1. Sia E una curva su $\mathbf{R}$ di equazione $Y^2 = X^3 + aX + b$. Verificare che è una curva regolare di $\mathbf{R}^2$ (senza punti singolari) se e solo se il discriminante $27b^2 + 4a^3$ è diverso da zero.

2. Sia E una curva ellittica su $\mathbf{R}$ di equazione $Y^2 = X^3 + aX + b$, con discriminante $27b^2 + 4a^3$ diverso da zero. Dati due punti distinti $P = (x_1, y_1)$ e $Q = (x_2, y_2)$ di E, la loro somma $P + Q$ è il punto cosí costruito. Sia r la retta passante per P e Q: se r è parallela all'asse Y, ossia interseca E nel punto all'infinito, allora $P + Q$ è per definizione il punto all'infinito; se r non è parallela all'asse Y, interseca E in un punto R; in tal caso $P+Q$ è per definizione il simmetrico di R rispetto all'asse X. Ricavare le coordinate della somma $P + Q = (x_3, y_3)$.

2.bis Sia E una curva ellittica su $\mathbf{R}$ di equazione $Y^2 = X^3 + aX + b$, con discriminante $27b^2 + 4a^3$ diverso da zero. Dato un punto $P = (x_1, y_1)$ di E, il suo duplicato $2P = P + P$ è il punto cosí costruito. Sia r la retta tangente alla curva in P: se r è parallela all'asse Y, ossia interseca E nel punto all'infinito, allora $2P$ è per definizione il punto all'infinito; se r non è parallela all'asse Y, interseca E in un punto R; in tal caso $2P$ è per definizione il simmetrico di R rispetto all'asse X. Ricavare le coordinate del duplicato $2P = (x_3, y_3)$.

3. Sia E la curva ellittica su $\mathbf{R}$ di equazione $Y^2 = X^3 - 2X$. Siano $P = (2, 2)$ e $Q = (-1, 1)$ due punti su E. Calcolare le coordinate dei punti $-P$, $P + Q$, $P - Q = P + (-Q)$ e $2P = P + P$.

4. Sia E la curva ellittica su $\mathbf{Z}_5$ di equazione $Y^2 = X^3 - 2X$.
   (a) Verificare che si tratta effettivamente di una curva ellittica.
   (b) Siano dati $P = (2, 2)$ e $Q = (-1, 1)$. Verificare che sono punti di E e calcolare le coordinate di $-P$, $P + Q$, $P - Q = P + (-Q)$ e $2P = P + P$.
   (c) Determinare tutti i punti di E.

5. Sia E la curva ellittica su $\mathbf{Z}_7$ di equazione $Y^2 = X^3 - 2X$.
   (a) Verificare che si tratta effettivamente di una curva ellittica.
   (b) Siano dati $P = (2, 2)$ e $Q = (-1, 1)$. Verificare che sono punti di E e calcolare le coordinate di $-P$, $P + Q$, $P - Q = P + (-Q)$ e $2P = P + P$.
   (c) Determinare tutti i punti di E.

6. 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 $P + P + \cdots + P$ (n volte). Per $n < 0$ definiamo nP come il punto inverso di $(-n)P$. Il più piccolo intero $n > 0$ tale che $nP = O = (\infty, \infty)$ si chiama *l'ordine* del punto P.
   (a) Determinare l'ordine del punto $P = (2, 1)$ 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 $Y^2 = X^3 - X + 1$.

7. 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.

8. 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 $E(\mathbf{Z}_5)$.
(b) 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).

9. 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 $\{P \in E(\mathbf{Z}_p) : nP = O = (\infty, \infty)\}$ è un sottogruppo di $E(\mathbf{Z}_p)$.

10. 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 $\{P \in E(\mathbf{Z}_p) : 2P = O = (\infty, \infty)\}$ è isomorfo a $\mathbf{Z}_2$, a $\mathbf{Z}_2 \times \mathbf{Z}_2$ oppure al gruppo banale.

11. 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 $P = (0, 0)$ con se stesso. Far vedere che l'ordine del punto $P = (0, 0)$ è uguale a 2.
(b) Determinare i punti di ordine 2 di E.
(c) Sia $E[2] = \{P \in E(\mathbf{Z}_p) : P + P = O = (\infty, \infty)\}$. Dimostrare che $E[2]$ è un gruppo di ordine 4 isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_2$.

12. 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

$$3x^4 + 6Ax^2 + 12Bx - A^2 = 0.$$

(b) Dimostrare che ci sono al più 8 punti di ordine 3.
(c) Dimostrare che il gruppo $\{P \in E(\mathbf{Z}_p) : 3P = O = (\infty, \infty)\}$ è isomorfo a $\mathbf{Z}_3$ oppure a $\mathbf{Z}_3 \times \mathbf{Z}_3$ oppure al gruppo banale.

13. Sia $p = 7$ e sia E la curva ellittica su $\mathbf{Z}_7$ di equazione $Y^2 = X^3 + 2$.
(a) Determinare i punti di ordine 3 di E.
(c) Sia $E[3] = \{P \in E(\mathbf{Z}_p) : P + P + P = O = (\infty, \infty)\}$. Dimostrare che $E[3]$ è un gruppo di ordine 9 isomorfo a $\mathbf{Z}_3 \times \mathbf{Z}_3$.

14. Sia E la curva su $\mathbf{Z}_{35}$ di equazione $Y^2 = X^3 - X - 2$.
(a) Dimostrare che si tratta effettivamente di una curva ellittica.
(b) Sia $P = (2, 2)$ in $E(\mathbf{Z}_{35})$. Calcolare $2P = P + P$.
(c) Calcolare $3P$ e dare un'interpretazione del risultato.