

1. Sia  $E$  la curva ellittica su  $\mathbf{R}$  di equazione  $Y^2 = X^3 - 2X$ . Sia  $P$  il punto  $(2, 2)$  e sia  $Q = (-1, 1)$ . Calcolare le coordinate dei punti  $-P$ ,  $P + Q$ ,  $P - Q = P + (-Q)$  e  $2P = P + P$ .
2. Sia  $p$  un primo e sia  $E$  una curva ellittica su  $\mathbf{Z}_p$ . Per un punto  $P \in E(\mathbf{Z}_p)$  e un intero  $n \geq 0$  definiamo  $nP$  come  $P + P + \dots + P$  ( $n$  volte). Per  $n < 0$  definiamo  $nP$  come il punto inverso di  $(-n)P$ . Il più piccolo intero  $n > 0$  tale che  $nP = \infty$  si chiama *l'ordine* del punto  $P$ .
  - (a) Determinare l'ordine del punto  $(2, 1)$  sulla curva ellittica  $E$  su  $\mathbf{Z}_5$  di equazione  $Y^2 = X^3 + X + 1$ .
  - (b) Determinare l'ordine di tutti i punti sulla curva ellittica  $E$  su  $\mathbf{Z}_3$  di equazione  $Y^2 = X^3 - X - 1$ . Stessa domanda per la curva di equazione  $Y^2 = X^3 - X + 1$ .
3. Sia  $E$  la curva  $Y^2 = X^3 + X + 1$  su  $\mathbf{Z}_5$ .
  - (a) Dimostrare che si tratta di una curva ellittica.
  - (b) Esibire tutti i punti di  $E$  con coordinate in  $\mathbf{Z}_5$  (ce ne sono nove).
  - (c) Esibire un punto di ordine 9 e concludere che il gruppo  $E(\mathbf{Z}_5)$  è ciclico.
4. Sia  $a \in \mathbf{Z}_5$  e sia  $E$  la curva su  $\mathbf{Z}_5$  di equazione  $Y^2 = X^3 + aX + 1$ .
  - (a) Far vedere che per  $a \neq 3$ , si tratta di una curva ellittica.
  - (b) Per  $a \in \mathbf{Z}_5^*$  diverso da 3, determinare il numero di punti di  $E(\mathbf{Z}_5)$ .
  - (c) Per  $a \in \mathbf{Z}_5^*$  diverso da 3, determinare la struttura del gruppo  $E(\mathbf{Z}_5)$  (cioè scrivere  $E(\mathbf{Z}_5)$  come prodotto di gruppi ciclici).
5. Sia  $p$  un numero primo e sia  $E$  una curva ellittica su  $\mathbf{Z}_p$ . Dimostrare che per ogni  $n \in \mathbf{Z}$  l'insieme  $\{P \in E(\mathbf{Z}_p) : nP = \infty\}$  è un sottogruppo di  $E(\mathbf{Z}_p)$ .
6. Sia  $p > 2$  un numero primo e sia  $E$  la curva ellittica su  $\mathbf{Z}_p$  di equazione  $Y^2 = X^3 - X$ .
  - (a) Calcolare la somma del punto  $(0, 0)$  con se stesso. Far vedere che l'ordine del punto  $(0, 0)$  è uguale a 2.
  - (b) Determinare i punti di ordine 2 di  $E$ .
  - (c) Sia  $E[2] = \{P \in E(\mathbf{Z}_p) : 2P = \infty\}$ . Dimostrare che  $E[2]$  è un gruppo di ordine 4 isomorfo a  $\mathbf{Z}_2 \times \mathbf{Z}_2$ .
7. Sia  $p > 3$  un numero primo e sia  $E$  una curva ellittica su  $\mathbf{Z}_p$  di equazione  $Y^2 = X^3 + AX + B$ .
  - (a) Dimostrare che un punto  $P = (x, y) \in E(\mathbf{Z}_p)$  ha ordine 2 se e solo se
 
$$x^3 + Ax + B = 0$$
  - (b) Dimostrare che ci sono al più 3 punti di ordine 2.
  - (c) Dimostrare che il gruppo  $\{P \in E(\mathbf{Z}_p) : 2P = \infty\}$  è isomorfo a  $\mathbf{Z}_2$ ,  $\mathbf{Z}_2 \times \mathbf{Z}_2$  o al gruppo banale.
8. Sia  $p > 3$  un numero primo e sia  $E$  una curva ellittica su  $\mathbf{Z}_p$  di equazione  $Y^2 = X^3 + AX + B$ .
  - (a) Dimostrare che un punto  $P = (x, y) \in E(\mathbf{Z}_p)$  ha ordine 3 se e solo se
 
$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

PER IL SEGUENTE ESERCIZIO È UTILE UN COMPUTER.

9. (Esperimento fattorizzare usando il metodo "p-1") Sia  $M = 2^3 \cdot 3^2 \cdot 5 \cdot 7$ 
  - (a) Sia  $n = 95431706263$ . Scegliere  $\bar{a} \in \mathbf{Z}_n^*$  a caso. Calcolare  $\bar{b} = \bar{a}^M \pmod{n}$ . Calcolare il divisore  $d = \text{mcd}(b - 1, n)$  di  $n$  ed il cofattore  $n/d$ .
  - (b) Sia  $n = 57841557763361$ . Scegliere  $\bar{a} \in \mathbf{Z}_n^*$  a caso. Calcolare  $\bar{b} = \bar{a}^M \pmod{n}$ . Calcolare il divisore  $d = \text{mcd}(b - 1, n)$  di  $n$  ed il cofattore  $n/d$ .
  - (c) Come mai l'algoritmo trova queste due fattorizzazioni?