1. *Sia p un numero primo.*
   (a) Dimostrare che $\bar{x} \in \mathbb{Z}_p^*$ è un quadrato, ossia x è un quadrato modulo p, se e solo se $\bar{x}^{\frac{p-1}{2}} \equiv \bar{1} \bmod p$ (sfruttare il fatto che $\mathbb{Z}_p^*$ è ciclico).
   (b) Sia $\bar{x} \in \mathbb{Z}_p^*$ un quadrato. Quante radici quadrate ha in $\mathbb{Z}_p^*$?

Sol. (a) Sia $\bar{a}$ una radice primitiva di $\mathbb{Z}_p^*$. Scriviamo $\bar{x} = \bar{a}^m$. Se $\bar{x}$ è un quadrato, allora m è pari, ossia $m = 2k$, con $k \in \mathbb{Z}$. Ne segue che $\bar{x}^{\frac{p-1}{2}} \equiv \bar{a}^{k(p-1)} \equiv \bar{1} \bmod p$, per il Piccolo Teorema di Fermat.
Viceversa, supponiamo che $\bar{x}^{\frac{p-1}{2}} \equiv \bar{a}^{m\frac{(p-1)}{2}} \equiv \bar{1} \bmod p$. Vogliamo dimostrare che m è pari. Infatti se m fosse dispari $m = 2h + 1$, con $h \in \mathbb{Z}$, avremmo

$$\bar{a}^{m\frac{(p-1)}{2}} \equiv \bar{a}^{(2h+1)\frac{(p-1)}{2}} \equiv \bar{a}^{h(p-1)} \cdot \bar{a}^{\frac{(p-1)}{2}} \equiv \bar{1} \cdot \bar{a}^{\frac{(p-1)}{2}} \equiv \bar{1} \quad \bmod p.$$

Poiché $\frac{(p-1)}{2}$ è un intero minore di $p-1$, questo contraddice il fatto che $\bar{a}$ è una radice primitiva, di ordine $p-1$. In conclusione $\bar{x}^{\frac{p-1}{2}} \equiv \bar{1} \bmod p$ se e solo se $\bar{x} = \bar{a}^m$, con m pari, ossia $\bar{x}$ è un quadrato modulo p.
(b) Un quadrato $\bar{x} \in \mathbb{Z}_p^*$ ha esattamente due radici quadrate: $\pm\bar{a} \in \mathbb{Z}_p^*$ tali che $\bar{a}^2 = (-\bar{a})^2 = \bar{x}$. Se invece $\bar{x} = \bar{0} \in \mathbb{Z}_p$, allora $\bar{x}$ ha un'unica radice quadrata: $\bar{0}$.

2. *Sia $p = 13$.*
   (a) Determinare tutti i quadrati in $\mathbb{Z}_{13}^*$.
   (b) Per ogni quadrato $\bar{a} \in \mathbb{Z}_{13}^*$, determinare le radici quadrate di $\bar{a}$ in $\mathbb{Z}_{13}^*$.
   (c) Per ogni $a \in \mathbb{Z}$ che è un quadrato modulo 13, determinare tutte le soluzioni $x \in \mathbb{Z}$ della congruenza $x^2 \equiv a \bmod p$.

Sol. (a) Poiché modulo 13

$$\bar{1}^2 = \bar{1},\ \bar{2}^2 = \bar{4},\ \bar{3}^2 = \bar{9},\ \bar{4}^2 = \bar{3},\ \bar{5}^2 = \overline{12},\ \bar{6}^2 = \overline{10},\ \bar{7}^2 = \overline{10},\ \bar{8}^2 = \overline{12},\ \bar{9}^2 = \bar{3},\ \overline{10}^2 = \bar{9},\ \overline{11}^2 = \bar{4},\ \overline{12}^2 = \bar{1},$$

i quadrati in $\mathbb{Z}_{13}^*$ sono $Q = \{\bar{1},\ \bar{4},\ \bar{3},\ \bar{9},\ \overline{10},\ \overline{12}\}$.
(b) Le rispettive radici quadrate sono date da

$$\sqrt{\bar{1}} = \bar{1}, \overline{-1} = \overline{12}, \quad \sqrt{\bar{4}} = \bar{2}, \overline{-2} = \overline{11}, \quad \sqrt{\bar{3}} = \bar{4}, \overline{-4} = \bar{9}, \quad \sqrt{\bar{9}} = \bar{3}, \overline{-3} = \overline{10},$$

$$\sqrt{\overline{10}} = \bar{6}, \overline{-6} = \bar{7}, \quad \sqrt{\overline{12}} = \bar{5}, \overline{-5} = \bar{8}.$$

(c) Sia ad esempio $\bar{a} = \bar{3}$, che ha radici quadrate $\sqrt{\bar{3}} = \bar{4}, \overline{-4} = \bar{9}$ in $\mathbb{Z}_{13}^*$. Le soluzioni intere della congruenza $x^2 \equiv 3 \bmod 13$ sono costituite dalle due famiglie di interi

$$x = 4 + 13k, \quad k \in \mathbb{Z}, \qquad\qquad x = 9 + 13h, \quad h \in \mathbb{Z}.$$

3. *Sia p un numero primo che soddisfa $p \equiv 5 \bmod 8$ e sia a un quadrato modulo p.*
   (a) Dimostrare che ci sono due possibilità: $a^{\frac{p-1}{4}} \equiv 1 \bmod p$ oppure $a^{\frac{p-1}{4}} \equiv -1 \bmod p$.
   (b) Verificare che se $a^{\frac{p-1}{4}} \equiv 1 \bmod p$, allora $a^{\frac{p+3}{8}}$ è una radice quadrata di a modulo p.
   (c) Verificare che se $a^{\frac{p-1}{4}} \equiv -1 \bmod p$, allora $2a \cdot (4a)^{\frac{p-5}{8}}$ è una radice quadrata di a modulo p (usare il seguente risultato: 2 è un quadrato modulo p se e solo se $p \equiv \pm 1 \bmod 8$).

Sol. Se p è un numero primo, $\mathbb{Z}_p^*$ è ciclico. Sia $g \in \mathbb{Z}_p^*$ una radice primitiva. Allora $a \in \mathbb{Z}_p^*$ è un quadrato modulo p se e solo se $a = g^m$, con esponente pari $m = 2\alpha$, con $\alpha \in \mathbb{Z}$.
(a) Sia $a = g^{2\alpha}$ un quadrato modulo p, con $\alpha \in \mathbb{Z}$. Per il Piccolo Teorema di Fermat, abbiamo che

$$a^{(p-1)/2} = (a^{(p-1)/4})^2 \equiv (g^{2\alpha})^{(p-1)/2} \equiv g^{\alpha(p-1)} \equiv 1 \bmod p.$$

In altre parole $a^{(p-1)/4}$ è una radice del polinomio $Z^2-1 \in \mathbb{Z}_p[Z]$. Ne segue che $a^{(p-1)/4} \equiv 1, -1 \bmod p$.
(b) Assumiamo $a^{(p-1)/4} \equiv 1 \bmod p$. Verifichiamo che $(a^{(p+3)/8})^2 \equiv a \bmod p$:
$$(a^{(p+3)/8})^2 = a^{(p+3)/8} \cdot a^{(p+3)/8} = a^{(p+3)/4};$$
$$a^{(p+3)/4} \equiv a \bmod p \quad \Leftrightarrow \quad a^{-1}a^{(p+3)/4} \equiv 1 \bmod p \quad \Leftrightarrow \quad a^{-1+(p+3)/4} \equiv a^{(p+3-4)/4} \equiv a^{(p-1)/4} \equiv 1 \bmod p.$$
(c) Assumiamo $a^{(p-1)/4} \equiv -1 \bmod p$. Verifichiamo che $\left(2a \cdot (4a)^{\frac{p-5}{8}}\right)^2 \equiv a \bmod p$:
$$\left(2a \cdot (4a)^{\frac{p-5}{8}}\right)^2 \equiv 4a^2(4a)^{\frac{p-5}{4}} \equiv a(4a)^{1+\frac{p-5}{4}} \equiv a(4a)^{(p-1)/4} \equiv a4^{(p-1)/4}a^{(p-1)/4} \equiv -a2^{(p-1)/2}.$$
Per ottenere l'ultima congruenza abbiamo usato l'ipotesi $a^{(p-1)/4} \equiv -1 \bmod p$ e abbiamo scritto $4^{(p-1)/4} = 2^{(p-1)/2}$. Consideriamo adesso l'elemento $2^{(p-1)/2}$. Poiché per il Piccolo Teorema di Fermat, $(2^{(p-1)/2})^2 \equiv 1 \bmod p$, ne segue che $2^{(p-1)/2} \equiv 1, -1$ (deve coincidere con una delle due radici di 1 modulo p). Ricordiamo che per $x \in \mathbb{Z}_p^*$ vale $x^{(p-1)/2} \equiv 1 \bmod p$ se e solo se x è un quadrato modulo p. D'altra parte, poiché 2 non è un quadrato modulo p (dal risultato: *2 è un quadrato modulo p se e solo se $p \equiv \pm 1 \bmod 8$*), necessariamente $2^{(p-1)/2} \equiv -1$. A questo punto abbiamo
$$\left(2a \cdot (4a)^{\frac{p-5}{8}}\right)^2 \equiv -a2^{(p-1)/2} \equiv a,$$
come richiesto.

4. *Sia n un intero e sia p un primo.*
   (a) Verificare che un intero della forma x^2-n è divisibile per p se e solo se n è un quadrato modulo p.
   (a) Sia n un quadrato modulo p e siano $\bar{a}$ e $\bar{b}$ le due radici quadrate di $\bar{n}$ in $\mathbb{Z}_p^*$. Determinare tutti gli interi della forma x^2-n che sono divisibili per p.

Sol. (a) $x^2-n \equiv 0 \bmod p$ se e solo se $x^2 \equiv n \bmod p$, ossia n è un quadrato modulo p.
(b) Gli interi che sono soluzioni della congruenza $x^2-n \equiv 0 \bmod p$ sono tutti e soli quelli della forma
$$x = a + kp, \quad k \in \mathbb{Z}, \qquad\qquad x = b + hp, \quad h \in \mathbb{Z}.$$
Verifichiamo che ad esempio gli interi $x = a + kp$, $k \in \mathbb{Z}$, soddisfano la congruenza:
$$x^2 = (a+kp)^2 = a^2 + k^2p^2 + 2kp \equiv a^2 \equiv n \bmod p.$$

5. *Usare la congruenza* $294^2 \equiv 10^2 \bmod 1349$ *per determinare una fattorizzazione non banale di 1349.*

Sol. Siano $a \equiv 294 \bmod 1349$, $b \equiv 10 \bmod 1349$, $a+b \equiv 304 \bmod 1349$ e $a-b \equiv 284 \bmod 1349$.
$$\gcd(a+b,n) = \gcd(304,1349) = 19, \qquad \gcd(a-b,n) = \gcd(284,1349) = 71, \qquad 1349 = 19 * 71.$$

6. *Sia n intero dispari (dunque $n \equiv 1,3,5,7 \bmod 8$) e sia $x = 2k+1$, $k \in \mathbb{Z}$, un numero dispari. Si hanno le seguenti possibilità:*
$$\begin{cases} n \equiv 3,7 \bmod 8 \Rightarrow \ x^2-n \text{ è divisibile per 2 e per nessun'altra potenza di 2;} \\ n \equiv 5 \quad \bmod 8 \Rightarrow \ x^2-n \text{ è divisibile per 4 e per nessun'altra potenza di 2;} \\ n \equiv 1 \quad \bmod 8 \Rightarrow \ x^2-n \text{ è divisibile per 8 e possibilmente per altre potenze } 2^k, \text{ per } k \geq 4. \end{cases}$$

Sol. - Assumiamo $n \equiv 3 \bmod 8$, ossia $n-1 = 2+8M$, $M \in \mathbb{Z}$. Calcolando x^2-n troviamo:
$x^2-n = (2k+1)^2-n = 4k^2+4k+1-n = 4k(k+1)-(n-1) = 4k(k+1)-2-8M = -2+8R, \quad R \in \mathbb{Z}$,
dove abbiamo usato il fatto che $k(k+1)$ è necessariamente divisibile per 2. Ora è evidente che $(2k+1)^2-n$ è divisibile per 2, ma non per potenze 2^a, con $a > 1$.
Il caso $n \equiv 7 \bmod 8$ si tratta in modo analogo.
- Assumiamo $n \equiv 5 \bmod 8$, ossia $n-1 = 4+8M$, $M \in \mathbb{Z}$. Calcolando x^2-n troviamo:
$x^2-n = (2k+1)^2-n = 4k^2+4k+1-n = 4k(k+1)-(n-1) = 4k(k+1)-4-8M = -4+8R, \quad R \in \mathbb{Z}$.
Ora è evidente che $(2k+1)^2-n$ è divisibile per 4, ma non per potenze 2^a, con $a > 2$.
- Assumiamo $n \equiv 1 \bmod 8$, ossia $n-1 = 8M$, $M \in \mathbb{Z}$. Calcolando x^2-n troviamo:
$$x^2-n = (2k+1)^2-n = 4k^2+4k+1-n = 4k(k+1)-(n-1) = 4k(k+1)-8M = 8R, \quad R \in \mathbb{Z}.$$
Ora è evidente che $(2k+1)^2-n$ è divisibile per 8, e possibilmente anche per altre potenze 2^a, con $a \geq 4$.