

CRITTOGRAFIA: raccolta di esercizi (ECC).

Esercizio 1

Il punto $P = (4, 7)$ appartiene alla curva ellittica $y^2 = x^3 - 5x + 5$ sui numeri reali?
Sì, infatti sostituendo $x=4$ nella curva, si ottiene $y^2 = 49 = 7^2$.

Esercizio 2

Nella curva ellittica sui reali $y^2 = x^3 - 36x$, siano $P = (-3, 9)$ e $Q = (-2, 8)$. Trovare $P + Q$ e $2P$.

Risulta $P+Q = (6, 0)$ e $2P = (25/4, -35/8)$

Esercizio 3

La curva ellittica di equazione $y^2 = x^3 + 10x + 5$ definisce un gruppo su Z_{17} ?

No, perché $4Q^3 + 27L^2 = (4 \cdot 10^3 + 27 \cdot 5^2) \bmod 17 = (5+12) \bmod 17 = 0$

Esercizio 4

Determinare i punti appartenenti alla curva ellittica $E_{11}(1, 6)$. VEDI NELLE PAGINE SUCCESSIVE

Esercizio 5

Calcolare gli opposti dei seguenti punti su curva ellittica su Z_{17} : $P = (5, 8)$, $Q = (3, 0)$, $R = (0, 6)$.

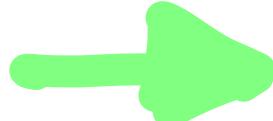
$-P = (5, -8 \bmod 17) = (5, 9)$; $-Q = (3, 0)$; $-R = (0, -6 \bmod 17) = (0, 11)$

Esercizio 6

Nella curva ellittica $E_{17}(1, 7)$, siano $P = (1, 3)$ e $Q = (2, 0)$. Trovare $P + Q$ e $2P$.

Esercizio 7

Nella curva ellittica $E_{23}(14, 12)$, sia $P = (1, 2)$. Calcolare $11P$.



Esercizio 8

Impiegando una curva ellittica $E_p(a,b)$ su un campo finito:

- Spiegare come si esegue in modo efficiente la moltiplicazione di un punto P per una costante intera k .
- Spiegare cosa si intende per "logaritmo discreto" (se esiste) di un punto R in base P .
- Descrivere un algoritmo di scambio di chiavi basato sulla crittografia ellittica e spiegare perché può ritenersi sicuro.

Esercizio 9

Impiegando una curva ellittica prima su un campo finito:

- Spiegare come trasformare un numero intero in un punto della curva.
- Descrivere un algoritmo di scambio di messaggi cifrati e spiegare perché può ritenersi sicuro.
- Trasformare il messaggio $m = 5$ in un punto della curva prima $E_{23}(1,1)$, usando il parametro $h = 3$.

ESERCIZIO 4

Determinare i punti della curva $E_{11}(1,6)$

$$y^2 = x^3 + x + 6 \pmod{11}$$

Per prima cosa identifichiamo i residui quadratici in \mathbb{Z}_{11} .

y	0	1	2	3	4	5	6	7	8	9	10
y^2	0	1	4	9	5	3	3	5	9	4	1

→ i residui quadratici sono $0, 1, 3, 4, 5, 9$

$x = 0$	$y^2 = 6$	→ nessuna soluzione	
$x = 1$	$y^2 = 8$	→ nessuna soluzione	
$x = 2$	$y^2 = 5$	→ $y = 4, 7 \Rightarrow (2, 4), (2, 7)$	
$x = 3$	$y^2 = 3$	→ $y = 5, 6 \Rightarrow (3, 5), (3, 6)$	
$x = 4$	$y^2 = 8$	→ nessuna soluzione	
$x = 5$	$y^2 = 4$	→ $y = 2, 9 \Rightarrow (5, 2), (5, 9)$	
$x = 6$	$y^2 = 8$	→ nessuna soluzione	
$x = 7$	$y^2 = 4$	→ $y = 2, 9 \Rightarrow (7, 2), (7, 9)$	
$x = 8$	$y^2 = 9$	→ $y = 3, 8 \Rightarrow (8, 3), (8, 8)$	
$x = 9$	$y^2 = 7$	→ nessuna soluzione	
$x = 10$	$y^2 = 4$	→ $y = 2, 9 \Rightarrow (10, 2), (10, 9)$	

Dunque risulta

$$E_{11}(1,6) = \{(2, 4), (2, 7), (3, 5), (3, 6), (5, 2), (5, 9), (7, 2), (7, 9), (8, 3), (8, 8), (10, 2), (10, 9)\} \cup \{0\}$$

L'ordine della curva è dunque 13.

ESERCIZIO 7

$$E_{17}(1,7)$$

$$y^2 = x^3 + x + 7 \pmod{17}$$

$$P = (1, 3) \quad Q = (2, 0)$$

SOMMA DI PUNTI
 $x_{P+Q} = \lambda^2 - x_P - x_Q$
 $y_{P+Q} = \lambda(x_P - x_{P+Q}) - y_P$

P+Q

$$\lambda = \frac{y_Q - y_P}{x_Q - x_P} \pmod{p} = \frac{0 - 3}{2 - 1} \pmod{17} = -3 \pmod{17} = 14$$

$$x_{P+Q} = 14^2 - 1 - 2 \pmod{17} = 6$$

$$y_{P+Q} = (14(1 - 6) - 3) \pmod{17} = 12$$

$$\Rightarrow P+Q = (6, 12)$$

2P

$$\lambda = \frac{3x_P^2 + Q}{2y_P} \pmod{p} = \frac{3+1}{6} \pmod{17} = 4 * 6^{-1} \pmod{17}$$

$$6^{-1} \pmod{17} = 3$$

$$\Rightarrow \lambda = 4 * 3 \pmod{17} = 12$$

$$x_{2P} = 12^2 - 1 - 1 \pmod{17} = 6$$

$$y_{2P} = 12(1 - 6) - 3 \pmod{17} = 5$$

$$\Rightarrow 2P = (6, 5)$$

ESERCIZIO 7

$$E_{23}(1, 12)$$

$$P = (1, 2) \quad \text{calcolare} \quad 11P$$

$$11P = (1 + 2 + 8)P = P + 2P + 8P$$

$$\rightarrow \text{se calcoliamo } 2P, 4P = 2(2P) \in 8P = 2(4P)$$

2P:

$$\lambda = \frac{3x_p^2 + a}{2y_p} \bmod p = \frac{3+16}{4} \bmod 23 = 17 * 4^{-1} \bmod 23 = 17 * 6 \bmod 23 = 10$$

$$\alpha_{2P} = \lambda^2 - 2x_p \bmod p = 10^2 - 2 \bmod 23 = 6$$

$$Y_{2P} = \lambda(x_p - \alpha_{2P}) - y_p \bmod p = 10 * (1-6) - 2 \bmod 23 = 17$$

$$2P = (6, 17)$$

$$4P = 2(2P) = 2(6, 17) = (0, 14)$$

$$8P = 2(4P) = 2(0, 14) = (6, 6)$$

$$\Rightarrow 11P = (1, 2) + (6, 17) + (6, 6) = (2, 18) + (6, 6) = (1, 2)$$

ESERCIZIO 8

1. Metodo dei raddoppi ripetuti (vedi testo)

2. E' il più piccolo intero k (\exists esiste) tale che

$$R = kP$$

3. Vedi testo (DH su curve ellittiche)

ESERCIZIO 9

1. Descrizione algoritmo di Koblitz (vedi testo)

2. Vedi testo (protocollo per lo scambio di messaggi crittati)

3. Cenni $E_{23}(1,1)$

$$h = 3 \quad m = 5$$

$$(m+1)h < p$$

$$6 * 3 = 18 < 23$$

RESIDUO QUADRATICO in \mathbb{Z}_{23}

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19	20	21	22
1	4	9	16	2	13	3	18	12	8	6	6	12	4	9	1	

I residui quadratici sono dunque

$$1, 2, 3, 4, 6, 8, 9, 12, 13, 16, 18$$

SITUAZIONE ALGORITMO DI KORBLITZ:

$$0 \leq i \leq h-1$$

$$0 \leq i \leq 2$$

$$i=0 \quad x = mh + i = 5*3 + 0 = 15$$

$$y^2 \bmod 23 = (15^3 + 15 + 1) \bmod 23 = 10 \quad \text{NON} \in \mathbb{R}\mathbb{Q}.$$

$$i=1 \quad x = 15 + 1 = 16$$

$$y^2 \bmod 23 = (16^3 + 16 + 1) \bmod 23 = 19 \quad \text{NON} \in \mathbb{R}\mathbb{Q}.$$

$$i=2 \quad x = 15 + 2 = 17$$

$$y^2 \bmod 23 = (17^3 + 17 + 1) \bmod 23 = \frac{9}{3^2} \quad \text{E' UN R.Q.}$$

$$m \rightarrow P_m = (17, 3)$$