

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?

Esercizio 2

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

Esercizio 3

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

Esercizio 4

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

Esercizio 5

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

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:

1. Spiegare come si esegue in modo efficiente la moltiplicazione di un punto P per una costante intera k .
2. Spiegare cosa si intende per “logaritmo discreto” (se esiste) di un punto R in base P .
3. 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:

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