

CRITTOGRAFIA

lezione di mercoledì 17/11

ore 16:15

ECC



CURVE ELLITTICHE

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

Somma di punti

$$E(a, b) = \{ (x, y) \in \mathbb{R}^2 \mid y^2 = x^3 + ax + b \text{ e } y \neq 0 \}$$

Idea:

ogni retta interseca una curva in al più 3 punti;

- } 1) - 3 punti di intersezione (tre soluzioni reali delle equazioni)
 2) - 1 punto di intersezione (1 soluzione reale, e 2 complesse coniate)

↳ Se una retta interseca $E(a, b)$ in 2 punti \Rightarrow le interseca anche in un terzo punto

si usa per definire l'operazione
 "SOMMA"

DEFINIZIONE

$$P, Q, R \in E(a, b)$$

se P, Q ed R sono disposti su una retta, si pone

$$P+Q+R = 0$$

$$\Rightarrow P+Q = -R$$



METODO PER SOMMARE DUE PUNTI

$$P, Q \in E_a(a, b)$$

$$Q \neq \pm P$$

retta \overline{PQ}

si calcola il terzo punto di inter. fra $E(a, b) \cap \overline{PQ}$

(R)

si pone

$$P+Q = -R$$

$$\left. \begin{array}{l} R \in E(a, b) \\ -R \in E(a, b) \end{array} \right\}$$

$$Q = -P$$

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

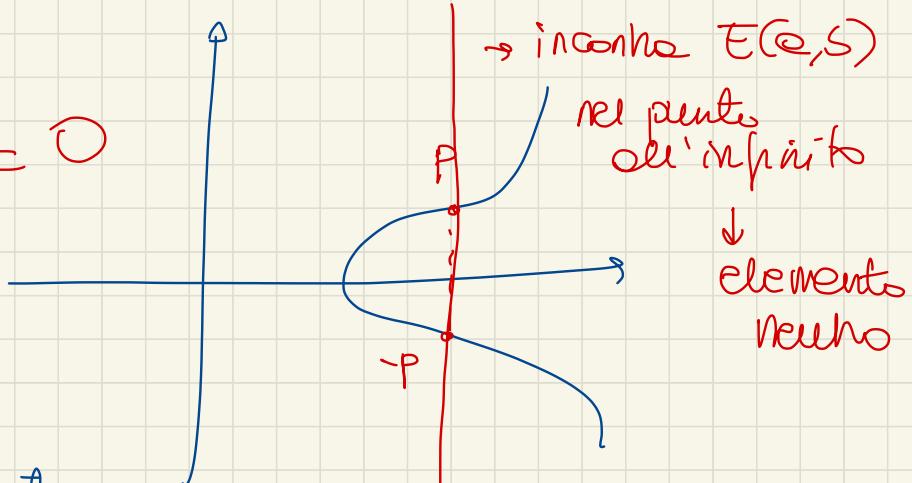
$$Q = P$$

si considera la tangente
alla curva nel punto P

(sempre definito per costruzione, in quanto $40^2 + 276^2 \neq 0$)

si prende l'opposto del punto di intersezione fra
la tangente in P e la curva

(può essere O)



SOMMA

Proprietà

• CHIUSURA

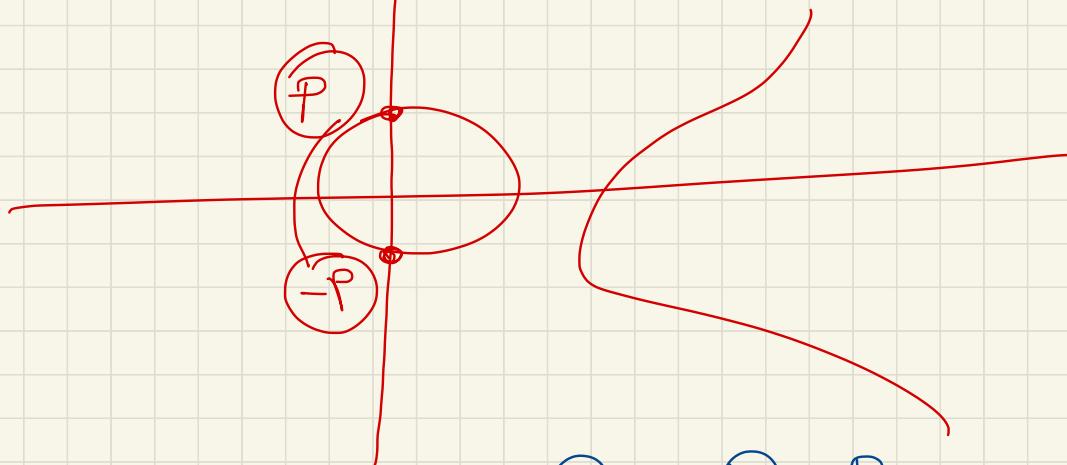
$$\forall P, Q \in E(\mathbb{Q}, S)$$

$$P+Q \in E(\mathbb{Q}, S)$$

• ELEMENTO NEUTRO

$$\forall P \in E(\mathbb{Q}, S)$$

$$P + \mathbb{O} = \mathbb{O} + P = P$$



• INVERSO

$$\forall P \in E(\mathbb{Q}, S)$$

$$\exists! Q \in E(\mathbb{Q}, S) \text{ t.c.}$$

$$P + \underline{Q} = \mathbb{O} = Q + P$$

$$Q = -P$$

$$P = (x, y) \quad -P = (x, -y)$$

PROPRIETÀ COMMUTATIVA:

$$\forall P, Q \in E(\alpha, \beta) \quad P+Q = Q+P$$

PROPRIETÀ ASSOCIAVA

$$\forall P, Q, R \in E(\alpha, \beta) \quad (P+Q)+R = P+(Q+R)$$

Formularazione operativa

$$P = (x_P, y_P) \quad Q = (x_Q, y_Q)$$

$$S = P+Q$$

$$(1) \quad Q \neq \pm P$$

$$S = (x_S, y_S)$$

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

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

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P}$$

$$(2) P = Q$$

stetige Brücke, m2

$$\lambda = \frac{3x_p^2 + a}{2y_p}$$

$$(\text{se } y_p = 0, \quad P+P = \bigcirc)$$

$$(3) Q = -P$$

$$P+Q = \bigcirc$$

CURVE ELIPTICHE SU CAMPI FINITI

Curve prime

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

p numero primo

$$\text{char } \mathbb{Z}_p = p$$

($p > 3$, primo)

Curve liriche

$$k = \text{GF}(2^m) \quad m \in \mathbb{N}$$

\uparrow
char $k = 2$

$$E_p(a, b) = \left\{ (x, y) \in \mathbb{Z}_p^2 \mid y^2 \bmod p = x^3 + ax + b \bmod p \right\}$$

\cup

$x \quad y$

$$[0, p-1]$$

simmetria rispetto a $y = \frac{p}{2}$

$$P = (x, y) \in E_p(0, 5) \Rightarrow -P = (x, p-y) \in E_p(0, 5)$$

$$y^2 = x^3 + 0x + b$$

$$(p-y)^2 \neq p^2 - 2yp + y^2 = y^2$$

$$P = (17, 41) \in E_{67}(-1, 1)$$

$$-P = (17, -41) = (17, 67-41) = (17, 26) \in E_{67}(-1, 1)$$

$$(4a^3 + 27b^2) \bmod p \neq 0$$

↪ per definiere un grupp obereis

ORDINE # punti della curva

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

$$\cong (2p) + 1$$

per
y

soltuoni
altre per
i valori di
 $x \in \{0, p-1\}$

TEOREMA di HASSE

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

$$x \in \mathbb{Z}_p$$

p valori per x

$$\mathbb{Z}_p$$

$\frac{p-1}{2}$ sono repliche
quadratiche

N = ordine di una curva pratica
 $E_p(0, b)$

ESEMPIO

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

0, 1 e 4 sono i residui quadrati

$$x=0 \quad y^2 = 4 \Rightarrow (0, 2), (0, 3) \in E_5(4, 4)$$

$$x=1 \quad y^2 = 4 \Rightarrow (1, 2), (1, 3) \in E_5(4, 4)$$

$$x=2 \quad y^2 = 0 \Rightarrow y=0 \quad (2, 0) \in E_5(4, 4)$$

$$x=3 \quad y^2 = 3 \Rightarrow \text{nessuna soluzione} \quad \nexists \text{ punti di ascissa } 3$$

$$x=4 \quad y^2 = 4 \Rightarrow (4, 2), (4, 3) \in E_5(4, 4)$$

ORDINE = 8 (compriso il punto ∞)

<u>y</u>	<u>y^2</u>
0	0
1	1
2	4
3	4
4	1

Algebra modulare

moltiplicazione

fixed un intero k :

elemento alle
potenza k

(one-way)

$$y^k = y \cdot y \cdots \cdot y$$

$\underbrace{\quad}_{k \text{ volte}}$

k volte



Curve ellittiche

Somma di punti



"moltiplicazione scalare"

di un punto P delle
curve per un intero k

$$kP = P + P + \cdots + P$$

$\underbrace{\quad}_{k \text{ volte}}$

k volte

Costo
di punto
di punto

$$Q = kP$$

temp
poly.
con
RADDOPPI
RIPETUTI

femone one way: moltiplicazione scalare

ONE WAY:

Calcolare $Q = kP$, dati $k \in \mathbb{P}$ è facile
si può fare con $\Theta(\log k)$ operazioni

↳ RANDOPP RIPIEUTI

$$Q = 13P = (1 + 4 + 8)P$$

$$P \xrightarrow{*} 2P \xrightarrow{*} 2(2P) = 4P \xrightarrow{*} 2(4P) = 8P$$

con 3 randoppi calcolo 8P

con 2 somme

Calcolo $Q = P + 4P + 8P$

Algoritmo generale

$$k = \sum_{i=0}^t k_i 2^i \quad (k_t k_{t-1} \dots k_2 k_1 k_0)_2 = k$$

$$t+1 = \lfloor \log_2 k \rfloor + 1 \quad \# \text{bit}$$

1) si calcolano i punti

$$2P, 4P, \dots, 2^t P$$

$\left\{ \begin{array}{l} t \\ \text{raddoppi} \end{array} \right.$ $\Theta(\log k)$

che sono come raddoppi del punto precedente.

2) si calcola Q come:

$$Q = \sum_{i: k_i = 1} (2^i P) \quad \left\{ \begin{array}{l} O(t) \\ \text{somme} \end{array} \right.$$

$O(\log k)$

Operazione inversa della moltiplicazione scalare: se esiste

Dati $P \in Q$, sulla curva $E_P(e, S)$, trovare il più
piccolo k tale che

$$Q = k P$$

$$k = \log_P Q$$

↳ Problema del logaritmo discreto per le C.E.

non si conoscono algoritmi polinomiali
e neppure subpolynomiali

$$E_{23}(9,17)$$

$$Q = (4, 5) \in E_{23}(9, 17)$$

$$P = (16, 5) \in E_{23}(9, 17)$$

$$(4, 5) = k(16, 5)$$

$$k = ?$$

$$P = (16, 5)$$

$$2P = (20, 20)$$

$$3P = (14, 14)$$

:

:

$$9P = (4, 5)$$

$$k = 9$$

Protocollo DH su curve ellittiche.

Preparazione

Alice e Bob scelgono una curva ellittica e un punto B della curva di **ORDINE molto grande**.

Ordine n di
un punto B = più piccolo intero n t.c.
 $nB = \mathbb{O}$

(B "com'è spesso" il generatore g del DH standard)

Curva e punto B sono pubblici

Alice

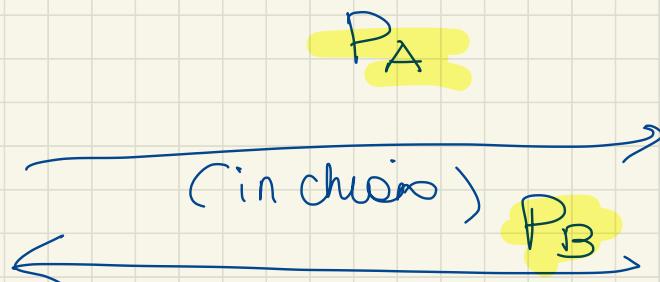
$E_p(0,5)$ $\rightarrow E_p(0,5)$
di ordine n

Bob

eshoes
 $n_A < n$ casuale
(chiavi private)

calcola le
chiavi pubbliche

$$P_A = n_A B$$



nicce P_B c

calcola
 $S = n_A P_B = n_A n_B B$
 $k \text{ (sessione)} = \alpha_S \bmod 2^{256}$

eshoes
 $n_B < n$ casuale
(chiavi private)
calcola le chiavi
pubbliche
 $P_B = n_B B$

nicce P_A c
calcola

$$S = n_B P_A = n_B n_A B$$

$$k \text{ (sessione)} = \alpha_S \bmod 2^{256}$$

Eve: (certosa e nolisca)

Conosce le ans, il punto B , intercette P_A e P_B
per calcolare S delle house n_A t.c.

$$n_A B = P_A$$

Oppure $n_B + c.$ $n_B B = P_B$

quindi deve risolvere il problema alle leg. di ser. C.F.

Protocollo soggetto a attacchi altri
"man in the middle"