

lezione di lunedì

---

22 novembre 2021

CRIPTO GRAFICA

ore 16:15

---

---

---

---



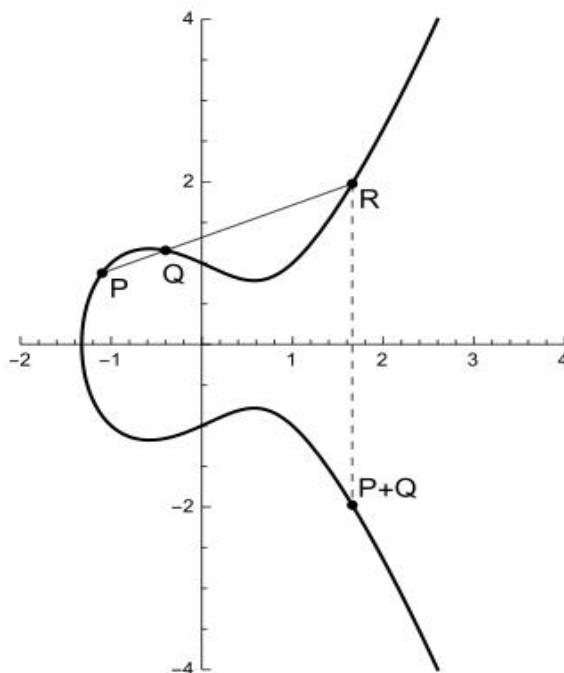
# Curve ellittiche: somma di punti

Quindi **se una retta interseca la curva  $E(a, b)$  in due punti  $P$  e  $Q$ , coincidenti se la retta è una tangente, allora la retta interseca  $E(a, b)$  anche in un terzo punto  $R$**

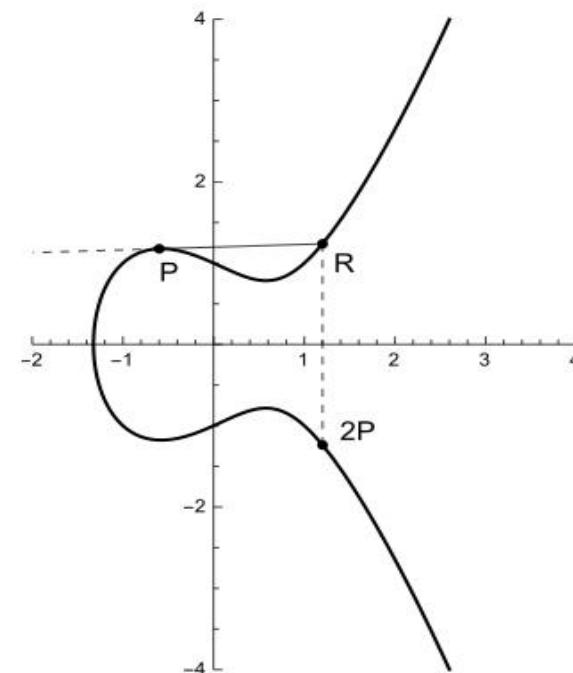
Dati tre punti  $P, Q, R \in E(a, b)$ , se  $P, Q$  e  $R$  sono disposti su una retta, si pone

$$P + Q + R = O$$

Da questa definizione, si ricava la regola per sommare due punti  $P$  e  $Q$



(a) Somma di due punti  $P$  e  $Q$ .



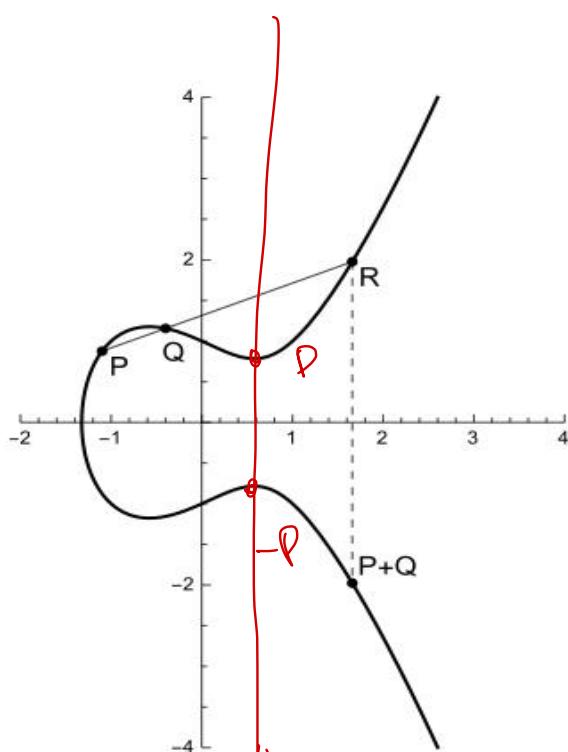
(b) Raddoppio di un punto  $P$

# Curve ellittiche: somma di punti

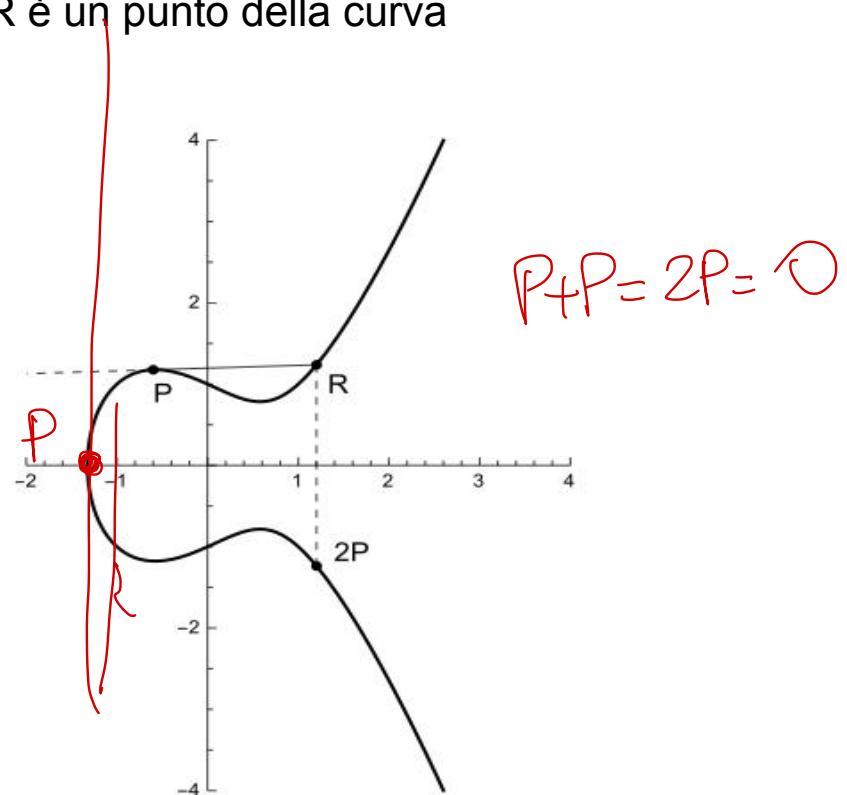
- Si considera la **retta passante per P e Q**, oppure la **tangente in P** se P e Q coincidono
- Si determina il **terzo punto di intersezione R** tra la curva e la retta (o la tangente)
- Si definisce somma di P e Q il punto simmetrico a R rispetto all'asse delle ascisse

$$P + Q = -R$$

La somma è ben definita in quanto anche  $-R$  è un punto della curva



(a) Somma di due punti  $P$  e  $Q$ .



(b) Raddoppio di un punto  $P$

# Curve ellittiche: somma di punti

Siano  $P = (x_P, y_P)$  e  $Q = (x_Q, y_Q)$  due punti della curva  $E(a, b)$

1.  $P \neq \pm Q$

$$S = P + Q$$

$$x_S = \lambda^2 - x_P - x_Q$$

$$y_S = -y_P + \lambda(x_P - x_S)$$

$\lambda = \frac{(y_Q - y_P)}{(x_Q - x_P)}$   $\leadsto$  coefficiente angolare della retta per  $P$  e  $Q$

2.  $P = Q$

$$S = P + Q = 2P$$

$$x_S = \lambda^2 - x_P - x_Q$$

$$y_S = -y_P + \lambda(x_P - x_S)$$

$\lambda = \frac{(3x_P^2 + a)}{2y_P}$   $\leadsto$  coefficiente angolare della tangente alla curva in  $P$  ( $y_P \neq 0$ )

Se  $y_P = 0$ ,  $S = 2P = O$

$P + P$

3.  $Q = -P$

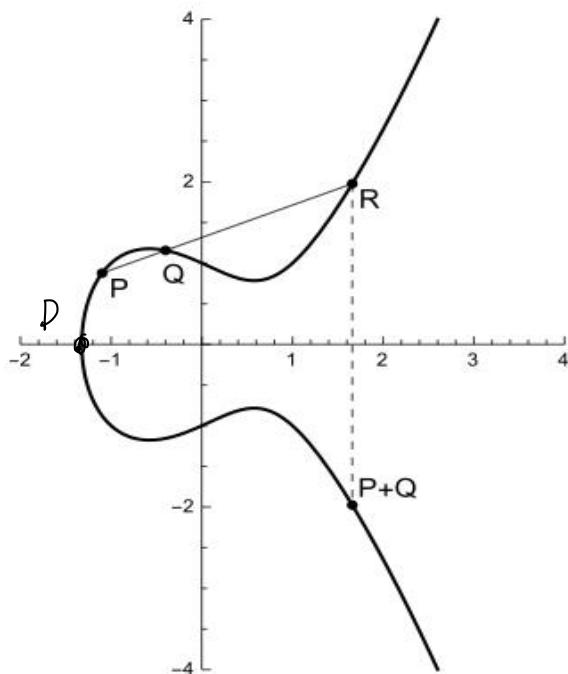
$$S = P + Q = P + (-P) = O$$

# Curve ellittiche: somma di punti

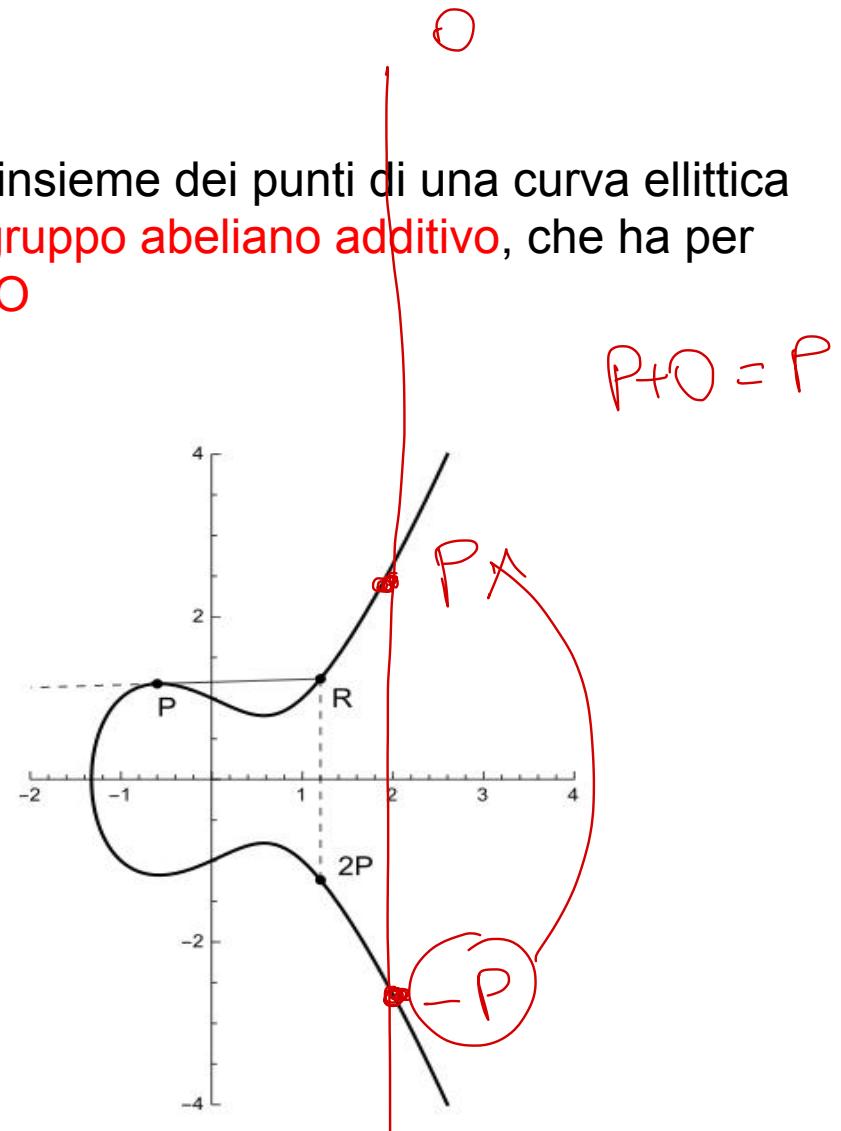
Se  $4a^3 + 27b^2 \neq 0$

la legge di addizione attribuisce all'insieme dei punti di una curva ellittica  $E(a, b)$  la struttura algebrica di un **gruppo abeliano additivo**, che ha per elemento neutro il punto all'infinito  $O$

$$P+O = P$$



(a) Somma di due punti  $P$  e  $Q$ .



(b) Raddoppio di un punto  $P$

# Curve ellittiche: somma di punti

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

la legge di addizione attribuisce all'insieme dei punti di una curva ellittica  $E(a, b)$  la struttura algebrica di un **gruppo abeliano additivo**, che ha per **elemento neutro il punto all'infinito  $O$**

**Chiusura:**  $\forall P, Q \in E(a, b), P + Q \in E(a, b);$

**Elemento neutro:**  $\forall P \in E(a, b), P + O = O + P = P$  (infatti le rette passanti per  $O$  sono verticali, dunque la retta per  $P$  e  $O$  interseca la curva in  $-P$ , il cui simmetrico è  $P$ ); ✓

**Inverso:**  $\forall P \in E(a, b)$ , esiste un unico  $Q = -P \in E(a, b)$  tale che  $P + Q = Q + P = O;$  ✓

**Associatività:**  $\forall P, Q, R \in E(a, b), P + (Q + R) = (P + Q) + R;$  ✓

**Commutatività:**  $\forall P, Q \in E(a, b), P + Q = Q + P.$  ✓

# Curve ellittiche su campi finiti

- Gli algoritmi crittografici hanno infatti bisogno di aritmetica veloce e precisa e non possono utilizzare le curve ellittiche sui reali che richiedono elaborazioni lente e inaccurate a causa degli errori di arrotondamento
- Nell'aritmetica modulare alcuni problemi divengono computazionalmente difficili

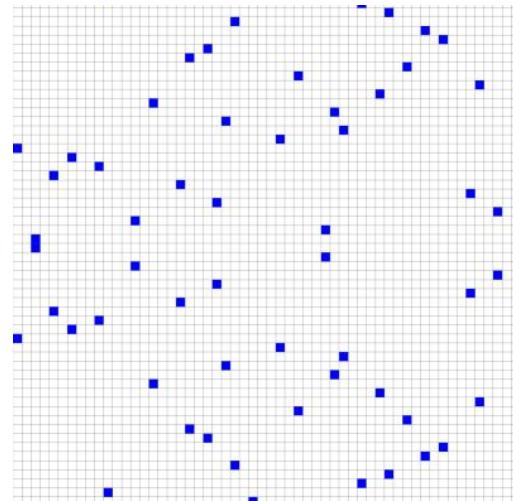
## Curve ellittiche prime

variabili e coefficienti ristretti agli elementi del campo  $Z_p$ ,  $p$  numero primo

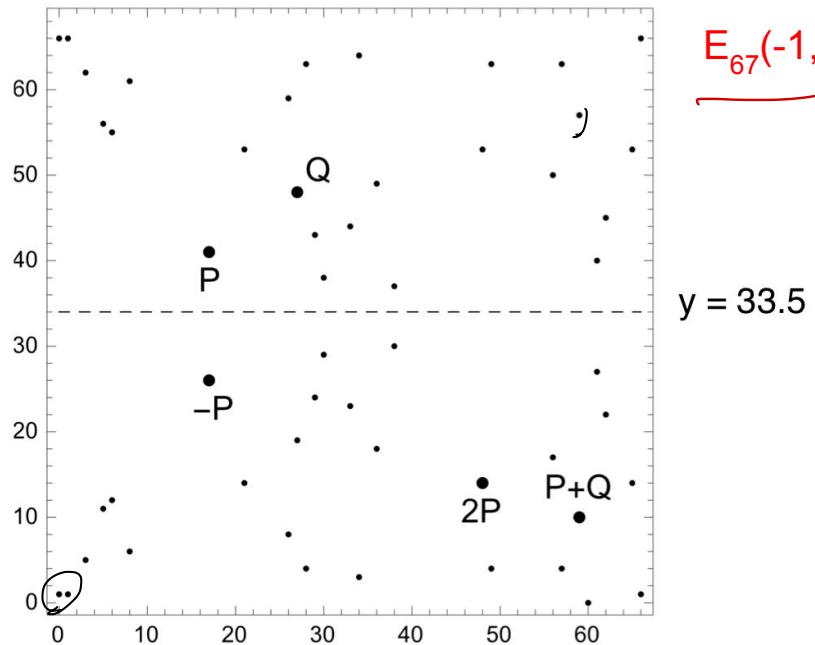
$a, b \in Z_p$ ,  $p > 3$

$$E_p(a, b) = \{ (x, y) \in Z_p^2 \mid y^2 \bmod p = (x^3 + ax + b) \bmod p \} \cup \{O\}$$

Una curva ellittica prima contiene un numero finito di punti, e non è più rappresentata da una curva nel piano



# Curve ellittiche su campi finiti



$E_{67}(-1, 1)$

$y = 33.5$

La curva ellittica prima  $E_p(a, b)$  risulta **simmetrica rispetto alla retta**  
 $y = p/2$

INVERSO di un punto P

$$P = (x, y) \in E_p(a, b)$$

$$-P = (x, -y) = (x, p - y) \in E_p(a, b)$$

$$\rightarrow y \bmod p \equiv \boxed{p - y} \bmod p$$

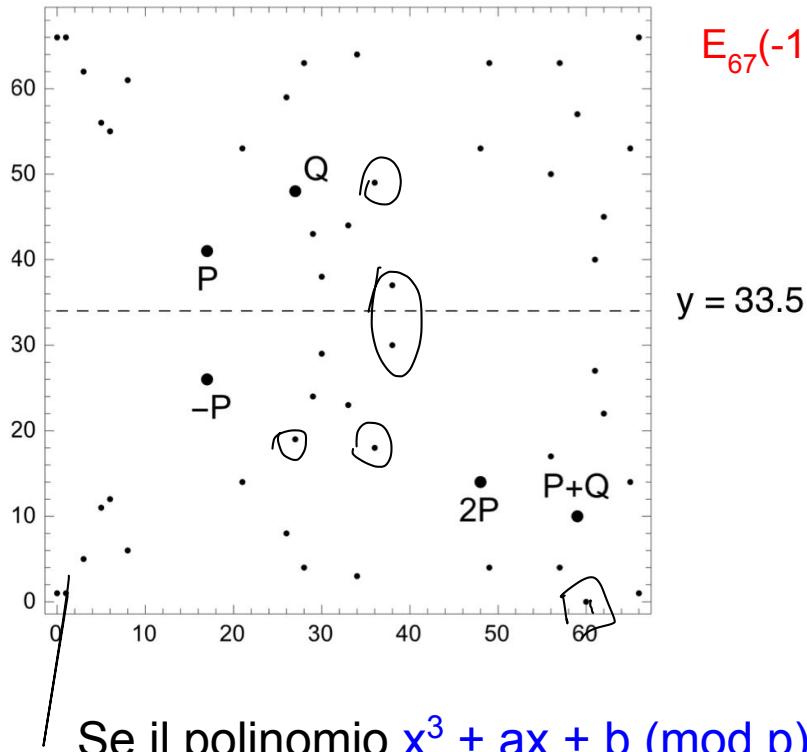
$$y^2 = x^3 + ax + b$$

$$(x, y)$$

$$(x, \boxed{p-y})$$

$$(p-y)^2 = \cancel{x^3} + \cancel{ax} + b - 2py$$

# Curve ellittiche su campi finiti



$E_{67}(-1, 1)$

La curva ellittica prima  $E_p(a, b)$  risulta **simmetrica rispetto alla retta  $y = p/2$**

INVERSO di un punto P

$$P = (x, y) \in E_p(a, b)$$

$$-P = (x, -y) = (x, p - y) \in E_p(a, b)$$

Se il polinomio  $x^3 + ax + b \pmod{p}$  non ha radici multiple, ovvero se

$$4a^3 + 27b^2 \pmod{p} \neq 0$$

i punti della curva  $E_p(a, b)$  formano un **gruppo abeliano additivo finito**

Regole e formulazione algebrica della somma definite per le curve ellittiche  
sui numeri reali si adattano al caso finito, con accortezza di intendere ed  
eseguire tutte le operazioni in algebra modulare.

## curve P-384

It's the elliptic curve that the NSA recommends everyone use until post-quantum methods have been standardized. It provides 192 bits of security, whereas more commonly used curves provide 128 bits.

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

$$\text{modulo } p = 2^{384} - 2^{128} - 2^{96} + 2^{32} - 1$$

$$a = -3$$

b è compreso tra  $2^{383}$  e  $2^{384}$

$$b = 275801935599597058778490118403890480930569058563615685214287073 \\ 01988689241309860865136260764883745107765439761230575$$

P-384 contains  $2^{384} - 2^{190}$  points

Curve prime

$$k = \mathbb{Z}_p$$

$p$  numero primo

caratteristica  $\rightarrow p$

$$E_p(2, 5) = \{ y^2 \equiv \cancel{x}^3 + ax + b \pmod{p} \}$$

$$p \neq 2, 3$$

Curve binarie

$$K = GF(2^m)$$

$$\text{char } k = 2$$

l'equazione delle curve  
non si può ridurre alla  
forma normale di  
Weierstrass

$\Rightarrow$  regole

formule algebriche  
per le somme di punti  
sono diverse

ESEMPIO

$E_5(4,4)$

$$4 \cdot 4^3 + 27 \cdot 4^2 \pmod{5} \neq 0$$

$$\underbrace{4 \cdot 4^3}_1 + \underbrace{27 \cdot 4^2}_{27} \pmod{5}$$

$$\rightarrow 3 \pmod{5} \neq 0 \quad \checkmark$$

$$y^2 \equiv x^3 + 4x + 4 \pmod{5}$$

$y$	0	1	2	3	4
$y^2$	0	1	4	4	1

$x$	$y^2$	$y$
0	4	2, -2
1	4	2, -2
2	0	0
3	3	
4	4	2, -2

$$y^2 = x^3 + 4x + 4$$

1 4 4 mod 5

$(0, 2) \quad (0, 3)$   
 $(1, 2) \quad (1, 3)$   
 $(2, 0)$

→ NON ci sono PUNTI DELLA CURVA  
 DI ASCISSA 3

$(4, 2) \quad (4, 3)$

ORDINE della curva → 8  
 (# dei suoi punti)  $(7 \text{ punti} + 0 \text{ punti})$  all'infinito

## Teorema di Hasse

$N = \text{ordine della curva} \quad \text{primo} \quad E_p(0, b)$

$$|N - (p+1)| \leq 2\sqrt{p}$$

$$N \sim p$$

$$\mathbb{Z}_p$$

$$\begin{matrix} p-1 \\ \hline \mathbb{Z} \end{matrix}$$

punti di  $\mathbb{Z}_p$  sono  
forniti quadratici

$$y^2 \equiv x^3 + Qx + b$$



Funzione one-way hash door

addizione di punti

CE



moltiplicazione  
di interi mod p

"moltiplicazione scalare"  
di un punto  $P \in E_p(0, b)$   
per un intero k



$$kP = \underbrace{P + P + \dots + P}_{k \text{ volte}}$$

k interi positivi



$kP$  si calcola in tempi

polinomiale, con

$\Theta(\log k)$  addizioni e  
moltiplicazioni

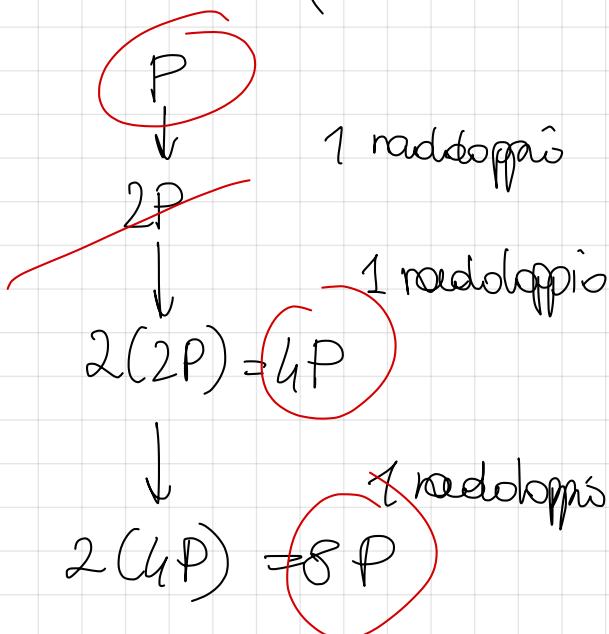
elemento o  
potenza su  $\mathbb{Z}_p$

$$\begin{aligned} y^k \bmod p &= \\ y \cdot y \cdots y &\bmod p \\ \underbrace{\quad\quad\quad}_{k \text{ volte}} \end{aligned}$$

↓  
si calcola in tempi  
polinomiale  
 $\Theta(\log k)$  moltiplicazioni

## Algoritmo dei radicandi ripetuti

$$13P = (8 + 4 + 1)P = \textcircled{8P} + \textcircled{4P} + P$$



$$= 8P + 4P + P$$

3 radicandi  
e 2 somme di punti

in generale

$\lfloor \log_2 k \rfloor$  radicandi

e  $O(\log k)$  somme

## Algoritmo generale

$P \in E_p(Q, b)$

$$k = \sum_{i=0}^t k_i 2^i \quad k_i \in \{0, 1\}$$

$$k_{10} = \underbrace{(k_t k_{t-1} \dots k_2 k_1 k_0)}_{\text{codifica binaria}}_2$$

1) Si calcolano i punti

$$2P, 2^2 P, 2^3 P, \dots, 2^t P$$

(risulta come raddoppio del precedente)  
 (risulta come raddoppio del precedente)

$$t = \lfloor \log_2 k \rfloor$$

$t$  raddoppi

2) Si ottiene  $Q = kP$

$$Q = \sum_{i: k_i=1}^t (2^i P) \quad \rightarrow \leq t \text{ somme}$$

Algoritmo da eseguire

$$\Theta(T) = \Theta(\log k) \cancel{\Theta(k)}$$

somme / raddoppi

# Problema del locaritmo DISCRETO su C.E.

$$Q = kP$$

↑

calcolare  $Q$  da  $k \in P$   
~~ten~~ riducere tempi  
permanenze

Dati  $Q \in P$  hours, se conosci il più  
piccolo intero  $k$  t.c.

$$Q = kP \Rightarrow k = \log_P Q$$

è un problema "difficile"

Cominciamo solo algoritmi esponentiali

$$P, 2P, 3P, 4P, \dots$$



(nessun algoritmo solo polinomiale  
o anche subpolinomiale)

Funzione one-way map door su  $\mathcal{C}^E$ :

moltiplicazione scalare di un punto delle  
curve per un intero  $\rightarrow Q = kP$

(inverso: logaritmo discreto su  $\mathcal{C}^E$ )

$$Q \approx kP$$

## Protocollo di Diffie-Hellman sul CE

Alice e Bob scelgono uno stesso elenco primi  $E_p(Q, G)$  e un punto  $B \in E_p(Q, G)$  di ORDINE  $n$  elevato.

$$\left( \begin{array}{c} f \\ g \end{array} \right)$$

Ordine di un punto = il più piccolo intero  $n$  t.c.  
 $B^n = 0$

Alice

- sceglie a caso un intero  $n_A < n$

- calcola

$$P_A = n_A B$$

- calcola

$$K = n_A P_B (= n_A n_B B)$$

Eve

Bob

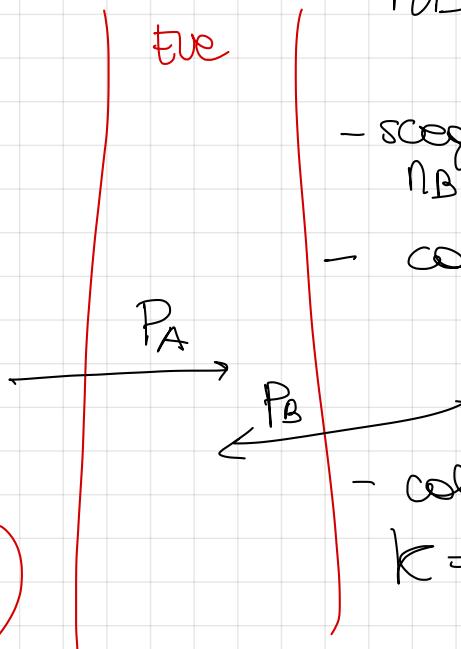
- sceglie a caso un intero  $n_B < n$

- calcola

$$P_B = n_B B$$

- calcola

$$K = n_B P_A (= n_A n_B B)$$



$$k = (x_k, y_k)$$

$x_k \bmod 2^{256}$  → chiede  $x$   
 $\text{AES}(256)$

### Attacki

Attack possibili: (Roberto rispetta ogni attacki possibili)

E se conosce  $E_p(a, b)$ ,  $B$ ,  $P_A$  e  $P_B$

per calcolare il punto  $K$  ha bisogno

di  $n_A$  o  $n_B$

→ deve risolvere il problema dell  
 logaritmo diretto su CE

$$n_A = \log_B P_A$$

$$n_B = \log_B P_B$$

Protocollo di ElGamal ~~è~~ se viene ellittico

(~~cifra~~ cifrano a chiavi pubbliche)

Il protocollo richiede di "incapsulare" il messaggio  
in un punto di una CE

$$m \rightarrow P_m \in E_p(a, b)$$

$$y^2 = \underbrace{x^3 + ax + b}$$

$$x = m \rightarrow P(m, \dots)$$

Se sostituisco  $m$  a  $x$ ,  $b$

Così  $x^3 + ax + b$  corrisponde a un random  
quadratico con probabilità  $\approx 1/2$

$\Rightarrow$

## Algoritmo di Koblitz

$$E_p(0, b)$$

si sceglie un intero  $h \in \mathbb{Z}$ .

$$(m+1)h \leq p$$

$$x = m \cdot h + i \quad 0 \leq i < h$$

$\Rightarrow$  passo per  $h$  tentativi

$$\text{Prob. di fallimento} \sim \left(\frac{1}{2}\right)^h$$

$\Downarrow$

$$\text{Prob. di successo: } 1 - \left(\frac{1}{2}\right)^h$$