Università degli Studi Roma Tre
Facoltà di Scienze M.F.N.
Corso di Laurea in Matematica

Tesi di Laurea Magistrale in Matematica

Counting Points on Elliptic Curves: Schoof Algorithm
(sintesi)

Candidata
Micaela De Santis

Relatore
Prof. Francesco Pappalardi

Anno Accademico 2008-2009
Febbraio 2010

1 Introduzione

Le curve ellittiche in crittografia sono l'argomento principale di questa tesi. Una persona potrebbe chiedersi perché le curve ellittiche sono usate in crittografia. La ragione è che queste permettono di raggiungere una sicurezza equivalente ai sistemi classici usando meno bits. Ad esempio, è stimato che una chiave di 4096 bits per il crittosistema RSA dà lo stesso livello di sicurezza di una chiave di 313 bits in un sistema su una curva ellittica. Ciò vuol dire che l'implementazione di un crittosistema basato sulle curve ellittiche richiede una complessità computazionale inferiore. Il problema di determinare l'ordine del gruppo dei punti razionali su una curva ellittica su un campo finito (il cosiddetto *point counting problem*) è di importanza cruciale nelle applicazioni come il test di primalità e la crittografia. Per le applicazioni crittografiche, viene richiesto che la curva ellittica non sia supersingolare e l'ordine del gruppo dei punti razionali sia divisibile per un fattore primo, sufficientemente grande, che nella pratica può arrivare ad essere lungo alcune centinaia di bits (a volte il minimo richiesto è di 160 bits). Il problema è difficile e richiede soluzioni innovative affinchè i risultati matematici siano abbinabili ad una implementazione pratica ragionevole.

Il problema di contare i punti razionali di una curva ellittica è trattato in questa tesi, dove vengono discussi dei metodi generali per i gruppi finiti ed alcuni metodi specifici per particolari gruppi.

Generare curve adatte alle applicazioni crittografiche dipende dall'abilità di risolvere il problema del contare i punti razionali di un'arbitraria curva ellittica su un campo finito con un numero elevato di elementi. La maggior parte della teoria riguardante questo problema è abbastanza generale, mentre quando il campo considerato ha cardinalità prima p o caratteristica 2, i casi verranno discussi separatamente.

2 Teoria Base

Il primo capitolo della tesi tratta i risultati principali relativi alla teoria base sulle curve ellittiche.

Si consideri un campo $\mathcal{K}$ (ad esempio $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$, $\mathbb{F}_q$, dove $q = p^n$), una curva ellittica, senza punti singolari, è definita dalla seguente **equazione di Weierstrass generale** della forma

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{1}$$

dove a_1, a_2, a_3, a_4, $a_6 \in \mathcal{K}$ sono costanti. L'insieme dei punti sulla curva ellittica con coordinate in un campo $\mathcal{L} \supset \mathcal{K}$ è così definito

$$E(\mathcal{L}) = \{\infty\} \cup \{(x, y) \in \mathcal{L} \times \mathcal{L} \mid y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\}$$

Se la caratteristica del campo è diversa da 2, mediante una trasformazione affine, possiamo trasformare l'Equazione (1) nella seguente:

$$y^2 = x^3 + ax^2 + bx + c.$$

Se la caratteristica del campo è anche diversa da 3, allora l'equazione che è possibile ricavare, con il nome di **equazione di Weierstrass** per una curva ellittica, è la seguente:

$$y^2 = x^3 + Ax * B$$

dove $-(4A^3 + 27B^2) \neq 0$, ovvero la curva non è singolare (sul caso delle curve singolari ci soffermeremo in seguito). Se così non fosse ci troveremmo nel caso particolare in cui $(x^3 + Ax + B)$ ha radici multiple, ma questo caso verrà trattato separatamente.

Quando la caratteristica del campo è 2 allora la curva ellittica può avere una delle seguenti forme:

1. $y^2 + xy = x^3 + a_2x^2 + a_6$ con $a_6 \neq 0$,
2. $y^2 + a_3y = x^3 + a_4x + a_6$ con $a_3 \neq 0$.

Sulle curve ellittiche è possibile definire un'operazione di somma e, di seguito, viene riportata nel caso in cui la caratteristica del campo è diversa da 2 e da 3:

$$P_1 +_E P_2 = \begin{cases} P_1 & \text{se } P_2 = \infty \\ \infty & \text{se } P_1 = (x_1, y_1),\ P_2(x_2, y_2) \\ & \text{e } x_1 = x_2 \text{ o } y_1 = y_2 = 0 \\ (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1) & m = \frac{y_2 - y_1}{x_2 - x_1} \text{ se } x_2 \neq x_1 \\ (m^2 - x_1 - x_2, m(x_1 - x_3) - y_1) & m = \frac{3x_1^2 + A}{2y_1} \text{ se } x_1 = x_2 \text{ e} \\ & y_1 = y_2 \neq 0 \end{cases}$$

E' possibile dimostrare che i punti con coordinate in $\mathcal{K}$, della curva ellittica E, uniti al punto all'infinito, formano un gruppo rispetto alla somma sopra definita, con ∞ come elemento neutro.

Sia $\mathcal{K}$ un campo, la relazione d'equivalenza $\sim$ tra due terne in $\mathcal{K}^3 \setminus \{(0,0,0)\}$ è così definita

$$(x, y, z) \sim (x_1, y_1, z_1) \Leftrightarrow \exists \lambda \in \mathcal{K}^* \text{ tale che } x = \lambda x_1,\ y = \lambda y_1,\ z = \lambda z_1.$$

Lo spazio proiettivo $\mathbb{P}^2_{\mathcal{K}}$ è dato dall'insieme delle classi d'equivalenza $[x : y : z]$ dove $x,\ y,\ z \in \mathcal{K}$ e $(x, y, z) \neq (0, 0, 0)$:

$$\mathbb{P}^2_{\mathcal{K}} = \{[x : y : z] \mid (x, y, z) \in \mathcal{K}^3 \setminus \{(0,0,0)\}\}.$$

In particolare i punti con $z \neq 0$ sono i punti finiti nel piano proiettivo, mentre i punti del tipo $[x, y, 0]$ sono i punti all'infinito. Possiamo considerare l'inclusione tra il piano affine 2-dimensionale e il piano proiettivo

$$\begin{aligned} \mathbb{A}^2_K &\hookrightarrow \mathbb{P}^2_K \\ (x, y) &\longmapsto [x : y : 1]. \end{aligned}$$

Così facendo, è possibile identificare il piano affine con i punti finiti nello spazio proiettivo. Se consideriamo una curva piana C, ad essa sarà associata una curva proiettiva $\mathbb{P}C$. Allora, un punto (x, y) sulla curva originaria è associato al punto $(x, y, 1)$ della rispettiva curva proiettiva e l'unico punto all'infinito ∞ sulla curva ellittica corrisponde al punto $(0, 1, 0)$ sulla curva proiettiva. Il lemma utilizzato per quantificare l'ordine con cui una retta interseca una curva, è il seguente:

Lemma 2.1. *Sia $G(u, v)$ un polinomio omogeneo non nullo e sia $(u_0 : v_0) \in \mathbb{P}^1_{\mathcal{K}}$. Allora esiste un intero $k \geq 0$ e un polinomio $H(u, v)$ con $H(u_0, v_0) \neq 0$ tale che*

$$G(u, v) = (v_0 u - u_0 v)^k H(u, v).$$

Un'importante quantità associata ad una curva ellittica è il j**-invariante** che, nel caso in cui la caratteristica del campo è diversa da 2 e 3, è così esprimibile

$$j = j(E) = 1728 \frac{4A^3}{4A^3 + 27B^2},$$

altrimenti ci sono altre formule che dipendono sempre dai coefficienti della curva.

Definizione 2.1.

1. Se due curve ellittiche hanno lo stesso j-invariante allora noi diciamo che le due curve sono una **twist** dell'altra.
2. Sia $E : y^2 = x^3 + Ax + B$ una curva ellittica definita su un campo $\mathbb{F}_q$, sia $g \in \mathbb{F}_q \setminus \mathbb{F}_q^2$, allora $E_g : y^2 = x^3 + Axg^2 + Bg^3$ viene detta la curva **twist**.

Molto spesso, in questa tesi si parlerà di endomorfismi ed è quindi utile darne una definizione formale.

Definizione 2.2. Sia $\alpha : E(\overline{\mathcal{K}}) \to E(\overline{\mathcal{K}})$ un omomorfismo. α è un **endomorfismo** di E se esistono due funzioni razionali $R_1(x, y)$, $R_2(x, y) \in \overline{\mathcal{K}}(x, y)$, tali che, per ogni punto $P \in E(\mathcal{K})$, dove $\alpha P \neq \infty$, $\alpha(P) = (R_1(x, y), R_2(x, y))$.

In particolare si può dimostrare che $\alpha(P) = (r_1(x), yr_2(x))$, dove r_1, r_2 sono funzioni razionali nella sola incognita x. Uno degli endomorfismi che più useremo in questo lavoro è la moltiplicazione per un intero n. Ovvero $[n] : P \mapsto nP$ dove P, $nP \in E(\overline{\mathcal{K}})$.

Definizione 2.3. Sia $\alpha(P) = (\frac{p(x)}{q(x)}, yr(x))$, con $\gcd(p(x), q(x)) = 1$, definiamo

- il **grado** di α il massimo tra i gradi di $p(x)$ e $q(x)$;
- $\alpha \neq 0$, si dice **separabile** se la derivata $(p(x)/q(x))'$ non è identicamente nulla. α si dice **non separabile** altrimenti.

In particolare si dimostra che la moltiplicazione per n è un endomorfismo di grado n^2 e separabile se e solo se la caratteristica del campo non divide n

Finora abbiamo considerato le curve ellittiche in cui $x^3 + Ax + B$ non ammette radici multiple. Nel caso in cui questo avviene la curva viene detta **singolare**. A meno di traslazioni, possiamo dividerle in due categorie:

- $y^2 = x^3$, con una radice tripla in $x = 0$;
- $y^2 = x^2(x + a)$, con una radice doppia in $x = 0$.

Questo tipo di curve ha un problema principale, i punti su di esse non generano un gruppo; quindi per essere utilizzabili in crittografia bisogna considerare i punti non singolari.

Consideriamo sempre un campo $\mathcal{K}$ e la sua rispettiva chiusura algebrica $\overline{\mathcal{K}}$, sia $n \in \mathbb{N}_{>1}$, definiamo il **sottogruppo di torsione** $E[n] \stackrel{def}{=} \{P \in E(\overline{\mathcal{K}})$ tale che $nP = \infty\}$. Questi sottogruppi di $E(\overline{\mathcal{K}})$ sono di fondamentale importanza nello studio teorico delle curve ellittiche. Uno dei teoremi fondamentali riguardante questo argomento è il seguente

Teorema 2.1. *Sia E una curva ellittica su un campo $\mathcal{K}$ di caratteristica 0 o p primo. Sia n un intero positivo, se p non divide n o la caratteristica è zero, allora*

$$E[n] = C_n \times C_n.$$

Se p divide n, posto $n = p^r n'$ con $p \nmid n'$, allora

$$E \simeq C_{n'} \times C_{n'} \text{ or } C_n \times C_{n'}.$$

Per descrivere la mappa su una curva ellittica, definita in un campo con caratteristica diversa da 2 e da 3, data dalla moltiplicazione per un intero, introduciamo i **polinomi di divisione** $\psi_m(x, y)$ definiti dalle seguenti formule ricorsive:

$$\begin{aligned}
&\psi_0 = 0,\\
&\psi_1 = 1,\\
&\psi_2 = 2y,\\
&\psi_3 = 3x^4 + 6Ax^2 + 12Bx - A^2,\\
&\psi_4 = 4y(x^6 + 5Ax^4 + 20Bx^3 - 5A^2x^2 - 4ABx - 8B^2 - A^3),\\
&\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m-1}\psi_{m+1}^3,\ m \geq 2,\\
&\psi_{2m} = (\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2)\psi_m/2y,\ m > 2.
\end{aligned}$$

Dove A, B sono i coefficienti dell' Equazione di Weierstrass. Ora è possibile definire i polinomi θ_m and ω_m

$$\theta_m = x\psi_m^2 - \psi m - 1\psi_{m+1},\ m \geq 1,$$
$$\omega_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{4y},\ m \geq 1.$$

Il seguente teorema ci permette di calcolare m volte un punto.

Teorema 2.2. *Sia E una curva ellittica definita su un campo $\mathcal{K}$ e sia m un intero positivo. Esistono dei polinomi ψ_m, θ_m, $\omega_m \in \mathcal{K}[x, y]$, tali che, se $[m]P \neq \infty$, risulta*

$$[m]P = \left(\frac{\theta_m(x,y)}{\psi_m(x,y)^2}, \frac{\omega_m(x,y)}{\psi_m(x,y)^3}\right). \tag{2}$$

Uno dei risultati più importanti, riguardante la teoria base delle curve ellittiche e il relativo problema di calcolare la cardinalità dei punti su di essa con coordinate in un campo finito, è il seguente Teorema di Hasse.

Teorema 2.3 (Hasse)**.** *Sia E una curva ellittica definita su un campo finito $\mathbb{F}_q$. Allora l'ordine di $E(\mathbb{F}_q)$ soddisfa la relazione che segue*

$$\mid q + 1 - \sharp \mathrm{E}(\mathbb{F}_q) \mid \leq 2\sqrt{q}.$$

Sia $\mathbb{F}_q$ un campo finito con q elementi nella chiusura algebrica $\overline{\mathbb{F}_q}$ e sia

$$\begin{aligned} \Phi_q : E(\overline{\mathbb{F}_q}) &\to E(\overline{\mathbb{F}_q}) \\ (x, y) &\mapsto (x^q, y^q) \\ \infty &\mapsto \infty \end{aligned}$$

la mappa di Frobenius che agisce sulle coordinate dei punti in $E(\overline{\mathbb{F}_q})$. É possibile dimostrare che Φ_q è un endomorfismo non separabile di grado q. Il teorema che verrà enunciato di seguito ci permette di definire il **polinomio caratteristico di Frobenius** che verrà utilizzato spesso nel corso della tesi.

Teorema 2.4. *Sia E una curva ellittica definita su $\mathbb{F}_q$. Sia $a \stackrel{def}{=} q + 1 - \sharp E(\mathbb{F}_q)$, allora*

$$\Phi_q^2 - a\Phi_q + q = 0$$

è un endomorfismo di E e a è l'unico intero tale che

$$\Phi_q^2 - k\Phi_q + q = 0.$$

In altre parole se $(x, y) \in E(\overline{\mathbb{F}_q})$, allora

$$(x^{q^2}, y^{q^2}) - a(x^q, y^q) + q(x, y) = \infty,$$

e a è l'unico intero tale che questa relazione vale per tutti $(x, y) \in E(\overline{\mathbb{F}_q})$.

Il polinomio caratteristico dell'endomorfismo di Frobenius è pertanto $X^2 - aX + q$.

3 Calcolare la Cardinalità di una Curva Ellittica. Prima di Schoof

In questa sezione affronteremo il problema di calcolare la cardinalità dei punti su una curva ellittica prima del 1985, anno in cui Schoof pubblicò il suo articolo diffondendo un algoritmo con tempo computazionale polinomiale.

Sia E una curva ellittica definita su $\mathbb{F}_q$ di cui già si conosce la cardinalità, se vogliamo trovare l'ordine della stessa in un'estensione $\mathbb{F}_{q^n}$ abbiamo delle formule ricorsive che ci permettono di fare direttamente questo calcolo. Supponiamo che α e β siano le radici del polinomio caratteristico, ovvero che $X^2 + AX + B = (X - \alpha)(X - \beta)$.

Teorema 3.1. *Sia* $\sharp E(\mathbb{F}_q) = q + 1 - a$, *allora*

$$\sharp \mathrm{E}(\mathbb{F}_{q^n}) = q^n + 1 - (\alpha^n + \beta^n)$$

per ogni $n \geq 1$.

Definiamo

$$\begin{aligned} s_0 &= 2, \\ s_1 &= a, \\ s_{n+1} &= a s_n - q s_{n-1}. \end{aligned}$$

Allora possiamo concludere con il seguente enunciato

Lemma 3.1. $s_n = \alpha^n + \beta^n$ *per ogni* $n \geq 1$.

Definizione 3.1. Definiamo l'**ordine** $P \in E(\mathbb{F}_q)$ il più piccolo intero k tale che $kP = \infty$. In altre parole

$$\mathrm{ord}(P) \stackrel{def}{=} min\{t \in \mathbb{N}_{\geq 1} \text{ tale che } tP = \infty\}.$$

Uno dei metodi per calcolare la cardinalità di una curva, è il metodo di Legendre. Ricordiamo che il simbolo di Legendre per un dato primo p è definito nel seguente modo

$$\left(\frac{x}{p}\right) = \begin{cases} +1 & \text{se } t^2 \equiv x \pmod{p} \text{ ha due soluzioni in } \mathbb{F}_p, \\ -1 & \text{se } t^2 \equiv x \pmod{p} \text{ non ha soluzioni in } \mathbb{F}_p \\ 0 & \text{se } x \equiv 0 \pmod{p}. \end{cases}$$

Qust'ultimo può essere generalizzato ad un campo finito $\mathbb{F}_q$, con q dispari, per $x \in \mathbb{F}_q$,

$$\left(\frac{x}{\mathbb{F}_q}\right) = \begin{cases} +1 & \text{se } t^2 = x \text{ ha soluzioni } t \in \mathbb{F}_q{}^*, \\ -1 & \text{se } t^2 = x \text{ non ha soluzioni } t \in \mathbb{F}_q, \\ 0 & \text{se } x = 0. \end{cases}$$

Questo simbolo di Legendre generalizzato viene usato nel seguente modo:

Teorema 3.2. *Sia E una curva ellittica su $\mathbb{F}_q$ definita da $y^2 = x^3 + Ax + B$, allora*

$$\sharp E(\mathbb{F}_q) = q + 1 + \sum_{x \in \mathbb{F}_q} \left(\frac{x^3 + Ax + B}{\mathbb{F}_q} \right).$$

Un altro metodo per calcolare la cardinalità di E sul campo finito $\mathbb{F}_q$, è quello di trovare un punto $P \in E(\mathbb{F}_q)$ in modo che il suo ordine k è tale che $k \geq 4\sqrt{q}$. In questo modo, essendo l'intervallo di Hasse di ampiezza di $4\sqrt{q}$ e sapendo che la cardinalità della curva si trova in quell'intervallo, basterà prendere l'unico multiplo dell'ordine del punto P , questo sarà l'ordine di $E(\mathbb{F}_q)$ cercato.

La conferma del fatto che questo potrebbe risultare un metodo utilizzabile è il seguente teorema, dovuto a Mestre.

Teorema 3.3 (Mestre)**.** *Sia $p > 229$ un primo e sia E una curva ellittica definita su $\mathbb{F}_p$, allora una tra $E(\mathbb{F}_p)$ o la rispettiva curva twist $E'(\mathbb{F}_p)$ ha un punto P tale che il suo ordine ha solo un multiplo nell'intervallo di Hasse, ovvero tale che $ord(P) > 4\sqrt{p}$.*

Se non troviamo subito un punto con ordine maggiore di $4\sqrt{q}$, è possibile acquisire comunque informazioni ed eventualmente, dopo aver considerato un altro punto random (o più) e trovato il rispettivo ordine, possiamo restringere ulteriormente i casi nell'intervallo di Hasse considerando i multipli del minimo comun multiplo tra i vari ordini.

Uno dei metodi più usati per calcolare l'ordine di un punto, è l'algoritmo **Baby Step Giant Step** (BSGS).

Baby Step Giant Step (BSGS)	
INPUT:	E, curva ellittica su $\mathbb{F}_q$ $P \in E(\mathbb{F}_q)\backslash\{\infty\}$.
OUTPUT:	L'ordine del punto P.
1.	$Q \longleftarrow (q+1)P$.
2.	Fissare $m \in \mathbb{N}$ tale che $m > q^{1/4}$, (cioè $m = [q^{1/4}] + 1$). ($m = \vartheta(q^{1/4})$).
3.	$R \longleftarrow 2mP$.
4.	Calcolare e memorizzare jP per $j = 0, 1, \cdots, m$ (Baby Step).
5.	Calcolare $Q + kR$ per $k = -m, -m+1, \cdots, m-1, m$ finchè si trovi un'uguaglianza $Q + kR = \pm jP$ per qualche j (Giant Step).
6.	RETURN $N = q + 1 + 2mk \mp j$.
7.	Fattorizzare N.
8.	Per ogni primo $l \mid N$, calcolare $\frac{N}{l}P$.
9.	Se $\frac{N}{l}P = \infty$, allora $N \longleftarrow \frac{N}{l}$ e tornare al passo 7.
10.	Se $\frac{N}{l}P \neq \infty$ allora andare al passo successivo.
11.	RETURN ord$(P) = N$.

L'algoritmo converge, cioè esiste $k \in [-m, m]$ tale che $Q + kR = \pm jP$ per qualche $j = 0, 1, \cdots, m$ se e solo se esistono k, j tale che $(q+1+2km \mp j)P = \infty$, ma è noto che $\sharp E(\mathbb{F}_q) = q + 1 - a_q$ allora $\mid a_q \mid \leq 2\sqrt{q} = 2m^2$. Notare che se k varia tra $-m$ e m, anche $-k$ varia tra $-m$ e m, la stessa cosa è per $j_0 \in (-m, m]$ allora $\mp j \in [-m, m]$. Ciò deriva dal seguente lemma

Lemma 3.2. *Sia $m \in \mathbb{N}$ e $a \in \mathbb{Z}$ tale che $\mid a \mid \leq 2m^2$, allora esistono $a_0 \in (-m, m]$ e $a_1 \in [-m, m]$ tali che $a = a_0 + 2ma_1$.*

allora esiste $k \in [-m, m]$ e $j_0 \in (-m, m]$ tale che

$$a_q = j_0 + 2km,$$

cioè

$$(q + 1 - 2km - j_0)P = \infty.$$

Riguardo la complessità di questo algoritmo, i punti (1), (2), (3) richiedono $\vartheta(\lg^3 q)$ operazioni bit, infatti dobbiamo calcolare n volte un punto con l'algoritmo dei quadrati successivi. Il punto (4) richiede m somme in $\mathbb{F}_q$ che corrispondono a $\vartheta(m \lg^3 q)$ operazioni bit. Abbiamo la stessa complessità nel punto (5), perché dobbiamo effettuare $2m$ somme in $\mathbb{F}_q$, e il fattore 2 non cambia la complessità. Infine gli altri punti hanno al più la stessa complessità. In conclusione, visto che $m = \vartheta(q^{1/4})$, la complessità totale è

$\vartheta(q^{1/4} \lg^3 q)$. Possiamo usare qualche strada alternativa in particolare per evitare il sovraccarico nella fase della memorizzazione, ad esempio memorizzando solo la coordinata x dei punti jP e calcolare solo quando necessario la coordinata y. Invece, per compiere operazioni di entità minore possiamo ad esempio, piuttosto che calcolare $Q + kR$ per ogni k richiesto, calcolare il primo per $k = -m$ e poi sommare ogni volta R eseguendo, così, solo una somma.

Alcune curve speciali hanno metodi più diretti e facili per calcolare la loro cardinalità; sono ad esempio quelle del tipo

$$E : y^2 = x^3 - kx, \text{ con } k \not\equiv 0 \pmod{p},$$

oppure le curve supersingolari. Le prime soddisfano il seguente teorema

Teorema 3.4. *Sia p un primo dispari e sia $k \not\equiv 0 \pmod{p}$. Sia $N_p = \sharp E(\mathbb{F}_p)$, dove $E : y^2 = x^3 - kx$.*

1. *Se $p \equiv 3 \pmod 4$, allora $N_p = p + 1$.*
2. *Se $p \equiv 1 \pmod 4$, possiamo scrivere $p = a^2 + b^2$, (ciascun primo $p \equiv 1 \pmod 4$ può essere scritto come somma di due quadrati), dove a e b sono interi tali che b è pari e $a + b \equiv 1 \pmod 4$, allora*
   - *$N_p = p + 1 - 2a$ se $k \in (\mathbb{F}_p{}^*)^4$,*
   - *$N_p = p + 1 + 2a$ se $k \in (\mathbb{F}_p{}^*)^2 \setminus (\mathbb{F}_p{}^*)^4$,*
   - *$N_p = p + 1 \pm 2b$ se $k \notin (\mathbb{F}_p{}^*)^2$.*

Ora, daremo una definizione formale delle curve del secondo tipo.

Definizione 3.2. Sia E una curva ellittica definita su $\mathbb{F}_q$, allora diciamo che E è **supersingolare** se $E[p] = \{\infty\}$

É importante che il termine supersingolare non venga confuso con singolare. L'unica cosa che accomuna questi due tipi di curve è il termine singolare che fa riferimento al fatto che entrambe hanno il loro gruppo di endomorfismi isomorfo ad un anello più grande di $\mathbb{Z}$.

Proposzione 3.1. *Sia* E *una curva ellittica su $\mathbb{F}_q$ dove q è una potenza di un primo p. Sia $a = q + 1 - \sharp E(\mathbb{F}_q)$. Allora* E *è supersingolare se e solo se*

$$a \equiv 0 \pmod{p},$$

cioè, se e solo se $\sharp E(\mathbb{F}_q) \equiv 1 \pmod p$.

Corollario 3.1. *Supponiamo $p > 5$ primo, allora E è una curva supersingolare se e solo se $a = 0$, cioè se e solo se $\sharp E(\mathbb{F}_p) = p + 1$.*

Proposzione 3.2. *Supponiamo che q sia dispari e $q \equiv 2 \pmod 3$. Sia $B \in \mathbb{F}_q{}^*$. Allora la curva ellittica E data da $y^2 = x^3 + B$ è supersingolare.*

Osservazione 3.1. Un importante sviluppo sulle curve supersingolari è che l'implementazione per calcolare un numero intero di volte un punto sulla curva ellittica, può essere più veloce del previsto. Infatti, assumiamo $a = 0$, allora

$$\Phi_q^2 + q = 0,$$

è il polinomio caratteristico. Allora abbiamo che

$$q(x, y) = -\Phi_q^2(x, y) = (x^{q^2}, -y^{q^2}).$$

Quindi x^{q^2}, y^{q^2} coinvolge un'aritmetica su campi finiti, che in generale è più rapida rispetto alle operazioni sulle curve ellittiche.

4 Un Algoritmo con Tempo Computazionale Polinomiale: Schoof

In questo Capitolo verrà trattato l'argomento centrale della tesi, che dà anche il nome a tutto il lavoro, ovvero l'algoritmo con complessità polinomiale di Schoof, pubblicato in un articolo del 1985. Il risultato di questo algoritmo è comunque ancora poco utilizzabile in crittografia, ma ha, comunque, aperto molte starde a significativi miglioramenti.

Consideriamo una curva ellittica definita su un campo $\mathbb{F}_q$ con caratteristica diversa da 2 e da 3, $E : y^2 = x^3 + Ax + B$. Per il Teorema di Hasse

$$\sharp E(\mathbb{F}_q) = q + 1 - a,$$

e

$$\mid a \mid \leq 2\sqrt{q}.$$

a soddisfa la relazione $\Phi_q^2(P) - a\Phi_q(P) + qP = \infty$, per ogni $P \in E(\overline{\mathbb{F}_q})$. L'idea di Schoof è di calcolare il valore a modulo ciascun primo $l = 2, 3, \cdots, L$ differente dalla caratteristica del campo p e con L tale che la produttoria di tali primi sia maggiore di $4\sqrt{q}$. In questo modo, applicando il Teorema Cinese dei Resti, posso calcolare a modulo tale produttoria. Tale valore sarà univocamente determinato dalla condizione del Teorema di Hasse. Chiamiamo S l'insieme di tale primi. Il caso in cui $l = 2$ va trattato separatamente rispetto agli altri. Infatti, in questo caso è sufficiente notare se ci sono o meno punti di ordine 2, ovvero della forma $(x, 0)$. É possibile scrivere $x^3 + Ax + B = (x - e_1)(x - e_2)(x - e_3)$ con $e_i \in \overline{\mathbb{F}_q}$. Esiste un punto di ordine 2 se e solo se esiste i tale che $e_i \in \mathbb{F}_q$. Quindi è necessario controllare se il massimo comun divisore tra $x^3 + Ax + B$ e $x^q - x$ (le cui radici sono tutti e

soli gli elementi di $\mathbb{F}_q$) è uguale o diverso da 1. Nel caso in cui è uguale a 1 allora $2 \nmid \sharp E(\mathbb{F}_q)$, ne segue che

$$a \equiv 1 \pmod 2,$$

altrimenti $2 \mid \sharp E(\mathbb{F}_q)$ e quindi

$$a \equiv 0 \pmod 2.$$

Consideriamo ora il caso in cui $l > 2$. Notiamo che l è dispari e quindi $\psi_l(x)$, l'l-esimo polinomio di divisione, dipende solo da x e si ha quindi che $(x, y) \in E[n] \Leftrightarrow \psi_n(x) = 0$. Sia Φ_q l'endomorfismo di Frobenius definito prima, per quello che abbiamo detto, abbiamo che $\Phi_q^2(P) - a\Phi_q(P) + q(P) = \infty$, per ogni $P \in E(\overline{\mathbb{F}_q})$. Sia $(x, y) \in E[l]$, dato che $E[l] \subset E(\overline{\mathbb{F}_q})$ abbiamo che $(x^{q^2}, y^{q^2}) + q(x, y) = a(x^q, y^q)$. Sia $q \equiv q_l \pmod l$ tale che $\mid q_l \mid < \frac{l}{2}$, poichè (x, y) è un punto di l-torsione, $q(x, y) = q_l(x, y)$ e quindi

$$(x^{q^2}, y^{q^2}) + q_l(x, y) = a(x^q, y^q). \tag{3}$$

Notiamo che se $(x, y) \in E[l]$ allora anche $(x^q, y^q) \in E[l]$. Ora affrontiamo tre diversi casi

1. Se
$$\Phi_q^2(x, y) = -q_l(x, y)$$
per qualche $(x, y) \in E[l]$, abbiamo che
$$\infty = (\Phi_q^2 - a\Phi_q + q)(x, y) = -a\Phi_q(x, y).$$
Dato che $\Phi_q(x, y) \neq 0$, ed è un punto di l-torsione, allora $a \equiv 0 \pmod l$.

2. Consideriamo invece ora il caso in cui
$$\Phi_q^2(x, y) = (x^{q^2}, y^{q^2}) = q_l(x, y).$$
Possiamo dedurre che esiste $\omega \in \mathbb{F}_q$ tale che $q \equiv \omega^2 \pmod l$ e concludere quindi che, se $gcd(\text{numerator}(x^q - x_\omega), \psi_l) \neq 1$, dove con x_ω stiamo indicando la coordinata x di ω volte il punto, allora esiste qualche $(x, y) \in E[l]$ tale che $\Phi_q(x, y) = \pm\omega(x, y)$. Se ciò accade calcoliamo anche la coordinata y per determinarne il segno. Se il massimo comun divisore è 1, non possiamo trovarci in questo caso. In conclusione, trovato ω possiamo concludere che
$$a \equiv \pm 2\omega \pmod l.$$

3. Infine consideriamo che

$$(x^{q^2}, y^{q^2}) \neq \pm q_l(x, y)$$

per qualche $(x, y) \in E[l]$. Allora

$$(x', y') \stackrel{def}{=} (x^{q^2}, y^{q^2}) + q_l(x, y) \neq \infty,$$

e quindi $a \not\equiv 0 \pmod{l}$. Qui la somma di due punti sulla curva ellittica è definita dalla legge di gruppo che abbiamo citato precedentemente. Per prima cosa, notiamo che la coordinata x' è ben definita date le condizioni che abbiamo imposto. Lo scopo, qui, è quello di trovare un intero j tale che $(x', y') = (x_j^q, y_j^q)$. Ovvero per $j = 1, \cdots, \frac{l-1}{2}$ dobbiamo verificare che $x' = x_j^q$, cioè che $x' - x_j^q \equiv 0 \pmod{\psi_l}$. Qui stiamo usando il fatto che ψ_l ha solo radici semplici, altrimenti otterremmo solo che ψ_l divide una qualche potenza di $x' - x_j^q$. Questo intero così cercato è unico. Una volta individuato j_0, si calcola y' e il rispettivo $y_{j_0}^q$ per vedere se il valore cercato è j_0 o $-j_0$ verificando se $\frac{y' - y_{j_0}^q}{y} \equiv 0 \pmod{\psi_l}$ o meno. Possiamo quindi concludere che

$$a \equiv \pm j_0 \pmod{l}$$

L'ultimo passo consiste nel raccogliere tutte le informazioni ottenute, applicare il Teorema Cinese dei Resti e trovare, infine, il valore di a cercato, rispettando la condizione del Teorema di Hasse. Concludendo, il numero dei punti è

$$\sharp E(\mathbb{F}_q) = q + 1 - a.$$

Algoritmo di Schoof

INPUT: Una curva ellittica su un campo $\mathbb{F}_q$ data da $y^2 = x^3 + Ax + B$, dove la caratteristica del campo p è diversa da 2 e da 3.

OUTPUT: La cardinalità della curva su $\mathbb{F}_q$.

1. Scegliere un insieme di primi $S = \{2, 3, 5, \cdots, L\}$ con $p \notin S$, tali che $\prod_{l \in S} l > 4\sqrt{q}$.
2. Se $l = 2$,
3. se $gcd(x^3 + Ax + B, x^q - x) \neq 1$ allora $a \equiv 0 \pmod 2$,
4. altrimenti, se $gcd(x^3 + Ax + B, x^q - x) = 1$ allora $a \equiv 1 \pmod 2$.
5. Per ciascun primo $l > 2$
6. Se $\Phi_q^2(x, y) = -q(x, y)$ allora $a \equiv 0 \pmod l$.
7. Se $\Phi_q^2(x, y) = q(x, y)$ allora $\omega^2 \equiv q \pmod l$, quindi si ha che $gcd(\text{numerator}(x^q - x_\omega), \Psi_l) \neq 1$ e
8. se $gcd(\text{numerator}\left(\frac{y^q - y_\omega}{y}\right), \Psi_l) \neq 1$ allora $a \equiv 2\omega \pmod l$,
9. se $gcd(\text{numerator}\left(\frac{y^q - y_\omega}{y}\right), \Psi_l) = 1$ allora $a \equiv -2\omega \pmod l$.
10. Se $\Phi_q^2(x, y) \neq \pm q(x, y)$ allora
11. Sia $q_l \equiv q \pmod l$, con $\mid q_l \mid < l/2$
12. Calcolare la coordinata x, cioè x', di $(x', y') = (x^{q^2}, y^{q^2}) + q_l(x, y)(mod \quad \Psi_l)$.
13. Per $j = 1, \cdots, \frac{l-1}{2}$ fare le seguenti operazioni
14. Calcolare la coordinata x, x_j di $(x_j, y_j) = j(x, y)$.
15. Se $x' - x_j \equiv 0 \pmod{\psi_l}$, passare al punto successivo. (Dobbiamo trovare j, altrimenti non sarebbe il caso 3).
16. Calcolare y' e y_j. Se $(y' - y_j)/y \equiv 0 \pmod{\psi_l}$, allora, $a \equiv j \pmod l$. Altrimenti, $a \equiv -j \pmod l$.
17. Usando i valori noti $a \pmod l$, per ogni $l \in S$ per calcolare $a \pmod{\prod l}$. Si sceglie il valore di a che soddisfa la congruenza ed è tale che $\mid a \mid \leq 2\sqrt{q}$.
18. Return $\sharp E(\mathbb{F}_q) = q + 1 - a$.

La complessità dell'algoritmo è alta perché i calcoli computazionalmente più complessi da effettuare sono x^q, y^q, x^{q^2}, y^{q^2}, riducibili modulo ψ_l, il cui grado è $\vartheta(l^2) = \vartheta(\lg^2 q)$. Se usiamo un'aritmetica semplice, ciascuna di queste moltiplicazioni nell'anello $\mathbb{F}_q[x]/\langle\psi_l(x)\rangle$ richiede $\vartheta(\lg^4 q)$ moltiplicazioni in $\mathbb{F}_q$, ciascuna delle quali richiede $\vartheta(\lg^2 q)$ operazioni bits. Questi valori vengono calcolati una volta per ogni primo e dato che il numero dei primi l che considero è $\vartheta(\lg q)$, allora possiamo concludere che la complessità totale è di $\vartheta(\lg^8 q)$ operazioni bits. Il resto è trascurabile rispetto a queste complessità, ad esempio anche il calcolo dei polinomi di divisione è $\vartheta(\lg^7 q)$. Usando un'aritmetica più sofisticata possiamo ridurre la complessità $\vartheta(\lg^{5+\epsilon} q)$ operazioni bits, ma questo è un risultato più teorico che realmente implementabile.

5 I Polinomi Modulari

Il problema principale dell'Algoritmo di Schoof, è di diminuire il grado dei polinomi per cui si effettuano le riduzioni. In questa sezione introduciamo i **polinomi modulari**, che sono alla base della teoria dei miglioramenti di Elkies ed Atkin, per arrivare così all'implementazione dell'Algoritmo Schoof-Elkies-Atkin (detto SEA).

Esiste una corrispondenza tra il gruppo quoziente $\mathbb{C}$ modulo un reticolo $\Lambda = \mathbb{Z}\omega_1 + \mathbb{Z}\omega_2$ con $\omega_1, \omega_2 \in \mathbb{C}$ e una curva ellittica definita su $\mathbb{C}$. ω_1, ω_2 sono i periodi della funzione $\wp$ di Weierstrass doppiamente periodica

$$\wp(z) = \frac{1}{z^2} + \sum_{\omega\in\Lambda\setminus 0}\left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2}\right). \tag{4}$$

Questa funzione soddisfa la seguente equazione differenziale

$$\wp'^2 = 4\wp^3 - g_2\wp - g_3,$$

per qualche costante g_2, g_3. La corrispondenza è data da

$$\begin{aligned} \mathbb{C}/\Lambda &\longrightarrow E \\ z + \Lambda &\mapsto (\wp(z), \wp'(z)/2), z \notin \Lambda \\ \Lambda &\mapsto \infty \end{aligned}$$

Denotiamo con $\tau = \omega_1/\omega_2$ il rapporto che ci permette di dire che due curve relative ad un dato reticolo sono isomorfe e indichiamo con E_τ questo insieme di curve. Possiamo considerare il j-invariante della curva come una funzione di τ su $\mathcal{H}$, ovvero $\tau \in \mathbb{C}$ tale che $\Im(\tau) > 0$, $j(\tau) = j(E_\tau)$.

Lemma 5.1. *Per ogni matrice*

$$A = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z})$$

dove $SL_2(\mathbb{Z})$ è il gruppo lineare speciale delle matrici 2×2 su $\mathbb{Z}$ tali che il loro determinate è 1, allora abbiamo

$$j\left(\frac{a\tau + b}{c\tau + d}\right) = j(\tau).$$

Anche $j(\tau)$ è una funzione periodica di periodo 1 e ha come serie di Fourier

$$j(\tau) = \frac{1}{q} + 744 + 196884q + 21493760q^2 + \sum_{n\geq 3} c_n q^n, \tag{5}$$

dove $q = e^{2\pi i\tau}$, e c_n sono interi positivi.

Ora enunciamo solamente alcune funzioni e serie che sono definite da espansioni nella variabile $q = e^{2\pi i\tau}$ e che sono in relazione al j-invariante.

$$\Delta(\tau) = \Delta(E_\tau) = q\prod_{n=1}^{\infty}(1-q^n)^{24}, \tag{6}$$

quest'ultima è la 24-esima potenza di una nota funzione ovvero la funzione η di Dedekind. Useremo le seguenti serie

$$\begin{aligned} E_2(\tau) &= 1 - 24\sum_{n=1}^{\infty}\frac{nq^n}{1-q^n}, \\ E_4(\tau) &= 1 + 240\sum_{n=1}^{\infty}\frac{n^3q^n}{1-q^n}, \\ E_6(\tau) &= 1 - 504\sum_{n=1}^{\infty}\frac{n^5q^n}{1-q^n}. \end{aligned} \tag{7}$$

Queste possono essere messe in relazione con le serie del discriminante e del j-invariante come segue

$$\begin{aligned} \Delta(\tau) &= \frac{E_4(\tau)^3 - E_6(\tau)^2}{1728}, \\ j(\tau) &= \frac{E_4(\tau)^3}{\Delta(\tau)}. \end{aligned} \tag{8}$$

Dal lemma precedente possiamo dire che j è un invariante sotto la trasformazione della forma $\tau' = (a\tau + b)/(c\tau + d)$, dove $\left(\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right) \in SL_2(\mathbb{Z})$. In generale, per una matrice

$$\alpha = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{GL}_2(\mathbb{R}), \quad det(\alpha) > 0,$$

dove $GL_2(\mathbb{R})$ è il gruppo lineare generale delle matrici 2×2 su $\mathbb{R}$ con determinante un unità in $\mathbb{R}$, definiamo $j \circ \alpha(\tau) = j\left(\frac{a\tau+b}{c\tau+d}\right)$. Per un intero n, sia

$$D_n^* = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} : a,\, b,\, c,\, d \in \mathbb{Z},\, ad - bc = n,\, \gcd(a,b,c,d) = 1 \right\},$$

e

$$S_n^* = \left\{ \begin{pmatrix} a & b \\ 0 & d \end{pmatrix} \in D_n* : d > 0,\, 0 \leq b < d \right\}.$$

Definizione 5.1. Un morfismo non costante, cioè un'applicazione definita da funzioni razionali, $\phi : E_1 \to E_2$, che mappa l'identità di E_1 nell'identità di E_2, è chiamato **isogenia** (in altre parole un omomorfismo suriettivo).

É ora possibile definire i polinomi modulari:

Definizione 5.2. Un **polinomio modulare** di ordine n è dato da

$$\Phi_n(x, j) = \prod_{\alpha \in S_n^*} (x - j \circ \alpha).$$

Questo è un polinomio simmetrico a coefficienti in $\mathbb{Z}$ nelle variabili j, x, di grado $\sharp S_n^*$ in ciascuna variabile. Il seguente lemma ci permette di affermare che esiste un'isogenia di grado n da E_1 e E_2 se e solo se $\Phi_n(j(E_1), j(E_2)) = 0$, $(j(E_2) = j \circ \alpha(\tau),\, \alpha \in S_n^*)$.

Lemma 5.2. *Siano E_1, E_2 due curve ellittiche su $\mathbb{C}$, con j-invariante $j(E_1) = j(\tau)$ e $j(E_2)$ rispettivamente e sia n un intero positivo. Allora*

$$j(E_2) = j \circ \alpha(\tau), \quad \alpha \in S_n^*,$$

se e solo se esiste un isogenia tra E_1 e E_2 il cui nucleo è ciclico di grado n

Un aspetto importante dei polinomi modulari è il loro grado relativamente basso (se consideriamo l'l-esimo polinomio questo ha grado $l + 1$), permettendoci di calcolare un fattore del polinomio di divisione di grado $\frac{l-1}{2}$, fatto importante per gli sviluppi di Elkies. Un'altra loro caratteristica fondamentale è il fatto che dalla loro scomposizione possiamo classificare il tipo di primo con cui stiamo lavorando, ma sull'argomento torneremo successivamente. Il fattore negativo, però, è che i loro coefficienti in $\mathbb{Z}$, diventano presto molto grandi e quindi difficili da calcolare o maneggiare. Per risolvere tale problema sono state proposte varie strade. Una consiste nel calcolare delle varianti con le stesse proprietà ma con coefficienti più facili da gestire, ma a volte è più difficile calcolarli rispetto a quelli tradizionali. Un'altra alternativa consiste nel calcolarli direttamente modulo la caratteristica del campo in cui ci troviamo. Bisogna cercare un giusto compromesso affinchè non diventi più complicato calcolarli piuttosto che effettuare le operazioni per le quali sono stati chiamati in causa.

6 Dopo Schoof: l'Algoritmo di Schoof-Atkin-Elkies

Ora abbiamo tutto il necessario per descrivere i miglioramenti apportati da Atkin ed Elkies all'Algoritmo di Schoof. Consideriamo una curva ellittica E in un campo finito $\mathbb{F}_q$, con caratteristica prima diversa da 2 e da 3, data dall'Equazione di Weierstrass, $y^2 = x^3 + Ax + B$

Notazione 6.1. In questa sezione, per evitare di confondere i polinomi modulari con l'endomorfismo di Frobenius, denoteremo quest'ultimo con φ_q.

Consideriamo l'equazione caratteristica di Frobenius $\mathcal{F}_l(X) = X^2 - a_l X + q_l = 0$ modulo un primo l; a seconda se ha radici in $\mathbb{F}_l$ o meno, ovvero se, il discriminante $\Delta_a = a^2 - 4q$ è un quadrato o no in $\mathbb{F}_l$, possiamo classificare il primo l come segue.

Definizione 6.1.
1. Se Δ_a è un quadrato in $\mathbb{F}_l$, allora l è detto **primo di Elkies**.
2. Se Δ_a non è un quadrato modulo l, allora l è detto **primo di Atkin**.

Il problema, però, è che noi non conosciamo il discriminante del polinomio caratteristico e di conseguenza non possiamo dedurre da ciò di che categoria è il primo. L'l-esimo polinomio modulare ci permette di valutare se l è di Atkin o di Elkies in base alla sua *scomposizione tipo*. Qui viene enunciata la proposizione che permette di determinare di che tipo è il primo in questione.

Proposzione 6.1. *Sia E una curva ellittica non supersingolare su $\mathbb{F}_q$, con j-invariante diverso da 0 e 1728. Sia $\Phi_l(x, j) = f_1 f_2 \cdots f_s$ la fattorizzazione di $\Phi_l(x, j) \in \mathbb{F}_q[x]$ come prodotto di fattori polinomiali irriducibili, allora ci sono tre possibili scomposizioni rispetto ai gradi di $f_1, f_2, \cdots, f_s$:*

1. $$1 \text{ e } l;$$
   in altre parole $\Phi_l(x, j)$ si fattorizza come prodotto di un fattore lineare e un fattore irriducibile di grado l. In questo caso l divide il discriminante $a^2 - 4q$ e poniamo $r = l$.
2. $$1, 1, r, r, \cdots, r;$$
   in questo caso $a^2 - 4q$ è un quadrato modulo l, il grado r divide $l - 1$ e φ_q agisce su $E[l]$ come la matrice $\begin{pmatrix} \lambda & 0 \\ 0 & \mu \end{pmatrix}$, dove $\lambda, \mu \in \mathbb{F}_l^*$.

3.

$$r, r, \cdots, r;$$

per qualche $r > 1$, in questo caso $a^2 - 4q$ non è un quadrato in $\mathbb{F}_l$, r divide $l+1$ e φ_q agisce su $E[l]$, mediante una matrice 2×2 il cui polinomio caratteristico è irriducibile modulo l.

In tutti e tre i casi, r è l'ordine di φ_q nel gruppo $PGL_2(\mathbb{F}_l)$, ovvero il gruppo lineare proiettivo di $\mathbb{F}_l$ di dimensione 2, e la traccia a di φ soddisfa l'equazione

$$a^2 = q(\zeta + 2 + \zeta^{-1})$$

su $\mathbb{F}_l$, per qualche r-esima radice primitiva dell'unità $\zeta \in \overline{\mathbb{F}_l}$.

Notiamo che i primi due casi si riferiscono ad un primo di Elkies e l'ultimo caso fa invece riferimento ad un primo di Atkin.

Supponiamo, ora, che l sia un primo di Elkies, allora esistono λ, $\mu \in \mathbb{F}_l$ radici del polinomio caratteristico. Supponiamo anche $\lambda \neq \mu$, altrimenti è facile notare che, $a \equiv \pm\sqrt{q} \pmod{l}$. L'insieme dei punti di l-torsione ammette due sottogruppi ciclici, C_1 e C_2, stabili sotto l'endomorfismo di Frobenius, cioè $\varphi_q(P_1) = \lambda P_1$ per ogni $P_1 \in C_1$ and $\varphi_q(P_2) = \mu P_2$ per ogni $P_2 \in C_2$. Possiamo concludere che $a \equiv \lambda + \frac{q}{\lambda} \pmod{l}$ e che, per determinare l'autovalore λ, è necessario un punto $P = (x, y)$ e un valore $\lambda \in \{1, 2, \cdots, l-1\}$, tale che $(x^q, y^q) = [\lambda](x, y)$. In questo caso, dobbiamo comunque calcolare x^q, y^q e, nonostante non sia richiesto x^{q^2}, y^{q^2}, hanno comunque la stessa complessità computazionale. Il reale miglioramento nella complessità, si ottiene dal trovare un fattore del polinomio l-esimo di divisione di grado $d = \frac{l-1}{2}$. Per costruire tale polinomio, bisogna considerare E_1, una curva isogena ad E, mediante un'isogenia di grado l, ovvero, il nucleo dell'isogenia ha cardinalità l. Chiamiamo quest'ultimo gruppo C, che altro non è che uno dei sottogruppi tra C_1 o C_2 detti sopra; si noti che C è stabile sotto la mappa di Frobenius, e quindi il polinomio

$$F_l(x) = \prod_{\pm P_i \in C \setminus \{\infty\}} (x - (P_i)_X)$$

è definito su $\mathbb{F}_q$, il campo di definizione della curva. Con $(P)_X$ si intende la coordinata x del punto P; il grado di $F_l(x)$ è $(l-1)/2$ e tale polinomio, così definito, divide l'l-esimo polinomio di divisione. Se la curva originale ha j-invariante j, allora la curva isogena avrà come j-invariante che è lo zero dell'l-esimo polinomio modulare. Nel caso di un primo di Elkies uno dei due possibili j-invarianti viene scelto e si calcola, attraverso il procedimento sintetizzato nella tabella sotto riportata, il fattore cercato. In breve, di seguito, vengono schematizzati gli pseudo-codici relativi al calcolo del fattore di grado $(l-1)/2$ e alla procedura di Elkies.

Fattore del polinomio di divisione $F_l(x)$

INPUT: Una curva ellittica su $\mathbb{F}_p$ e un primo Elkies l.
OUTPUT: A factor $F_l(x)$ of degree $d = \frac{l-1}{2}$ of $\psi_l(x)$.

1. Calcolare $j = j(E) = 1728\frac{4A^3}{4A^3+27B^2}$.
2. Calcolare $\overline{E}_4(q) = -48A$, $\overline{E}_6(q) = 864B$.
3. Calcolare $j' = -\frac{\overline{E}_6}{\overline{E}_4}j$.
4. Sia $\tilde{j} \leftarrow$ una radice di $\Phi_l(x, j)$ in $\mathbb{F}_p$.
5. Calcolare $\tilde{j}' = -\frac{j'\Phi_x(j,\tilde{j})}{l\Phi_y(j,\tilde{j})}$.
6. Calcolare $\tilde{A} = -\frac{1}{48}\frac{(\tilde{j}')^2}{\tilde{j}(\tilde{j}-1728)}$ e $\tilde{B} = -\frac{1}{864}\frac{(\tilde{j}')^3}{\tilde{j}^2(\tilde{j}-1728)}$.
7. Calcolare $\overline{E}_4(q^l) = -48\tilde{A}$ and $\overline{E}_6(q^l) = 864\tilde{B}$.
8. Calcolare $\frac{j''}{j'} - l\frac{\tilde{j}''}{\tilde{j}'} =$
$= -\frac{j'^2\Phi_{xx}(j,\tilde{j})+2lj'\tilde{j}'\Phi_{xy}(j,\tilde{j})+l^2\tilde{j}'^2\Phi_{yy}(j,\tilde{j})}{j'\Phi_x(j\tilde{j})}$.
9. Calcolare $p_1 = \frac{l}{2}\left(\frac{j''}{j'} - l\frac{\tilde{j}''}{\tilde{j}'}\right) + \frac{l}{4}\left(\frac{\overline{E}_4^2(q)}{\overline{E}_6(q)} - l\frac{\overline{E}_4^2(q^l)}{\overline{E}_6(q^l)}\right)$
$+\frac{l}{3}\left(\frac{\overline{E}_6(q)}{\overline{E}_4(q)} - l\frac{\overline{E}_6(q^l)}{\overline{E}_4(q^l)}\right)$.
10. Calcolare c_k e $\tilde{c}_k$ per $k < d$, dalle equazioni
$c_1 = -\frac{A}{5}$, $\quad c_2 = -\frac{B}{7}$ e
$c_k = \frac{3}{(k-2)(2k+3)}\sum_{j=1}^{k-2} c_j c_{k-1-j}$, $\quad k \geq 3$,
mentre $\tilde{c}_1 = -\frac{\tilde{A}l^4}{5}$, $\quad \tilde{c}_2 = -\frac{\tilde{B}l^6}{7}$ e
$c_k = \frac{3}{(k-2)(2k+3)}\sum_{j=1}^{k-2} \tilde{c}_j \tilde{c}_{k-1-j}$, $\quad k \geq 3$.
11. Otteniamo i coefficienti di $F_l(x)$ dalla seguente formila ricorsiva. $F_{l,d} = 1$,
$F_{l,d-i} = [A(\omega)]_i - \sum_{k=1}^{i}\left(\sum_{j=0}^{k}\binom{d-i+k}{k-j}[C(\omega)^{k-j}]_j\right)F_{l,d-i+k}$.
12. Return $F_l(x)$.

Notazione 6.2. Se $B(\omega)$ è un'arbitraria serie di potenze in ω, denotiamo con $[B(\omega)]_i$ il coefficiente relativo a ω^i.

Procedura di Elkies

INPUT: Una curva ellittica E su $\mathbb{F}_q$, un primo di Elkies l, un fattore $F_l(x)$ del polinomio di divisione $\psi_l(x)$.
OUTPUT: La traccia a modulo l.

1. Per $\lambda = 1, \cdots, (l-1)/2$,
2. calcolare $h(x) = \left((x^p - x)\psi_\lambda^2(x,y) + \psi_{\lambda-1}(x,y)\psi_{\lambda+1}(x,y)\right) \pmod{F_l(x),\ y^2 - x^3 - Ax - B}$.
3. Se $\gcd(h(x), F_l(x)) = 1$, vai al passo 1.
4. Se $\gcd(h(x), F_l(x)) \neq 1$, allora
5. Se $y^p \equiv y_\lambda \pmod{F_l(x),\ y^2 - x^3 - Ax - B}$ λ è l'autovalore cercato,
6. altrimenti l'autovalore è $-\lambda$
7. $a \equiv \lambda + q/\lambda \pmod{l}$.

Supponiamo ora che l sia un primo di Alkin ovvero la scomposizione dell'l-esimo polinomio modulare, rispetto alla proposizione enunciata, ha fattori irriducibili tutti di grado r, (con $r > 1$). La procedura di Atkin non porta ad un valore univoco di $a \pmod{l}$, ma il risultato che si ottiene è quello di un insieme con $\varphi_{Eul}(r)$ elementi che altro non sono che i possibili valori di $a \pmod{l}$. La procedura è la seguente:

Procedura di Atkin

INPUT: Una curva ellittica E su $\mathbb{F}_q$ e un primo l di Atkin.
OUTPUT: Una coppia (T, l), dove T è l'insieme delle possibili tracce $a \pmod{l}$.

1. $T \leftarrow \{\}$.
2. Determinare la *scomposizione tipo* di $\Phi_l(x, j)$ in $\mathbb{F}_q$.
3. Determinare r usando la precedente proposizone.
4. Determinare un generatore g di $\mathbb{F}_{l^2}^* = \mathbb{F}_l[\sqrt{d}]^*$.
5. $S \leftarrow \{g^{i(l^2-1)/r} : \gcd(i, r) = 1\}$.
6. Per ogni $\gamma_r \in S$:
7. porre $\gamma_r = g_1 + g_2\sqrt{d}$;
8. $z \leftarrow q(g_1 + 1)/2 \pmod{l}$;
9. se z è un quadrato modulo l allora:
10. $x \leftarrow \sqrt{z} \pmod{l}$,
11. $T \leftarrow T \cup \{2x, -2x\}$.
12. Return (T, l).

Una volta raccolte le informazioni necessarie per un numero sufficiente di primi, applichiamo il Teorema Cinese dei Resti, per ridurre i casi, ma se sono presenti nel calcolo dei primi di Atkin, la traccia a non viene univocamente determinata. Per questo si ricorre all'utilizzo dell'Algoritmo Baby Stab Giant Step, al fine di ridurre ulteriormente i casi. Brevemente, la procedura dell'intero algoritmo SEA è di seguito riportata.

Algoritmo di Schoof-Elkies-Atkin (SEA)

INPUT: Una curva ellittica E su un campo finito $\mathbb{F}_q$.
OUTPUT: L'ordine di $E(\mathbb{F}_q)$.

1. $M \leftarrow 1$, $l \leftarrow 2$, $A \leftarrow \{\}$ e $E \leftarrow \{\}$.
2. Mentre $M < 4\sqrt{q}$, allora:
3. Decidere quando l è un primo di Atkin o Elkies, trovando la *fattorizzazione tipo* dell'l-esimo polinomio modulare.
4. Se l è un primo di Elkies, allora:
5. Determinare il polinomio $F_l(x)$.
6. Trovare un autovalore, λ, modulo l.
7. $a \leftarrow \lambda + q/\lambda \pmod{l}$.
8. $E \leftarrow E \cup \{(a, l)\}$.
9. Altrimenti:
10. Determinare un (piccolo) insieme T tale che $a \pmod{l} \in T$.
11. $A \leftarrow A \cup \{(T, l)\}$.
12. $M \leftarrow M \times l$.
13. $l \leftarrow$nextprime(l).
14. Trovare a, usando gli insieme A e E, il CRT e BSGS
15. Return $q + 1 - a$.

Concludiamo con un accenno alla complessità dell'Algoritmo SEA. Per quanto riguarda la procedura di Elkies, la difficoltà maggiore è nel calcolare x^q, y^q modulo il fattore del polinomio di divisione. Con un'analisi simile all'Algoritmo di Schoof, possiamo concludere che la complessità è di $\vartheta(\lg^5 q)$ in aritmetica semplice e $\vartheta(\lg^{3+\epsilon} q)$ in aritmetica più sofisticata. Per trarre vantaggi da questi miglioramenti bisogna fare in modo che, per calcolare il fattore del polinomio di divisione, non venga superata una complessità limite che li renderebbe non più convenienti; questa soglia non deve eccedere $\vartheta(\lg^3 q)$ in aritmetica semplice e $\vartheta(\lg^{2+\epsilon} q)$ in aritmetica più sofisticata. Siccome il numero dei primi di Elkies è nell'ordine di $\vartheta(\lg q)$, arriviamo ad una complessità di $\vartheta(\lg^6 q)$ in aritmetica semplice, $\vartheta(\lg^{4+\epsilon} q)$ altrimenti. La

parte di Atkin è da considerarsi solo di supporto per ricevere comunque informazioni aggiuntive, ma notiamo che, la complessità non è conveniente tanti più sono i primi di Atkin su cui lavorare. A volte è addirittura preferibile applicare la procedura di Elkies ad un primo più grande del necessario piuttosto che utilizzare primi di Atkin con molti possibili valori della traccia a.

Riferimenti bibliografici

[1] M. Artin. *Algebra*. Bollati Boringhieri.

[2] A.O.L. Atkin. *A public message*, 1992.

[3] C. Batut, K. Belabas, D. Bernardi, H. Choen, M. Olivier. *User's guide to PARI/GP*. Last change, 2009.

[4] F. Blake, J.A. Csirik, M. Rubinstein, G. Seroussi. *On the computation of modular polynomials for elliptic curves*. Hewlett-Packard Laboratories, Department of Mathematics University of Texas at Austin.

[5] I.F. Blake, G. Seroussi, N.P. Smart. *Elliptic curves in cryptography*, volume 265 of London Mathematical Society Lecture Note Series. Cambridge University Press, Cambridge 2000. Reprint of 1999 original.

[6] P. Cohen. *On the coefficients of the transformation polynomials for the elliptic modular function*. Math. Proc. Camb. Phil. Soc., 95, 389-402,1984.

[7] N.D. Elkies. *Elliptic and modular curves over finite fields and related computational issues*. Based on a talk given at the conference computational perspectives on number theory, in honor of A.O.L. Atkin, 1997.

[8] A. Enge. *Computing modular polynomials in quasi-linear time*. Mathematics of computation, volume 78, number 267, Pages 1809-1824, July 2009.

[9] N. Koblitz. *A course in number theory and cryptography, 2ed*. GTM 114, Springer, 1994.

[10] F. Morain. *Calcul du nombre de points su une courbe elliptique dans un corps fini: aspects algorithmiques*. J. Théorie des nombres de Bordeaux, 7, 255-282, 1995.

[11] R. Schoof. *Elliptic curves over a finite fields and the computation of a square roots mod p*. Math. comp., 44, 483-494, 1985.

[12] R. Schoof. *Counting points on elliptic curves over finite fields*. J. Théorie des nombres de Bordeaux, 7, 219-254, 1995.

[13] Joseph H. Silverman. *The arithmetic of elliptic curves*. Springer-Verlag, GTM 106, 1986.

[14] Lawrence C. Washington. *Elliptic curves number theory and cryptography, 2ed*. Taylor & Francis Group,LLC, 2008.