Università degli Studi di Padova

Facoltà di Scienze MM. FF. NN.

Corso di Laurea in Matematica

Tesi di Laurea

Curve ellittiche su campi finiti: alcune applicazioni alla Crittografia

Candidato: Anna Morra

Relatore: Prof. Alessandro Languasco

Anno Accademico 2003/2004

Indice

Capitolo 1

Introduzione

Le curve ellittiche sono un argomento molto vasto della geometria algebrica che, negli ultimi vent'anni, ha destato un notevole interesse grazie ai suoi utilizzi pratici, soprattutto in ambito crittografico.

La trattazione teorica delle curve ellittiche in questo lavoro sarà finalizzata soprattutto alla descrizione di queste applicazioni. Per tale ragione, si preferirà uno studio algebrico (limitato all'utilizzo dell'equazione di Weierstrass) delle equazioni che descrivono tali curve, tralasciando invece i possibili approfondimenti geometrici.

L'applicazione delle curve ellittiche alla crittografia ha inizio nel 1985, quando viene proposta, indipendentemente, da Neal Koblitz e Victor Miller.

L'idea di Koblitz, che è quella che seguiremo prevalentemente in questa tesi, è riprendere alcuni crittosistemi a chiave pubblica già esistenti, riutilizzandoli sul gruppo costituito dai punti di una curva ellittica su un campo finito con l'operazione di addizione tra punti. Questo permette di poter variare molteplici gruppi su uno stesso campo finito, al variare dei coefficienti dell'equazione che descrive la curva ellittica; un altro vantaggio delle curve ellittiche rispetto ai campi finiti si ha dal punto di vista computazionale, in quanto esse permettono di utilizzare parametri più piccoli pur garantendo lo stesso livello di sicurezza.

Un'ulteriore utilizzo delle curve ellittiche si ha nello studio del problema della fattorizzazione di interi come è stato provato da H. W. Lenstra nel 1987. Sebbene l'efficienza di questo algoritmo non sia tale da renderne possibile un uso pratico, tuttavia, esso ha aperto una nuova strada ricca di possibili sviluppi.

Infine, descriveremo un algoritmo per testare la primalità di un intero, proposto da Goldwasser e Kilian nel 1999. Anche in questo caso, esso è più interessante dal punto di vista teorico che da quello pratico, in quanto si tratta di un metodo probabilistico che non può competere con l'algoritmo deterministico AKS, ideato da Agrawal Kayal e Saxena nel 2002. Tuttavia, presenta anche qualche utilità pratica, poiché, nei casi in cui termina correttamente, esso permette di costruire dei brevi certificati di primalità.

Capitolo 2

Introduzione alle curve ellittiche

Ricordiamo in questo capitolo alcune proprietà fondamentali.

Piano proiettivo

Un piano proiettivo su un campo $\Bbbk$ è l'insieme delle terne $(x, y, z) \neq (0, 0, 0)$ con $x, y, z \in \Bbbk$, quozientato rispetto alla relazione di equivalenza

$$(x, y, z) \sim (x', y', z') \text{ se e solo se } \exists \lambda \in \Bbbk \setminus \{0\} \text{ per cui } (x', y', z') = (\lambda x, \lambda y, \lambda z).$$

Siccome le classi di equivalenza dipendono solo dai rapporti tra le tre coordinate, allora le rappresentiamo nella seguente maniera $(x : y : z)$.

Se $(x : y : z)$ è un punto del piano proiettivo con $z \neq 0$ allora si ha $(x : y : z) = \left(\frac{x}{z} : \frac{y}{z} : 1\right)$. Tutti i punti di questo tipo sono detti punti *finiti* del piano proiettivo (in quanto possiamo metterli in corrispondenza biunivoca con i punti del piano affine, associando al punto proiettivo $(X : Y : 1)$ il punto affine (X, Y)), mentre gli altri, ovvero quelli con $z = 0$, sono detti *punti all'infinito* (in quanto, immaginando di procedere come nel caso precedente, calcolando il limite di $\frac{x}{z}$ e $\frac{y}{z}$ si otterrebbe proprio ∞).

Curva non singolare

Una curva si dice *non singolare* (o *liscia*) se in ogni punto è definita, in modo univoco, la sua tangente.

Un criterio per controllare che una curva sia non singolare è verificare che le derivate parziali della sua equazione implicita non si annullino contemporaneamente in nessuno dei suoi punti.

2.1 Equazioni che descrivono curve ellittiche

Definizione 2.1

Una *curva ellittica* E su un campo $\Bbbk$ è una curva non singolare di grado tre nel piano proiettivo, costituita dall'insieme delle coppie $(X, Y) \in \Bbbk^2$ che soddisfano l'equazione

affine (detta *equazione di Weierstrass generalizzata*)

$$Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{2.1}$$

(dove $a_i \in \mathbb{k}$) piú il punto all'infinito O (mostreremo in seguito che l'omogeneizzata di questa equazione ammette un unico punto all'infinito). L'insieme dei punti appartenenti a questa curva si denota generalmente con $E(\mathbb{k})$.

Come già detto, tale curva dev'essere liscia (cioè nessun punto di $E(\bar{\mathbb{k}})$, dove con $\bar{\mathbb{k}}$ intendiamo la chiusura algebrica di $\mathbb{k}$, deve annullare entrambe le derivate parziali dell'equazione implicita della curva) e quindi il sistema

$$\begin{cases} a_1Y = 3X^2 + 2a_2X + a_4 \\ 2Y + a_1X + a_3 = 0 \end{cases}$$

non deve ammettere soluzioni.

Caratteristica importante delle curve ellittiche

Una curva dotata delle proprietà sopra descritte, sul piano proiettivo, ha una caratteristica che sarà molto importante per i nostri scopi: ogni retta la interseca in esattamente tre punti (se contati con la giusta molteplicità: un punto di tangenza ha molteplicità 2 ed un punto di flesso ha molteplicità 3). La dimostrazione di questa proprietà verrà data al paragrafo 2.2 in cui proveremo la formula che, data una retta passante per due punti (anche coincidenti) di una curva ellittica, ci permette di trovare il terzo punto di intersezione.

Proposizione 2.2 (Punti all'infinito delle curve ellittiche)

Mostriamo che ogni curva ellittica (definita dall'equazione sopra descritta) ha uno e un solo punto all'infinito nel piano proiettivo.

Dimostrazione

Consideriamo l'equazione omogeneizzata dell'equazione (2.1)

$$Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3 \tag{2.2}$$

e osserviamo che, per trovare i punti all'infinito, dobbiamo porre $Z = 0$. Si ottiene immediatamente: $X = 0$. Quindi il punto all'infinito è uno ed uno solo, con coordinate proiettive $(0 : 1 : 0)$. □

D'ora in poi avremo quindi $O = (0 : 1 : 0)$.

2.1.1 Equazione delle curve ellittiche su campi di caratteristica 2

Proposizione 2.3

Se $\text{char}(\mathbb{k}) = 2$, osserviamo che non può mai verificarsi $a_1 = a_3 = 0$ (altrimenti la curva non è liscia). Quindi possono presentarsi due casi:

1. *caso supersingolare* (se $a_1 = 0$ e quindi $a_3 \neq 0$): l'equazione affine della curva si può ridurre, senza perdita di generalità, a

$$Y^2 + a_3 Y = X^3 + a_4 X + a_6; \tag{2.3}$$

2. *caso non supersingolare* (se $a_1 \neq 0$): l'equazione affine della curva si può ridurre, senza perdita di generalità, a

$$Y^2 + XY = X^3 + a_2 X^2 + a_6. \tag{2.4}$$

Dimostrazione

Mostriamo, innanzitutto, che se nell'equazione (2.1) si ha $a_1 = a_3 = 0$, allora la curva non è liscia, dunque non è una curva ellittica. L'equazione che si ottiene è

$$Y^2 = X^3 + a_2 X^2 + a_4 X + a_6.$$

Chiamiamo x uno zero della derivata rispetto a X del membro di destra. Prendiamo $y = \sqrt{x^3 + a_2 x^2 + a_4 x + a_6}$[1]. Si ha che il punto $(x, y) \in E(\bar{\mathbb{k}})$ ed annulla entrambe le derivate parziali dell'equazione implicita.

Analizziamo ora i due casi che si hanno, a seconda che a_1 sia nullo oppure no:

1. Nel caso in cui $a_1 = 0$, l'equazione della curva è

$$Y^2 + a_3 Y = X^3 + a_2 X^2 + a_4 X + a_6.$$

Mostriamo ora che si può supporre, senza perdita di generalità, $a_2 = 0$. Osserviamo, infatti, che applicare una trasformazione lineare alle coordinate (X, Y) non cambia la curva in questione, ma solo il suo rapporto con il sistema di riferimento. Consideriamo quindi la trasformazione

$$(X, Y) \to (X, Y + cX),$$

dove $c^2 = a_2$ dell'equazione (2.1). Come membro di sinistra dell'equazione (2.1), abbiamo quindi

$$Y^2 + c^2 X^2 + a_3 Y + a_3 cX = Y^2 + a_2 X^2 + a_3 Y + a_3 cX.$$

In conclusione l'equazione (2.1) diviene

$$Y^2 + a_3 Y = X^3 + (a_4 - a_3 c)\, X + a_6,$$

che è proprio della forma

$$Y^2 + a_3 Y = X^3 + a_4' X + a_6$$

in cui $a_4' = (a_4 - a_3 c)$.

[1] Siamo certi che x e y esistano nella chiusura algebrica di $\mathbb{k}$.

2. Se $a_1 \neq 0$, applichiamo per prima cosa la trasformazione lineare

$$(X, Y) \to (X - \frac{a_3}{a_1}, Y)$$

all'equazione (2.1). Si ottiene

$$Y^2 + a_1\left(X - \frac{a_3}{a_1}\right)Y + a_3 Y = \left(X - \frac{a_3}{a_1}\right)^3 + a_2\left(X - \frac{a_3}{a_1}\right)^2 + a_4\left(X - \frac{a_3}{a_1}\right) + a_6,$$

da cui

$$Y^2 + a_1XY - a_3Y + a_3Y = X^3 - \frac{a_3^3}{a_1^3} - \frac{a_3}{a_1}X^2 + \frac{a_3^2}{a_1^2}X + a_2X^2 + \frac{a_2a_3^2}{a_1^2} + a_4X - \frac{a_3a_4}{a_1} + a_6$$

e quindi

$$Y^2 + a_1XY = X^3 + \left(a_4 - \frac{a_3}{a_1}\right)X^2 + \left(\frac{a_3^2}{a_1^2} + a_4\right)X + \left(\frac{a_2a_3^2}{a_1^2} - \frac{a_3^3}{a_1^3} - \frac{a_3a_4}{a_1} + a_6\right),$$

che è della forma

$$Y^2 + a_1XY = X^3 + a_2'X^2 + a_4'X + a_6',$$

dove $a_2' = \left(a_4 - \frac{a_3}{a_1}\right)$, $a_4' = \left(\frac{a_3^2}{a_1^2} + a_4\right)$ e $a_6' = \left(\frac{a_2a_3^2}{a_1^2} - \frac{a_3^3}{a_1^3} - \frac{a_3a_4}{a_1} + a_6\right)$. Ora applichiamo la trasformazione

$$(X, Y) \to (a_1^2X, a_1^3Y)$$

ed il membro di sinistra risulta $a_1^6Y^2 + a_1^6XY$; dividiamo ora per a_1^6 ed otteniamo

$$Y^2 + XY.$$

Infine, usando l'applicazione lineare

$$(X, Y) \to (X, Y + a_4)$$

sulla (2.1), ricaviamo l'equazione

$$Y^2 + a_4^2 + XY + a_4X = X^3 + a_2X^2 + a_4X + a_6,$$

che è della forma

$$Y^2 + XY = X^3 + a_2X^2 + a_6',$$

con $a_6' = a_6 - a_4^2$. □

Possiamo ora dare la seguente definizione.

Definizione 2.4

Sui campi di caratteristica 2 esistono due tipi di curve ellittiche:

1. *Curva ellittica supersingolare:* è l'insieme delle coppie $(x, y) \in \Bbbk^2$ che soddisfano l'equazione
$$y^2 + cy = x^3 + ax + b \tag{2.5}$$
dove a, b, $c \in \Bbbk$, $c \neq 0$, (in questo caso non si richiede che $x^3 + ax + b$ non abbia radici multiple, infatti la derivata rispetto a y dell'equazione (2.5) è $c \neq 0$) piú il punto all'infinito O.

2. *Curva ellittica non supersingolare:* è l'insieme delle coppie $(x, y) \in \Bbbk^2$ che soddisfano l'equazione
$$y^2 + xy = x^3 + ax^2 + b \tag{2.6}$$
dove a, $b \in \Bbbk$, $b \neq 0$, piú il punto all'infinito O. (Anche in questo caso non serve dare ulteriori condizioni affinché la curva sia liscia, infatti le derivate parziali dell'equazione (2.6) sono x e $3x^2 + b$, che non si annullano mai contemporaneamente, essendo $b \neq 0$).

2.1.2 Equazione delle curve ellittiche su campi con caratteristica $\neq 2$

Proposizione 2.5

Se $\Bbbk$ ha caratteristica diversa da 2, allora possiamo, senza perdita di generalità, porre: $a_1 = a_3 = 0$ nell'equazione (2.1).

Dimostrazione

Possiamo applicare la trasformazione definita da
$$(X, Y) \to (X, Y - \frac{a_1X + a_3}{2}).$$
Così facendo, il membro di sinistra dell'equazione della curva diventa

$$\begin{aligned}
Y^2 \quad & +\tfrac{a_1^2X^2+a_3^2+2a_1a_3X}{4} \quad -2Y\left(\frac{a_1X + a_3}{2}\right) + a_1XY - \frac{a_1^2X^2}{2} - \frac{a_1a_3X}{2} + a_3Y \\
& \qquad\qquad -\frac{a_1a_3X}{2} - \frac{a_3^2}{2} \\
= Y^2 + \tfrac{a_1^2X^2}{4} + \tfrac{a_3^2}{4} \quad & +\frac{a_1a_3X}{2} - a_1XY - a_3Y + a_1XY - \frac{a_1^2X^2}{2} - \frac{a_1a_3X}{2} + a_3Y \\
& \qquad\qquad -\frac{a_1a_3X}{2} - \frac{a_3^2}{2} \\
= Y^2 - \tfrac{a_1^2X^2}{4} - \tfrac{a_3^2}{4} \quad & -\frac{a_1a_3X}{2}.
\end{aligned}$$

Quindi l'equazione nelle nuove coordinate è

$$Y^2 = X^3 + \left(a_2 - \frac{a_1^2}{4}\right) X^2 + \left(a_4 - \frac{a_1 a_3}{2}\right) X + \left(a_6 - \frac{a_3^2}{4}\right)$$

che, ovviamente, possiamo riscrivere come segue

$$Y^2 = X^3 + b_2 X^2 + b_4 X + b_6$$

($b_i \in \Bbbk$). □

Nel caso caso si abbia un campo di caratteristica 3 si può dare la seguente

Definizione 2.6

Sia char($\Bbbk$) = 3. Una curva ellittica E su $\Bbbk$ è l'insieme delle coppie $(x, y) \in \Bbbk^2$ che soddisfano l'equazione

$$y^2 = x^3 + ax^2 + bx + c \tag{2.7}$$

(dove a, b, $c \in \Bbbk$, e $x^3 + ax^2 + bx + c$ non ha radici multiple su $\Bbbk$) piú il punto all'infinito O.

2.1.3 Equazione delle curve ellittiche su campi con caratteristica $\neq$2, 3

Proposizione 2.7

Se char($\Bbbk$) $\neq 2, 3$ allora l'equazione generale di una curva ellittica si può ridurre a

$$Y^2 = X^3 + aX + b \tag{2.8}$$

e la condizione che la curva sia liscia è equivalente a richiedere che il membro di destra non abbia radici multiple, ossia

$$4a^3 + 27b^2 \neq 0.$$

Dimostrazione

Applicando la trasformazione

$$(X, Y) \to (X - \frac{1}{3}a_2, Y),$$

il membro di destra dell'equazione (2.8) diviene

$$X^3 - a_2 X^2 + \frac{1}{3}a_2^2 X - \frac{1}{27}a_2^3 + a_2 X^2 + \frac{1}{9}a_2^3 - \frac{2}{3}a_2^2 X + a_4 X - \frac{1}{3}a_2 a_4 + a_6$$

e si elide il termine in X^2. Sappiamo che la curva è liscia se e solo se le derivate parziali non si annullano mai contemporaneamente; poiché la derivata parziale dell'equazione implicita

della curva rispetto a Y è $2Y$, essa si annulla solo per $Y = 0$. Consideriamo quindi le coppie $(x, 0)$ tali che x annulla il membro di destra. Perché tale x annulli anche la derivata parziale, essa deve essere una radice multipla del polinomio di destra. Quindi la condizione da porre affinché la curva sia liscia è che $X^3 + aX + b$ non abbia radici multiple, ossia che il suo discriminante sia diverso da 0. Ricordiamo che la formula per il discriminante di un polinomio monico di grado d con radici r_1,...,r_d è

$$\prod_{i \neq j}(r_i - r_j) = (-1)^{\frac{d(d-1)}{2}} \prod_{i<j}(r_i - r_j)^2$$

che, in questo caso, diviene $-(4a^3+27b^2)$. □

Quindi nel caso di caratteristica >3 ricaviamo la seguente definizione:

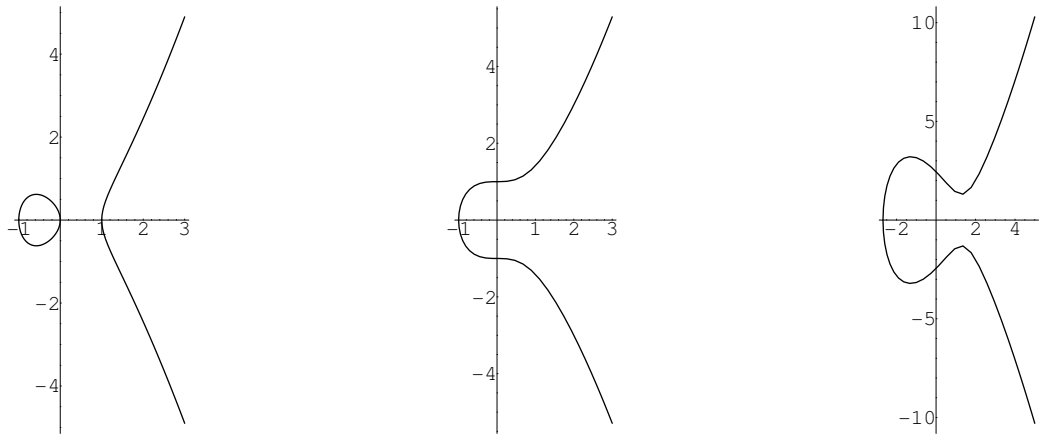
Definizione 2.8

Una curva ellittica E sul campo $\Bbbk$ (char $\Bbbk > 3$) è l'insieme delle coppie $(x, y) \in \Bbbk^2$ che soddisfano l'equazione (detta *equazione di Weierstrass*)

$$y^2 = x^3 + ax + b, \tag{2.9}$$

dove a, $b \in \Bbbk$ e $x^3 + ax + b$ non ha radici multiple (cioè la curva è liscia), piú il punto all'infinito O.

Esempi



Sopra: i grafici delle curve ellittiche sul campo $\mathbb{R}$, date dalle equazioni: $y^2 = x^3 - x$; $y^2 = x^3 + 1$; $y^2 = x^3 - 5x + 6$.

2.2 Struttura di gruppo abeliano additivo

Vogliamo ora dotare E di una struttura di gruppo abeliano. Definiamo un'operazione di somma tra i punti, in modo che goda delle seguenti proprietà:

1. O (il punto all'infinito) è l'elemento neutro di tale gruppo ($-O = O$ e $P + O = O + P = P$);

2. se $P \neq O$, allora $-P$ è l'unico altro punto della curva ($\neq O$) che ha la stessa ascissa di P;

3. se P, Q hanno ascisse diverse, allora $P + Q$ si ottiene tracciando la retta ℓ che congiunge P e Q, trovando quindi l'unica altra intersezione R (si vedano i paragrafi successivi per il calcolo del terzo punto di intersezione e, quindi, la dimostrazione che esso esiste ed è unico) di tale retta con la curva ellittica E e definendo $P+Q = -R$;

4. se $Q = -P$ allora $P + Q = O$;

5. se $Q = P$ allora si traccia la retta ℓ tangente alla curva nel punto P, si trova l'unico altro punto di intersezione R di ℓ con E e si definisce $P + Q = 2P = -R$.

La dimostrazione che l'insieme dei punti di una curva ellittica, dotato di questa operazione di somma, è un gruppo abeliano, si può affrontare in varie maniere, o dal punto di vista algebrico, o da quello dell'analisi complessa, oppure dal punto di vista della geometria proiettiva, che è quello che utilizzeremo noi.

Proposizione 2.9

$(E(\mathbb{R}), +)$ è gruppo abeliano.

Dimostrazione

Per dimostrare che E è un gruppo abeliano rispetto alla somma sopra definita bisogna mostrare che:

1. l'operazione di somma è interna al gruppo;

2. vale la proprietà associativa;

3. esiste l'elemento neutro;

4. ogni elemento ha inverso;

5. vale la proprietà commutativa.

Di questi punti, solo il 2 presenta qualche difficoltà. Gli altri quattro si dimostrano facilmente osservando che, per costruzione, la somma di due punti è un altro punto della curva (punto 1), O è l'elemento neutro per la definizione di somma che abbiamo dato (punto 3) e sappiamo calcolare l'opposto di ogni punto (punto 4). Infine, sempre dalla definizione di somma, osserviamo che l'ordine con cui prendiamo i due punti da sommare non ha alcuna importanza (punto 5).

Per dimostrare il punto 2, utilizziamo una proposizione della geometria proiettiva (per la dimostrazione si veda Washington, [15], pagg. 20-32).

Proposizione 2.10

Siano $\ell_1,\ \ell_2,\ \ell_3$ tre rette che intersecano una cubica in nove punti: P_1, ..., P_9 (contati con la loro molteplicità) e siano $\ell'_1,\ \ell'_2,\ \ell'_3$ tre rette che intersecano la cubica nei punti Q_1, ..., Q_9. Se $P_i = Q_i$ per $i = 1, ..., 8$ allora $P_9 = Q_9$.

Proviamo adesso 2. Vogliamo mostrare che

$$(A + B) + C = A + (B + C).$$

Consideriamo le tre rette:

1. ℓ_1 che interseca la curva ellittica nei punti A, B e $-(A + B)$;
2. ℓ_2 che interseca la curva nei punti O, C e $-C$;
3. ℓ_3 che interseca la curva nei punti $-A$, $-(B + C)$ e $A + (B + C)$.

E le tre rette:

1. ℓ'_1 che interseca la curva nei punti B, C e $-(B + C)$;
2. ℓ'_2 che interseca la curva nei punti O, A e $-A$;
3. ℓ'_3 che interseca la curva nei punti $-C$, $-(A + B)$ e $(A + B) + C$.

Osservando che otto dei punti di intersezione di $\ell_1,\ \ell_2$ e ℓ_3 con la curva ellittica coincidono con otto dei punti di intersezione di $\ell'_1,\ \ell'_2,\ \ell'_3$ con tale curva ed applicando la proposizione precedente, si ottiene

$$(A + B) + C = A + (B + C).$$

□

Analizziamo ora i vari casi, a seconda della caratteristica del campo, e troviamo le formule per calcolare l'opposto e la somma di due punti.

2.2.1 Caratteristica 2 - Curva supersingolare

Proposizione 2.11 (Opposto)

Data la curva E, definita dall'equazione (2.5), abbiamo che, se P è il punto di coordinate (x, y), allora $-P = (x, y + c)$.

Dimostrazione

Vogliamo trovare il secondo punto $\neq O$ che abbia ascissa x. Si verifica che se la coppia (x, y) soddisfa l'equazione (2.5), anche la coppia $(x, y + c)$ la soddisfa. Infatti, il lato destro dell'uguaglianza resta invariato, mentre il lato sinistro (calcolando in caratteristica 2) è

$$(y + c)^2 + c(y + c) = y^2 + c^2 + cy + c^2 = y^2 + cy$$

che è uguale al lato di sinistra dell'equazione (2.5). □

Proposizione 2.12 (Somma di due punti)

Siano $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, con $P \neq -Q$ (altrimenti $P + Q = O$). Si possono avere due casi:

1. se $P \neq Q$ allora le coordinate di $R = P + Q$ sono
$$\begin{cases} x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + x_1 + x_2 \\ y_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)(x_1 + x_3) + y_1 + c; \end{cases}$$
2. se $P = Q$ allora le coordinate di $R = P + Q$ sono
$$\begin{cases} x_3 = \frac{x_1^4+a^2}{c^2} \\ y_3 = \left(\frac{x_1^2+a}{c}\right)(x_1 + x_3) + y_1 + c. \end{cases}$$

Dimostrazione

Analizziamo separatamente i due casi che possono presentarsi:

1. $P \neq Q$: la retta ℓ passante per P e Q è data dall'equazione
$$y = \alpha x + \beta,$$
con $\alpha = \frac{y_2-y_1}{x_2-x_1} = \frac{y_1+y_2}{x_1+x_2}$ (possiamo dividere per $(x_2 - x_1)$ perché sappiamo che $P \neq \pm Q$ e quindi i due punti non hanno la stessa ascissa), $\beta = y_1 - \alpha x_1 = y_1 + \alpha x_1$. Sostituiamo dunque $\alpha x + \beta$ al posto di y nell'equazione della curva ed otteniamo
$$(\alpha x + \beta)^2 + c(\alpha x + \beta) = x^3 + ax + b.$$
Ricordiamo che la somma degli zeri di un polinomio di grado n è uguale all'opposto del coefficiente del termine di grado $(n - 1)$; in questo caso l'opposto del coefficiente del termine di secondo grado è α^2; dunque si ricava che l'ascissa di R (terza intersezione della retta con la curva) è
$$x_3 = \alpha^2 - x_1 - x_2 = \alpha^2 + x_1 + x_2 = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)^2 + x_1 + x_2.$$
Svolgendo i calcoli otteniamo quindi che
$$y_3 = \alpha x_3 + \beta + c = \alpha(x_1 + x_3) + y_1 + c = \left(\frac{y_1 + y_2}{x_1 + x_2}\right)(x_1 + x_3) + y_1 + c.$$
2. Se $P = Q$, la retta ℓ tangente alla curva nel punto P è data dall'equazione $y = \alpha x + \beta$, dove: $\alpha = \frac{dy}{dx} = \frac{3x_1^2+a}{2y_1+c} = \frac{x_1^2+a}{c}$, $\beta = y_1 - \alpha x_1 = y_1 + \alpha x_1$. Procedendo come nel caso precedente, ricaviamo
$$\begin{cases} x_3 = \alpha^2 + 2x_1 = \alpha^2 = \frac{x_1^4+a^2}{c^2} \\ y_3 = \alpha x_3 + \beta + c = \alpha(x_1 + x_3) + y_1 + c = \left(\frac{x_1^2+a}{c}\right)(x_1 + x_3) + y_1 + c. \end{cases}$$

□

2.2.2 Caratteristica 2 - Curva non supersingolare

Proposizione 2.13 (Opposto)

Data la curva E, definita dall'equazione (2.6), abbiamo che, se P è il punto di coordinate (x, y), allora $-P = (x, y + x)$.

Dimostrazione

Cerchiamo l'unico altro punto $\neq O$ della curva, con ascissa x. La coppia (x, y) soddisfa l'equazione (2.6). Calcoliamo la stessa equazione nel punto $(x, y + x)$. Il lato di destra rimane inalterato, mentre il termine di sinistra diviene

$$(y + x)^2 + x(y + x) = y^2 + x^2 + xy + x^2 = y^2 + xy,$$

che è uguale al lato di sinistra dell'equazione (2.6). □

Proposizione 2.14 (Somma di due punti)

Siano $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, con $P \neq -Q$ (altrimenti $P + Q = O$). Si possono avere due casi:

1. se $P \neq Q$ allora le coordinate di $R = P + Q$ sono

$$\begin{cases} x_3 = \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a \\ y_3 = \frac{y_1+y_2}{x_1+x_2}(x_1 + x_3) + x_3 + y_1; \end{cases}$$

2. se $P = Q$ allora le coordinate di $R = P + Q$ sono

$$\begin{cases} x_3 = x_1^2 + \frac{b}{x_1^2} \\ y_3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3. \end{cases}$$

Dimostrazione

Analizziamo separatamente i due casi che possono presentarsi:

1. Se $P \neq Q$, la retta ℓ passante per P e Q è data dall'equazione $y = \alpha x + \beta$, con $\alpha = \frac{y_2-y_1}{x_2-x_1} = \frac{y_1+y_2}{x_1+x_2}$, $\beta = y_1 - \alpha x_1 = y_1 + \alpha x_1$. Sostituiamo dunque $\alpha x + \beta$ al posto di y nell'equazione della curva ed otteniamo che

$$(\alpha x + \beta)^2 + x(\alpha x + \beta) = x^3 + ax^2 + b.$$

In questo caso l'opposto del coefficiente del termine di secondo grado è

$$\alpha^2 + \alpha - a = \alpha^2 + \alpha + a$$

e quindi abbiamo

$$\begin{aligned} x_3 &= \alpha^2 + \alpha + a - x_1 - x_2 \\ &= \left(\frac{y_1+y_2}{x_1+x_2}\right)^2 + \frac{y_1+y_2}{x_1+x_2} + x_1 + x_2 + a \\ y_3 &= \alpha x_3 + \beta + x_3 = \alpha(x_1+x_3) + y_1 + x_3 = \frac{y_1+y_2}{x_1+x_2}(x_1+x_3) + x_3 + y_1. \end{aligned}$$

2. Se $P = Q$, la retta ℓ tangente alla curva nel punto P è data dall'equazione $y = \alpha x + \beta$, dove: $\alpha = \frac{dy}{dx} = \frac{x_1^2+y_1}{x_1} = x_1 + \frac{y_1}{x_1}$, $\beta = y_1 - \alpha x_1 = y_1 + \alpha x_1 = y_1 + x_1\left(x_1 + \frac{y_1}{x_1}\right) = x_1^2$. Procedendo come nel paragrafo precedente, si ricava

$$\begin{aligned} x_3 &= \alpha^2 + \alpha + a + 2x_1 = \alpha^2 + \alpha + a = \frac{x_1^4 + y_1^2}{x_1^2} + \frac{x_1^2 + y_1}{x_1} + a \\ &= \frac{x_1^4 + (y_1^2 + x_1^3 + x_1 y_1 + a x_1^2)}{x_1^2} = x_1^2 + \frac{b}{x_1^2}, \\ y_3 &= \alpha x_3 + \beta + x_3 = x_1^2 + \left(x_1 + \frac{y_1}{x_1}\right) x_3 + x_3. \end{aligned}$$

2.2.3 Caratteristica 3

Proposizione 2.15 (Opposto)

Data la curva E, definita dall'equazione (2.7), abbiamo che, se P è il punto di coordinate (x, y), allora $-P = (x, -y)$.

Dimostrazione

Si osserva immediatamente che sostituendo $-y$ al posto di y nell'equazione (2.7) entrambi i lati dell'uguaglianza restano invariati. □

Proposizione 2.16 (Somma di due punti)

Siano $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, con $P \neq -Q$ (altrimenti $P + Q = O$). Si possono avere due casi:

1. se $P \neq Q$ allora le coordinate di $R = P + Q$ sono

$$\begin{cases} x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - a - x_1 - x_2 \\ y_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3) - y_1; \end{cases}$$

2. se $P = Q$ allora le coordinate di $R = P + Q$ sono

$$\begin{cases} x_3 = \left(\frac{2ax_1+b}{2y_1}\right)^2 - a - 2x_1 \\ y_3 = \left(\frac{2ax_1+b}{2y_1}\right)(x_1 - x_3) - y_1. \end{cases}$$

Dimostrazione

Distinguiamo i due casi possibili:

1. $P \neq \pm Q$: la retta passante per P e Q ha equazione $y = \alpha x + \beta$, dove $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$, $\beta = y_1 - \alpha x_1$. Sostituendo $\alpha x + \beta$ al posto di y nell'equazione della curva si ottiene

$$(\alpha x + \beta)^2 = x^3 + ax^2 + bx + c$$

e quindi il termine di secondo grado è $(a - \alpha^2)$. Di conseguenza

$$\begin{cases} x_3 = \alpha^2 - a - x_1 - x_2 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - a - x_1 - x_2 \\ y_3 = -(\alpha x_3 + \beta) = -\alpha x_3 - y_1 + \alpha x_1 = \alpha(x_1 - x_3) - y_1 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3) - y_1. \end{cases}$$

2. $P = Q$: si procede come al punto precedente ma con $\alpha = \frac{dy}{dx} = \frac{3x_1^2 + 2ax_1 + b}{2y_1} = \frac{2ax_1 + b}{2y_1}$ (ricordiamo che siamo in caratteristica 3) e si ottiene

$$\begin{cases} x_3 = \alpha^2 - a - 2x_1 = \left(\frac{2ax_1 + b}{2y_1}\right)^2 - a - 2x_1 \\ y_3 = \alpha(x_1 - x_3) - y_1 = \left(\frac{2ax_1 + b}{2y_1}\right)(x_1 - x_3) - y_1. \end{cases}$$

2.2.4 Caratteristica >3

Proposizione 2.17 (Opposto)

Data la curva E, definita dall'equazione (2.9), abbiamo che, se P è il punto di coordinate (x, y), allora $-P = (x, -y)$.

Dimostrazione

Si osserva immediatamente che sostituendo $-y$ al posto di y nell'equazione (2.9) entrambi i lati dell'uguaglianza restano invariati. □

Proposizione 2.18 (Somma di due punti)

Siano $P = (x_1, y_1)$ e $Q = (x_2, y_2)$, con $P \neq -Q$ (altrimenti $P + Q = O$). Si possono avere due casi:

1. se $P \neq Q$ allora le coordinate di $R = P + Q$ sono

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = -y_1 + \frac{(y_2 - y_1)(x_1 - x_3)}{x_2 - x_1}; \end{cases}$$

2. se $P = Q$ allora le coordinate di $R = P + Q$ sono

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3). \end{cases}$$

Dimostrazione

Bisogna distinguere i due casi:

1. $P = (x_1, y_1)$, $Q = (x_2, y_2)$, con $x_1 \neq x_2$: la retta ℓ passante per P e Q sarà del tipo $y = \alpha x + \beta$, con $\alpha = \frac{y_2 - y_1}{x_2 - x_1}$, $\beta = y_1 - \alpha x_1$. Quindi i punti della retta saranno $(x, \alpha x + \beta)$ e le ascisse dei punti appartenenti all'intersezione tra la retta ℓ e la curva E saranno gli zeri dell'equazione

$$(\alpha x + \beta)^2 = x^3 + ax + b.$$

Siccome la somma degli zeri di un polinomio di grado n è uguale all'opposto del coefficiente del termine di grado $(n-1)$, si ricava che l'ascissa di R (terza intersezione della retta con la curva) è

$$x_3 = \alpha^2 - x_1 - x_2 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2,$$

da cui, sostituendo nell'equazione della retta otteniamo

$$y_3 = -(\alpha x_3 + \beta) = -(\alpha x_3 + y_1 - \alpha x_1) = \alpha(x_1 - x_3) - y_1 = -y_1 + \frac{(y_2 - y_1)(x_1 - x_3)}{x_2 - x_1}.$$

2. Infine, se $P = Q$ si procede come al punto precedente ma con $\alpha = \frac{dy}{dx} = \frac{3x_1^2 + a}{2y_1}$. Ricordandoci che $x_1 = x_2$, si ricava

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3). \end{cases}$$

□

2.2.5 Multipli dei punti

Definizione 2.19

Sia P un punto su una curva ellittica E. Sia k un intero. Definiamo kP nella maniera seguente:

1. $kP = O$ se $k = 0$;
2. $kP = P + P + ... + P$ (k volte), se $k > 0$;
3. $kP = (-P) + (-P) + ... + (-P)$ ($|k|$ volte), se $k < 0$.

Per diminuire il numero dei calcoli da svolgere, si può utilizzare il seguente algoritmo (dei *raddoppiamenti successivi)*, che ci permette di calcolare kP in tempo $O(\log k)$

1. si pongono $a \leftarrow k$[2], $B \leftarrow O$, $C \leftarrow P$;
2. se a è pari, $a \leftarrow \frac{a}{2}$, $C \leftarrow 2C$, B invariato;
3. se a è dispari, $a \leftarrow a-1$, $B \leftarrow B+C$, C invariato;
4. se $a \neq 0$ si ritorna al punto 2;
5. si restituisce come risultato B.

2.3 Curve ellittiche sui campi finiti

2.3.1 Numero di punti di una curva ellittica su un campo finito

Sia $\mathbb{k}$ un campo finito $\mathbb{F}_q$, $q = p^r$, p primo. Sia E una curva ellittica su $\mathbb{k}$. Si nota facilmente che E può avere al piú $2q+1$ punti (basta osservare che, per ognuna delle q scelte possibili per la x, esistono al più due y che soddisfano l'equazione; così si ottengono al piú $2q$ punti, a cui va aggiunto il punto all'infinito O).

Tuttavia, siccome solo metà degli elementi di $\mathbb{F}_q^*$ ha radice quadrata, siamo portati a pensare che, in effetti, E abbia "circa" q punti.

Sia χ il *simbolo di Legendre-Jacobi* di $\mathbb{F}_q$, cioè quella funzione

$$\chi : \mathbb{F}_q \to \{0, 1, -1\}$$

tale che

$$\chi(x) = \begin{cases} 0 & \text{se } x \equiv 0 \pmod{p} \\ +1 & \text{se } x \text{ ha radice quadrata su } \mathbb{F}_q \\ -1 & \text{se } x \text{ non ha radice quadrata su } \mathbb{F}_q. \end{cases}$$

Ricordiamo che, generalmente, il simbolo di Legendre su un campo di caratteristica p, p primo, si indica con $(x \mid p)$, dove

$$\left(\frac{x}{p}\right) = \begin{cases} 0 & \text{se } x \equiv 0 \pmod{p} \\ +1 & \text{se } x \text{ ha radice quadrata } \pmod{p} \\ -1 & \text{se } x \text{ non ha radice quadrata } \pmod{p}, \end{cases}$$

mentre il simbolo di Legendre-Jacobi su un campo di caratteristica n qualunque è:

$$\left(\frac{x}{n}\right)_J = \begin{cases} 0 & \text{se } \mathrm{mcd}(x,n) > 1 \\ \left(\frac{x}{p_1}\right)\left(\frac{x}{p_2}\right)...\left(\frac{x}{p_k}\right) & \text{se } \mathrm{mcd}(x,n) = 1 \text{ e } n = p_1 p_2 ... p_k. \end{cases}$$

E' immediato osservare che il numero di soluzioni dell'equazione $y^2 = u$ su $\mathbb{F}_q$ è $1+\chi(u)$. Quindi possiamo calcolare il numero di punti della curva ellittica E su $\mathbb{F}_q$ è dato da

$$\#\ E(\mathbb{F}_q) = 1 + \sum_{x \in \mathbb{F}_q} \big(1 + \chi(x^3 + ax + b)\big) = q + 1 + \sum_{x \in \mathbb{F}_q} \chi(x^3 + ax + b).$$

[2]Il simbolo $\leftarrow$ indica un'assegnazione.

Per calcolare il risultato della sommatoria, trattando i valori assunti da $(x^3 + ax + b)$ come valori casuali, e osservando che gli unici valori non nulli assunti da χ sono $+1$ e -1, ricordiamo il *cammino aleatorio:* si lancia una moneta n volte e si fa un passo avanti o indietro a seconda che esca testa o croce. Il calcolo delle probabilità ci dice che il cammino percorso dopo n lanci è circa $\sqrt{n}$ (si veda Koblitz, [6], pagg. 157-158).

Tale tipo di ragionamento può essere formalizzato e conduce a provare che $\sum_{x \in \mathbb{F}_q} \chi(x^3 + ax + b) \leq 2\sqrt{q}$. Questo è il **teorema di Hasse** (si veda Koblitz [6], pag. 158) di cui riportiamo l'enunciato.

Teorema 2.20 (Teorema di Hasse)

Sia $\mathbb{F}_q$ campo finito con $q = p^r$, p primo. Sia E una curva ellittica su $\mathbb{F}_q$. Allora

$$| \# E(\mathbb{F}_q) - (q+1) | \leq 2\sqrt{q}.$$

2.3.2 Struttura del gruppo abeliano dei punti di una curva ellittica su un campo finito

Sia G il gruppo abeliano dei punti di una curva ellittica su un campo finito. Si può provare che G è isomorfo al prodotto di al piú due gruppi ciclici

$$G \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2},$$

dove $d_2 \mid d_1$. ($d_2 = 1$ se G è ciclico). (cfr. Koblitz [6], pag. 158).

Nel caso in cui si lavori con una curva ellittica E su un anello del tipo $\mathbb{Z}_{n_1 n_2}$, con n_1, n_2 dispari e $\mathrm{mcd}(n_1, n_2) = 1$. Si può dimostrare che

$$E(\mathbb{Z}_{n_1 n_2}) \cong E(\mathbb{Z}_{n_1}) \times E(\mathbb{Z}_{n_2}).$$

(Per la dimostrazione si veda Washington, [15], pagg. 65-66).

Capitolo 3

Applicazione delle curve ellittiche alla crittografia

3.1 Crittografia. Cenni introduttivi.

3.1.1 Introduzione storica

La crittografia, ovvero l'arte di cifrare i messaggi in modo tale che, anche se intercettati da terzi, risultino inintelleggibili, ha origini molto antiche, si pensi per esempio alla *scìtala lacedemone* (che si suppone risalga al 900 a.C.) o al metodo di trasposizione utilizzato da Giulio Cesare. In seguito, questa scienza ha continuato ad avere molti utilizzi, soprattutto in campo politico e bellico.

Tuttavia, i metodi utilizzati fino agli anni '70 del secolo scorso avevano dei grossi difetti:

1. *Problema dello scambio della chiave*: tutti questi metodi erano basati sull'utilizzo di una *chiave segreta* necessaria per codificare e decodificare il messaggio. Se questa cadeva in mano a terzi, la segretezza e l'affidabilità del metodo erano perse. Perciò era necessario avere un canale sicuro per lo scambio della chiave; chiaramente ciò costituiva un problema, anche perché, in presenza di un canale sicuro, veniva a cadere l'utilità del metodo crittografico stesso.

2. *Necessità della segretezza del metodo* e degli eventuali parametri utilizzati: se un intruso veniva a sapere il crittosistema utilizzato o altre informazioni sulla cifratura, era facilitato nell'impresa di decifrare il messaggio.

3. *Lunghezza della chiave per ottenere un sistema "perfetto"*: si chiama *crittosistema perfetto* un metodo crittografico tale che il testo cifrato non fornisca alcuna informazione sul messaggio originario, tranne, al piú, la sua lunghezza (ad esempio il cifrario di Vernam). Nel 1948, Shannon ha dimostrato che, per ottenere questo, la chiave dev'essere lunga almeno quanto il testo da codificare e dev'essere utilizzata un'unica volta. Ciò non è assolutamente economico né dal punto di vista computazionale né, soprattutto, per quanto riguarda lo scambio della chiave.

Proprio per queste ragioni, questi metodi prendono il nome di *crittosistemi a chiave segreta* (o *crittosistemi classici*) e non soddisfano il *principio di Kerchoffs,* il quale afferma che la sicurezza di un crittosistema deve dipendere dal tenere celato il minor numero possibile di informazioni.

Questa situazione è stata drasticamente cambiata nel 1976 quando *Diffie* ed *Hellman* hanno proposto il primo metodo crittografico a *chiave pubblica* (si veda: Diffie-Hellman [3]). In realtà non si trattava di un vero e proprio crittosistema, ma semplicemente di un algoritmo per lo scambio sicuro di una chiave (da utilizzare poi con un crittosistema classico).

Questo sistema, come molti altri in seguito, si basava su un problema matematico, il problema del *logaritmo discreto.* Indicato con $\mathbb{Z}_p^*$ l'insieme degli elementi invertibili della classe residuale $\mathbb{Z}_p$ [(1)], il problema del logaritmo discreto si può enunciare come segue:

fissati un primo p sufficientemente grande ed un generatore g di $\mathbb{Z}_p^*$,
dato un elemento $a = g^x \in \mathbb{Z}_p^*$, ricavare x, cioè il logaritmo in base g di a.

Attualmente, questo problema non è risolvibile con complessità polinomiale nel numero delle cifre di a, ma tutt'al piú subesponenziale (ossia $O(\exp(\varepsilon \log a))$ per ogni $\varepsilon > 0$). Un esempio di algoritmo con complessità subesponenziale è l'*index calculus* (si veda l'Osservazione al paragrafo 3.2.1).

3.1.2 Metodo di Diffie-Hellman per lo scambio delle chiavi

Due utenti, Alice e Bob, devono costruire e scambiare una chiave per un crittosistema classico.

1. Di comune accordo fissano un primo sufficientemente grande p e un generatore g di $\mathbb{Z}_p^*$. Entrambe queste informazioni sono pubbliche.
2. Alice sceglie casualmente un elemento $a \in \{2, ..., p-1\}$ e calcola $A = g^a$. Alice rende pubblico A.
3. Bob sceglie casualmente un elemento $b \in \{2, ..., p-1\}$ e calcola $B = g^b$. Bob rende pubblico B.
4. Entrambi calcolano $C = g^{ab} = (g^a)^b = \left(g^b\right)^a$, che sarà la chiave segreta del loro crittosistema a chiave segreta.

Si osservi che nella comunicazione sono stati trasmessi solo A e B. Un intruso, Carlo, che voglia conoscere C, dovrebbe saper risolvere il *problema di Diffie-Hellman:*

dati p primo e $g \in \mathbb{Z}_p^*$ generatore, g^a e g^b, ricavare g^{ab}.

Di sicuro, se Carlo sa risolvere il problema del logaritmo discreto, egli è anche in grado di risolvere il problema di Diffie-Hellman. Il viceversa non è stato provato, tuttavia si

(1) In questa tesi utilizzeremo sempre $\mathbb{Z}_p$ per indicare l'insieme delle classi residuali modulo p (ovvero $\mathbb{Z}/p\mathbb{Z}$) e *non* l'anello degli interi $p-$adici.

congettura che questi due problemi siano equivalenti.

Introduciamo ora altri due crittosistemi a chiave pubblica, la cui conoscenza ci sarà utile in seguito.

3.1.3 Crittosistema di Massey - Omura

Questo crittosistema si basa sull'algoritmo del doppio lucchetto.

3.1.3.1 Algoritmo del doppio lucchetto

Due utenti, Alice e Bob, vogliono comunicare segretamente.

Si suppone che ciascuno possieda un lucchetto infrangibile e inviolabile che solo il proprietario può aprire; chiamiamoli rispettivamente A e B. Si suppone anche che i due lucchetti godano della "proprietà commutativa" cioè l'ordine in cui si applicano (o si aprono) è indifferente.

Allora, se Alice vuole mandare il messaggio M a Bob, lo chiude col suo lucchetto, A, ottenendo $A(M)$. Bob, ricevuto questo, non tenta nemmeno di aprire il lucchetto (il che peraltro è, per definizione, impossibile) e aggiunge ad $A(M)$ il suo lucchetto B; ottiene quindi $B(A(M))$ che rispedisce ad Alice. Ella può aprire il suo lucchetto, ottenendo $B(M)$ che rispedisce a Bob. Infine, Bob apre il lucchetto B e legge il messaggio M.

L'efficienza di questo algoritmo sta nel fatto che in tutti i passaggi ciò che viene spedito è protetto da almeno uno dei lucchetti e quindi è inviolabile da terzi. L'unico difetto sta nel rischio che un terzo utente, Carlo, possa intercettare il primo messaggio, quando Alice invia $A(M)$ a Bob, e rispondere lui, inviando ad Alice $C(A(M))$, dove C è il suo lucchetto, che Alice non può distinguere da quello di Bob. Il rischio è quindi che Alice, sentendosi sicura del lucchetto C, apra il proprio, rispondendo a Carlo, e non a Bob come crede, $C(M)$, svelando a Carlo il messaggio M.

3.1.3.2 Crittosistema di Massey - Omura. Algoritmo

1. Tutti gli utenti si accordano su un primo p sufficientemente grande.
2. Ogni utente sceglie un elemento $e \in \mathbb{Z}_{p-1}^*$ e calcola $d \equiv e^{-1} (\mathrm{mod}\ (p-1))$.

Sia e che d sono tenuti segreti.

A questo punto, se Alice vuole inviare il messaggio $M \in \mathbb{Z}_p$ a Bob, i due utenti agiscono nella seguente maniera:

1. Alice calcola $A = M^{e_A} (\mathrm{mod}\ p)$ e lo invia a Bob;
2. Bob calcola $B = A^{e_B} = M^{e_A e_B} (\mathrm{mod}\ p)$ e lo rimanda ad Alice;
3. Alice calcola $C = B^{d_A} = B^{e_A^{-1}} = M^{e_A e_B d_A} = M^{e_A e_B e_A^{-1}} = M^{e_B} (\mathrm{mod}\ p)$ e lo invia a Bob. (Alice ha tolto il suo lucchetto);
4. A questo punto Bob può calcolare $D = C^{d_B} = C^{e_B^{-1}} = M^{e_B e_B^{-1}} = M \pmod{p}$.

Questo crittosistema ha gli stessi pregi e difetti dell'algoritmo del doppio lucchetto. Per ovviare il rischio di un'intrusione, è necessario aggiungere all'algoritmo un sistema di firma digitale (ossia un metodo che consenta di autenticare l'identità del mittente mediante la funzione di decifratura di un crittosistema a chiave pubblica).

3.1.4 Crittosistema di ElGamal

Questo è un altro crittosistema che utilizza il problema del logaritmo discreto.

1. Tutti gli utenti si accordano su un primo abbastanza grande p ed un generatore g di $\mathbb{Z}_p^*$;
2. Ogni utente sceglie la propria *chiave privata* $x \in \mathbb{Z}_p^*$ e rende pubblico g^x .

Supponiamo che ci siano due utenti, Alice e Bob, che vogliano comunicare. Alice ha chiave privata x e chiave pubblica $a = g^x$; Bob ha chiave privata y e chiave pubblica $b = g^y$. Se Alice vuole inviare a Bob il messaggio M:

1. Alice sceglie a caso un elemento $k \in \mathbb{Z}_p^*$;
2. Alice invia a Bob la coppia $(g^k,\ Mb^k)$;
3. Bob calcola $g^{ky} = b^k$ e quindi ricava $M = Mb^k g^{-ky}$.

3.2 Applicazione delle curve ellittiche alla crittografia

L'applicazione delle curve ellittiche alla crittografia è stata proposta indipendentemente nel 1985 da Neal Koblitz e da Victor Miller. I vantaggi che le curve ellittiche presentano rispetto ai campi finiti sono:

1. il molteplice numero di gruppi abeliani (costituiti dai punti di una curva) che si può costruire su uno stesso campo finito;
2. il fatto che, a differenza dei campi finiti, non esistono algoritmi subesponenziali per risolvere il problema del logaritmo discreto sulle curve ellittiche non supersingolari;
3. il fatto che richiedono chiavi piú corte per garantire la stessa sicurezza[(2)].

3.2.1 DLP e ECDLP

Le curve ellittiche permettono di formulare un problema analogo a quello del logaritmo discreto su un campo finito (**DLP**, Discrete Logaritm Problem).

[(2)]Per esempio è stato stimato che una chiave a 4096 bit per l'RSA garantisce la stessa sicurezza di una chiave a 313 bit con un crittosistema basato sulle curve ellittiche, e questo è più vantaggioso non solo per la minore memoria richiesta, ma anche per il minor tempo necessario per la creazione della chiave (si veda Washington [15] pag. 159).

Problema

Siano dati una curva ellittica E su $\mathbb{F}_q$ e un punto $B \in E$. Il *"problema del logaritmo discreto* su E in base B" (**ECDLP**, Elliptic Curve Discrete Logaritm Problem) è:

$$\text{dato } P \in E \text{ trovare, se esiste, } x \in \mathbb{Z} \text{ tale che } xB = P.$$

Osservazione

Sui campi finiti, esiste un algoritmo (detto *"index calculus"*) che, tramite opportune pre-computazioni, permette di calcolare il logaritmo discreto con complessità subesponenziale. Questo è possibile perchè sui campi finiti esistono due operazioni: somma e prodotto. Al contrario, sulle curve ellittiche, che hanno solamente la struttura additiva, questo tipo di calcolo indicizzato non è possibile, conseguentemente le operazioni risultano piú laboriose.

Concludendo, la sicurezza dei crittosistemi basati sulle curve ellittiche si basa sulla non esistenza, finora, di algoritmi efficienti per risolvere il problema dell'ECDLP, nel caso generale.

Esistono tuttavia alcuni tipi di curve ellittiche sulle quali il problema del logaritmo discreto è piú facilmente risolubile.

3.2.2 Attacchi al logaritmo discreto sulle curve ellittiche

3.2.2.1 Menezes, Okamoto e Vanstone

Nel 1993, Menezes, Okamoto e Vanstone (si veda Menezes-Okamoto-Vanstone, [11]) hanno elaborato un metodo per trasformare il problema su $E(\mathbb{F}_q)$ in un problema su $\mathbb{F}^*_{q^k}$. Tuttavia questa riduzione risulta vantaggiosa e permette di passare ad un tempo subesponenziale solamente nel caso in cui k sia piccolo, e questo si verifica essenzialmente per le curve ellittiche supersingolari (cioè quelle curve E su $\mathbb{F}_q$ tali che $\#E(\mathbb{F}_q) \equiv 1 \pmod{p}$). Infatti, per queste si ha, generalmente, $k = 2$, mentre per quasi tutte le altre non si riescono ad ottenere miglioramenti significativi.

L'esistenza di questo metodo è particolarmente svantaggiosa dal punto di vista crittografico, in quanto costringe a scartare le curve supersingolari, che invece permetterebbero maggiore rapidità di calcolo[(3)].

3.2.2.2 Algoritmo di Silver-Pohlig-Hellman

Definizione 3.1

Sia T un numero reale positivo. Un intero si dice *T-liscio* se non è divisibile da nessun primo maggiore di T.

[(3)]Infatti, su una curva supersingolare è possibile calcolare i multipli di un punto con un particolare algoritmo che sostituisce alcune operazioni sulla curva con operazioni su un campo finito, quindi meno laboriose; si veda Washington, [15], pagg. 122-123.

Algoritmo di Silver Pohlig Hellman (SPH)

Se l'ordine di un gruppo G è T-liscio, per T sufficientemente piccolo, allora il problema del logaritmo discreto si può risolvere in maniera efficiente con il seguente algoritmo di Silver-Pohlig-Hellman.

Sia G un gruppo di ordine $\#G = \prod p_i^{s_i}$. Se $\#G$ è T-liscio (cioè $p_i \leq T$ per ogni i) per T abbastanza piccolo, allora possiamo utilizzare il seguente algoritmo per trovare il logaritmo discreto di $y \in G$ in base $g \in G$ (dove g non è necessariamente un generatore). Innanzitutto, determiniamo l'ordine esatto di g[4]. Dobbiamo ora trovare $x < N$ tale che $xg = y$ oppure, se tale x non esiste, l'algoritmo deve risponderci che esso non esiste.

L'idea su cui si basa l'algoritmo è di cercare $x \pmod{p^r}$ (al variare di p^r nelle potenze prime che compaiono in N) anzichè $x \pmod{N}$ e, infine, utilizzare il Teorema Cinese del Resto per calcolare $x \pmod{N}$ (ricordando che $N = \prod p^r$).

Per calcolare $x \pmod{p^r}$ supponiamo che sia: $x \equiv x_0 + x_1 p + ... + x_{r-1} p^{r-1} \pmod{p^r}$, con $0 \leq x_i \leq p-1$ per $i = 0, ..., r-1$.

Per trovare x_0 moltiplichiamo entrambi i membri dell'uguaglianza: $xg = y$ per $N' = \frac{N}{p}$ ricavando

$$x_0(N'g) = N'y$$

(ricordiamo che $Ng = O$). Se p è abbastanza piccolo, possiamo trovare $x_0 \in \{0, ..., p-1\}$ per tentativi (e se non lo troviamo vuol dire che y non è nel sottogruppo generato da g) in $O(p)$ passi. Se invece, p è troppo grande, possiamo utilizzare l'algoritmo di Shank, *baby step-giant step*[5].Una volta trovato x_0, troviamo x_1 moltiplicando la solita uguaglianza $gx = y$ per $N'' = \frac{N}{p^2}$. Abbiamo, quindi,

$$(x_0 + x_1 p)N''g = N''y$$

o equivalentemente

$$x_1(N'g) = N''(y - x_0 g).$$

A questo punto, per determinare x_1 procediamo esattamente come abbiamo fatto per x_0. Una volta trovato x_1, cerchiamo $x_2, ..., x_{r-1}$ analogamente (per induzione).

Procedendo in questo modo per tutti i $p \mid N$, conosceremo $x \pmod{p^r}$ per ognuno di questi p. Applicando il Teorema Cinese del Resto, potremo finalmente trovare x, $1 \leq x \leq N$. □

Osservazioni

1. A differenza dell'algoritmo "index calculus" che si utilizza per calcolare il logaritmo discreto sui campi finiti (in cui la maggior parte dei calcoli sono pre-computazioni

[4]Per trovare l'ordine di g, calcoliamo $\left(\frac{\#G}{p_i}\right) g$ al variare di i, poi per gli indici i per i quali $\left(\frac{\#G}{p_i}\right) g = O$ calcoliamo anche $\left(\frac{\#G}{p_i^2}\right) g$ e così via finchè non troviamo il più piccolo intero $N = \prod p_i^{r_i}$ tale che $Ng = O$.

[5]Sia $b = \lfloor \sqrt{p} \rfloor + 1$. Poniamo $x_0 = ib - j$, con $1 \leq i, j \leq b$. Calcoliamo $i(bN'g)$ per $1 \leq i \leq b$ e $N'y + jN'g$ per $1 \leq j \leq b$, e confrontiamo i risultati ottenuti. Se per qualche coppia (i, j) troviamo che $ibN'g = N'y + jN'g$, allora sappiamo che $x_0 = ib - j$.

che possono essere effettuate una sola volta) questo algoritmo dev'essere ripetuto interamente per ogni logaritmo discreto.

2. Si sono fatti grossi sforzi per migliorare, anche di poco, il tempo di esecuzione. Un algoritmo leggermente piú rapido è quello basato sul metodo ρ di Pollard, proposto da Van Oorschot e Wiener (per approfondimenti si vedano: Van Oorschot-Wiener [13, 14]).

3. Se la sicurezza di un sistema è basata sulla difficoltà del problema del logaritmo discreto, è importante scegliere il gruppo G in modo tale che non abbia ordine liscio, cioè che $\#G$ sia divisibile da un primo molto grande (Koblitz, in [7] (pag.134), nel 1998 suggeriva un primo di almeno 40 cifre decimali).

Iniziamo ora a introdurre dei crittosistemi che utilizzano il problema del logaritmo discreto sulle curve ellittiche.

3.2.3 Scambio della chiave (analogo di Diffie-Hellman)

Supponiamo di avere due utenti, Alice e Bob, che vogliano accordarsi su una chiave segreta da utilizzare per un crittosistema classico.

1. Innanzi tutto, essi devono fissare (pubblicamente) un campo $\mathbb{F}_q$, dove $q = p^r$, ed una curva ellittica E definita su questo campo.

2. Il passo successivo è rendere pubblico un punto $B \in E$ (detto *base*) (che avrà un ruolo analogo a quello del generatore g nell'algoritmo di Diffie-Hellman). In questo caso, non ci preoccupiamo che B sia un generatore di E, ma supponiamo che abbia un ordine m sufficientemente grande.

3. Alice sceglie un intero a che abbia all'incirca lo stesso numero di cifre di m, che terrà segreto, e invia (pubblicamente) a Bob la quantità aB.

4. Allo stesso modo Bob sceglie b dello stesso ordine di grandezza, e invia ad Alice la quantità bB.

5. A questo punto entrambi possono calcolare abB che servirà (opportunamente convertito in un intero, secondo una regola precedentemente concordata[6]) da chiave segreta.

Esattamente come nell'algoritmo di Diffie-Hellman, si congettura che il problema di ricavare abB conoscendo solamente aB e bB (*problema di Diffie-Hellman per le curve ellittiche*) sia equivalente al problema del logaritmo discreto con le curve ellittiche, sulla cui difficoltà abbiamo già discusso al paragrafo precedente.

[6]Per esempio, potrebbero essersi accordati per prendere le ultime 256 cifre dell'ascissa del punto, oppure per applicare una certa funzione hash su tale ascissa.

3.2.4 Crittosistemi

3.2.4.1 Analogo di Massey-Omura

Questo crittosistema si basa sull'algoritmo del doppio lucchetto ed è analogo al crittosistema di Massey-Omura. Si fissa una curva ellittica E su un campo $\mathbb{F}_q$ (q sufficientemente grande). Si calcola il numero di punti della curva N.

A questo punto, ciascun utente sceglie un intero casuale e, compreso tra 1 e N, tale che $\text{mcd}(e, N) = 1$ e calcola, utilizzando l'algoritmo euclideo, $d \equiv e^{-1} (\text{mod } N)$.

I messaggi vengono opportunamente convertiti in punti appartenenti alla curva ellittica, in modo da poter trasmettere punti della curva al posto del testo originario.

Se Alice vuole trasmettere a Bob il messaggio $M \in E$, i due agiscono nella seguente maniera:

1. Alice invia $e_A M$ a Bob.
2. Bob, che non conosce né e_A né d_A, non tenta nemmeno di decifrare il messaggio, e rispedisce ad Alice la quantità $e_B e_A M$.
3. Alice, a questo punto, può eliminare e_A, calcolando $d_A(e_B e_A M) = e_B M$ e invia il risultato trovato a Bob.
4. Bob è ora in grado di leggere il messaggio, calcolando $d_B(e_B M) = M$.

Un eventuale intruso che intercettasse i messaggi in maniera passiva, potrebbe solo venire a conoscenza di $e_A M$, $e_B e_A M$ ed $e_B M$. Se fosse in grado di risolvere il logaritmo discreto sulle curve ellittiche (ECDLP) potrebbe ricavare M, ma sappiamo che questo è un problema attualmente intrattabile se i parametri sono sufficientemente grandi. Non è stato provato il viceversa, cioè che per ricavare M, essendo noti $e_A M$, $e_B e_A M$ ed $e_B M$, sia necessario saper risolvere il logaritmo discreto, ma si congettura che ciò sia vero.

Un altro problema è quello di accertare l'identità di Bob (si vedano i paragrafi 3.1.3.1 e 3.1.3.2), ma lo si può risolvere con un algoritmo di firma digitale.

3.2.4.2 Analogo di ElGamal

Viene fissata una curva ellittica E su un campo $\mathbb{F}_q$, ed una base $B \in E$. Ogni utente sceglie un intero casuale a, che sarà la sua chiave segreta, e pubblica aB.

Se Alice vuole spedire a Bob il messaggio $M \in E$, essi agiscono nella seguente maniera:

1. Alice sceglie un intero casuale k ed invia a Bob la coppia $(kB, M + k(a_B B))$, dove $(a_B B)$ è la chiave pubblica di Bob;
2. Bob può risalire al messaggio originario calcolando:

$$M = M + k(a_B B) - a_B(kB),$$

utilizzando la propria chiave segreta a_B.

E' evidente che un intruso che sapesse risolvere il problema del logaritmo discreto ellittico potrebbe ricavare a_B e da questo risalire al messaggio. In caso contrario, non appare possibile determinare a_B.

3.2.5 Firma digitale: ECDSA

L'algoritmo di firma digitale ECDSA (utilizzato dal governo degli Stati Uniti) è l'analogo sulle curve ellittiche dell'algoritmo DSA.

Inizialmente, bisogna fissare una curva ellittica E su un campo $\mathbb{F}_q$. Supponiamo, per semplicità, che q sia primo. Poi si fissa un punto $P \in E$ che abbia ordine primo p. $\mathbb{F}_q$, q, p, P sono pubblici.

Per generare le proprie chiavi, ciascun utente del sistema agisce nella seguente maniera:

1. sceglie un intero casuale $d \in [1, p-1]$;
2. calcola $Q = dP$;
3. la sua chiave privata è d, quella pubblica è Q.

Dopo aver generato le proprie chiavi, l'utente A può firmare il messaggio M nel seguente modo:

1. sceglie un intero casuale $k \in [1, p-1]$;
2. calcola $kP = (x_1, y_1)$ e $r \leftarrow x_1 (\text{mod } p)$ [7] (x_1 viene trattato come un intero compreso tra 1 e $q-1$). Se $r = 0$ si ritorna al passo 1. (se r fosse 0, A non dimostrerebbe di conoscere d, quindi non proverebbe la propria identità);
3. calcola $k^{-1} (\text{mod } p)$;
4. calcola $s \leftarrow k^{-1}(h(M) + dr) \ (\text{mod } p)$, dove h è la funzione hash (ad esempio, viene usato il Secure Hash Algorithm). Se $s = 0$ si torna al passo 1. (perché, per verificare la firma, serve poter invertire s). NB: solo A, che conosce la propria chiave privata d, può calcolare correttamente s;
5. La firma per il messaggio m è la coppia (r, s).

Un altro utente, B, può verificare la firma di A svolgendo i seguenti passi:

1. B si procura Q, ossia una copia autenticata della chiave pubblica di A.
2. Verifica che $r, s \in [1, p-1]$.
3. Calcola $w \leftarrow s^{-1} (\text{mod } p)$.
4. Calcola $u_1 \leftarrow h(M)w \ (\text{mod } p)$ e $u_2 \leftarrow rw \ (\text{mod } p)$.
5. Calcola $R = u_1 P + u_2 Q = (x_0, y_0)$ e $v \leftarrow x_0 \ (\text{mod } p)$.
6. Accetta la firma se e solo se $v = r$.

[7] D'ora in poi, in questo paragrafo, scrivendo $x \leftarrow a \ (\text{mod } p)$ intenderemo che alla variabile $x \in \mathbb{Z}_p$ assegniamo il valore $a \ (\text{mod } p)$, intendendo con questo il *minimo residuo positivo* di a modulo p, ovvero l'unico intero $b \in \{1, ..., p-1\}$ tale che $b \equiv a \ (\text{mod } p)$.

Proposizione 3.2

L'algoritmo ECDSA funziona correttamente.

Dimostrazione

Per prima cosa, mostriamo che se la firma è corretta allora $v = r$. Infatti $u_1P + u_2Q = h(m)wP + rwdP = [(h(m) + rd)w]\, P = kP$ da cui segue che $x_0 = x_1$ e quindi $v = r$.

Inoltre, dimostriamo che se $v = r$ allora la firma è stata prodotta correttamente, il che è possibile solo per A (nessun altro conosce la chiave segreta d).

Supponendo $v = r$ si ottiene $x_0 \equiv x_1 \pmod p$ da cui $y_0 \equiv \pm y_1 \pmod p$ (affinché i punti R e kP appartengano alla curva $E \pmod p$).

Se $y_0 \equiv y_1 \pmod p$, allora $R \equiv kP \pmod p$, Da ciò segue $u_1 + u_2 d \equiv k \pmod p$ ossia $h(m)w + rwd \equiv k \pmod p$. Quindi abbiamo $k \equiv (h(m) + rd)s^{-1} \pmod p$ da cui segue $s \equiv k^{-1}(h(m) + rd) \pmod p$. Si noti che questo poteva calcolarlo solo A.

Se $y_0 \equiv -y_1 \pmod p$, allora $R \equiv -kP$. Ragionando come al punto precedente si ottiene $-s \equiv k^{-1}(h(m)+rd) \pmod p$ e, ovviamente, saper calcolare s o $-s$ è equivalente (quindi lo poteva fare solo A). □

Capitolo 4

Fattorizzazione con le curve ellittiche

4.1 Il metodo $(p-1)$ di Pollard

La fattorizzazione con le curve ellittiche è stata proposta da Lenstra (in Lenstra, [10]). Attualmente, il metodo di Lenstra permette al più di fattorizzare numeri di 60 cifre decimali, oppure, su numeri più grandi, di trovare fattori di circa 20-30 cifre decimali (cfr. Washington, [15], pag.180). Sebbene abbia costituito un importante passo nella ricerca, questo metodo non è abbastanza efficiente per minare la sicurezza degli algoritmi basati sulla difficoltà della fattorizzazione, in quanto per questi generalmente si scelgono numeri composti del tipo $n = pq$ con fattori di circa 75 cifre decimali ciascuno, che richiedono algoritmi più efficienti, come come Quadratic Sieve o Number Field Sieve (tuttavia in questi algoritmi viene talvolta utilizzato anche il metodo di Lenstra, per trovare fattori di media misura di numeri che compaiono nei passi intermedi) (cfr. Washington, [15], pag. 182).

Il metodo di Lenstra assomiglia molto al metodo $(p-1)$ di Pollard sui campi finiti.

4.1.1 Algoritmo del metodo $(p-1)$ di Pollard

Si suppone di avere un numero composto n e di volerne trovare un fattore.

1. Si prende un numero k che sia divisibile per tutti (o quasi) gli interi minori o uguali ad un certo B[(1)] (per esempio, potremmo prendere $k = B!$ oppure $k = \text{mcm}(1, 2, ..., B)$).
2. Si sceglie un intero a tale che $\text{mcd}(a, n) = 1$.
3. Si calcola $a_1 \equiv a^k (\text{mod } n)$.[(2)]
4. Si calcola $d = \text{mcd}(a_1 - 1, n) (= \text{mcd}(a^k - 1, n)$ ma si riducono i calcoli).

[(1)] Per fini pratici, Washington ([15], pag. 181) consiglia B dell'ordine di grandezza di 10^8.

[(2)] Non bisogna calcolare a^k e poi ridurlo (mod n) perché questo potrebbe causare un overflow del computer. Bisogna invece calcolarlo ricorsivamente, con la formula $a^{b!} \equiv (a^{(b-1)!})^b$ (mod n) per $b = 2, 3, 4, ..., B$, oppure si può scrivere $B!$ in base binaria e fare un'esponenziazione modulare col metodo dei quadrati ripetuti.

5. Se d non è un divisore proprio di n si sceglie un nuovo a oppure si cambia k.

4.1.2 Funzionamento dell'algoritmo

Ci proponiamo ora di spiegare perché l'algoritmo funziona.

Supponiamo che n sia un numero composto e che k sia multiplo di tutti gli interi minori o uguali a B.

Supponiamo anche che n abbia un fattore primo p tale che $p-1$ sia prodotto di potenze prime piccole, tutte minori o uguali a B. Allora $p-1 \mid k$. Per il Piccolo Teorema di Fermat (si veda, ad esempio, Languasco-Zaccagnini, [9], pag. 49), si ha che $a^k \equiv 1 \pmod{p}$, e quindi $p \mid \mathrm{mcd}(a^k - 1, n)$.

Il metodo fallisce se $\mathrm{mcd}(a^k - 1, n) = 1$ oppure $\mathrm{mcd}(a^k - 1, n) = n$; in tal caso si può provare a cambiare k oppure a, ma non si può essere certi di riuscire nell'intento.

4.2 Premesse

4.2.1 Curve ellittiche modulo n

Definizione 4.1

Siano $n \in \mathbb{Z}$ e x_1, $x_2 \in \mathbb{Q}$, entrambi tali che, scritti ai minimi termini, abbiano denominatore coprimo con n. Si dice che $x_1 \equiv x_2 (\mathrm{mod}\ n)$ se $x_1 - x_2$, scritto ai minimi termini, ha numeratore divisibile per n.

Abbiamo la seguente proprietà

Proposizione 4.2 (Koblitz [6], pag.172)

Per ogni $x_1 \in \mathbb{Q}$ (con denominatore coprimo con n) esiste un unico $x_2 \in \mathbb{Z}$, $0 \leq x_2 \leq n-1$, tale che $x_1 \equiv x_2 (\mathrm{mod}\ n)$. In questo caso si può scrivere: $x_2 = x_1 (\mathrm{mod}\ n)$.

4.2.1.1 Riduzione di una curva ellittica modulo n

Sia data una curva ellittica E su $\mathbb{Q}$ (o piú in generale su un campo di numeri), definita dall'equazione

$$y^2 = x^3 + ax + b.$$

Ridurre tale curva ellittica $(\mathrm{mod}\ n)$ significa considerare la curva $E(\mathrm{mod}\ n)$ su $\mathbb{Z}_n$ di equazione

$$y^2 = x^3 + (a(\mathrm{mod}\ n)\ )x + (b(\mathrm{mod}\ n)).$$

In particolare se il punto $P = (x, y) \in E$, allora il punto:

$$P(\mathrm{mod}\ n)\ = (x\ (\mathrm{mod}\ n),\ y\ (\mathrm{mod}\ n)) \in E\ (\mathrm{mod}\ n).$$

Inoltre definiamo $O(\mathrm{mod}\ n) = O \in E(\mathrm{mod}\ n)$.

La somma di punti si comporta bene rispetto alla riduzione modulo n.

Lemma 4.3

Siano $L,\ M \in E$, E curva ellittica su $\mathbb{Z}_n$, $p \mid n$. Se la somma $L + M$ è definita, allora $(L + M) \pmod p = L \pmod p + M \pmod p$.

Dimostrazione

Nel caso in cui almeno uno tra L e M è uguale a O, la tesi segue facilmente.

Siano quindi $L = (x_1, y_1)$, $M = (x_2, y_2)$; $L,\ M \neq O$. Quando calcoliamo la somma di questi due punti si possono avere tre casi:

1. $x_1 = x_2$, $y_1 = -y_2$. Allora $L + M = O$ e $L \pmod p + M \pmod p = O \pmod p$;
2. $x_1 = x_2$, $y_1 = y_2 \neq 0$. Nella formula per il calcolo della somma troviamo a denominatore una potenza di $2y_1$. Per ipotesi sappiamo che $L + M$ è definito e quindi y_1 è invertibile (mod n). Allora $y_1 \not\equiv 0 \pmod p$; di conseguenza, anche calcolando $L \pmod p + M \pmod p$ ci troviamo in questo stesso caso e $2y_1 \pmod p$ è invertibile.
3. $x_1 \neq x_2$. Nella formula per il calcolo della somma il denominatore è una potenza di $(x_2 - x_1)$. Se $x_1 \not\equiv x_2 \pmod p$ allora possiamo applicare la formula in questione e concludere. Se invece si avesse $x_1 \equiv x_2 \pmod p$ allora $p \mid x_2 - x_1$ e non sapremmo calcolare l'inverso di $x_2 - x_1$ modulo n; in contraddizione con l'ipotesi iniziale.

□

Presentiamo ora un'altra proprietà importante della riduzione modulo n.

Proposizione 4.4

Sia E la curva ellittica definita dall'equazione $y^2 = x^3 + ax + b$, con $a,\ b \in \mathbb{Z}$, $\mathrm{mcd}(4a^3 + 27b^2, n) = 1$ (tale condizione implica che il membro di destra non abbia zeri multipli né (mod n), né (mod p), per ogni p divisore primo di n).

Siano $P_1,\ P_2 \in E$, con denominatori coprimi con n, $P_1 \neq -P_2$. Si ha che:

$P_1 + P_2 \in E$ ha coordinate con denominatore coprimo con n se e solo se non esiste p primo, $p \mid n$, tale che

$$P_1 \pmod p + P_2 \pmod p = O \pmod p \in E \pmod p.$$

Dimostrazione

$\Longrightarrow$) Siano $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$. $P_1 + P_2 \in E$ abbia coordinate con denominatore coprimo con n e sia p un fattore primo di n. Dobbiamo mostrare che

$$P_1 \pmod p + P_2 \pmod p \neq O \pmod p \in E \pmod p.$$

Cominciamo distinguendo due casi:

1. $x_1 \not\equiv x_2 \pmod p$;

2. $x_1 \equiv x_2 (\text{mod } p)$.

Nel primo caso si arriva facilmente alla conclusione, in quanto $P_1(\text{mod } p) + P_2(\text{mod } p) \neq O(\text{mod } p) \in E(\text{mod } p)$ per la definizione di addizione (la somma di due punti con ascissa diversa non dà mai O).

Quindi, possiamo ridurci al secondo caso $x_1 \equiv x_2(\text{mod } p)$.

Anche qui dobbiamo considerare due casi:

2a. $P_1 = P_2$;

2b. $P_1 \neq P_2$.

Supponiamo che $P_1 = P_2$. Allora $P_1 + P_2 = 2P_1 = (x_3, y_3)$, dove

$$\begin{cases} x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\frac{3x_1^2+a}{2y_1}\right)(x_1 - x_3). \end{cases}$$

Le coordinate di $2P_1(\text{mod } p)$ si trovano con le stesse formule, ma sostituendo ogni termine col suo ridotto modulo p.

Per mostrare che $P_1(\text{mod } p) + P_2(\text{mod } p) \neq O(\text{mod } p)$ basta mostrare che $p \nmid 2y_1$ (infatti, se $p \nmid 2y_1$ allora $p \nmid y_1$ cioè $y_1 \not\equiv 0 \pmod p$, e quindi $P_1(\text{mod } p) + P_2(\text{mod } p) \neq O(\text{mod } p)$).

Procediamo per assurdo. Se $p \mid 2y_1$ allora, siccome il denominatore di x_3 non è divisibile per p (per ipotesi), abbiamo $p \mid (3x_1^2 + a)$. Quindi x_1 è radice multipla di $x^3 + ax + b$, il che contraddice le ipotesi iniziali.

Supponiamo ora che $x_1 \equiv x_2 \pmod p$ e $P_1 \neq P_2$. Siccome $x_1 \neq x_2$, possiamo scrivere

$$x_2 = x_1 + p^r x,$$

con $r \geq 1$ tale che né il numeratore, né il denominatore di x siano divisibili per p. Sappiamo inoltre che il denominatore di $P_1 + P_2$ non è divisibile per p.

Le formule che ci forniscono le sue coordinate sono

$$\begin{cases} x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2 \\ y_3 = -y_1 + \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3). \end{cases}$$

Siccome $x_2 - x_1 = p^r x$ allora $\frac{y_2-y_1}{x_2-x_1}$ dev'essere tale che, ridotto ai minimi termini, il denominatore non sia divisibile per p; segue quindi che $y_2 - y_1 = p^r y$ (y può anche essere divisibile per p).

Poiché $P_2 \in E$, sappiamo che

$$y_2^2 = x_2^3 + ax + b = (x_1 + p^r x)^3 + a(x_1 + p^r x) + b.$$

Svolgendo il membro di destra e riducendolo $(\text{mod } p^{r+1})$ si ricava

$$\begin{aligned} y_2^2 &\equiv x_1^3 + 3x_1^2 p^r x + ax_1 + ap^r x + b \equiv p^r x(3x_1^2 + a) + x_1^3 + ax_1 + b \qquad (4.1) \\ &\equiv y_1^2 + p^r x(3x_1^2 + a) \ (\text{mod } p^{r+1}). \end{aligned}$$

Sappiamo che $x_2 \equiv x_1 \pmod{p^r}$ e che $y_2 \equiv y_1 \pmod{p^r} \Rightarrow P_1(\text{mod } p) = P_2(\text{mod } p)$.

Segue che

$$P_1(\text{mod } p) + P_2(\text{mod } p) = 2P_1(\text{mod } p)$$

e quindi

$$P_1(\text{mod } p) + P_2(\text{mod } p) = O(\text{mod } p) \Leftrightarrow y_1 \equiv y_2 \equiv 0(\text{mod } p).$$

Per assurdo, se fosse $P_1(\text{mod } p)+P_2(\text{mod } p) = O(\text{mod } p)$, si avrebbe $y_1 \equiv y_2 \equiv 0 \pmod{p}$, ma allora $y_1 \equiv -y_2 \pmod{p}$ e quindi $y_2^2 - y_1^2 = (y_2 - y_1)(y_2 + y_1)$ sarebbe divisibile per p^{r+1} ossia $y_2^2 \equiv y_1^2 \pmod{p^{r+1}}$.

Ma allora, osservando l'equazione (4.1), abbiamo che

$$(3x_1^2 + a) \equiv 0 \pmod{p},$$

e ciò contraddice l'ipotesi che il polinomio $x^3 + ax + b$ non abbia radici multiple.

$\Longleftarrow$) Supponiamo ora che per ogni $p \mid n$, p primo, $P_1(\text{mod } p)+P_2(\text{mod } p) \neq O(\text{mod } p)$ e mostriamo che, allora, $P_1 + P_2$ ha coordinate che, ridotte ai minimi termini, hanno denominatori coprimi con n.

Fissiamo $p \mid n$. Consideriamo i due casi:

1) $x_1 \not\equiv x_2(\text{mod } p)$;

2) $x_1 \equiv x_2(\text{mod } p)$.

Nel caso 1), osservando le coordinate della somma

$$\begin{cases} x_3 = \left(\frac{y_2-y_1}{x_2-x_1}\right)^2 - x_1 - x_2 \\ y_3 = -y_1 + \left(\frac{y_2-y_1}{x_2-x_1}\right)(x_1 - x_3) \end{cases}$$

e tenendo conto che $p \nmid x_2 - x_1$ si vede immediatamente che p non divide il denominatore. Ci riduciamo perciò al secondo caso: $x_1 \equiv x_2(\text{mod } p)$. Si osserva che $y_2 \equiv \pm y_1(\text{mod } p)$. Siccome $P_1(\text{mod } p) + P_2(\text{mod } p) \neq O(\text{mod } p)$ abbiamo che $y_2 \equiv y_1 \not\equiv 0(\text{mod } p)$, e dobbiamo distinguere le due possibilità che si presentano:

2a) $P_1 = P_2$;

2b) $P_1 \neq P_2$.

Caso 2a): $P_1 = P_2$. Ricordando che

$$\begin{cases} x_3 = \left(\frac{3x_1^2+a}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\frac{3x_1^2+a}{2y_1}\right)(x_1 - x_3) \end{cases}$$

e che $y_1 \not\equiv 0 \pmod{p}$, si osserva che i denominatori sono coprimi con p.

Caso 2b): $P_1 \neq P_2$. Scriviamo nuovamente $x_2 = x_1 + p^r x$, con $p \nmid x$. Abbiamo già calcolato che

$$y_2^2 \equiv y_1^2 + p^r x(3x_1^2 + a)(\text{mod} p^{r+1})$$

ed allora

$$y_2^2 \equiv y_1^2 + p^r x(3x_1^2 + a) \pmod{p}.$$

Ricordando che $p^r x = x_2 - x_1$, otteniamo

$$\frac{y_2^2 - y_1^2}{x_2 - x_1} \equiv (3x_1^2 + a) \pmod{p}.$$

Osservando che il lato di destra ha il denominatore coprimo con p, possiamo concludere che anche il lato di sinistra gode della stessa proprietà.

Ora, siccome $p \nmid (y_2 + y_1) \equiv 2y_1 (\mathrm{mod}\ p)$, posso dividere per $(y_2 + y_1)$, ottenendo così

$$\frac{y_2^2 - y_1^2}{(x_2 - x_1)(y_2 + y_1)} = \frac{y_2 - y_1}{x_2 - x_1}$$

ed anche questo termine ha denominatore coprimo con p. Ma, osservando le formule per calcolare le coordinate di $P_1 + P_2$, ossia

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3), \end{cases}$$

segue immediatamente che tali coordinate hanno denominatore non divisibile per p.

□

4.3 Metodo di Lenstra

4.3.1 Fattorizzazione con le curve ellittiche

Sia n un numero composto dispari. Vogliamo trovare un fattore non banale d di n, $1 < d < n$.

Per iniziare, prendiamo una curva ellittica E, definita dall'equazione

$$y^2 = x^3 + ax + b,$$

con a, $b \in \mathbb{Z}$ e un punto $P = (x, y) \in E$.

Osservazione: la coppia (E, P) è stata trovata, probabilmente, con un metodo casuale, proviamo a usarla per fattorizzare n, se non riusciamo nell'intento prendiamo un'altra coppia (E', P') e ricominciamo. Se la probabilità di fallire un tentativo è $\rho < 1$ allora dopo m prove, la probabilità di aver fallito sempre è ρ^m che è un numero "molto piccolo" per m "molto grande". Questo garantisce buone probabilità di successo in un numero ragionevole di tentativi.

Una volta fissata la coppia (E, P), scegliamo un intero k divisibile per potenze di piccoli primi, del tipo l^{α_l}, con l primo, $l \leq B$, $l^{\alpha_l} \leq C$. Quindi prendiamo:

$$k = \prod_{l \leq B} l^{\alpha_l},$$

con $\alpha_l = \left\lfloor \frac{\log C}{\log l} \right\rfloor$ (è il massimo esponente tale che $l^{\alpha_l} \leq C$) .

Adesso cerchiamo di calcolare kP, col metodo dei raddoppiamenti successivi, lavorando (mod n) a ogni iterazione. Questo calcolo risulta inutile, tranne nel caso in cui, in una delle iterazioni, cercando di calcolare l'inverso di $(x_2 - x_1)$ oppure di $2y_1$ (a seconda della formula per l'addizione che ci serve in quella determinata iterazione), troviamo un numero che *non sia coprimo con* n. Questo accade quando stiamo calcolando un multiplo k_1P (somma parziale) che per qualche $p \mid n$ è tale che:

$$k_1(P(\text{mod } p)) = O(\text{mod } p),$$

ossia l'ordine di $P(\text{mod } p) \in E(\text{mod } p)$ divide k_1. In tal caso ricordiamo che è utile effettuare la verifica di coprimalità (tra il numero che vogliamo invertire ed n) mediante l'algoritmo euclideo perché esso ci permette di trovare l'inverso che cercavamo se i due numeri sono coprimi oppure, in caso contrario, restituisce il massimo comun divisore tra i due.

Quel massimo comun divisore può essere un divisore proprio di n, e abbiamo terminato, oppure può essere proprio n.

Nel secondo caso, si ha che il denominatore è divisibile per n, e quindi che

$$k_1(P(\text{mod } p)) = O(\text{mod } p)$$

per ogni p divisore primo di n (questo è molto improbabile se n ha due o piú divisori primi molto grandi).

Quindi è molto probabile che, quando cerchiamo di calcolare k_1P (mod n), per un k_1 che è multiplo dell'ordine di $P(\text{mod } p)$ (per qualche $p \mid n$) troveremo un divisore proprio di n.

Osservazione

Spieghiamo ora perchè il metodo di Lenstra funziona.

Quando cerchiamo di fattorizzare n, supponiamo che esso sia della forma $n = pq$, come è solito essere negli algoritmi basati sulla difficoltà della fattorizzazione. L'algoritmo cerca di trovare una curva ellittica E tale che $\#\ (E(\text{mod } p))$ sia B-liscia e quindi $kP(\text{mod } p) = O(\text{mod } p)$ (perchè $\#\ (E(\text{mod } p)) \mid k$). E' improbabile, a questo punto, che si verifichi anche $kP(\text{mod } q) = O(\text{mod } q)$; tuttavia, se ciò accadesse, è sufficiente cambiare la coppia (E, P) oppure scegliere B più piccolo. Si arriva quindi al caso

$$\begin{cases} kP(\text{mod } p) = O(\text{mod } p) \\ kP(\text{mod } q) \neq O(\text{mod } q); \end{cases}$$

questo significa che, calcolando kP si trova un denominatore che è divisibile per p ma non per q, e quindi, calcolando il massimo comun divisore con n si ottiene proprio p.

In particolare, l'algoritmo di Lenstra ha buone probabilità di successo se $p < 10^{40}$ (si veda Washington, [15], pag.182).

4.3.2 Somiglianza col metodo $(p-1)$ di Pollard

Si nota subito la somiglianza di questo metodo con quello di Pollard, sebbene, mentre in quest'ultimo si utilizza il gruppo $\mathbb{Z}_p^*$, qui invece utilizziamo $E(\text{mod } p)$.

Differentemente dal metodo di Pollard, in cui il gruppo utilizzabile era soltanto uno, con il metodo di Lenstra, se la curva E non va bene (cioè, se per ogni $p \mid n$, $E(\text{mod } p)$ non ha ordine $B-$liscio, e quindi $kP(\text{mod } p)$ non dà come risultato $O(\text{mod } p)$ per k trovato come prima), possiamo cambiare la curva ellittica E ed il punto $P \in E$.

4.3.3 Algoritmo (metodo probabilistico di Lenstra)

Sia n un intero composto dispari. Sia E una curva ellittica, definita dall'equazione $y^2 = x^3 + ax + b$, con a, $b \in \mathbb{Z}$ e sia dato un punto $P = (x, y) \in E$.

Verifichiamo che $\text{mcd}(4a^3 + 27b^2, n) = 1$.

Si noti che, se $\text{mcd}(4a^3 + 27b^2, n) \neq 1$ si possono avere due casi: o il massimo comun divisore è minore di n e in tal caso abbiamo già trovato un divisore non banale, oppure è n e allora ricominciamo con un'altra coppia (E, P).

Costruiamo

$$k = \prod_{l \leq B} l^{\alpha_l},$$

con $\alpha_l = \left\lfloor \frac{\log C}{\log l} \right\rfloor$ (come al paragrafo 3.3.1), scegliendo B e C in modo tale che siano sufficientemente grandi da alzare le possibilità di trovare un divisore di n ma anche abbastanza piccoli da limitare il tempo necessario al calcolo.

Ora calcoliamo

$$2P_1, 2(2P_1), 2(4P_1), ..., 2^{\alpha_2}P_1, 3(2^{\alpha_2}P_1), 3(3 \cdot 2^{\alpha_2}P_1), ..., (3^{\alpha_3} \cdot 2^{\alpha_2})P_1, ..., \left(\prod_{l \leq B} l^{\alpha_l}\right) P_1.$$

Per svolgere le divisioni $(\text{mod } n)$ utilizziamo l'algoritmo di Euclide. Se fallisce, allora troviamo o un divisore non banale di n e in tal caso abbiamo concluso, oppure troviamo n come massimo comun divisore tra il denominatore ed n e allora è necessario ricominciare con una nuova coppia (E, P).

Capitolo 5

Test di primalità con le curve ellittiche

5.1 Premesse

Presentiamo questo test di primalità per vedere un'altra interessante applicazione delle curve ellittiche sui campi finiti, sebbene nel 2002, Agrawal Kayal e Saxena abbiano presentato un algoritmo di primalità polinomiale (AKS) (si veda Agrawal-Kayal-Saxena, [1]).

Prima di descrivere l'algoritmo di Goldwasser-Kilian (Goldwasser-Kilian, [4]), che è l'obiettivo di questo capitolo, introduciamo il lavoro da svolgere.

Vogliamo utilizzare il gruppo dei punti di una curva ellittica su $\mathbb{F}_n$ per verificare se n è primo.

Prima di utilizzare il test di Goldwasser-Kilian, vogliamo essere abbastanza sicuri che si tratti di un numero primo, per questo motivo, applicheremo prima il test probabilistico di pseudo-primalità forte di Rabin-Miller .

Una volta applicato con successo tale test, tratteremo n come se esso fosse primo (per esempio supponendo che ogni elemento non nullo sia invertibile (mod n)).

Ovviamente, se nel corso dell'algoritmo di Goldwasser-Kilian, troveremo un elemento non nullo che non sia invertibile (mod n), allora l'algoritmo terminerà immediatamente, rispondendo che n è composto (anzi, calcolando il massimo comun divisore di tale elemento non invertibile con n troveremo anche un fattore di n).

Supponiamo che la curva ellittica che vogliamo utilizzare sia la curva E, definita dall'equazione

$$y^2 = x^3 + ax + b,$$

dove $\text{mcd}(4a^3 + 27b^2, n) = 1$. Possiamo inoltre ipotizzare $\text{mcd}(n, 6) = 1$.

Sommiamo i punti di E come se n fosse primo. L'unica eventualità che si può presentare è che qualche divisione sia impossibile, ma questo significherebbe che n è composto e farebbe terminare l'algoritmo.

Quindi d'ora in poi supporremo che tutte le operazioni si svolgano senza problemi.

5.2 Test di Goldwasser-Kilian

Proposizione 5.1

Sia n intero, $\text{mcd}(n, 6) = 1$, $n \neq 1$. Sia E una curva ellittica su $\mathbb{Z}_n$.

Supponiamo di conoscere $m \in \mathbb{Z}$ e $P \in E$ tale che:

1. Esiste q primo, $q \mid m$ tale che $q > (\sqrt[4]{n} + 1)^2$;
2. $mP = O$ (cioè è il punto $(0 : 1 : 0)$ sul piano complesso);
3. $\left(\frac{m}{q}\right) P = (x : y : t)$ con $t \in \mathbb{Z}_n^*$.

Allora n è primo.

Dimostrazione

Sia $p \mid n$, p primo. Riducendo (mod p) la curva E, sappiamo che P (mod p) ha ordine k, dove $k \mid m$, ma k non divide $\frac{m}{q}$ perché $t \in \mathbb{Z}_n^*$. Siccome q è primo allora $q \mid k$.

Sappiamo che

$$q \leq \#(E(\text{mod } p)).$$

Ma, per il Teorema di Hasse (paragrafo 2.3.1),

$$q < (\sqrt{p} + 1)^2.$$

Per assurdo, se n non fosse primo, allora potremmo scegliere per p il piú piccolo fattore primo di n. Sicuramente, $p < \sqrt{n}$, allora

$$q < \left(\sqrt[4]{n} + 1\right)^2,$$

il che contraddice l'ipotesi 1).

□

Ora il problema è: se n è primo, come possiamo scegliere E, P ed m che ci permettano di dimostrare la sua primalità?

Per far questo, ci sarà utile la seguente proposizione.

Proposizione 5.2

Sia n primo, $\text{mcd}(n, 6) = 1$. Sia E una curva ellittica su $\mathbb{Z}_n$. Sia $m = \#E(\mathbb{Z}_n)$.

Se m ha un fattore primo q tale che $q > (\sqrt[4]{n} + 1)^2$ allora esiste $P \in E$ tale che:

1. $mP = O$;
2. $\frac{m}{q} P = (x : y : t)$ con $t \in \mathbb{Z}_n^*$.

Dimostrazione

Innanzitutto, notiamo che ogni punto $P \in E$ soddisfa $mP = O$.
Se n è primo, allora la seconda condizione è equivalente ad affermare $t \neq 0$, il che a sua volta è equivalente ad affermare $\frac{m}{q}P \neq O$.

Per assurdo, supponiamo che per ogni $P \in E$ si abbia $\frac{m}{q}P = O$.
Allora l'ordine di ogni $P \in E$ è un divisore di $\frac{m}{q}$ e quindi l'*esponente* e di $E(\mathbb{Z}_n)$ divide $\frac{m}{q}$, cioè $e \mid \frac{m}{q}$ (ricordiamo che l'*esponente* di un gruppo abeliano è il minimo comune multiplo degli ordini degli elementi del gruppo).

Ricordiamo che (si veda il paragrafo 2.3.2)

$$E(\mathbb{Z}_n) \cong \mathbb{Z}_{d_1} \times \mathbb{Z}_{d_2},$$

dove $d_2 \mid d_1$. Quindi l'esponente di $E(\mathbb{Z}_n)$ è $e = d_1$ e $\#E(\mathbb{Z}_n) = d_1 d_2 \leq d_1^2$.

Di conseguenza otteniamo che $m = \#E(\mathbb{Z}_n) \leq d_1^2 \leq \left(\frac{m}{q}\right)^2$ e quindi $q^2 \leq m$.

Utilizzando ora l'ipotesi sulla dimensione di q ed il teorema di Hasse otteniamo

$$\left(\sqrt{n}+1\right)^2 \geq q^2 > \left(\sqrt[4]{n}+1\right)^4$$

da cui segue $\left(\sqrt[4]{n}+1\right)^2 < \left(\sqrt{n}+1\right)$; che è evidentemente falso per ogni n.

□

5.2.1 Idea dell'algoritmo di Goldwasser-Kilian

Descriviamo ora l'idea sui cui si basa l'algoritmo di Goldwasser-Kilian.

Utilizziamo, innanzi tutto, l'algoritmo di Schoof, che ci permette di calcolare $\#E(\mathbb{Z}_n)$ in un tempo polinomiale, per la precisione: $O(\log^8 n)$ (per approfondimenti, si veda Schoof, [12]). Non siamo certi che l'algoritmo di Schoof termini, ma se esso fallisce possiamo già concludere che n è composto.

Poi cerchiamo di dividere m per piccoli primi, sperando di trovare come parte non fattorizzata uno pseudo-primo forte sufficientemente grande.

Goldwasser e Kilian hanno uno scopo puramente teorico, quindi suppongono

$$m = 2q,$$

con q pseudoprimo forte, $q > \left(\sqrt[4]{n}+1\right)^2$.

Supponiamo, per il momento, che q sia primo e cerchiamo casualmente un punto $P \in E$ che soddisfi le ipotesi della Proposizione 5.1. Sappiamo che esso esiste per la Proposizione 5.2. Se troviamo un tale P, è sufficiente provare che q è primo.

Dunque ripetiamo l'algoritmo ricorsivamente, applicandolo ogni volta su un numero che è circa metà del precedente. La ricorsione termina dopo $O(\log n)$ iterazioni.

In realtà ci fermiamo quando n è sufficientemente piccolo per poter verificare la sua primalità con qualche altro metodo (per esempio la divisione per tentativi).

5.2.2 Algoritmo (Goldwasser-Kilian)

Sia n un intero positivo, $n \neq 1$, $\mathrm{mcd}(n, 6) = 1$. L'algoritmo cerca di dimostrare che n è primo. Se n è composto, non è detto che esso termini, in questo caso rischia di andare avanti indefinitamente; per questa ragione, dobbiamo assolutamente utilizzare il test probabilistico di Rabin-Miller prima di applicare questo algoritmo.

1. **inizializzazione:** $i \leftarrow 0$, $n_i \leftarrow n$.

2. **n_i è piccolo?** se $n_i < 2^{30} \Rightarrow$ divisione per tentativi per tutti i primi $< 2^{15}$. Se n_i non è primo $\Rightarrow$ andiamo al punto 9.

3. **Scegli casualmente una curva:** scegliamo casualmente a, $b \in \mathbb{Z}_{n_i}$; verifichiamo $4a^3 + 27b^2 \in \mathbb{Z}_{n_i}^*$ (in caso contrario, torniamo all'inizio del punto 3). Sia E la curva ellittica la cui equazione affine è $y^2 = x^3 + ax + b$.

4. **Usa l'algoritmo di Schoof:** usando l'algoritmo di Schoof calcoliamo $m = \#\ E(\mathbb{Z}_{n_i})$. Se l'algoritmo di Schoof non termina, andiamo al punto 9.

5. **m è ok?** controlliamo se $m = 2q$, dove q passa il test di Rabin-Miller (piú in generale, si divide per tentativi m per primi minori di un piccolo limite e si controlla che il fattore rimanente q superi il test di Rabin-Miller e sia $> \left(\sqrt[4]{n_i} + 1\right)^2$). Se questo passaggio fallisce, andiamo al punto 3.

6. **Trova P:** scegliamo casualmente $x \in \mathbb{Z}_{n_i}$ finché il simbolo di Legendre-Jacobi $\left(\frac{x^3+ax+b}{n_i}\right)$ (descritto al paragrafo 1.3.1) è uguale a 0 o a 1 (questo succederà dopo al piú dopo pochi tentativi). Quindi, calcoliamo $y \in \mathbb{Z}_{n_i}$ tale che $y^2 = x^3 + ax + b$ (con l'algoritmo della radice quadrata (mod n_i)). Se l'algoritmo fallisce, andiamo al punto 9. Altrimenti, definisci $P = (x, y)$.

7. **Controlla P:** calcoliamo $P_1 = mP$ e $P_2 = \left(\frac{m}{q}\right) P$. Se, durante i calcoli, qualche divisione risultasse impossibile, andiamo al punto 9. Altrimenti, controlliamo che $P_1 = O$ (in coordinate proiettive, $P_1 = (0 : 1 : 0)$); se $P_1 \neq O$ andiamo al punto 9. Se $P_2 = O$ andiamo al punto 6.

8. **Ricorsione:** $i = i + 1$, $n_i = q$. Andiamo al punto 2.

9. **Non primo:** (arriviamo qui se n_i non è primo ed è molto improbabile che questo accada) se $i = 0$ rispondiamo in output "n composto" e l'algoritmo termina. Altrimenti, $i = i - 1$, andiamo al passo 3.

Spieghiamo brevemente il funzionamento di questo algoritmo.

Si inizia con $n_0 = n$. Ad ogni iterazione, si testa se n_i è abbastanza piccolo da poterne verificare la primalità con un altro metodo, poi si sceglie casualmente una curva ellittica E su $\mathbb{Z}_{n_i}$ e si calcola la sua cardinalità m. In seguito si cerca di scrivere m come prodotto

di un primo "piccolo" per uno pseudoprimo forte q e si cerca un punto $P \in E$ in modo tale da soddisfare le ipotesi della Proposizione 5.1. Se qualcosa non funziona, vuol dire che il numero n_i che stavamo analizzando non è primo (e quindi andiamo al punto 9) e bisogna ripartire da n_{i-1}, per cercarne un altro n_i che sia primo.

5.2.3 Osservazioni

In realtà il test di Goldwasser-Kilian non è un vero e proprio "algoritmo" bensì un "algoritmo probabilistico". Infatti, esso corre il rischio di restare in esecuzione indeterminatamente, nel caso in cui n non sia primo; inoltre, anche quando n è primo, affinché temini correttamente è necessario trovare la curva E ed il punto $P \in E$ appropriati.

Se accettiamo un'ipotesi ragionevole sulla distribuzione dei primi in piccoli intervalli (vedi Goldwasser-Kilian, [4], pag. 452), allora il tempo di esecuzione è $O(\log^{12} n)$ cioè è polinomiale in $\log n$.

Questo algoritmo non è stato ideato per un uso pratico, bensì per finalità teoriche. Tuttavia, una sua ulteriore utilità è quella di fornire dei *certificati di primalità* nel caso in cui n sia primo e l'algoritmo termini correttamente. Infatti, in questo caso, l'insieme dei valori $n_0 = n,\ n_1, ...,\ n_i, ...,$ unito agli E_i ed ai P_i serve per dimostrare la primalità di n (questi elementi sono difficili da trovare ma, una volta noti, permettono di verificare facilmente le ipotesi della Proposizione 5.1 con $q = n_{i+1}$ e sono quindi un "certificato" della primalità di n). Con questo metodo è stata dimostrata la primalità di numeri con più di mille cifre decimali.

Bibliografia

[1] M. Agrawal, N. Kayal, N. Saxena, "Primes is in P", disponibile sul sito http://www.cse.iitk.ac.in/news/primality_v3.pdf .

[2] H. Cohen, "A course in computational algebraic number theory", GTM 138, Springer-Verlag , 1991.

[3] W. Diffie, M.E. Hellman, "New directions in cryptography", IEEE Transactions on Information Theory, **22** (1976), 644-654.

[4] S. Goldwasser, J. Kilian, "Primality testing using elliptic curves", Journal of the ACM, **46** (1999), 450-472.

[5] D. Husemöller, "Elliptic Curves", GTM 111, Springer-Verlag , 1987.

[6] N. Koblitz, "A course in number theory and cryptography", Springer-Verlag, 1987.

[7] N. Koblitz, "Algebraic aspects of cryptography", Springer-Verlag, 1998.

[8] N. Koblitz, A. Menezes, S. Vanstone, "The state of elliptic curve cryptography", Designs, Codes and Cryptography **19** (2000), 173-193.

[9] A. Languasco, A. Zaccagnini, "Introduzione alla Crittografia", Hoepli editrice, in corso di pubblicazione.

[10] H.W. Lenstra, Jr., "Factoring integers with elliptic curves", Annals of Mathematics, **126**, (1987), 649-673.

[11] A. Menezes, T. Okamoto, S. Vanstone, "Reducing elliptic curve logarithms to logarithms in a finite field", IEEE Transactions on Information Theory, **39** (1993), 1639-1646.

[12] R. Schoof, "Elliptic Curves Over Finite Fields and the computation of square roots mod p", Math. Comp. **43** (1985), 483-494.

[13] P. van Oorschot, M. Wiener, "Parallel collision search with application to hash functions and discrete logarithms", 2nd ACM Conf. on Computer and Communications Security, ACM Press (1994), 210-218.

[14] P. van Oorschot, M. Wiener, "Parallel collision search with cryptanalytic applications", Journal of Cryptology, **12** (1999), 1-28.

[15] L.C. Washington, "Elliptic Curves: Number Theory and Cryptography", Chapman and Hall/CRC, 2003.