12 Crittosistemi basati su curve ellittiche

12.1 Costruzione di una curva ellittica

Nella costruzione di sistemi crittografici basati sulle curve ellittiche, la prima operazione da fare è la scelta di una curva ellittica $\mathcal{E}$ definita su $GF(q)$ e di un suo punto P. Entrambi possono essere determinati contemporaneamente dal seguente metodo probabilistico basato sul **Teorema 11.12**:

1. Si fissa un campo finito $GF(q)$;
2. A seconda della caratteristica del campo, si presentano situazioni diverse:

   2a) Supponiamo che la caratteristica del campo sia maggiore strettamente di 3. Quindi, in tal caso, si sceglie una terna (x_0, y_0, a) di elementi di $GF(q)$ e si calcola $b = y_0^2 - (x_0^3 + ax_0)$. Successivamente si calcola $4a^3 + 27b^2$.

   - Se $4a^3 + 27b^2 \neq 0$ in $GF(q)$, allora $\mathcal{E}: \ y^2 - x^3 - ax - b = 0$ è una curva ellittica e $P = (x_0, y_0)$ è un suo punto;
   - Se $4a^3 + 27b^2 = 0$ si ritorna a scegliere una terna (x_0', y_0', a') e si ripete il procedimento;

   2b) Se la caratteristica del campo è uguale a 3, si sceglie una terna (x_0, y_0, a) di elementi di $GF(q)$ e si calcola $c = y_0^2 - (x_0^3 + ax_0^2 + bx_0)$. Successivamente si calcola $-a^3c + a^2b^2 - b^3$.

   - Se $-a^3c + a^2b^2 - b^3 \neq 0$ in $GF(q)$, allora risulta che $\mathcal{E}: \ y^2 - x^3 - ax^2 - bx - c = 0$ è una curva ellittica e $P = (x_0, y_0)$ è un suo punto;
   - Se $-a^3c + a^2b^2 - b^3 = 0$ si ritorna a scegliere una terna (x_0', y_0', a') e si ripete il procedimento.

   2c) Se la caratteristica del campo è uguale a 2, si distinguono due sottocasi a seconda che la curva sia supersingolare o meno.

   - Se la curva che si vuole costruire è supersingolare, si sceglie una terna (x_0, y_0, a) di elementi di $GF(q)$ e si calcola $b = y_0^2 + cy_0 - (x_0^3 + ax_0)$. Successivamente si valuta c.
     - Se $c \neq 0$ in $GF(q)$, allora risulta che $\mathcal{E}: \ y^2 + cy - x^3 - ax^2 - b = 0$ è una curva ellittica e $P = (x_0, y_0)$ è un suo punto;
     - Se $c = 0$ si ritorna a scegliere una terna (x_0', y_0', a') e si ripete il procedimento.

- Se la curva che si vuole costruire è non supersingolare, si sceglie una terna (x_0, y_0, a) di elementi di $GF(q)$ e si calcola $b = y_0^2 + x_0y_0 - (x_0^3 + ax_0)$. Successivamente si valuta b.
  - Se $b \neq 0$ in $GF(q)$, allora risulta che $\mathcal{E}: y^2+xy-x^3-ax^2-b = 0$ è una curva ellittica e $P = (x_0, y_0)$ è un suo punto;
  - Se $b = 0$ si ritorna a scegliere una terna (x_0', y_0', a') e si ripete il procedimento.

12.2 Conversione delle unità di messaggio in chiaro in punti di una curva ellittica

Ora bisogna convertire le unità di messaggio in chiaro in punti di una fissata curva ellittica definita su un campo finito $GF(q)$, q dispari.

Fissata una curva ellittica $\mathcal{E}$ definita dall'equazione di Weierstrass $y^2 = f(x)$ su $GF(q)$ dove $q = p^r$ è un numero dispari elevato, il seguente metodo probabilistico permette di trasformare le unità di messaggio in chiaro in punti di $\mathcal{E}$.

Sia k un intero sufficientemente grande e supponiamo che

1. le unità di messaggio in chiaro siano rappresentate da interi m tali che $0 \leq m < M$,
2. $q = p^r$ sia scelto in modo tale che $q > Mk$.

Gli interi compresi tra 1 ed Mk si possono rappresentare nella forma $mk+j$, dove $1 \leq j \leq k$. Rappresentato in base p, l'intero $mk + j = \sum_{i=0}^{r-1} a_i p^i$ con $0 \leq a_i \leq p-1$. Quindi $mk + j$ corrisponde alla r–upla $(a_{r-1}, \ldots, a_1, a_0)$ dello spazio vettoriale $GF(p)^r$ e quindi ad un unico elemento $x_j \in GF(q)$. Pertanto, fissato m, per ogni $j = 1, 2, \ldots, k$ ad ogni intero $mk + j$ corrisponde un unico elemento x_j di $GF(q)$. Se $f(x_j)$ è un quadrato in $GF(q)$ e y_j è tale che $y_j^2 = f(x_j)$, allora la coppia (x_j, y_j) definisce il punto $P_m = (x_j, y_j)$ della curva ellittica $\mathcal{E}$ di equazione $y^2 = f(x)$. Se $f(x_j)$ non è un quadrato, allora si ripete il procedimento appena visto per l'elemento x_{j+1} corrispondente all'intero $mk + j + 1$.

Vediamo ora il procedimento inverso, cioè supponiamo di avere a disposizione un punto $Q = P_m$ della curva ellittica e di voler determinare l'unità di messaggio in chiaro m da cui esso proviene. Sia $Q \in \mathcal{E}$ un punto di coordinate (x_Q, y_Q). Poiché sussiste l'isomorfismo di spazi vettoriali $GF(q) \cong GF(p)^r$, x_Q è in corrispondenza biunivoca con la r–upla $(a_0, \ldots, a_{r-1})_p$ e quindi, per quanto visto in precedenza, anche con $\tilde{x}_Q = \sum_{i=0}^{r-1} a_i p^i$. Pertanto si ha che: $Q = P_m$ se e solo se $\tilde{x}_Q = mk + j$. Allora consideriamo $\tilde{x}_Q - 1 = mk + j - 1$ e dividiamo tutto per k ottenendo

$$\frac{\tilde{x}_Q - 1}{k} = \frac{mk + j - 1}{k} = m + \frac{j-1}{k}. \tag{12.1}$$

Osserviamo che $1 \leq j \leq k$, cioè $0 \leq j-1 \leq k-1$ da cui segue $0 \leq \frac{j-1}{k} < 1$. Pertanto, passando alla parte intera di (12.1), abbiamo:

$$\left\lfloor m + \frac{j-1}{k} \right\rfloor = m.$$

Quindi, se questo procedimento ha successo, esso permette di costruire una corrispondenza biunivoca tra l'insieme delle unità di messaggio in chiaro ed un opportuno sottoinsieme di punti di $\mathcal{E}$.

Vediamo quale è la probabilità che questo metodo per convertire un'unità di messaggio m in un punto P_m della curva ellittica $\mathcal{E}$, fallisca.

Consideriamo x_j e osserviamo che la probabilità che $f(x_j)$ sia un non quadrato (e quindi la probabilità che il metodo fallisca), è di circa $\frac{1}{2}$. Più precisamente, la probabilità che $f(x)$ sia un quadrato al variare di x in $GF(q)$, è data da $\frac{N}{2q}$, cioè dal rapporto tra il numero dei punti della curva ellittica $\mathcal{E}$ e il numero delle possibili coppie del tipo $(x, \pm\sqrt{f(x)})$ con $\sqrt{f(x)}$ in un'estensione quadratica di $GF(q)$. Da (11.28) segue che

$$\frac{\left(\sqrt{q}-1\right)^2}{2q} \leq \frac{N}{2q} \leq \frac{\left(\sqrt{q}+1\right)^2}{2q}$$

che può essere espresso nella forma:

$$\frac{1}{2}\left(1-\frac{1}{\sqrt{q}}\right)^2 \leq \frac{N}{2q} \leq \frac{1}{2}\left(1+\frac{1}{\sqrt{q}}\right)^2.$$

Quindi

$$\lim_{q\to+\infty} \frac{N}{2q} = \frac{1}{2}$$

Pertanto la probabilità che $f(x_j)$ sia un non quadrato per ogni $1 \leq j \leq k$, è circa $\frac{1}{2^k}$. Possiamo quindi osservare che per $k \to +\infty$, segue che $q \to +\infty$ siccome $q > Mk$, e quindi la probabilità di successo del metodo, che è data da $1 - \frac{1}{2^k}$, tende ad 1.

12.3 Logaritmo discreto su una curva ellittica

In seguito è fornita la definizione di logaritmo discreto nell'ambito del gruppo associato ad una curva ellittica.

Definizione 12.1. (Logaritmo discreto su una curva ellittica)
Sia $(\mathcal{E}, +)$ il gruppo associato ad una curva ellittica su $GF(q)$ e sia B un suo punto. Sia ora $P \in \langle B \rangle$ allora esiste $x \in \mathbb{Z}$ tale che $P = xB$. L'intero x si dice **logaritmo di P in base B** e lo si denota $\log_B P$.

Il seguente crittosistema è l'analogo del crittosistema di ElGamal e fonda la sua sicurezza sull'intrattabilità computazione del problema del logaritmo discreto su curve ellittiche.

Definizione 12.2. (Crittosistema di ElGamal basato sulle Curve Ellittiche)
Siano $\mathcal{E}$ una curva ellittica su $GF(q)$ e sia B un suo punto di ordine n tale che il PLD in $(\langle B \rangle, +)$ è computazionalmente intrattabile. Inoltre siano:

1. $\mathcal{P} = \mathcal{E}$;
2. $\mathcal{C} = \mathcal{E} \times \mathcal{E}$;
3. $\mathcal{K} = \{(\mathcal{E}, B, m, P, n) : mB = P\}$, dove $(\mathcal{E}, P, B, n)$ è pubblica, mentre m è segreta.
4. Per $K = (\mathcal{E}, B, m, P, n)$ ed un elemento random (segreto) $k \in \mathbb{Z}_n^*$ vale che

$$\begin{aligned} e_{K,k} &: \mathcal{E} \longrightarrow \mathcal{E} \times \mathcal{E}, X \longmapsto (kB, X + k(mB)) \\ d_K &: \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}, (Y_1, Y_2) \longmapsto Y_2 - mY_1. \end{aligned}$$

Esempio 12.3. Si consideri la curva ellittica $\mathcal{E} : y^2 = x^3 + x + 6$ a coefficienti in $GF(11)$. Abbiamo visto nell'**Esempio 11.17** che $\mathcal{E} \cong Z_{13}$ e $B = (2, 7)$ è un suo generatore. L'utente sceglie, per esempio, $m = 7$ come chiave segreta e quindi $P = 7B = (7, 2)$. Allora la chiave pubblica è $(\mathcal{E}, (7, 2), (2, 7), 13)$. Viene generato un intero random $k \in \mathbb{Z}_{13}^*$. Allora

$$\begin{aligned} e_{K,3} &: \mathcal{E} \longrightarrow \mathcal{E} \times \mathcal{E}, X \longmapsto (k(7, 2), X + k(2, 7)) \\ d_K &: \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}, (Y_1, Y_2) \longmapsto Y_2 - 7Y_1. \end{aligned}$$

Se $X = (10, 9)$ e $k = 3$, allora l'utente trasmette

$$e_{K,k}(10, 9) = (3(7, 2), (10, 9) + 3(2, 7)) = ((8, 3), (10, 2)).$$

Una volta ricevuto $((8,3),(10,2))$, il destinatario prestabilito calcola

$$X = (8,3) - 7(10,2) = (8,3) - (3,5) = (8,3) + (3,6) = (10,9)$$

che è il messaggio originario.

□

Un crittosistema di tipo ElGamal è il crittosistema integrato basato sulle curve ellittiche (ECIES). E' qui di seguito presentata una versione semplificata.

Sia $\mathcal{E} : y^2 = x^3 + ax + b$ una curva ellittica su $GF(p)$, p primo, $p > 2$, e sia $P = (x,y)$ un suo punto proprio. Poiché

$$y \ mod\ p + (-y) \ mod\ p = p$$

e p è dispari allora $y \ mod\ p$ e $(-y) \ mod\ p$ hanno classe di parità distinta. Quindi, P è completamente determinato dalla coppia $(x, y \ mod\ 2)$ con $0 \leq x, y \leq p-1$. Viene così definita la seguente applicazione:

$$\text{PointCompress} : \mathcal{E} - \{\infty\} \longrightarrow \mathbb{Z}_p \times \mathbb{Z}_2, (x,y) \longmapsto (x, y \ mod\ 2)$$

Viceversa, il recupero di P da $(x, y \ mod\ 2)$ si ottiene dal seguente algoritmo

Algoritmo 12.4. **(PointDecompress(x,i))**

$z \longleftarrow x^3 + ax + b$
if z non è un residuo quadratico modulo p
then return ("Insuccesso")
else
$y \longleftarrow \sqrt{z} \ mod\ p$
if $y \equiv i \ mod\ 2$
then return (x,y)
else return $(x, p-y)$

Per il **Criterio di Eulero**, z è un quadrato se, e solo se, $z^{\frac{p-1}{2}} \equiv 1 \ mod\ p$ e inoltre le radici sono $\pm z^{\frac{p+1}{4}}$ se $p \equiv 3 \ mod\ 4$.

Usando, l'applicazione PointCompress i bit da memorizzare corrispondenti ai punti della curva ellittica sono al più il 50% a costo di calcoli aggiuntivi per il recupero delle coordinata y del punto.

Definizione 12.5. **(ECIES Semplificato)**
Siano $\mathcal{E}$ una curva ellittica su $GF(p)$ e sia B un suo punto di ordine n tale che il PLD in $(\langle B\rangle, +)$ è computazionalmente intrattabile. Inoltre siano:

1. $\mathcal{P} = \mathbb{Z}_p$;
2. $\mathcal{C} = (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p^*$;
3. $\mathcal{K} = \{(\mathcal{E}, B, m, P, n) : mB = P\}$, dove $(\mathcal{E}, P, B, n)$ è pubblica, mentre m è segreta.
4. Per $K = (\mathcal{E}, B, m, P, n)$ ed un elemento random (segreto) $k \in \mathbb{Z}_n^*$ e $kP = (x_0, y_0)$ e $x_0 \neq 0$, allora

$$e_{K,k} : \mathbb{Z}_p \to (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p^*, x \mapsto (\text{PointCompress}(kB), xx_0 \ mod\ p)$$
$$d_K : (\mathbb{Z}_p \times \mathbb{Z}_2) \times \mathbb{Z}_p^* \to \mathbb{Z}_p, (y_1, y_2) \mapsto y_2 \left(x_0^{-1}\right) \ mod\ p.$$

dove $(x_0, y_0) = m\text{PointDecompress}(y_1)$.

Esempio 12.6. Si consideri la curva ellittica $\mathcal{E} : y^2 = x^3 + x + 6$ a coefficienti in $GF(11)$ dell'**Esempio 11.17**. Abbiamo visto che $\mathcal{E} \cong Z_{13}$ e $B = (2, 7)$ è un suo generatore.

L'utente sceglie, per esempio, $m = 7$ come chiave segreta e quindi $P = 7B = (7, 2)$. Supponiamo che voglia cifrare il testo in chiaro $x = 9$ e che abbia scelto il numero casuale $k = 6$. Allora si calcolano

$$\begin{aligned} 6B &= 6(2,7) = (7,9) \\ 6P &= 6(7,2) = (8,3) \end{aligned}$$

Quindi $x_0 = 8$. Successivamente, si calcola

$$e_{K,6}(9) = (\text{PointCompress}(7,9), (9 \times 8) \ mod\ 11) = ((7,1),6)$$

Una volta ricevuto $((7,1),6)$, il destinatario calcola

$$\begin{aligned} \text{PointDecompress}(7,1) &= (7,9) \\ 7(7,9) &= (8,3) \end{aligned}$$

e quindi

$$d_{K,6}(((7,1),6)) = 6 \times 8^{-1} \ mod\ 11 = 9$$

che era il testo in chiaro originario.

□

12.4 Fattorizzare attraverso l'uso delle curve ellittiche

In questa sezione tratteremo un'ulteriore applicazione delle curve ellittiche che riguarda la fattorizzazione di un intero composito dispari. Tale applicazione è nota come **algoritmo di Lenstra**.

Prima di procedere alla descrizione di questo metodo, premettiamo alcuni risultati relativi alle rappresentazioni binarie con segno che permettono di calcolare più speditamente i multipli di un punto di una curva ellittica.

12.4.1 Rappresentazione NAF

Definizione 12.7. **(Rappresentazione binaria con segno)**
Sia c un intero, una **rappresentazione binaria con segno** di c è una ℓ-pla $(c_{\ell-1}, ..., c_0)$ con $c_i \in \{-1, 0, 1\}$ per ogni $0 \leq i \leq \ell - 1$ tale che

$$c = \sum_{i=0}^{\ell-1} c_i 2^i.$$

Esempio 12.8. In generale esiste più di una rappresentazione binaria di uno stesso intero. Infatti,

$$11 = 2^3 + 2^1 + 2^0 = 2^4 - 2^2 - 2^0$$

e quindi $(0, 1, 0, 1, 1)$ e $(1, 0, -1, 0, -1)$ sono rappresentazioni binarie con segno di 11.

□

Definizione 12.9. **(Rappresentazione NAF)**
Una rappresentazione binaria con segno $(c_{\ell-1}, ..., c_0)$ di un intero c tale che $(c_{i+1}, c_i) \neq (\pm 1, \pm 1)$ si dice **forma non adiacente** (o, semplicemente, rappresentazione **NAF**).

Teorema 12.10. *Ogni intero ammette un'unica rappresentazione NAF.*

Dimostrazione.

- **Esistenza.** Sia $(b_{k-1}, ..., b_0)$ la rappresentazione binaria del generico intero c. Quindi,
$$c = \sum_{j=0}^{k-1} b_j 2^j,\ b_j \in \{0,1\}.$$
Sia
$$h = \min\{0 \le j \le k-1 : (b_{j+1}, b_j) = (1,1)\},$$
allora $b_{h-1} = 0$ e quindi
$$c = \sum_{j=h+2}^{k-1} b_j 2^j + 2^{h+1} + 2^h + \sum_{j=0}^{h-1} b_j 2^j =$$
$$= \sum_{j=h+2}^{k-1} b_j 2^j + 2^{h+2} - 2^h + \sum_{j=0}^{h-1} b_j 2^j.$$
Quindi,
$$c = \sum_{j=0}^{k-1} b'_j 2^j$$
dove $b'_j = b_j$ per $0 \le j \le h-1$ con $b'_{h-1} = b_{h-1} = 0$, e dove $b_h = -1$ e $b_{h+1} = 0$. Quindi,
$$h + 2 \le \min\left\{0 \le j \le k-1 : (b'_{j+1}, b'_j) = (1,1)\right\}.$$
Pertanto dopo al piu $k - 1 - (h-2) + 1 = k - h + 2$ passi si ottiene una rappresentazione in NAF.

- **Unicità.** Supponiamo che
$$c = \sum_{i=0}^{m-1} c_i 2^i = \sum_{j=0}^{n-1} c'_j 2^j$$
siano due rappresentazioni NAF distinte dell'intero c. Sia
$$e = \max\left\{0 \le i \le \min(m,n) : c_j = c'_j \text{ per ogni } 0 \le j \le i\right\}.$$
Se C denota l'intero $\frac{c - \sum_{i=0}^{e} c_i 2^i}{2^{e+1}}$, allora
$$C = \sum_{i=0}^{m-e-2} C_i 2^i = \sum_{j=0}^{n-e-2} C'_j 2^j,$$
con $C_i = c_{e+1-i}$ e $C'_i = c'_{e+1-i}$ sono due rappresentazioni NAF di C con $C_0 = c_{e+1} \neq c'_{e+1} = C'_0$. Quindi, possiamo assumere senza perdere di generalità che $c_0 \neq c'_0$. Eventualmente sostituendo c con $-c$, possiamo assumere che $c_0 = 1$. Allora c è dispari e quindi $c'_0 = -1$. Allora, $c_1 = c'_1 = 0$ essendo rappresentazioni NAF. Ma ciò è un assurdo, poiché $\sum_{i=0}^{m-1} c_i 2^i \equiv 1 \ mod\ 4$ mentre $\sum_{i=0}^{n-1} c'_i 2^i \equiv -1 \ mod\ 4$. Pertanto, vale l'unicità della rappresentazione NAF.

□

Esempio 12.11. $c = 3895 = 2^{11} + 2^{10} + 2^9 + 2^8 + 2^5 + 2^4 + 2^2 + 2^1 + 2^0$.

$$\begin{array}{cccccccccccc} 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 \\ 1 & 1 & 1 & 1 & 0 & 0 & 1 & 1 & 1 & 0 & 0 & -1 \\ 1 & 1 & 1 & 1 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 \\ 1 & 0 & 0 & 0 & -1 & 0 & 1 & 0 & 0 & -1 & 0 & 0 & -1 \end{array}$$

Quindi la rappresentazione NAF di 3895 è $(1,0,0,0,-1,0,1,0,0-1,0,0,-1)$.

□

Sia P un punto di ordine n di una curva ellittica $\mathcal{E}$ su $GF(q)$ e sia $(c_{\ell-1},...,c_0)$ la rappresentazione binaria con segno di un intero c tale che $0 \le c \le n-1$. È possibile calcolare cP con una serie di raddoppi, addizioni e sottrazioni attraverso il seguente algoritmo.

Algoritmo 12.12. **(Raddoppi-Addizioni-Sottrazioni** $(P,(c_{\ell-1},\ldots,c_0))$**)**

$Q \longleftarrow \infty$
for $i \longleftarrow \ell - 1$ **downto** 0
do $\begin{cases} Q \longleftarrow 2Q \\ \textbf{if } c_i = 1 \\ \textbf{then } Q \longleftarrow Q + P \\ \textbf{else if } c_i = -1 \\ \textbf{then } Q \longleftarrow Q - P \end{cases}$
return (Q)

Si prova che, in media, il numero degli zeri presenti nella rappresentazione binaria e nella rappresentazione NAF di un intero di ℓ bit è $\ell/2$ e $2\ell/3$, rispettivamente. Pertanto,

- Se si utilizza la rappresentazione binaria di c nell'**Algoritmo 12.12**, il numero medio delle operazioni da eseguire $\ell+\ell/2$: ℓ raddoppi e $\ell/2$ addizioni.

- Se si utilizza la rappresentazione NAF di c nell'**Algoritmo 12.12**, il numero medio delle operazioni da eseguire $\ell + \ell/3$: ℓ raddoppi e $\ell/3$ tra addizioni e sottrazioni.

Quindi se assumiamo che il raddoppio impiega lo stesso tempo della somma o della sottrazione, il rapporto tra i tempi medi impiegati dallo stesso algoritmo nei due casi sopra descritti è

$$\frac{\ell + \ell/2}{\ell + \ell/3} = \frac{9}{8}.$$

Quindi, utilizzare la rappresentazioni NAF di un intero piuttosto che la rappresentazione binaria velocizza l'**Algoritmo 12.12** di circa 11%.

12.4.2 Algoritmo di Lenstra

In questo paragrafo descriviamo l'algoritmo randomizzato e basato sulle curve ellittiche dovuto a Lenstra, per fattorizzare un intero composito dispari n.

Figura 12.1: Hendrik Willem Lenstra Jr. (1949)

Come vedremo più avanti, il metodo di Lenstra è l'analogo del metodo $p-1$ di **Pollard**, basato sulle curve ellittiche.

Algoritmo 12.13. **($p-1$ di Pollard (n, B))**

$a \longleftarrow 2$
for $j \longleftarrow 2$ **to** B
do $\begin{cases} a \longleftarrow a^j \ \ mod\ n \\ d \longleftarrow \gcd(a^j \ \ mod\ n - 1, n) \end{cases}$
if $1 < d < n$
then return (d)
else return ("insuccesso")

Il principale limite del metodo di Pollard è che non è efficiente se $p-1$ è prodotto di potenze di primi piccoli, dove p è un divisore primo di n.

Definizione 12.14. Sia $m \in \mathbb{Z}$, allora per ogni $x_1, x_2 \in \mathbb{Q}$ scriveremo $x_1 \equiv_m x_2$ se, e solo se, $x_1 - x_2$ ridotto ai minimi termini ha numeratore divisibile per m.

Osservazione 12.15. Per ogni $x_1 \in \mathbb{Q}$ con denominatore primo con m esiste un unico $x_2 \in \mathbb{Z}$ tale che $0 \leq x_2 \leq m-1$ e $x_1 \equiv_m x_2$. Infatti, sia $x_1 \in \mathbb{Q}$, allora $x_1 = \frac{a}{b}$, con $mcd(a,b) = 1$. Siccome $mcd(b,m) = 1$, allora esiste un unico $0 \leq x_2 \leq m-1$ tale che $x_2 b \equiv_m a$. Quindi $m \mid a - x_2 b$ e, pertanto, $x_1 = \frac{a}{b} \equiv_m x_2$.

Sia $\mathcal{E}/\mathbb{Q} : y^2 = x^3 + ax + b$ una curva ellittica a coefficienti in $\mathbb{Q}$ e sia $n \in \mathbb{Z}$ tale che $mcd(\Delta, n) = 1$. Allora, per ogni punto $P = (x,y) \in \mathcal{E}/\mathbb{Q}$ le cui coordinate hanno denominatori primi con n e per ogni $p \in \mathbb{P}$, $p \mid n$ risulta $mcd(\Delta, p) = 1$, quindi è possibile considerare la curva $\mathcal{E}/GF(p) : y^2 = x^3 + ax + b$ a coefficienti in $GF(p)$. Inoltre, le coordinate del punto P hanno denominatori primi con p, pertanto $P \ mod\ p = (x \ mod\ p, y \ mod\ p)$, con $0 \leq x \ mod\ p, y \ mod\ p \leq p-1$ individuano un punto di $\mathcal{E}/GF(p)$.

Proposizione 12.16. Sia $\mathcal{E}/\mathbb{Q}$ una curva ellittica definita dall'equazione $y^2 = x^3 + ax + b$, dove $a, b \in \mathbb{Z}$ e $mcd(4a^3 + 27b^2, n) = 1$. Siano P_1, P_2 due punti su $\mathcal{E}/\mathbb{Q}$ le cui coordinate hanno denominatori primi con n e tali che $P_1 \neq -P_2$. Allora $P_1 + P_2 \in \mathcal{E}/\mathbb{Q}$ ha coordinate con denominatori primi con n se e solo se non esiste p primo tale che $p \mid n$ con la proprietà che $P_1 mod\ p + P_2 mod\ p = \infty mod\ p$.

Dimostrazione. Supponiamo dapprima che $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, $P_1 \neq -P_2$ e $P_1 + P_2 \in \mathcal{E}$ abbiano coordinate con denominatori primi con n. Sia p un qualunque divisore primo di n. Dobbiamo dimostrare che $P_1 mod\ p + P_2 mod\ p \neq \infty mod\ p$.

Se $x_1 \not\equiv x_2 mod\ p$, allora $P_1 mod\ p \neq P_2 mod\ p$ e quindi posso applicare

$$\begin{cases} x_3 &= \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 &= -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)\,. \end{cases} \tag{12.2}$$

e concludere che in questo caso $P_1 mod\ p + P_2 mod\ p \neq \infty mod\ p$.

Se invece $x_1 \equiv x_2 mod\ p$, ricordando che per ipotesi $P_1 \neq -P_2$, si possono verificare due casi: $P_1 = P_2$ oppure $P_1 \neq P_2$. Nel primo caso, essendo $P_1 = P_2$, allora le coordinate di $P_1 + P_2 = 2P_1$ sono date dalle formule

$$\begin{cases} x_3 &= \left(\frac{3x_1^2 + a}{2y_1}\right)^2 - 2x_1 \\ y_3 &= -y_1 + \left(\frac{3x_1^2 + a}{2y_1}\right)(x_1 - x_3)\,. \end{cases} \tag{12.3}$$

e $2P_1 mod\ p$ è dato dalle stesse formule con ciascun termine sostituito dal suo residuo $mod\ p$. Per mostrare che $P_1 mod\ p \neq \infty mod\ p$, basta dimostrare che il denominatore $2y_1$ che compare nelle formule (12.3) non è divisibile per p.
Procediamo per assurdo. Se $2y_1$ fosse divisibile per p, poiché per ipotesi il denominatore della prima coordinata del punto $2P_1$ non può essere divisibile per p, segue che dovrà essere divisibile per p il numeratore $3x_1^2 + a$. Ciò significa che x_1 è una radice in $GF(p)$ sia di $x^3 + ax + b$, che della sua derivata formale

$3x_1^2 + a$, contraddicendo la nostra ipotesi iniziale e cioè che non esistesse alcuna radice multipla di $x^3 + ax + b$ in $GF(p)$.

Ora supponiamo che $P_1 \neq P_2$. Poiché $x_1 \equiv x_2 mod\ p$ e $x_1 \neq x_2$, possiamo scrivere $x_2 = x_1 + p^r x$ con $r \geq 1$ scelto in modo tale che nè il numeratore nè il denominatore di x sia divisibile per p. Poiché abbiamo supposto che $P_1 + P_2$ abbia denominatore non divisibile per p, possiamo usare la formula (12.2) per concludere che y_2 è della forma $y_1 + p^r y$. Infatti, siccome $x_2 - x_1 = p^r x$, allora $\frac{y_2 - y_1}{x_2 - x_1}$ deve essere tale che, ridotto ai minimi termini, il denominatore non sia divisibile per p; segue che $y_2 - y_1 = p^r y$ (y può essere anche divisibile per p). Inoltre, poiché $P_2 \in \mathcal{E}/\mathbb{Q}$, vale che

$$\begin{aligned} y_2^2 &= (x_1 + p^r x)^3 + a(x_1 + p^r x) + b \\ &\equiv x_1^3 + ax_1 + b + p^r x(3x_1^2 + a)\ mod\ p^{r+1} \\ &= y_1^2 + p^r x(3x_1^2 + a)\ mod\ p^{r+1}. \end{aligned} \tag{12.4}$$

Poiché $x_2 \equiv x_1 mod\ p$ e $y_2 \equiv y_1 mod\ p$, segue che $P_1 mod\ p = P_2 mod\ p$ e quindi $P_1 mod\ p + P_2 mod\ p = 2P_1 mod\ p$ ma $2P_1 mod\ p = \infty mod\ p$ se e solo se $y_1 \equiv y_2 \equiv 0 mod\ p$. Se vale quest'ultima congruenza, significa che $y_1 + y_2 \equiv 0 mod\ p$ e ricordando che $y_1 \equiv y_2 mod\ p^r$, si ha che $y_1^2 - y_2^2 \equiv 0 mod\ p^{r+1}$. Pertanto, da (12.4), segue che $3x_1^2 + a \equiv 0 mod\ p$. Tuttavia ciò è impossibile perché il polinomio $x^3 + ax + b$ non ha radici multiple in $GF(p)$ e quindi x_1 non può essere radice sia di tale polinomio che della sua derivata. Pertanto possiamo concludere che $P_1 mod\ p + P_2 mod\ p \neq \infty mod\ p$.

Viceversa, supponiamo ora che per ogni p divisore primo di n, risulti $P_1 mod\ p + P_2 mod\ p \neq \infty mod\ p$ e mostriamo che, allora, $P_1 + P_2$ ha coordinate che, ridotte ai minimi termini, hanno denominatori primi con n.
Fissiamo p primo tale che $p \mid n$. Se $x_1 \not\equiv x_2\ mod\ p$, da (12.2) segue che p non divide il denominatore delle coordinate della somma. Se invece $x_1 \equiv x_2\ mod\ p$, allora $y_2 \equiv \pm y_1\ mod\ p$, ma poiché $P_1 mod\ p + P_2 mod\ p \neq \infty mod\ p$, dobbiamo avere $y_2 \equiv y_1 \not\equiv 0 mod\ p$. Pertanto, possono presentarsi due casi: $P_2 = P_1$ oppure $P_2 \neq P_1$.

Nel primo caso $y_1 \not\equiv 0 mod\ p$ poiché $2P_1 \neq \infty\ mod\ p$ per via della formula (12.3). Quindi le coordinate di $P_1 + P_2 = 2P_1$ hanno denominatore primo con p. Infine, nel secondo caso, scriviamo nuovamente $x_2 = x_1 + p^r x$ con x non divisibile per p. Da (12.4) segue che

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

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

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

Si noti che in questa congruenza il membro a destra ha denominatore primo con p. Ora, poiché p non divide $y_1 + y_2$, essendo $y_1 + y_2 \equiv 2y_1 mod\ p$, possiamo dividere per $y_1 + y_2$, ottenendo cosí

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

ed anche questo termine ha denominatore primo con p. Ricordando che le formule per calcolare le coordinate di P_1+P_2 sono date da (12.2), possiamo concludere che tali coordinate hanno denominatore non divisibile per p. Dall'arbitrarietà con cui è stato scelto p divisore primo di n, segue che $P_1 + P_2$ ha coordinate prime con n.

□

Esempio 12.17. Poiché vale $\Delta = 4+27\times6^2 = 976 \neq 0$, allora ha senso considerare la curva ellittica sui razionali

$$\mathcal{E}/\mathbb{Q} : y^2 = x^3 + x + 6$$

Applichiamo la **Proposizione 12.16** per fattorizzare $n = 1763$.
Vale che

$$mcd(\Delta, n) = mcd(976, 1763) = 1.$$

Basta sostituire nell'equazione della curva per verificare che $P_1 = (2,4)$ e $P_2 = \left(-\frac{87}{64}, \frac{747}{512}\right)$ appartengono alla curva ellittica $\mathcal{E}/\mathbb{Q}$ e hanno coordinate i cui denominatori sono primi con n. Inoltre, vale che $P_2 \neq -P_1$. Siccome $P_1 \neq P_2$, utilizzando la formula (12.2), si ha che $P_1 + P_2 = (x_3, y_3)$ con

$$\begin{cases} x_3 = \left(\frac{\frac{747}{512}-4}{-\frac{87}{64}-2}\right)^2 - 2 + \frac{87}{64} = -\frac{3166}{46\,225} = -\frac{2\times1583}{5^2\times43^2} \\ y_3 = -4 + \left(\frac{\frac{747}{512}-4}{-\frac{87}{64}-2}\right)\left(2 - \left(-\frac{3166}{46\,225}\right)\right) = -\frac{24\,203\,948}{9938\,375} = -\frac{2^2\times19\times318\,473}{5^3\times43^3} \end{cases}$$

Consideriamo $p = 43$. Allora $P_1 mod 43 = (2,4)$ e $P_2 mod 43 = (2,39)$ e quindi, avendo la stessa ascissa, segue che

$$P_1 \ mod\ 43 + P_2 \ mod\ 43 = \infty \ mod\ 43.$$

Quindi, applicando la **Proposizione 12.16**, vale che 43 divide $n = 1763$. Questo è vero, infatti

$$n = 1763 = 41 \times 43.$$

□

L'algoritmo opera come di seguito esposto.

1. Si generi la coppia $(\mathcal{E}, P)$, dove $\mathcal{E}$ è una curva ellittica definita dall'equazione $y^2 = x^3 + ax + b$ con $a, b \in \mathbb{Z}$ e $P = (x, y)$ è un suo punto. Si fissi inoltre un intero positivo h come numero massimo di curve da generare.
2. Si calcoli $m = (4a^3 + 27b^2, n)$.
   - Se $m = 1$, si vada al passo successivo;
   - Se $1 < m < n$, è stato trovato un divisore non banale di n, pertanto l'algoritmo termina;
   - Se $m = n$, si ritorni al punto (1) e si scelga un'altra coppia $(\mathcal{E}, P)$.
3. Si costruisca
$$k = \prod_{\substack{l \leq B \\ l \text{ primo}}} l^{\alpha_l} \tag{12.5}$$
con $\alpha_l = \left[\frac{logC}{logl}\right]$ dove B e C sono due interi positivi che rappresentano rispettivamente un limite per i primi l ed un limite per le potenze di tali primi che compaiono nella fattorizzazione di k. B e C devono essere sufficientemente grandi in modo tale da aumentare la probabilità di trovare un divisore di n e limitare i tempi previsti per il calcolo.
4. Si calcoli kP con il metodo dei raddoppi successivi (come abbiamo visto il calcolo si può accelerare di circa l' 11% utilizzando la rappresentazione NAF di k).

Ad ogni iterazione si utilizzino le formule (11.21) o (11.22) cioè le formule

$$\begin{cases} x_3 = \left(\frac{y_2 - y_1}{x_2 - x_1}\right)^2 - x_1 - x_2 \\ y_3 = -y_1 + \left(\frac{y_2 - y_1}{x_2 - x_1}\right)(x_1 - x_3)\,. \end{cases} \tag{12.6}$$

oppure

$$\begin{cases} x_3 = \left(\frac{3x_1^2 + A}{2y_1}\right)^2 - 2x_1 \\ y_3 = -y_1 + \left(\frac{3x_1^2 + A}{2y_1}\right)(x_1 - x_3)\,. \end{cases} \tag{12.7}$$

a seconda che i punti da sommare siano diversi o uguali, rispettivamente. In particolare, in ogni passaggio, viene utilizzato l'algoritmo euclideo per trovare gli inversi $mod\ n$ di $x_2 - x_1$ o $2y_1$, rispettivamente.

Se in un qualsiasi passo l'algoritmo euclideo fallisce nell'intento di trovare l'inverso $mod\ n$ richiesto, allora detto m il massimo comun divisore tra n ed il denominatore di (12.6) o di (12.7) rispettivamente, si presentano due possibilità:

(i) Se m è tale che $1 < m < n$, allora è stato trovato un divisore non banale di n e quindi l'algoritmo termina;

(ii) Se $m = n$ allora si ritorna al passo **(1)** e si ripete il procedimento descritto dall'algoritmo per una nuova coppia $(\mathcal{E}, P)$.

Per la **Proposizione 12.16**, le possibilità **(i)** e **(ii)** si verificano quando esiste un multiplo k_iP tale che $k_iP mod\ p = \infty mod\ p$ per qualche divisore primo p di n o per tutti i divisori primi di n.

Quindi il metodo di Lenstra determina un fattore non banale di n, oppure, quando esso fallisce, un punto di $\mathcal{E}$. Se non riusciamo a trovare un divisore non banale di n, l'algoritmo termina dopo h fallimenti, dove h rappresenta il numero massimo di curve che possiamo considerare.

Se la probabilità di fallire è $0 < \rho < 1$, allora l'**Algoritmo di Lenstra** è un $(h, 1-\rho^h)$ algoritmo di tipo Las Vegas e quindi

$$\lim_{h\to\infty} 1 - \rho^h = 1.$$

Pertanto, con un'alta probabilità, riusciremo a fattorizzare n in un numero ragionevole di tentativi.

Esempio 12.18. Utilizziamo il metodo di Lenstra per fattorizzare $n = 5429$.

Consideriamo la famiglia di curve ellittiche descritta dall'equazione

$$y^2 = x^3 + ax - a$$

con $a = 1, 2, \ldots$. Osserviamo che ogni curva ellittica che appartiene a questa famiglia, contiene il punto $P = (1, 1)$. Dopo aver verificato che $(4a^3 + 27a^2, 5429) = 1$, scegliamo $B = 3$ e $C = 92$ e quindi, tenendo conto di questi limiti, consideriamo $k = 2^6 3^4$. Per ciascun valore di a, calcoliamo kP con il metodo dei raddoppi successivi.

1. Per $a = 1$, risulta che $3^4 2^6 P mod\ p$ è un punto di $\mathcal{E} mod\ p$ per ogni $p \mid n$.
2. Per $a = 2$ troviamo che, quando cerchiamo di calcolare $3^2 2^6 P mod\ p$, otteniamo un denominatore f tale che $(f, 5429) = 61$. Questo massimo comun divisore rappresenta uno dei fattori propri di 5429. Cioè il punto $(1, 1)$ ha ordine che divide $3^2 2^6$ sulla curva $y^2 = x^3 + 2x - 2 mod\ 61$. Pertanto, il nostro secondo tentativo ha avuto successo.
3. Per $a = 3$, quando cerchiamo di calcolare $3^4 2^6 P$, otteniamo l'altro fattore primo di 5429 che è 89. Pertanto abbiamo ottenuto che $5429 = 61 \cdot 89$.

□

Osservazione 12.19. È evidente la somiglianza di questo metodo con il metodo di Pollard, sebbene, mentre in quest'ultimo si usa il gruppo $\mathbb{Z}_p^*$, qui invece utilizziamo il gruppo costituito dai punti di $\mathcal{E} mod\ p$. Il fatto che il metodo di Pollard dipende dal gruppo $\mathbb{Z}_p^*$ (più precisamente, dai vari gruppi di questo tipo, poiché p varia tra i divisori primi di n), costituisce un limite di tale metodo. Infatti, per un fissato n, i gruppi del tipo $\mathbb{Z}_p^*$, sono fissati. Se accade che tutti i gruppi $\mathbb{Z}_p^*$ hanno ordine divisibile per un primo elevato, ciò può costituire un problema.

Quindi la differenza principale tra i due metodi sta nel fatto che, **mentre nel metodo di Pollard il gruppo utilizzabile è soltanto uno, nel metodo di Lenstra, lavorando con le curve ellittiche su $GF(p)$, abbiamo una serie di gruppi da usare e realisticamente possiamo sperare sempre di trovare un gruppo il cui ordine non sia divisibile per un primo grande o per una sua potenza.** Infatti, se la curva $\mathcal{E}$ non va bene, cioè per ogni $p \mid n$ il gruppo $\mathcal{E} mod\ p$ ha ordine divisibile per un primo grande (e quindi è improbabile che $kP mod\ p$ sia uguale a $\infty mod\ p$ per k dato da (12.5), possiamo effettuare un'altra scelta della curva $\mathcal{E}$ e del punto $P \in \mathcal{E}$.

Il metodo di Lenstra presenta alcuni vantaggi rispetto ad altri algoritmi di fattorizzazione:

1. Esso è il solo metodo che è sostanzialmente più veloce se n è divisibile per un primo che è molto più piccolo di $\sqrt{n}$. Infatti, dal **Teorema di Hasse**, segue che quanto più è piccolo il divisore p di n, minore sarà il numero di punti sulla curva ellittica che stiamo considerando. Ciò comporta un minor numero di operazioni da effettuare per calcolare kP. Tale aspetto risulta rilevante quando la scelta della curva non è ottimale. In tal caso, infatti, un valore di p piccolo, consente di effettuare più velocemente i calcoli sulla curva data e quindi di passare in breve tempo ad una nuova scelta della coppia $(\mathcal{E}, P)$.

2. Dal **Teorema di Hasse** segue che il gruppo formato dai punti di una curva ellittica ha ordine del tipo $p + 1 - t_p$ dove $t_p \leq 2\sqrt{p}$; se per qualche divisore primo p di n il numero $p+1-t_p$ è costituito da fattori primi piccoli, allora l'algoritmo fornisce un divisore non banale di n, altrimenti no.

3. Come già visto nell'**Osservazione 12.19**, il metodo di Lenstra, qualora dovesse fallire con una determinata scelta di $(\mathcal{E}, P)$, permette di ritentare la fattorizzazione utilizzando altre coppie del tipo $(\mathcal{E}_i, P_i)$.

4. Il metodo descritto può essere utilizzato in combinazione con altri metodi quando è richiesta la fattorizzazione di alcuni numeri ausiliari.