1. Per $p = 11$ e 13 determinare il numero di curve ellittiche su $\mathbf{Z}_p$ a meno di isomorfismo.

2. Per $p = 11$ e 13 determinare il gruppo di automorfismi della curve ellittica su $\mathbf{Z}_p$ di equazione $Y^2 = X^3 + X$.

3. (a) Dimostrare che l'anello $\mathbf{Z}[\sqrt{-2}]$ è un anello Euclideo (rispetto alla norma).
   (b) Fattorizzare i numeri primi $p = 2$, 5 e 11 in $\mathbf{Z}[\sqrt{-2}]$.
   (c) Sia $p > 2$ un primo. Dimostrare che sono equivalenti: (i) $-2$ è un quadrato modulo $p$; (ii) $p \equiv 1, 3 \pmod 8$; (iii) $p = a^2 + 2b^2$ per certi $a, b \in \mathbf{Z}$.

4. Sia $d \in \mathbf{Z}_{<0}$ congruent to $0, 1 \pmod 4$ e sia $R_d$ l'ordine in $\mathbf{C}$ di discriminante $d$. Il *numero delle classi di Kronecker* $H(d)$ di $R_d$ è $\#Q(d)$, dove $Q(d)$ è l'insieme

$$Q(d) = \{(a, b, c) \in \mathbf{Z}^3 : \begin{cases} a > 0,\ b^2 - 4ac = d,\ |b| \le a \le c, \\ \text{dove } b > 0 \text{ se } |b| = a \text{ oppure } a = c. \end{cases}\}.$$

   Il *numero delle classi* $h(d)$ di $R_d$ è uguale a $\#\{(a, b, c) \in Q(d) : \mathrm{mcd}(a, b, c) = 1\}$.
   (a) Determinare $H(-39)$, $H(-64)$, $H(-100)$.
   (b) Determinare $h(-39)$, $h(-67)$, $h(-71)$ e $h(-100)$.

5. Sia $d = -39$. Per ogni terna $(a, b, c) \in Q(d)$ disegnare il reticolo $\mathbf{Z} + \frac{b+\sqrt{d}}{2a}\mathbf{Z}$. Stessa domanda per $d = -64$.

6. (a) Scrivere $p = 277$ nella forma $p = a^2 + b^2$ per certi $a, b \in \mathbf{Z}$. Per quante coppie $(a, b)$ si ha che $p = a^2 + b^2$?
   (b) Scrivere $p = 277$ nella forma $p = c^2 + cd + d^2$ per certi $c, d \in \mathbf{Z}$. Per quante coppie $(c, d)$ si ha che $c^2 + cd + d^2$?

7. Se possibile scrivere i primi $p = 101$, 103 e 107 nella forma $a^2 + ab + 10b^2$ per certi $a, b \in \mathbf{Z}$.

8. Sia $R_d$ l'ordine in $\mathbf{C}$ di discriminante $d$ e sia $(a, b, c) \in A(d)$. Sia $\tau = \frac{b+\sqrt{d}}{2a}$. Dimostrare che $|e^{2\pi i \tau}| \le e^{-\pi\sqrt{3}} < \frac{1}{200}$.

9. Sia $p = 107$ e sia $E$ una curva ellittica su $\mathbf{Z}_p$ con $\mathrm{End}(E)$ isomorfo all'ordine di discriminante $-7$. Allora ci sono due possibilità per $\#E(\mathbf{Z}_p)$. Determinarle.

10. Sia $p = 103$ e sia $E$ una curva ellittica su $\mathbf{Z}_p$ con invariante $j$ uguale a $j = -2^{15}$. Allora ci sono due possibilità per $\#E(\mathbf{Z}_p)$. Determinarle. Stessa domanda per $p = 101$. (Sugg. calcolare l'invariante $j$ del reticolo $\mathbf{Z} + \frac{1+\sqrt{-11}}{2}\mathbf{Z}$).