Introduzione alle curve ellittiche su campi finiti

Corso di EC - 2024

LE CURVE ELLITTICHE

Una curva ellittica è una curva definita da un'equazione in due incognite del tipo:

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

Le curve ellittiche svolgono un ruolo importante nella teoria dei numeri. Per esempio, furono utilizzate da Andrew Wiles per la risoluzione dell'ultimo teorema di Fermat.

Prof. Andrew Wiles

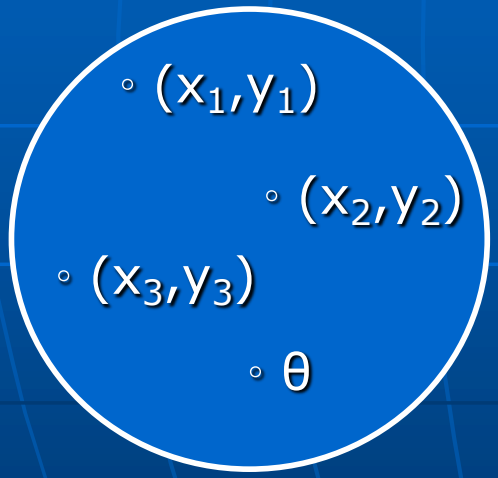
Applicazioni in Crittografia

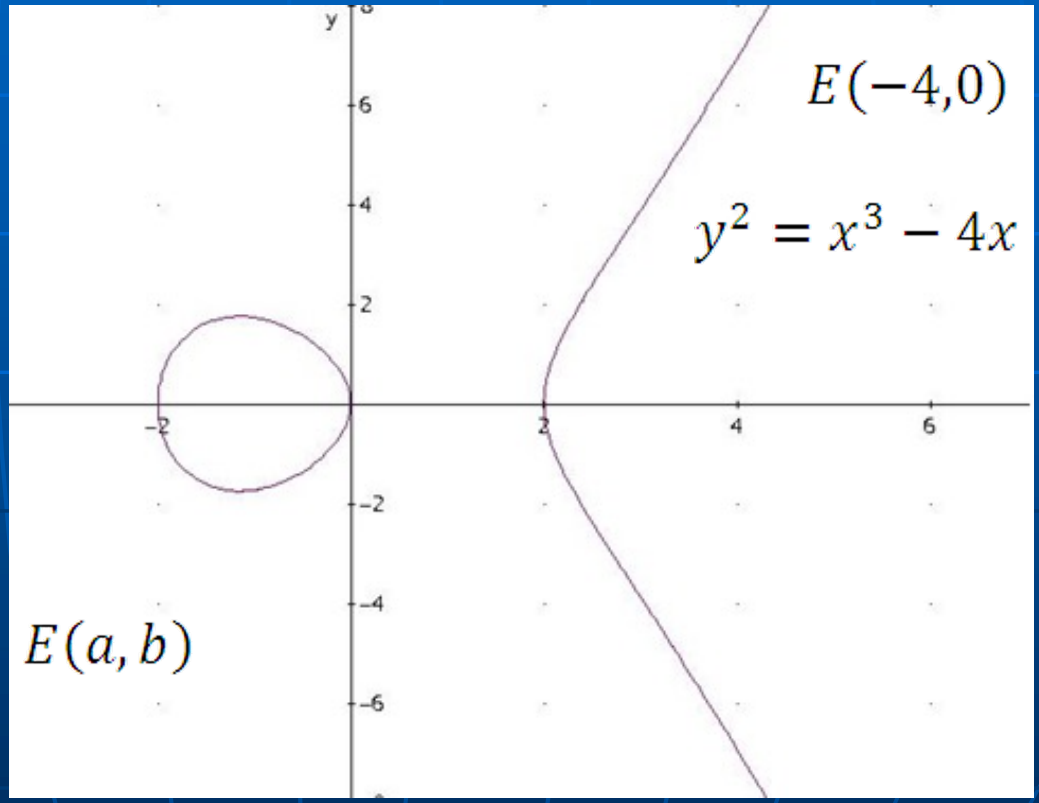
Neal Koblitz

Le curve ellittiche definite su campi finiti hanno molteplici applicazioni in crittografia. Il loro utilizzo venne proposto indipendentemente da Neal Koblitz e Victor S. Miller nel 1985.

CURVE ELLITTICHE SUI REALI

- **Definizione:** Siano a,b ϵ R t.c. $4a^3 + 27b^2 \neq 0$.
  Una curva ellittica non singolare è l'insieme E di soluzioni (x,y) ϵ RxR dell'equazione $y^2 = x^3 + ax + b$, più un punto speciale θ (detto punto all'infinito).





CURVE ELLITTICHE SUI REALI

Proviamo a definire l'operazione di somma tra punti della curva.

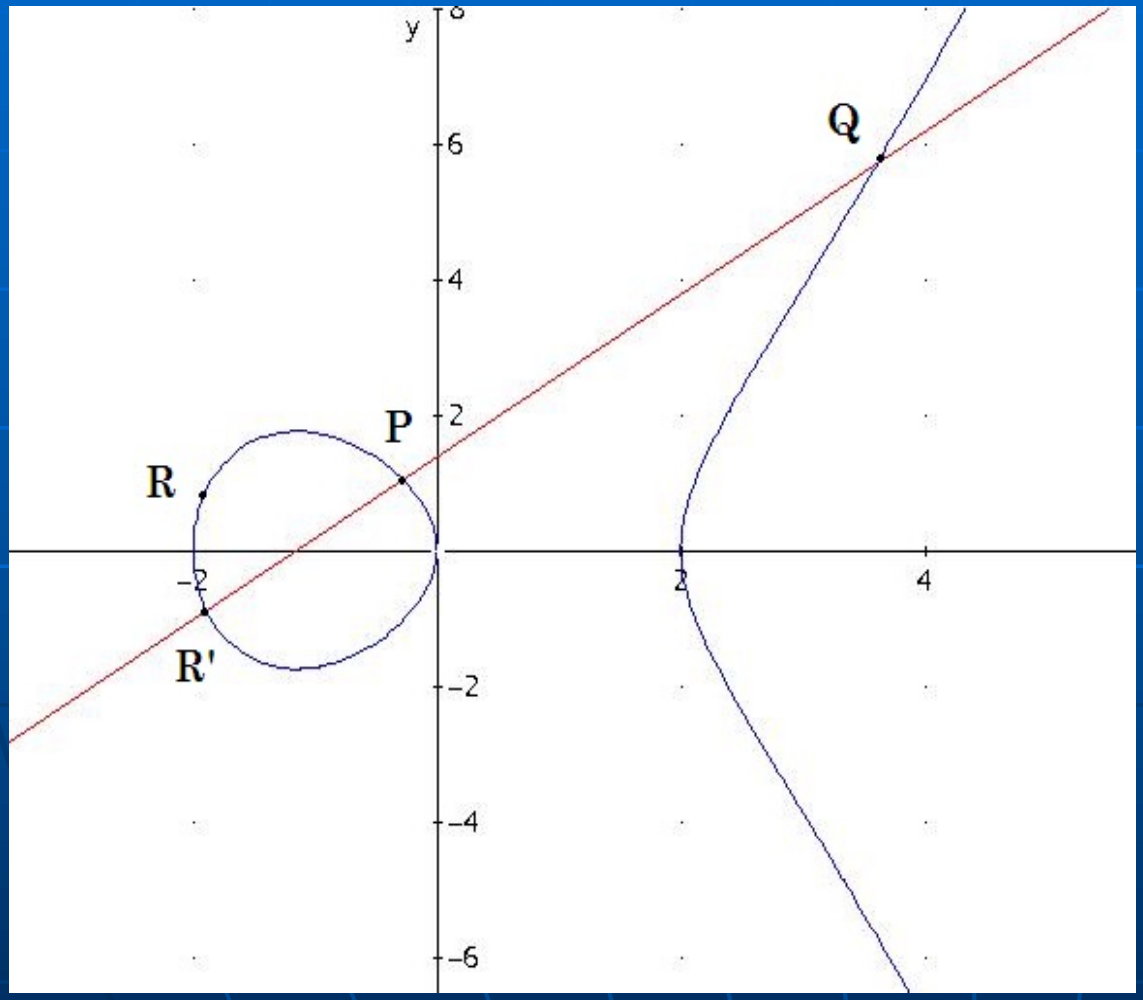
Sia $P \equiv (x_1,y_1)$ e $Q \equiv (x_2,y_2)$.

Consideriamo tre casi:

1. $x_1 \neq x_2$
2. $x_1 = x_2$ e $y_1 = -y_2$
3. $x_1 = x_2$ e $y_1 = y_2$

CASO 1

Sia L la retta che passa attraverso P e Q



La retta L interseca la curva E in P e Q e in un ulteriore punto R'. Riflettendo R' rispetto all'asse delle ascisse si ottiene un punto R.
Definiamo P+Q=R

CASO 1

Cerchiamo di capire come possiamo calcolare le coordinate del punto R

L'equazione della retta L è data da $y = \lambda x + v$

dove il coeff. angolare $\lambda = \dfrac{y_2 - y_1}{x_2 - x_1}$ e $v = y_1 - \lambda x_1 = y_2 - \lambda x_2$

Per trovare i punti $L \cap E$ sostituiamo l'equazione di L nell'equazione di E ottenendo:

$(\lambda x + v)^2 = x^3 + ax + b \rightarrow \lambda^2 x^2 + v^2 + 2\lambda xv = x^3 + ax + b \rightarrow$

$x^3 - \lambda^2 x^2 + x(a - 2\lambda v) + b - v^2 = 0$

L'equazione risultante è un'equazione cubica sui reali avente due radici reali, e quindi anche la terza sarà reale. La somma delle tre radici deve essere uguale a λ^2 , cioè l'opposto del coefficiente del termine quadratico

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

CASO 1

… la somma delle tre radici deve essere uguale a λ^2 , cioè l'opposto del coefficiente del termine quadratico …

Esempio

$P(x) = (x -2)(x-3)(x-4)$

$= (x^2 – 3x – 2x + 6)(x - 4)$

$= (x^3 – 4x^2 – 3x^2 – 12x – 2x^2 – 8x + 6x – 24)$

$= x^3 – (2+3+4)\, x^2 + (6+8+12)x - 24$

opposto somma radici

somma prodotti a due a due

opposto somma prodotti radici a tre a tre

CASO 1

Quindi x_3 è l'ascissa del punto R'. Indichiamo con $-y_3$ l'ordinata. Un modo facile per calcolare y_3 è usare il coefficiente angolare λ della retta L. Infatti è determinato da ogni coppia di punti della retta L. Cioè,

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1} \Leftrightarrow y_3 = \lambda(x_1 - x_3) - y_1$$

Trovato y_3 abbiamo trovato il punto R.
Quindi, nel caso 1, abbiamo derivato una formula per calcolare
$P + Q = (x_3, y_3)$

$$\lambda = \frac{y_2 - y_1}{x_2 - x_1}$$

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

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

CASI 2 e 3

Caso 2 $x_1 = x_2$ e $y_1 = -y_2$

Definiamo $(x,y) + (x,-y) = \theta$ per tutti i punti (x,y) ϵ E
Il punto θ è l'elemento unitario (identità), cioè $P + \theta = \theta + P = P$, per ogni P ϵ E. Inoltre, per ogni punto (x,y) ϵ E, il punto $(x,-y)$ funge da inverso.

Caso 3 $x_1 = x_2$ e $y_1 = y_2$

In questo caso stiamo sommando P a se stesso. Supponiamo $y_1 \neq 0$ altrimenti vale il caso precedente. E' possibile dimostrare che valgono le stesse regole di calcolo del caso 1. Varia soltanto il calcolo di λ che risulta uguale a:

$$\lambda = \frac{3x_1^2 + a}{2y_1}$$

In conclusione abbiamo costruito un gruppo E munito di un'operazione (+) tale che:

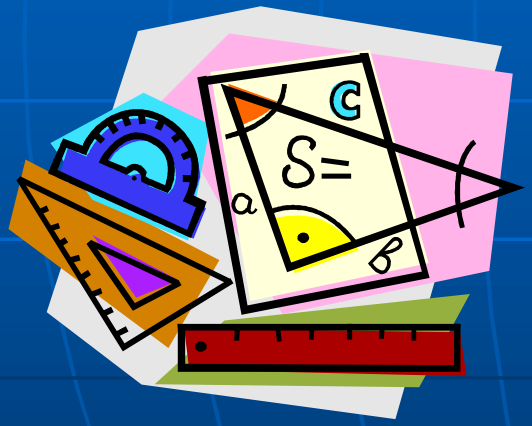
- ✓ E è chiuso rispetto a +
- ✓ L'operazione di somma (+) è commutativa
- ✓ θ è l'elemento neutro
- ✓ Ogni punto di E ha un reciproco
- ✓ L'operazione di somma (+) è associativa (complicato da mostrare)

CURVE ELLITTICHE SU CAMPI FINITI

Campo finito:

Un campo finito F consiste di un numero finito di elementi su cui sono definite due operazioni che godono di alcune proprietà (prop. di un campo).

L'ordine di un campo finito è il numero di elementi del campo.



Molti sistemi crittografici basati su curve ellittiche restringono l'ordine del campo o ad un primo dispari oppure a una potenza di *2*.

GF(p)

GF(2^n)

CURVE ELLITTICHE SU CAMPI FINITI

Invece del campo reale R, consideriamo il campo finito $(Z_p, +, \circ)$ con p primo

Definizione:

Sia $p > 3$ primo

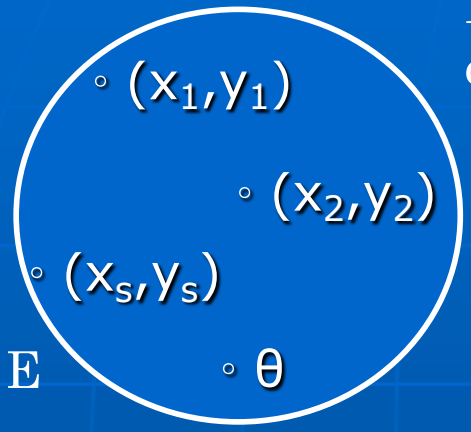
La curva ellittica $y^2 = x^3 + ax + b$ su Z_p è l'insieme delle soluzioni $(x,y) \in Z_p \times Z_p$ alla congruenza:

$$y^2 = x^3 + ax + b \bmod p$$

dove $a,b \in Z_p$ sono costanti tali che $4a^3 + 27\,b^2 \not\equiv 0 \pmod p$

con un punto speciale θ, detto punto all'infinito

L'OPERAZIONE DI SOMMA



L'operazione di somma $+_E$ tra punti di E si definisce come segue:

Siano $P = (x_1,y_1)$ e $Q = (x_2,y_2)$ punti di E

Se $x_2 = x_1$ e $y_2 = -y_1$ allora $P +_E Q = \theta$

Altrimenti

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

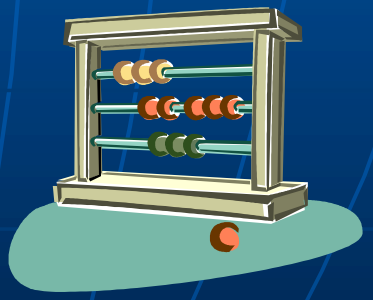
$$y_3 = \lambda(x_1 - x_3) - y_1$$

dove:

$$\lambda = \begin{cases} (y_2 - y_1)(x_2 - x_1)^{-1} & \text{se } P \neq Q \\ (3x_1^2 + a)(2y_1)^{-1} & \text{se } P = Q \end{cases}$$

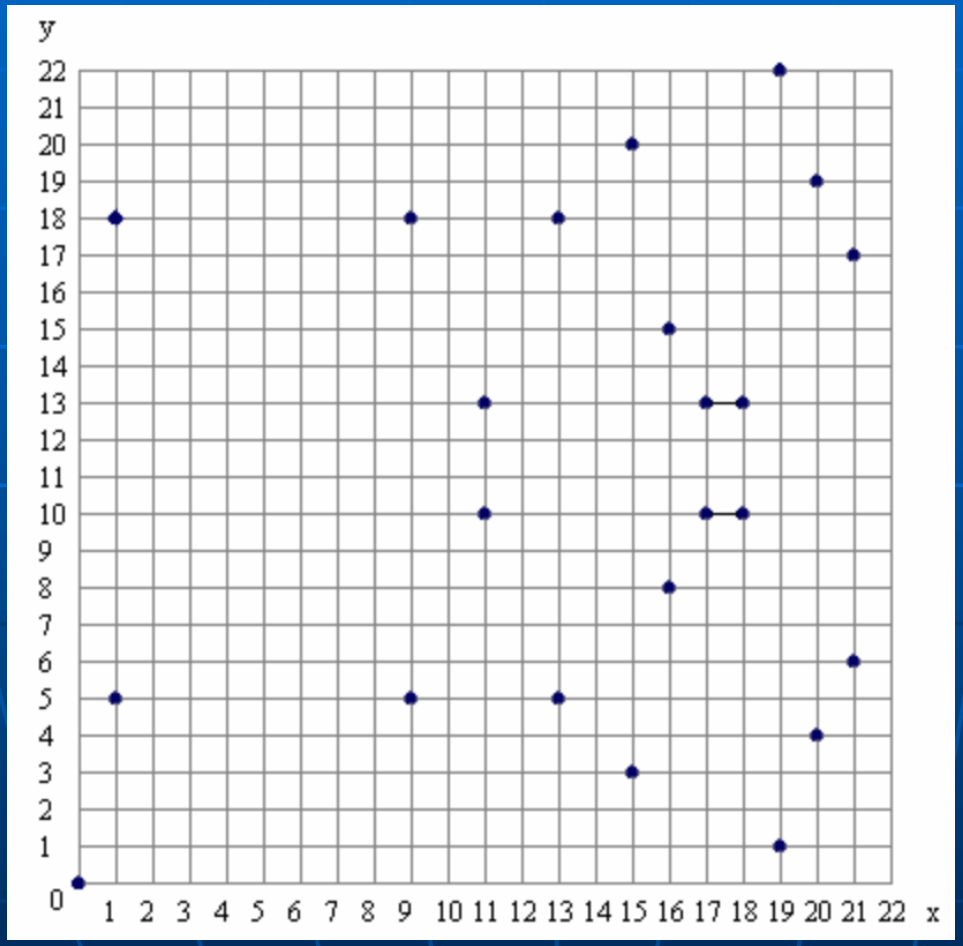
Risulta $\forall P \in E$

$$P +_E Q = Q +_E P$$



L'OPERAZIONE DI SOMMA

Nota: Non esiste come nel caso reale un'interpretazione geometrica per l'operazione di somma ma $(E, +_E)$ costituisce un gruppo abeliano



$y^2 = x^3 + x \mod 23$

CALCOLO DEI PUNTI

Esempio: Il nostro campo $Z_{11} = \{0,1,2,\ldots,10\}$

La nostra curva $E = y^2 = x^3 + x + 6 \bmod 11$

Calcoliamo i punti di E

Possiamo calcolare, per ogni x e Z_{11}, il valore $z = x^3 + x + 6 \bmod 11$

Possiamo poi applicare il criterio di Eulero per vedere se z è un residuo quadratico (i.e. $\exists w: w^2 = z \bmod p$)

Criterio di Eulero: sia p un primo dispari allora a è un residuo quadratico se e solo se $a^{(p-1)/2} \equiv 1 \bmod p$

CURVE ELLITTICHE SU CAMPI FINITI
CALCOLO DEI PUNTI

Inoltre se $p \equiv 3 \bmod 4$ è possibile calcolare le radici di z mod p applicando la formula:

$$\pm z^{\frac{p+1}{4}} \bmod p$$

nel nostro caso significa $\pm z^{\frac{11+1}{4}} \bmod 11 \rightarrow \pm z^3 \bmod 11$

x	$x^3+x+6 \bmod 11$	Test di Eulero	y
0	6	NO	
1	8	NO	
2	5	SI	4,7
3	3	SI	5,6
4	8	NO	
5	4	SI	2,9
6	8	NO	
7	4	SI	2,9
8	9	SI	3,8
9	7	NO	
10	4	SI	2,9

punti della curva ellittica

$y^2 = x^3 + x + 6 \bmod 11$

la curva ha in totale **13** punti compreso il punto all'infinito

CALCOLO DELLE POTENZE

Teorema: se l'ordine di un gruppo è primo, il gruppo è ciclico e ogni elemento (escluso θ) di G è un generatore.

Sia $\alpha = (2,7)$ il generatore. Allora possiamo calcolare le "potenze" di α (poiché l'operazione sugli elementi di E è $+_E$ le potenze sono multipli di α)

Per calcolare $2\alpha = \alpha + \alpha = (2,7) +_E (2,7)$
dobbiamo prima calcolare λ

$\lambda = (3 \times 2^2 + 1)(2 \times 7)^{-1} \bmod 11$
$= 2 \times 3^{-1} \bmod 11$
$= 2 \times 4 \bmod 11$
$= 8$

Calcoliamo (x_3,y_3)

$x_3 = 8^2 - 2 - 2 \bmod 11 = 5$

$y_3 = 8(2-5) - 7 \bmod 11 = 2$

quindi $2\alpha = (5,2)$

CALCOLO DELLE POTENZE

Calcoliamo la potenza successiva $3\alpha = \alpha + \alpha + \alpha = 2\alpha + \alpha = (5,2) +_E (2,7)$

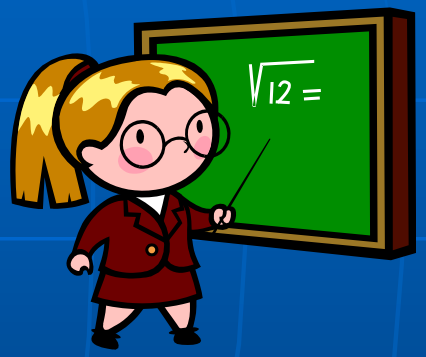
$$\lambda = (7 - 2)(2 - 5)^{-1} \bmod 11 = 5 \circ 7 \bmod 11 = 2$$

Calcoliamo (x_3, y_3)

$$x_3 = 2^2 - 5 - 2 \bmod 11 = 8$$

$$y_3 = 2(5 - 8) - 2 \bmod 11 = 3$$

quindi: $3\alpha = (8,3)$



Proseguendo si ottiene la sequenza completa di punti di E

$\alpha = (2,7)$	$2\alpha = (5,2)$	$3\alpha = (8,3)$
$4\alpha = (10,2)$	$5\alpha = (3,6)$	$6\alpha = (7,9)$
$7\alpha = (7,2)$	$8\alpha = (3,5)$	$9\alpha = (10,9)$
$10\alpha = (8,8)$	$11\alpha = (5,9)$	$12\alpha = (2,4)$

OSSERVAZIONI

Problema: vogliamo che il DLP sia difficile

Teorema di Hasse: sia E una curva ellittica definita su Z_p (p > 3 e primo). Il numero di punti di E, indicato con #E, risulta:

$$p + 1 - 2\sqrt{p} \leq \#E \leq p + 1 + 2\sqrt{p}$$

Quindi possiamo dire che su E ci saranno circa p punti. Il numero preciso può essere calcolato tramite un algoritmo efficiente (algoritmo di Schoof)

Nota: non è detto che E sia ciclico. Se #E è primo o è un prodotto di primi distinti, allora è ciclico

POINT COMPRESS – POINT DECOMPRESS

Dato x ci sono due valori di y tali che $y^2 = x^3 + ax + b \bmod p$.
Questi due valori sono uno il negato dell'altro. Poiché p è primo:

- ✓ uno sarà pari e l'altro dispari
- ✓ è possibile definire un punto P = (x,y) specificando il valore di x e usare un bit per indicare la parità.

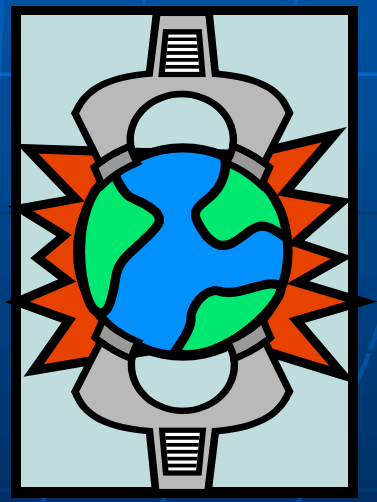
Formalmente possiamo definire un'operazione di compressione e decompressione di un punto

Point Compress:

$E \setminus \{\theta\} \rightarrow Z_p \times Z_2$

Point-Compress (P) = (x,y mod 2)

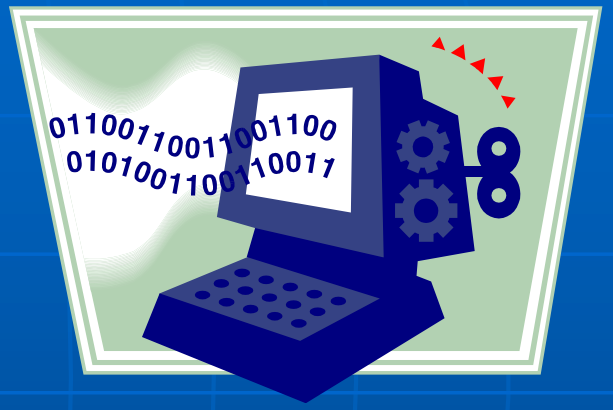
dove P=(x,y) є E



POINT COMPRESS –POINT DECOMPRESS

L'operazione inversa, Point-Decompress, ricostruisce il punto P(x,y)

Algoritmo:



Point_decompress(x,i)

$z \leftarrow x^3 + ax + b \bmod p$

se z non è un residuo quadratico

return "fallito"

altrimenti

$y \leftarrow \sqrt{z} \bmod p$

se $y \equiv i \pmod 2$ return (x, y)

altrimenti return (x, p – y)

EFFICIENZA DEI CRITTOSISTEMI BASATI SU CURVE ELLITTICHE

Sym	ECC	RSA
56	112	512
80	160	1024
112	224	2048
128	256	3072
192	384	7680
256	512	15360

Questa tabella mostra la dimensione delle chiavi dei crittosistemi a parità di sforzo computazionale richiesto dall'analisi crittografica

SQUARE AND MULTIPLY

L'operazione principale nella ECC è kP, i.e. calcolare multipli di un punto P. Si può fare questa operazione in modo efficiente

Esponenziazione modulare

x^c

$c = c_{l-1}\ c_{l-2} \cdots c_0$

$x^c \bmod n$

SQUARE AND MULTIPLY (x,c,n)

$z \leftarrow 1$

for $i \leftarrow l-1$ downto 0 do

- $z \leftarrow z^2 \bmod n$
- if $c_i = 1$ then $z \leftarrow (zx) \bmod n$

return z

SQUARE AND MULTIPLY

Nota: su una curva ellittica l'inverso additivo di un punto è facile da calcolare e.g. $P = (x,y) \rightarrow (x,-y)$

Sia c un intero. Una rappresentazione binaria con segno di c è un'equazione della forma:

$$\sum_{i=0}^{l-1} c_i \circ 2^i \qquad \text{dove } c_i \in \{1,0,-1\} \textit{ per ogni } i$$

Esempio

$11 = 8 + 2 + 1 = 16 - 4 - 1$

$(0,1,0,1,1)$

quindi (c_4,c_3,c_2,c_1,c_0)

$(1,0,-1,0,-1)$

Sono entrambe rappresentazioni binarie, con segno, di 11

DOUBLE AND (ADD OR SUBSTRACT)

Sia P un punto di ordine n di una curva ellittica

Data la rappresentazione binaria con segno $(c_{l-1}, \ldots, c_0)$ di un intero $0 \leq c \leq n-1$ è possibile calcolare il multiplo cP attraverso una serie di raddoppi (2P), addizioni e sottrazioni, usando il seguente algoritmo:

DOUBLE AND (ADD OR SUBSTRACT) $(P,(c_{l-1}, \ldots, c_0),n)$

$Q \leftarrow 0$

for $i \leftarrow l-1$ downto 0 do

{

$Q \leftarrow 2Q$

if $c_i = 1$ then $Q \leftarrow Q + P$

else if $c_i = -1$ then $Q \leftarrow Q - P$

return Q

RAPPRESENTAZIONE NAF (NON ADJACENT FORM)

Una rappresentazione binaria con segno $(c_{l-1}, \ldots, c_0)$ di un intero c è detta in forma non adiacente (NAF) se non ci sono due c_i consecutivi diversi da zero

Trasformazione

E' semplice trasformare la rappresentazione binaria di un intero c (positivo) in rappresentazione NAF.

L'idea alla base della trasformazione è di sostituire le sottostringhe di forma (0,1,1, … , 1) nella rappresentazione binaria tramite la sottostringa (1,0, … ,0,-1).

Tale sostituzione non cambia il valore di c poiché vale l'identità

$$2^i + 2^{i-1} + \ldots + 2^j = 2^{i+1} - 2^j$$

dove $i > j$

Questo processo viene ripetuto fin quando è necessario, partendo dai bit meno significativi e procedendo verso sinistra

RAPPRESENTAZIONE NAF (NON ADJACENT FORM)

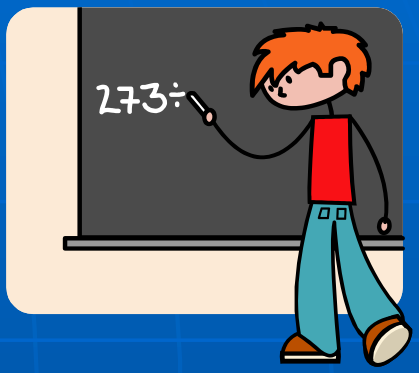
Esempio

1111 0011 0111

1111 0 011 1 00 –1

11110 100 –1 00 –1

1000 –10100 – 100 –1 → NAF



Quindi ogni intero non negativo ha una rappresentazione NAF.
Si può dimostrare che tale rappresentazione è UNICA

In genere una rappresentazione NAF contiene **più zeri** rispetto alla rappresentazione standard in binario di un intero positivo.

Infatti può essere dimostrato che un intero di l bit, in media, contiene:

- ✓ $\frac{l}{2}$ bit = 0 nella rappresentazione binaria tradizionale
- ✓ $\frac{2}{3}\,l$ bit = 0 nella rappresentazione NAF

NOTA FINALE

DOUBLE AND ADD $(P, c_{l-1}, \ldots, c_0, n)$ binaria tradizionale

l raddoppi

l / 2 addizioni

DOUBLE AND (ADD OR SUBSTRACT)

l raddoppi

l / 3 add. o sub.

Assumendo che un'operazione di raddoppio richieda circa lo stesso tempo di una add o substract il rapporto tra i tempi medi di soluzione tra i due algoritmi è

$$\frac{l+\frac{l}{2}}{l+\frac{l}{3}} \rightarrow \frac{\frac{3}{2}l}{\frac{4}{3}l} \rightarrow \frac{3}{2}l \cdot \frac{3}{4}l \rightarrow \frac{9}{8} \rightarrow 1.125$$

C'è, quindi, un guadagno dell' 11% circa

Riferimenti

- Doug Stinson e M. Paterson, “Cryptography: Theory and practice”, CRC Press, 2018

- A. H.Koblitz and N. Koblitz and A. Menezes, Elliptic Curve Cryptography: The Serpentine Course of a Paradigm Shift, *Journal of Number Theory*, 131 (2011), 781-814.

- Appunti forniti (Capitolo 10)

Nota: slide estratte e riadattate da una precedente presentazione di miei studenti (F. Apicella, R. De Feo e E. Travaglino) per un corso di “Complementi di sicurezza su reti”