Crittografia su curve ellittiche.

curva ellittica → cubica in $AG(2,\mathbb{K})$ di equazione del tipo

$$y^2 + m(x)y = x^3 + ax^2 + bx + c$$

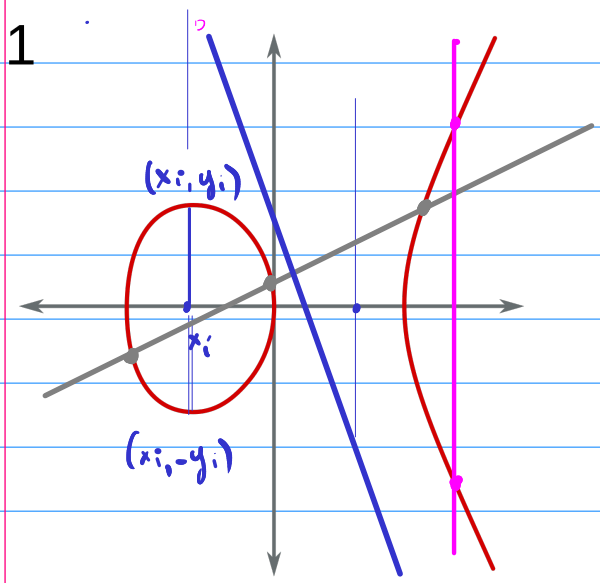
$$\deg m(x) \leq 1$$

non singolare

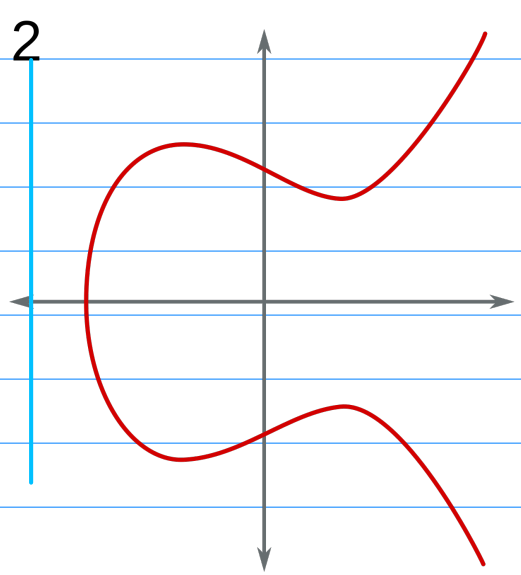
$\forall$ valore di x $\exists\ y_1, y_2 \in \mathbb{K}$: $(x, y_1) \in \mathcal{E}$, $(x, y_2) \in \mathcal{E}$

! se $\mathbb{K}$ non è algebricamente chiuso si considera il discriminante dell'eq. di II grado in y e si vede che dato x ci sono

o oppure 2 (eventualmente coincidenti) valori di y associati.



$y^2 = x^3 - x$



su $\mathbb{K} = \mathbb{R}$.

$y^2 = x^3 - x + 1$

In generale una cubica ellittica è una curva del III ordine, quindi una retta la interseca sempre in 3 punti contati con la debita molteplicità a patto di essere su di un campo algebricamente chiuso ed in ambito ampliato.

OSS: Supponiamo $\mathbb{K}$ non sia algebricamente chiuso ma che una retta r intersechi una cubica in 2 punti di $AG(2,\mathbb{K})$. Allora la retta r interseccherà la cubica in 3 punti in $PG(2,\mathbb{K})$ (contati con la debita molteplicità).

1) Il punto improprio di una cubica $y^2 + m(x)y \pm x^3 + \_\_\_$ è il punto $[(0,\pm 1,0)]$ ovvero il punto improprio dell'asse delle xy

$$\begin{cases} X_3X_2^2 + X_3(\_\_\_) = X_1^3 + X_3(aX_1^2 + bX_3X_1 + cX_3^2) \\ X_3 = 0 \end{cases} \longrightarrow$$

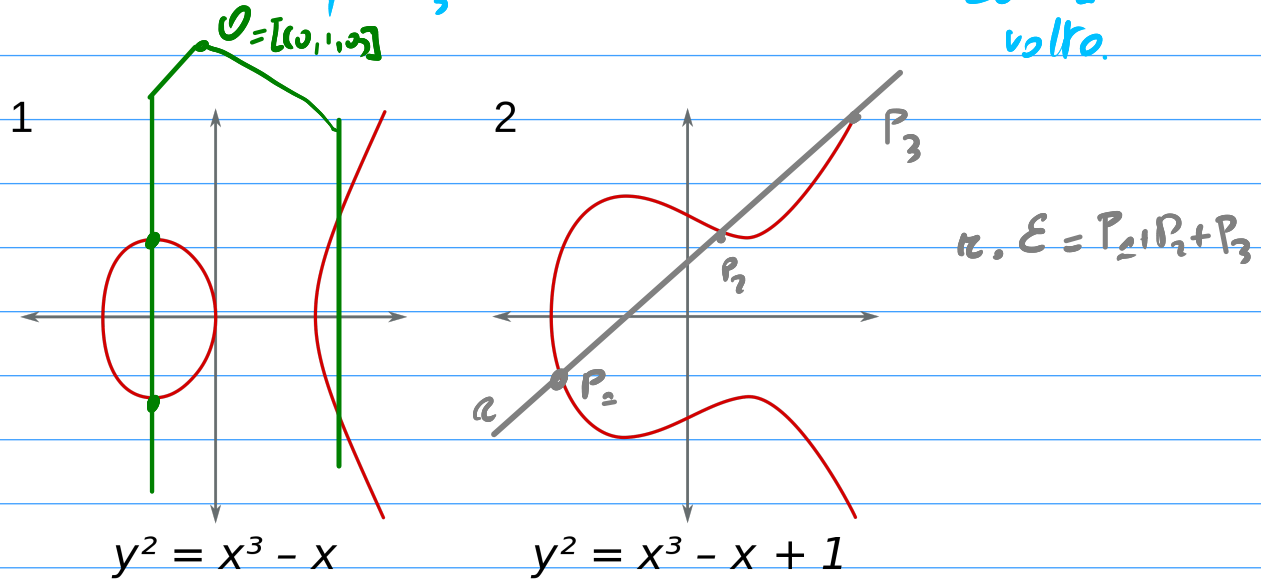
$$X_2 = 0$$

Le rette verticali intersecano la curva ellittica nel suo punto improprio $\mathcal{O} = [(0,\pm 1,0)]$.

Il punto $\mathcal{O}$ è un punto di flesso, nel senso che

la retta tangente alla curva in O interseca la curva stessa 3 volte in O ed essa è la retta impropria $x_3 = 0$

$$\begin{cases} \mathcal{E} \\ x_3 = 0 \end{cases} \rightarrow x_1^3 = 0 \Rightarrow \text{punto } O \text{ contato 3 volte.}$$



n. $\mathcal{E} = P_1P_2+P_3$

per dimostrare l'osservazione, sia

$r: y = ax + b$ una retta non parallela all'asse delle y.

$\Rightarrow$ Sostituendo nell'equazione di $\mathcal{E}$ si ottiene un polinomio di III grado in $x \rightarrow p(x)$

Ma osserviamo che se r ha almeno 2 punti in comune con $\mathcal{E} \Rightarrow \exists\, x_1, x_2$ tali che

$$\begin{matrix}(x-x_2) \mid p(x) \\ (x-x_1) \mid p(x)\end{matrix} \Rightarrow (x-x_1)(x-x_2) \mid p(x)$$

ma $p(x)$ è un polinomio di grado 3 $\Rightarrow$

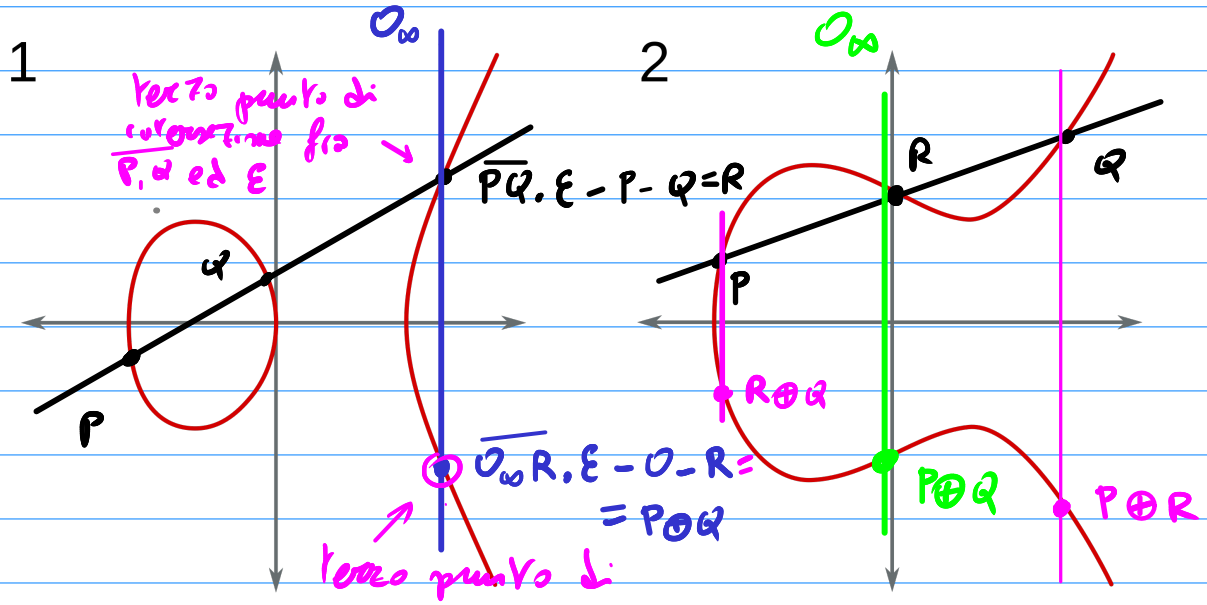
$p(x) = (x-x_1)(x-x_2)\cdot(ax-x_3)$ con $a \neq 0 \Rightarrow$ ha 3 radici

$\Rightarrow |r \cap \mathcal{E}| = 3$

Scriverò $r \cdot \mathcal{E} = P_1 + P_2 + P_3$ per indicare che la retta r e la curva $\mathcal{E}$ si intersecano nei punti P_1, P_2, P_3.

Se $P_1 = P_2 \Rightarrow r \cdot \mathcal{E} = P_1 + P_1 + P_3 = 2P_1 \cdot P_3$

Definiamo la nozione di somma di due punti su $\mathcal{E}$.

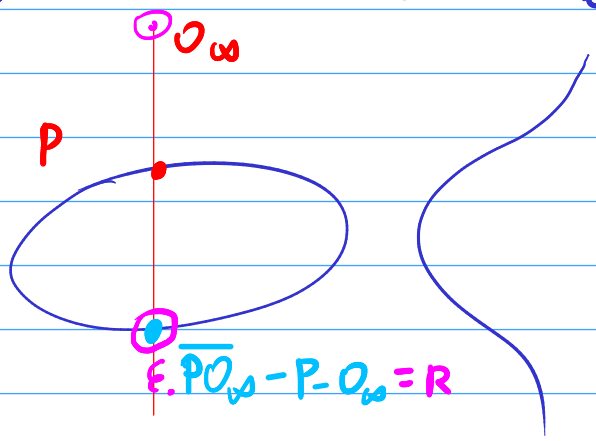


Oss: 1) L'operazione $\oplus : \mathcal{E} \times \mathcal{E} \longrightarrow \mathcal{E}$ è ben definita $\rightarrow$ perché abbiamo visto che i "terzi punti di intersezione" sono punti di $\mathcal{E}$ definiti sul campo $\mathbb{K}$.

2) L'operazione $\oplus$ è commutativa.

$\overline{PQ} \cdot \mathcal{E} - P - Q = \overline{QP} \cdot \mathcal{E} - P - Q$

3) $\mathcal{O}_\infty = [(0,1,0)]$ è l'elemento neutro per $\oplus$



$\overline{R\mathcal{O}_\infty}.\mathcal{E} - R - \mathcal{O}_\infty = P$ perché

$\overline{P\mathcal{O}_\infty}.\mathcal{E} = P + \mathcal{O}_\infty + R$

4) ogni elemento ammette inverso.

dato P definito $\ominus P := \overline{P\mathcal{O}_\infty}.\mathcal{E} - P - \mathcal{O}_\infty = S$

per calcolare $P \oplus \ominus P$ fatto

$$R = \overline{P \ominus P}.\mathcal{E} - P - \ominus P = \mathcal{O}_\infty$$

$$\overline{\mathcal{O}_\infty \mathcal{O}_\infty}.\mathcal{E} = \mathcal{O}_\infty + \mathcal{O}_\infty + \mathcal{O}_\infty$$

retta tg. in $\mathcal{O}_\infty$

$\Rightarrow P \oplus \ominus P = \mathcal{O}_\infty$ identità.

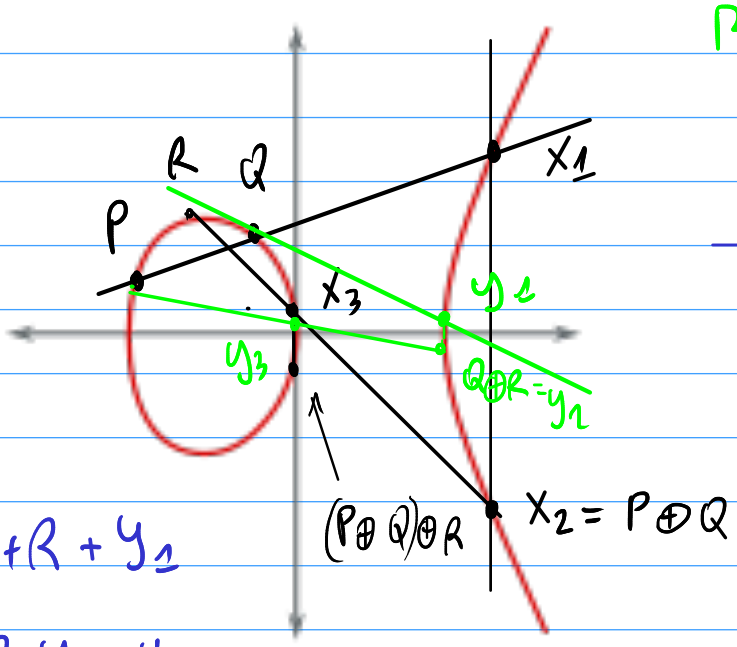
5) proprietà associativa.

(dimostrazione più semplice è quella di scrivere le formule che in coordinate descrivono la somma di 2 punti e vedere che $(X \oplus Y) \oplus Z = X \oplus (Y \oplus Z)$.

Teorema: Siano C_1, C_2 due cubiche e sia $X \subseteq C_1 \cap C_2$ un insieme di 8 punti. Allora $\exists P_9 \in C_1 \cap C_2$ tale che ogni cubica che contiene X contiene anche P_9.

La dimostrazione del teorema si basa sul fatto che per determinare una cubica in generale serve imporre il passaggio per 9 punti, quindi 8 punti in posizione generale determinano ∞^1 cubiche; d'altro canto 2 cubiche che si intersecano in 8 punti hanno necessariamente 9 intersezioni (e queste sono comuni a tutto il fascio che generano) da cui la condizione.

Legge associativa



Bisogna mostrare

$X_3 = Y_3$

$PQ \cdot \mathcal{E} = P + Q + X_1$

$X_1 O \cdot \mathcal{E} = X_1 + O + X_2$

$R X_2 \cdot \mathcal{E} = X_2 + X_3 + R$

$QR \cdot \mathcal{E} = Q + R + Y_1$

$Y_1 O \cdot \mathcal{E} = O + Y_1 + Y_2$

$P Y_2 \cdot \mathcal{E} = P + Y_2 + Y_3$

Consideriamo le cubiche $\mathcal{E}$

ℓ_1 $\quad PQX_1 \cup RX_3X_2 \cup Y_1Y_2O$

ℓ_2 $\quad PY_3Y_2 \cup X_1X_2O \cup RQY_1$

$\mathcal{E} \cap \ell_1 = \{P, Q, X_1, X_2, X_3, Y_1, Y_2, O\}$

$\mathcal{E} \cap \ell_2$ contiene gli 8 punti $P, Q, X_1, X_2, Y_3, Y_2, O$

$\Rightarrow \mathcal{E} \cap \ell_2$ deve contenere anche $X_3 \Rightarrow X_3 = Y_3$ □

Supponiamo ad esempio

$E: \boxed{y^2 = x^3 + ax + b}$ (questo si può sempre supporre a patto che $\mathbb{K} \neq \mathbb{F}_{2^m}, \mathbb{K} \neq \mathbb{F}_{3^n}$ mediante un cambio di coordinate).

$\Rightarrow \quad P = (x_1, y_1) \quad Q = (x_2, y_2)$

$\ominus P = (x_1, -y_1)$

$P \oplus Q = (x_3, y_3)$

$x_3 = \lambda^2 - x_1 - x_2$

$y_3 = \lambda (x_1 - x_3) - y_1$

con $\lambda = \begin{cases} \frac{y_2 - y_1}{x_2 - x_1} & \text{se } P \neq Q, P \neq \ominus Q \\ \frac{3x_1^2 + a}{2y_1} & \text{se } P = Q, y_1 \neq 0 \end{cases}$

se $y_1 = 0 \Rightarrow P = \ominus P \Rightarrow P \oplus P = \mathcal{O}_\infty$

L'elemento più difficile da descrivere è $\mathcal{O}_\infty$.

→ D'altro canto nei crittosistemi basati su DLOG $\mathcal{O}_\infty$ non è che serva poi tanto...

DH.

g

$g^a \longmapsto g^a$

$g^\beta \longleftarrow g^{\beta, \beta}$

$k = g^{a\beta}$ $g^{a\beta}$

serve calcolare le potenze

E G $\quad m \longmapsto (a,b) = (g^k, g^{dk} \cdot m)$

esponenti; prodotti

$b \cdot (a^k)^{-1} = m$

↳ moltiplicare per l'inverso di un esponente

→ prodotto
→ esponente
→ inverso.

Teorema (Hasse-Weil). Sia $E(\mathbb{K})$ una curva ellittica definita sul campo $\mathbb{K}$ e supponiamo

$$|\mathbb{K}| = q \Rightarrow q - 2\sqrt{q} + 1 \leq |E(\mathbb{K})| \leq q + 2\sqrt{q} + 1$$

$E(\mathbb{K})$ è detta supersingolare se $q = p^n$ e

$$|E| = q + 1 - t \qquad p \mid t$$

$$p \mid (|E| - (q+1)).$$

Nel gruppo $(E(\mathbb{K}), \oplus)$ il DLOG è considerato difficile.

per verificare la prop. associativa, si scrivono 3 punti $P = (x_1, y_1)$ $Q = (x_2, y_2)$ $R = (x_3, y_3)$

e si applicano le formule

$$(P \oplus Q) \oplus R = P \oplus (Q \oplus R).$$

Abbiamo definito su un opportuno sottoinsieme di $\mathbb{K}^2$ una operazione $\oplus$ che è "incompatibile" sia con la somma vettoriale "+" che con il prodotto per scalare.

$P = (x,y) \in \mathcal{E} \Rightarrow a(x,y) \in \mathcal{E}$

$\Leftrightarrow$ si tratta di un punto di intersezione della retta per O e P.

$(x,y) + (z,t) \in \mathcal{E}$ in generale non è vero se (x,y) e (z,t) sono punti di $\mathcal{E}$.

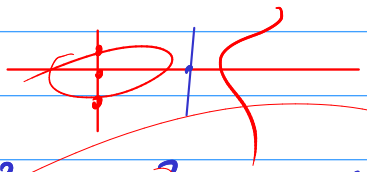
problema:

1) come rappresentare i messaggi come punti di E?

In generale un messaggio è un valore $x \in \mathbb{F}_q$

può essere $\exists y_1, y_2 : (x, y_1), (x, y_2) \in E$

può essere che non $\exists$ tali y_i



se $y^2 = x^3 + ax + b$ e $x^3 + ax + b \in \square$

$y = \pm\sqrt{x^3 + ax + b}$

$\Rightarrow$ abbiamo 2 punti

(x, y) $(x, -y)$ che

rappresentano lo stesso messaggio

x e dobbiamo trasmettere

2 elementi del campo per rappr.

un singolo valore.

↳ fattore 2 di overhead

Se $x^3 + ax + b \notin \square$ $\Rightarrow$ non avete nessun

punto su E con componente x data

$\rightarrow$ non potete codificare il mess.

direttamente con un punto di E.

(x) messaggio $\longrightarrow$ $(x, \pm y) \in E$ — serve una codifica con hash di x

oss: In generale bastano 2 bits oltre a quelli di x stesso.

1) Si osserva che x sistema in caratteristica 2 con una cubica ellittica di eq.

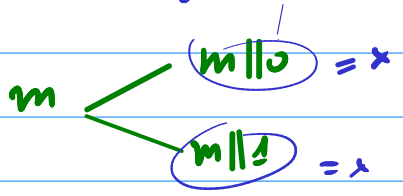
(W) $\quad y^2 + xy = x^3 + ax^2 + b$

$\forall x$ si ha che
- $\exists y$ t.c. che $(x,y) \in E$
- $\exists y$ t.c. che $(x+z, y) \in E$.

→ In generale sacrifichiamo un bit di x per poter codificare il messaggio m.

Cioè se x consta di t bits $\Rightarrow$

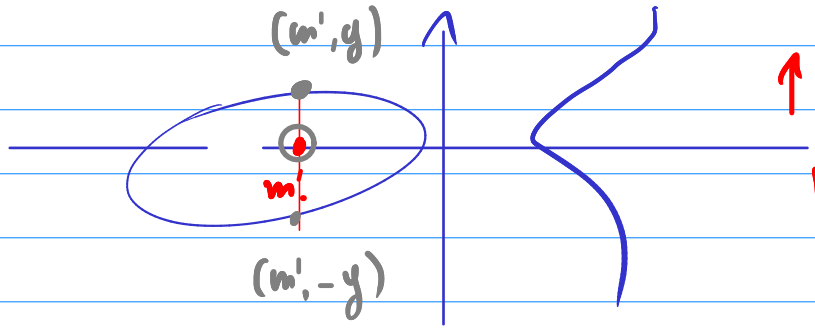
codifichiamo messaggi m di $(t-1)$ bits. scegliendo per come bit meno significativo di $x = x(m)$ esattamente quello che fa sì che x sia l'ordinata di un punto di E.



e noto anche che non c'è bisogno di trasmettere questo bit aggiuntivo.

$\mathbb{F}_{p^n} \cong \mathbb{F}_p^n$

7) per quanto riguarda la componente y, per ogni valore "legale" di x esistono 2 possibilità → basta riuscire a distinguere fra questo 2. → basta 1 bit di informazione



m

↑ dato m' uno basta dire "y nel semipiano superiore" su $\mathbb{R}$

o "y nel semipiano inferiore" su $\mathbb{R}$

← 1 bit di informazione

Se $|k = \mathbb{F}_q$, campo finito => non è ordinato, non si può dire "semipiano superiore/inferiore" ma comunque si può descrivere quale valore di y prendere mediante 1 bit.

0 < 1

$(1\ 1\ 0\ 1\ 0\ 1)$
$(0\ 1\ 1\ 0\ 1\ 1)$ ○

0 → la prima in ordine lex
1 → la seconda in ordine lex.

a b c d
a c d e

↓

in generale possiamo codificare un messaggio w

di t bits come punto di E
trasmettendo $t+1$ bits.

Trasmettere (m, b) ove $b \in \{0,1\}$,
vi dice quale
y scegliere
per il punto
(x, y) ove $x = m \| c$
tale che $(m\|c)$ sia
l'ascissa di un punto di E.

$t+1$ → RAPPRESENTAZIONE COMPRESSA

In sintesi → curve ellittiche usate
per costruire gruppi in cui
DLOG è difficile.
↳ i punti di una
cubica ellittica sono
rappresentati da coppie di
elementi di $\mathbb{F}_q$ → (x, y)
ma in pratica possiamo ridurci
a coppie (x, b) ove $x \in \mathbb{F}_q$
e $b \in \mathbb{Z}_2$ → abbiamo una
regola che associa a due
valori: $(x_2, b_2) \oplus (x_1, b_1) = (x_3, b_3)$

ove concentriamo la nostra att. sul valore di x_3

↳ la legge di somma di punti nelle cubiche ellittiche funziona perché dati P, Q il terzo punto di intersezione fra $\overline{P,Q}$ e la cubica appartiene ad essa per il teorema dell'ordine
(lo dim del)

↓

perché stiamo lavorando in un campo $\mathbb{K}$.

$y = ax + b$ $\qquad$ $y^2 = x^3 + mx + n$

CONSEGUENZE.

1) Si possono usare le cubiche ellittiche come test di primalità.

Idea: Sia $q \in \mathbb{N}$ e consideriamo $\mathbb{Z}_q$ ⇒ Scriviamo l'eq.

$E: \; y^2 = x^3 + ax + b$ con $a, b \in \mathbb{Z}_q$

presi a caso.

Consideriamo $(E, \oplus)$ con $\oplus$ definita come per le cubiche ellittiche.

→ Se q è primo $\Rightarrow (E, \oplus)$ è un gruppo.

Se q non è primo $\Rightarrow (E, \oplus)$ non è un gruppo (in particolare $\exists$ in $(E, \oplus)$ elementi non invertibili).

↓

si trovano elementi $P, Q \in E(\mathbb{Z}_q)$ tali che $P \oplus Q \notin E(\mathbb{Z}_q)$.

Test di primalità. Si prende

$P = (x, y)$ a caso su $E(\mathbb{Z}_q)$

e si considerano $a_i P = \underbrace{P \oplus \cdots \oplus P}_{a_i \text{ volte}}$.

e si guarda se l'op. di somma è eseguibile → se sì → q potrebbe essere primo

se no → q non è primo.

Algoritmo di fattorizzazione.

Consideriamo in $E(\mathbb{Z}_q)$ un punto P e tutti i suoi "multipli".

Supponiamo $a_i P$ si possa calcolare e $a_i P \oplus P = (a_i + 1) P$ no →

non otteniamo un punto sulla curva.

$P \oplus Q = (x_3, y_3)$ $\quad x_3 = \lambda - x_1 - x_2$

$y_3 = \lambda (x_1 - x_3) - y_1$

con $\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1} & \text{se } P \neq Q,\ P \neq \ominus Q \\ \dfrac{3x_1^2 + a}{2y_1} & \text{se } P = Q,\ y_1 \neq 0 \end{cases}$

vuol dire che stiamo dividendo per un el. non invertibile in $\mathbb{Z}_q$

cioè $(x_2 - x_1)$ non è invertibile in

$\mathbb{Z}_q \Rightarrow MCD(x_2 - x_1, q) \neq 1 \Rightarrow$ abbiamo trovato un fattore di q