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.*

Sol. Sia $P = (x, y)$ un punto che soddisfa l'equazione $Y^2 = X^3 + aX + b$. Ricordiamo che per definizione $P = (x, y)$ è un punto regolare di E se

$$\left(\frac{\partial F}{\partial X}(x, y), \frac{\partial F}{\partial Y}(x, y)\right) = (3x^2 + a, 2y) \neq (0, 0). \qquad (*)$$

Queste condizioni garantiscono che *in un intorno di P* la curva $\{(X, Y) \mid F(X, Y) = Y^2 - X^3 - aX - b = 0\}$ ammette retta tangente in ogni punto.
Mostriamo che il sistema

$$\begin{cases} 3X^2 + a = 0 \\ 2Y = 0 \\ Y^2 = X^3 + aX + b \end{cases} \quad \Leftrightarrow \quad \begin{cases} 3X^2 + a = 0 \\ Y = 0 \\ X^3 + aX + b = 0 \end{cases}$$

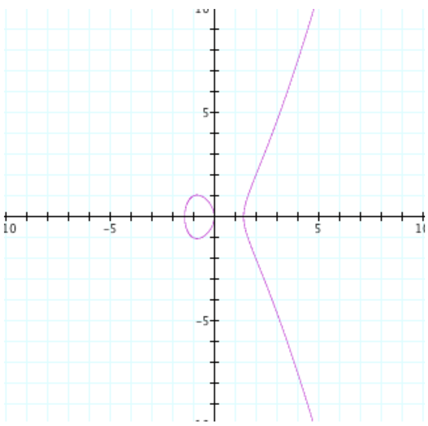
ammette soluzioni, ed in tal caso un'unica soluzione, se e solo se $\Delta = 27b^2 + 4a^3 = 0$.

$\Rightarrow$ Abbiamo che $\Delta = 0$ se e solo se $a = -3\sqrt{b^2/4}$. Se $a = b = 0$, allora $(0, 0)$ è l'unico punto singolare della curva. Se $a, b \neq 0$, dalla prima equazione del sistema ricaviamo $X^2 = -a/3$, che sostituito nella terza ci dà $X = -3b/2a$. In questo caso, l'unico punto singolare della curva è $(-3b/2a, 0)$.

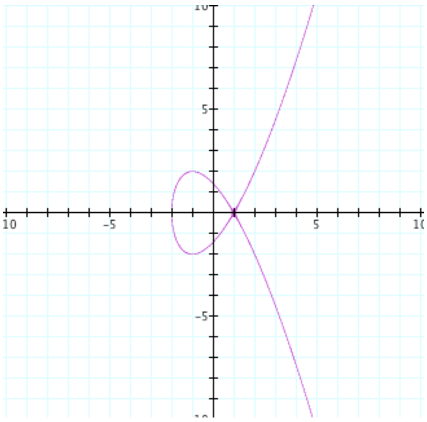
$\Leftarrow$ Se $a = 0$, allora anche $b = 0$ e $\Delta = 0$. Se $a \neq 0$, dal sistema ricaviamo l'unico punto singolare $(-3b/2a, 0)$. In particolare $X = -3b/2a$ deve soddisfare la prima equazione del sistema, da cui $(-3b/2a)^2 + a = 0$ se e solo se $4a^3 + 27b^2 = \Delta = 0$.

$$\left(-\frac{3b}{2a}, 0\right), \qquad \text{con } 27b^2 + 4a^3 = 0.$$

La condizione $27b^2 + 4a^3 \neq 0$ è dunque necessaria e sufficiente a garantire che la curva di equazione $Y^2 = X^3 + aX + b$ *non abbia punti singolari.*



La curva regolare di equazione $Y^2 = X^3 - 2X$.



La curva singolare di equazione $Y^2 = X^3 - 3X + 2$, col punto singolare $(1, 0)$.

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 $P + Q = (x_3, y_3)$.*

Sol. La retta r per P e Q è parallela all'asse Y se e solo se $x_1 = x_2$, e $y_1 = -y_2$. Come abbiamo detto in questo caso $P + Q$ è per definizione il punto all'infinito. Se $x_1 \neq x_2$, la retta r per P e Q ha un'equazione della forma

$$Y = mX + q, \qquad m = \frac{y_2 - y_1}{x_2 - x_1}, \quad q = -mx_1 + y_1.$$

Calcoliamo l'intersezione $r \cap E$ risolvendo il sistema

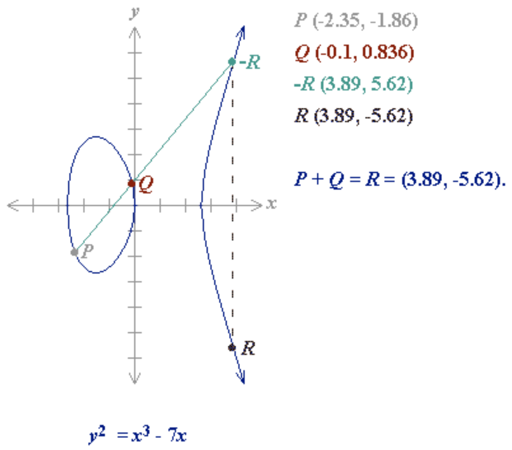
$$\begin{cases} Y^2 = X^3 + aX + b \\ Y = mX + q. \end{cases}$$

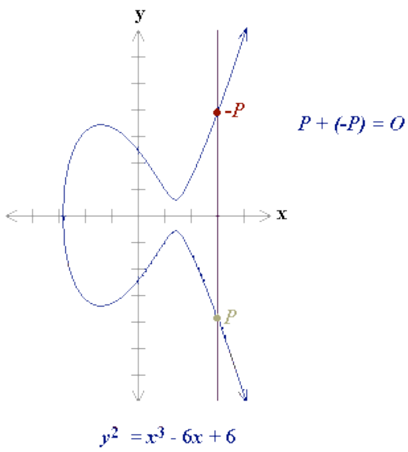
Elevando la seconda equazione al quadrato otteniamo $Y^2 = m^2X^2 + 2mqX + q^2$. Sostituendola nella prima, ricaviamo

$$\begin{cases} Y = mX + q \\ X^3 - m^2X^2 + (a - 2mq)X + (b - q^2) = 0. \end{cases}$$

Osserviamo adesso che i punti P, Q ed R stanno sulla curva, e che R e $P + Q$ hanno la stessa ascissa x_3. Dunque x_1, x_2 e x_3 sono le tre radici dell'equazione di terzo grado $X^3 - m^2X^2 + (a - 2mq)X + (b - q^2) = 0$. Inoltre vale $m^2 = x_1 + x_2 + x_3$. Ne ricaviamo le formule cercate

$$P + Q = (x_3, y_3), \qquad \text{con} \quad \begin{cases} x_3 = m^2 - x_1 - x_2, \\ y_3 = -(m(x_3 - x_1) + y_1). \end{cases}$$





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 $2P = (x_3, y_3)$.*

Sol. Il duplicato $2P$ di un punto $P = (x_1, y_1)$ è la somma di due punti $P + Q$, dove $Q = P$: la retta secante per P e Q diventa la retta tangente alla curva in P, che dunque interseca la curva nel punto P con molteplicità due. La retta tangente alla curva in P è parallela all'asse Y se e solo se $y_1 = 0$, ossia il punto P si trova sull'asse X. In questo caso $2P$ è per definizione il punto all'infinito. Supponiamo ora che la retta tangente alla curva in P non sia parallela all'asse Y e che abbia equazione $Y = mX + q$. Il problema è determinare m e q. Dopodiché tutto il resto procede come nel caso precedente. La curva ellittica E può essere vista come la curva di livello 0 della funzione $F(X, Y) = Y^2 - X^3 - AX - B$

$$E = \{(X, Y) \in \mathbf{R}^2 \mid F(X, Y) = 0\}.$$

Se $P = (x_1, y_1) \in E$, allora la retta r tangente ad E in P è la retta passante per P e ortogonale al gradiente di F in P

$$\mathrm{grad} F_{(x_1,y_1)} = \left(\frac{\partial F}{\partial X}, \frac{\partial F}{\partial Y}\right)_{(x_1,y_1)} = (-3x_1^2 - A, 2y_1).$$

Si ricava facilmente

$$Y = mX + q, \qquad m = \frac{3x_1^2 + A}{2y_1}, \quad q = -mx_1 + y_1$$

e le formule cercate risultano

$$2P = P + P = (x_3, y_3) = (m^2 - 2x_1, -m(x_3 - x_1) - y_1), \qquad m = \frac{3x_1^2 + A}{2y_1}.$$

3. *Sia E la curva 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 $2P = P + P$.*

Sol. Verifichiamo innanzitutto che E è una curva ellittica, cioè ha discriminante non nullo, e che P e Q soddisfano l'equazione di E:

$$27b^2 + 4a^3 = 27 \cdot 0 + 4 \cdot (-2)^3 = -32 \neq 0;$$

$$4 = 8 - 2 \cdot 2 = 4 \quad \Rightarrow \quad P \in E, \qquad 1^2 = (-1)^3 - 2(-1) = 1 \quad \Rightarrow \quad Q \in E.$$

Direttamente dalle formule della somma abbiamo

$$-P = (2, -2), \quad -Q = (-1, -1), \qquad P+Q = ((\frac{1-2}{-1-2})^2 - 2 + 1, -(\frac{1-2}{-1-2})(-\frac{8}{9} - 2) - (-2)) = (-\frac{8}{9}, \frac{28}{27}).$$

Verifichiamo che il punto trovato soddisfa l'equazione di E

$$\frac{784}{729} = (\frac{28}{27})^2 = -(\frac{8}{9})^3 + 2\frac{8}{9} = -\frac{512}{729} + \frac{16}{9} = \frac{784}{729} \quad \Rightarrow \quad P + Q \in E.$$

In modo simile troviamo

$$P - Q = ((\frac{-3}{-3})^2 - 2 + 1, -1(0 - 2) - 2) = (0, 0),$$

$$2P = P + P = (\frac{25}{4} - 2 \cdot 2, \frac{5}{2}(2 - \frac{9}{4}) - 2) = (\frac{9}{4}, -\frac{21}{8}), \qquad m = \frac{3 \cdot 2^2 + (-2)}{2 \cdot 2} = \frac{5}{2}.$$

Si verifica facilmente che $(0, 0)$ e $(5, 11)$ soddisfano l'equazione di E, per cui i punti trovati appartengono ad E.

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.*

Sol. Useremo gli stessi procedimenti dell'esercizio precedente, con la differenza che tutti i calcoli saranno fatti in $\mathbf{Z}_5$. Ricordiamo che in $\mathbf{Z}_5$ gli inversi sono dati da $\bar{3} = \bar{2}^{-1}$ e $\bar{4} = \bar{4}^{-1}$.
(a) Il discriminante di E è dato da

$$27b^2 + 4a^3 \equiv -32 \equiv 3 \not\equiv 0 \mod 5.$$

Dunque E è una curva ellittica anche su $\mathbf{Z}_5$.
(b) Ovviamente gli stessi calcoli fatti sopra dimostrano che le coordinate P e Q soddisfano l'equazione di E, anche su $\mathbf{Z}_5$:

$$4 = 8 - 2 \cdot 2 = 4 \quad \Rightarrow \quad P \in E, \qquad 1^2 = (-1)^3 - 2(-1) = 1 \quad \Rightarrow \quad Q \in E;$$

$$-P = (2, -2) \equiv (2, 3), \quad -Q = (-1, -1) \equiv (4, 4);$$

$P + Q :$

$$m = (1 - 2) \cdot (-1 - 2)^{-1} \equiv 4 \cdot 2^{-1} \equiv 4 \cdot 3 \equiv 2, \quad \text{da cui} \quad P + Q \equiv (3, 1);$$

Si verifica facilmente che il punto $P + Q$ così trovato soddisfa le equazioni di E su $\mathbf{Z}_5$: infatti

$$4^2 \equiv 1 \equiv 3^3 - 2 \cdot 3 \equiv 2 - 1 \equiv 1.$$

$P-Q$:

$$m \equiv 1 \quad \text{da cui} \quad P-Q=(0,0)$$

$2P=P+P$:

$$m \equiv (3\cdot 2^2-2)(2\cdot 2)^{-1} \equiv 0\cdot 4 \equiv 0 \quad \text{da cui} \quad 2P \equiv (1,3).$$

(c) Per determinare tutti i punti di E procediamo cosí: calcoliamo X^3-2X al variare di X fra $\bar{0},\bar{1},\ldots\bar{4}$ e controlliamo se il risultato è o meno un quadrato in $\mathbf{Z}_5$; ogni volta che l'espressione X^3-2X è un quadrato, si determinano due punti su E (possibilmente coincidenti) di coordinate rispettivamente $(X,\sqrt{X^3-2X})$ e $(X,-\sqrt{X^3-2X})$ modulo 5. Osserviamo che i punti $(X,\sqrt{X^3-2X})$ e $(X,-\sqrt{X^3-2X})$ sono *uno l'inverso dell'altro* nel gruppo $E(\mathbf{Z}_5)$.
Elevando al quadrato gli elementi di $\mathbf{Z}_5$ troviamo

$$\bar{0}^2=\bar{0}, \quad \bar{1}^2=\bar{4}^2=\bar{1}, \quad \bar{2}^2=\bar{3}^2=\bar{4},$$

da cui segue che i quadrati in $\mathbf{Z}_5$ sono $\bar{0}$, $\bar{1}$ e $\bar{4}$ e che le rispettive radici quadrate sono: $\sqrt{\bar{0}}=\bar{0}$, $\sqrt{\bar{1}}=\{\bar{1},\ \bar{4}\}$ ed infine $\sqrt{\bar{4}}=\{\bar{2},\ \bar{3}\}$.

$$X=\bar{0} \quad X^3-2X\equiv 0 \qquad (0,0)$$

$$\begin{array}{lll} X=\bar{1} & X^3-2X\equiv 4 & (1,2),\ (1,3) \\ X=\bar{2} & X^3-2X\equiv 4 & (2,2),\ (2,3) \\ X=\bar{3} & X^3-2X\equiv 1 & (3,1),\ (3,4) \\ X=\bar{4} & X^3-2X\equiv 1 & (4,1),\ (4,4). \end{array}$$

In totale, la curva ellittica E su $\mathbf{Z}_5$ ha dunque 10 punti: i 9 punti trovati qui sopra più il punto all'infinito $O=(\infty,\infty)$.

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.*

Sol. (a) Il discriminante di E è dato da

$$27b^2+4a^3 \equiv -32 \equiv 3 \not\equiv 0 \quad \mod 7.$$

Dunque E è una curva ellittica anche su $\mathbf{Z}_7$.
(b)

$$-P=(2,-2), \quad -Q=(-1,-1), \quad P+Q=(3,0), \quad P-Q=(0,0), \quad 2P=(4,0).$$

(c) Elevando al quadrato gli elementi di $\mathbf{Z}_7$ troviamo

$$\bar{0}^2=\bar{0}, \quad \bar{1}^2=\bar{6}^2=\bar{1}, \quad \bar{2}^2=\bar{5}^2=\bar{4}, \quad \bar{3}^2=\bar{4}^2=\bar{2},$$

da cui segue che i quadrati in $\mathbf{Z}_7$ sono $\bar{0}$, $\bar{1}$, $\bar{2}$ e $\bar{4}$ e che le rispettive radici quadrate sono: $\sqrt{\bar{0}}=\bar{0}$, $\sqrt{\bar{1}}=\{\bar{1},\ \bar{6}\}$, $\sqrt{\bar{2}}=\{\bar{3},\ \bar{4}\}$ ed infine $\sqrt{\bar{4}}=\{\bar{2},\ \bar{5}\}$.

$$X=\bar{0} \quad X^3-2X\equiv 0 \qquad (0,0)$$

$$X=\bar{1} \quad X^3-2X\equiv 6 \qquad \emptyset$$
$$X=\bar{2} \quad X^3-2X\equiv 4 \qquad (2,2),\ (2,5)$$
$$X=\bar{3} \quad X^3-2X\equiv 0 \qquad (3,0)$$
$$X=\bar{4} \quad X^3-2X\equiv 0 \qquad (4,0)$$
$$X=\bar{5} \quad X^3-2X\equiv 3 \qquad \emptyset$$
$$X=\bar{6} \quad X^3-2X\equiv 1 \qquad (6,1),\ (6,6).$$

In totale, la curva ellittica E su $\mathbf{Z}_7$ ha dunque 8 punti: i 7 punti trovati qui sopra più il punto all'infinito $O=(\infty,\infty)$.

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 $Y^2=X^3-X+1$.

Sol. (a) Verifichiamo innanzitutto che $P\in E$: infatti $1\equiv 8+2+1\equiv 1 \bmod 5$. Calcoliamo $2P=P+P$:

$$m=(3\cdot 4+1)\cdot 2^{-1}\equiv 3\cdot 3\equiv 4 \bmod 5$$

da cui

$$2P=(1-4,-4(1-6)-1)\equiv(2,-1)=-P \quad \text{in } E(\mathbf{Z}_5).$$

Ne segue che $3P=O=(\infty,\infty)$ e dunque P ha ordine 3 in $E(\mathbf{Z}_5)$.
(b) Determiniamo i punti della curva ellittica E di equazione $Y^2=X^3-X-1$ su $\mathbf{Z}_3$. I quadrati in $\mathbf{Z}_3$ sono $\bar{0}$ e $\bar{1}$ e le rispettive radici quadrate sono $\sqrt{\bar{0}}=\bar{0}$ e $\sqrt{\bar{1}}=\{\bar{1},\bar{2}\}$.

$$X=\bar{0} \quad X^3-X-1\equiv 2 \qquad \emptyset$$
$$X=\bar{1} \quad X^3-X-1\equiv 2 \qquad \emptyset$$
$$X=\bar{2} \quad X^3-X-1\equiv 2 \qquad \emptyset$$

Questa curva ellittica su $\mathbf{Z}_3$ contiene il solo punto all'infinito $O=(\infty,\infty)$, che ha ordine 1.
Determiniamo adesso i punti della curva ellittica E di equazione $Y^2=X^3-X+1$ su $\mathbf{Z}_3$.

$$X=\bar{0} \quad X^3-X+1\equiv 1 \qquad (0,1)\ (0,2)$$
$$X=\bar{1} \quad X^3-X+1\equiv 1 \qquad (1,1)\ (1,2)$$
$$X=\bar{2} \quad X^3-X+1\equiv 1 \qquad (2,1)\ (2,2)$$

Questa curva ellittica su $\mathbf{Z}_3$ contiene 7 punti: i 6 punti qui sopra e il punto all'infinito $O=(\infty,\infty)$. Il gruppo $E(\mathbf{Z}_3)$ è dunque un gruppo di ordine 7. Poiché 7 è primo, il gruppo è necessariamente ciclico e ogni elemento diverso da $O=(\infty,\infty)$ ha ordine 7 (ricordiamo che l'ordine di un elemento divide l'ordine del gruppo). Prendiamo ad esempio $P=(0,1)$. Abbiamo

$$P=(0,1),\quad 2P=(1,1),\quad 3P=(2,2),\quad 4P=(2,1),\quad 5P=(1,2),\quad 6P=(0,2),\quad 7P=O=(\infty,\infty).$$

7. *Sia E la curva $Y^2 = X^3 + X + 1$ su $\mathbf{Z}_5$.*
   (a) Dimostrare che si tratta effettivamente 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.

Sol. (a) Il discriminante della curva risulta $4a^3 + 27b^2 = 31 \equiv 1 \mod 5$, per cui E è una curva ellittica su $\mathbf{Z}_5$.
(b) Col solito procedimento troviamo che i punti di $E(\mathbf{Z}_5)$ sono dati da

$$(0,1), \quad (0,4), \quad (2,1), \quad (2,4), \quad (3,1), \quad (3,4), \quad (4,2), \quad (4,3), \quad (\infty,\infty).$$

(c) Poiché il gruppo $E(\mathbf{Z}_5)$ ha ordine 9, un elemento diverso da $O = (\infty,\infty)$ può avere ordine 3 oppure ordine 9. Se ogni elemento diverso da $O = (\infty,\infty)$ ha ordine 3, allora $E(\mathbf{Z}_5) \cong \mathbf{Z}_3 \times \mathbf{Z}_3$. Se c'è un elemento di ordine maggiore di 3, allora il suo ordine è necessariamente 9. In tal caso $E(\mathbf{Z}_5) \cong \mathbf{Z}_9$ ed è un gruppo ciclico.
Prendiamo ad esempio il punto $P = (0,1)$. Poiché

$$2P = (4,2), \quad 3P = (2,1) \not\equiv (\infty,\infty),$$

P ha ordine maggiore di 3. Dunque $E(\mathbf{Z}_5)$ è un gruppo ciclico di ordine 9 e P è un suo generatore. Per curiosità scriviamo tutti i multipli di P

$$P = (0,1), \quad 2P = (4,2), \quad 3P = (2,1), \quad 4P = (3,4), \quad 5P = (3,1),$$

$$6P = (2,4), \quad 7P = (4,3), \quad 8P = (0,4), \quad 9P = O = (\infty,\infty).$$

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).

Sol. (a) Il discriminante della curva è dato da $27 + 4a^3 \equiv 2 + 4a^3 \not\equiv 0 \mod 5$, per ogni $\bar{a} \neq \bar{3}$ in $\mathbf{Z}_5$. In tutti questi casi E è una curva ellittica. Invece per $a = 3$ il discriminante è 0 ed E non è una curva ellittica.
(b)(c) $a = 0$, $\quad E: \quad Y^2 = X^3 + 1$ ha 6 punti: il punto $O = (\infty,\infty)$ e i 5 punti dati da

$$X = \bar{0} \quad X^3 + 1 \equiv 1 \qquad (0,1)\ (0,4)$$

$$X = \bar{1} \quad X^3 + 1 \equiv 2 \qquad \emptyset$$

$$X = \bar{2} \quad X^3 + 1 \equiv 4 \qquad (2,2)\ (2,3)$$

$$X = \bar{3} \quad X^3 + 1 \equiv 3 \qquad \emptyset$$

$$X = \bar{4} \quad X^3 + 1 \equiv 0 \qquad (4,0).$$

Il gruppo $E(\mathbf{Z}_5)$ è necessariamente isomorfo al gruppo ciclico $\mathbf{Z}_6$ (ricordiamo che per il teorema cinese del resto moltiplicativo $\mathbf{Z}_6 \cong \mathbf{Z}_2 \times \mathbf{Z}_3$). Determiniamo un generatore: il punto $P = (4,0)$ ha ordine 2 (coincide col suo inverso); il punto $Q = (0,1)$ ha ordine tre: $2Q = (0,4)$, $3Q = O = (\infty,\infty)$; il punto $R = (2,2)$ ha ordine 6:

$$2R = (0,4), \quad 3R = (4,0), \quad 4R = (0,1), \quad 5R = (2,3), \quad 6R = (\infty,\infty).$$

In conclusione il gruppo $E(\mathbf{Z}_5)$ è isomorfo al gruppo ciclico $\mathbf{Z}_6$, con generatore $R = (2,2)$.

$a = 1, \quad E: \quad Y^2 = X^3 + X + 1$ ha 9 punti, etc...(vedi Esercizio 7).

$a = 2, \quad E: \quad Y^2 = X^3 + 2X + 1$ ha 7 punti: il punto $O = (\infty, \infty)$ e i 6 punti dati da

$$X = \bar{0} \quad X^3 + X + 1 \equiv 1 \qquad (0,1)\ (0,4)$$

$$X = \bar{1} \quad X^3 + X + 1 \equiv 4 \qquad (1,2)\ (1,3)$$

$$X = \bar{2} \quad X^3 + X + 1 \equiv 3 \qquad \emptyset$$

$$X = \bar{3} \quad X^3 + X + 1 \equiv 4 \qquad (3,2)\ (3,3)$$

$$X = \bar{4} \quad X^3 + X + 1 \equiv 3 \qquad \emptyset.$$

In questo caso $E(\mathbf{Z}_5)$ è necessariamente isomorfo al gruppo ciclico $\mathbf{Z}_7$ e qualunque elemento diverso da $O = (\infty, \infty)$ è un generatore.

$a = 4, \quad E: \quad Y^2 = X^3 + 4X + 1$ ha 8 punti: il punto $O = (\infty, \infty)$ e gli 7 punti dati da

$$X = \bar{0} \quad X^3 + 4X + 1 \equiv 1 \qquad (0,1)\ (0,4)$$

$$X = \bar{1} \quad X^3 + 4X + 1 \equiv 1 \qquad (1,1)\ (1,4)$$

$$X = \bar{2} \quad X^3 + 4X + 1 \equiv 2 \qquad \emptyset$$

$$X = \bar{3} \quad X^3 + 4X + 1 \equiv 0 \qquad (3,0)$$

$$X = \bar{4} \quad X^3 + 4X + 1 \equiv 1 \qquad (4,1)\ (4,4).$$

In questo caso $E(\mathbf{Z}_5)$ è isomorfo al gruppo ciclico $\mathbf{Z}_8$, perché contiene un unico elemento di ordine 2. Un generatore è dato da $P = (0,1)$: infatti

$$P = (0,1), \quad 2P = (4,1), \quad 3P = (1,4), \quad 4P = (3,0), \quad 5P = (1,1),$$

$$6P = (4,4), \quad 7P = (0,4), \quad 8P = O = (\infty, \infty).$$

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 $E(\mathbf{Z}_p)$.*

Sol. Siano P e Q punti di ordine n in $E(\mathbf{Z}_p)$. Facciamo vedere che $P + Q$ e $-P$ soddisfano la condizione richiesta:

$$(P + Q) + \ldots + (P + Q) = P + \ldots + P + Q + \ldots + Q = O + O = O;$$

$$(-P) + \ldots + (-P) = -(P + \ldots + P) = -O = O.$$

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.*

Sol. (a)(b) Un punto $P = (x, y) \in E(\mathbf{Z}_p)$ ha ordine 2, cioè $P + P = (\infty, \infty)$, se e solo se $m = \infty$ se e solo se $y = 0$. Dunque i punti di ordine 2 in $E(\mathbf{Z}_p)$ sono dati dalle soluzioni (x, y) del sistema

$$\begin{cases} Y = 0 \\ X^3 + AX + B = 0 \end{cases} \qquad (*)$$

in $\mathbf{Z}_p \times \mathbf{Z}_p$ e sono al massimo 3.
(c) Osserviamo che il sottogruppo $E[2]$ o è banale oppure ha ordine una potenza di due, perché ogni elemento di $E[2]$ diverso da $O = (\infty, \infty)$ ha ordine 2. Dunque se non è banale, $E[2]$ è un gruppo abeliano di ordine due o quattro.
Se il sistema (*) non ha soluzioni, il sottogruppo $E[2] = \{(\infty, \infty)\}$ è il sottogruppo banale.
Se il sistema (*) ha una sola soluzione, il sottogruppo $E[2] = \{P, (\infty, \infty)\}$ è isomorfo a $\mathbf{Z}_2$.
Se il sistema (*) ha tre soluzioni distinte, il sottogruppo $E[2] = \{P, Q, R, (\infty, \infty)\}$ è isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_2$: in generale un gruppo di ordine 4 è isomorfo a $\mathbf{Z}_4$ oppure a $\mathbf{Z}_2 \times \mathbf{Z}_2$; ma poichè $E[2]$ non contiene elementi di ordine 4, è necessariamente isomorfo a $\mathbf{Z}_2 \times \mathbf{Z}_2$.
(se il sistema (*) avesse due soluzioni distinte, $E[2]$ avrebbe ordine tre, che non è pari).

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* $\mathbf{Z}_2 \times \mathbf{Z}_2$.

Sol. (a) Si vede subito che $P \in E(\mathbf{Z}_p)$. Poiché $P + P = (\infty, \infty)$, il punto P ha ordine 2.
(b) I punti di ordine 2 in $E(\mathbf{Z}_p)$ sono dati dalle soluzioni del sistema

$$\begin{cases} Y = 0 \\ X^3 - X = 0. \end{cases}$$

In questo caso sono precisamente

$$(0, 0), \quad (1, 0), \quad (-1, 0) \equiv (p - 1, 0).$$

(c) Sia $E[2] = \{(0, 0), (1, 0), (-1, 0), (\infty, \infty)\}$. Poichè $E[2]$ non contiene elementi di ordine 4, è necessariamente 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.*

Sol. (a) Un punto $P = (x, y) \in E(\mathbf{Z}_p)$ ha ordine tre, ossia $3P = (\infty, \infty)$, se e solo se $2P = -P = (x, -y)$. Direttamente dalle formule troviamo che $2P = -P = (x, -y)$ se e solo se

$$(3x^2 + A)^2 \cdot (2y)^{-2} = 3x \quad \Leftrightarrow \quad (3x^2 + A)^2 = 3x \cdot (2y)^2 3x \quad \Leftrightarrow$$

$$\Leftrightarrow \quad 3x^4 + 6Ax^2 + 12Bx - A^2 = 0. \qquad (**)$$

(b) L'equazione qui sopra ha al più 4 soluzioni in $\mathbf{Z}_p$. Ad ognuna di tali soluzioni corrispondono al più due punti sulla curva, con ascissa uguale ed ordinata opposta. In totale, ci sono al più otto punti di ordine tre.
(c) Il sottogruppo $E[3]$ o è banale oppure ha ordine una potenza di tre, perché ogni elemento di $E[3]$ diverso da $O = (\infty, \infty)$ ha ordine 3. Precisamente tre o nove.
Se l'equazione (**) non ha soluzioni, il sottogruppo $E[3] = \{(\infty, \infty)\}$ è il sottogruppo banale.
Se l'equazione (**) ha due soluzioni distinte, il sottogruppo $E[3] = \{P, Q, (\infty, \infty)\}$ è isomorfo a $\mathbf{Z}_3$.
Se l'equazione (**) ha otto soluzioni distinte, il sottogruppo $E[3] = \{P, Q, R, S, T, L, M, N, (\infty, \infty)\}$ è isomorfo a $\mathbf{Z}_3 \times \mathbf{Z}_3$: in generale un gruppo di ordine 9 è isomorfo a $\mathbf{Z}_9$ oppure a $\mathbf{Z}_3 \times \mathbf{Z}_3$; ma poichè $E[3]$ non contiene elementi di ordine 9, è necessariamente isomorfo a $\mathbf{Z}_3 \times \mathbf{Z}_3$.

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 $\mathbf{Z}_3 \times \mathbf{Z}_3$.

Sol. (a) Le soluzioni del polinomio $3x^4 + 24x = 0$, o equivalentemente del polinomio $x(x^3 + 1) = 0$, in $\mathbf{Z}_7$ sono date da $x = 0$, $x = -1 \equiv 6$, $x = -2 \equiv 5$ e $x = -4 \equiv 3$. Questi valori sono le possibili ascisse dei punti di ordine 3. Calcolando $X^3 + 2$ al variare di $x = 0, 6, 5, 3$, si trova il quadrato dell'ordinata di tali punti.

$$\begin{array}{lll} x = 0 & X^3 + 2 \equiv 2 & (0,3),\ (0,4) \\ x = -1 & X^3 + 2 \equiv 1 & (6,1),\ (6,6) \\ x = -2 & X^3 + 2 \equiv 1 & (5,1),\ (5,6) \\ x = 3 & X^3 + 2 \equiv 1 & (3,1),\ (3,6) \end{array}$$

(b) Poiché $E[3]$ ha ordine 9 e non contiene elementi di ordine 9, è necessariamente 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.

Sol. Osserviamo che 35 non è un numero primo, ma procediamo come se lo fosse.
(a) Il discriminante della curva risulta

$$4a^3 + 27b^2 = 104 \equiv -1 \equiv 34 \mod 35, \qquad \gcd(34, 35) = 1,$$

per cui E è una curva ellittica su $\mathbf{Z}_{35}$.
(b) Sia $P = (2, 2)$ in $E(\mathbf{Z}_{35})$. Abbiamo $m = (3 \cdot 2^2 + (-1)) \cdot (2 \cdot 2)^{-1} \equiv 11 \cdot 9 \equiv 29 \mod 35$, da cui

$$2P = (29^2 - 4, -29(32) + 2) \equiv (32, 3) \quad \text{in } E(\mathbf{Z}_{35}).$$

(c) Per calcolare $3P = P + 2P$ come al solito determiniamo m:

$$m = (3 - 2) \cdot (32 - 2)^{-1} \equiv 1 \cdot 30^{-1}.$$

A questo punto però vediamo che $gcd(30, 35) \neq 1$, ossia 30 non è invertibile modulo 35. Quindi non possiamo fare la somma $P + 2P$ con le solite formule. In compenso nel constatare ciò, abbiamo individuato un fattore di 35..... Questo è quello che succede col metodo di fattorizzazione di Lenstra basato sulle curve ellittiche.