

$$\sum_{\chi\in X}\chi(n) = \sum_{\chi\in X}\chi(n)\chi'(n) = \chi'(n)\sum_{\chi\in X}\chi(n),$$

so $\sum_{\chi\in X}\chi(n) = 0$.

For a character $\chi\colon U(\mathbb{Z}/m\mathbb{Z})\to\mathbb{C}^*$ denote by the same notation χ the map $\mathbb{Z}\to\mathbb{C}$:

$$\chi(n) = \begin{cases} \chi(\overline{n}), & \text{if } m\not| n \\ 0, & \text{if } m|n. \end{cases}$$

The map χ is also called a character modulo m.

THEOREM. *Let a and $m\geqslant 2$ be relatively prime integers. Then there are infinitely many primes $p\equiv a \mod m$.*

Some ideas of the proof. We can assume $m>2$. Consider the case m is prime.

For a character χ modulo m Dirichlet defined a so called L-function by

$$L(s,\chi) = \sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}.$$

In particular,

$$L(s,\chi_1) = \sum_{n\geqslant 1, n\not\equiv 0 \bmod m}\frac{1}{n^s} = \sum_{n\geqslant 1}\frac{1}{n^s} - \sum_{n\geqslant 1}\frac{1}{m^s n^s} = (1-1/m^s)\zeta(s).$$

Similar to Lemma 1 we get

$$L(s,\chi) = \prod_p\bigl(1-\frac{\chi(p)}{p^s}\bigr)^{-1}$$

for $\mathrm{Re}(s)>1$.

Let an integer b satisfy $ab\equiv 1 \mod m$. Note that $-\log(1-x) = \sum_{k\geqslant 1}x^k/k$. Then

$$\frac{1}{m-1}\sum_{\chi\in X}\chi(b)\log L(s,\chi) = \frac{1}{m-1}\sum_{\chi\in X}\chi(b)\Bigl(-\sum_p\log\bigl(1-\frac{\chi(p)}{p^s}\bigr)\Bigr)$$

$$= \frac{1}{m-1}\sum_p\sum_{k=1}^{\infty}\sum_{\chi\in X}\chi(b)\chi(p^k)/kp^{sk} = \frac{1}{m-1}\sum_p\sum_{k=1}^{\infty}\Bigl(\sum_{\chi\in X}\chi(bp^k)\Bigr)/kp^{ks}.$$

Note that $bp^k\equiv 1 \mod m$ iff $p^k\equiv a \mod m$. Then Lemma 2 implies that

$$\frac{1}{m-1}\sum_{\chi\in X}\chi(b)\log L(s,\chi) = \sum_{p\equiv a \bmod m}\frac{1}{p^s} + \sum_{k=2}^{\infty}\sum_{p^k\equiv a \bmod m}\frac{1}{kp^{ks}}.$$

One can show that (this isn't easy)

(1) the second term of the RHS remains bounded when $s\to 1$.

(2) if $\chi\neq\chi_1$ then $L(s,\chi)$ remains bounded when $s\to 1$.

Since $\lim_{s\to 1+}L(s,\chi_1) = +\infty$ we conclude that

$$+\infty = \lim_{s\to 1+}\frac{1}{m-1}\sum_{\chi\in X}\chi(b)\log L(s,\chi) = \lim_{s\to 1+}\sum_{p\equiv a \bmod m}\frac{1}{p^s}.$$

Thus, there are infinitely many primes congruent a modulo m.