1. Il numero 2011 è primo. Quante radice primitive ci sono in $\mathbf{Z}_{2011}^*$?

2. Sia p un primo e sia $\overline{g}$ un generatore di $\mathbf{Z}_p^*$.
   (a) Dimostrare che $\overline{a}$ è un generatore di $\mathbf{Z}_p^*$ se e solo se $\overline{a} = \overline{g}^i$ per un esponente $i \in \mathbf{Z}$ che soddisfa $\mathrm{mcd}(i, p-1) = 1$.
   (b) Dimostrare che $\overline{a}$ è un quadrato in $\mathbf{Z}_p^*$ se e solo se $\overline{a} = \overline{g}^i$ per un $i \in \mathbf{Z}$ pari.
   (c) Dimostare che $\overline{a}$ è un quadrato in $\mathbf{Z}_p^*$ se e solo se $\overline{a}^{(p-1)/2} = \overline{1}$.

3. (a) Determinare una radice primitiva $\overline{g}$ in $\mathbf{Z}_{13}^*$.
   (b) Sia g la radice primitiva modulo 13 calcolata nella parte (a). Calcolare $m \in \mathbf{Z}$ tale che $\overline{2} = \overline{g}^m$ in $\mathbf{Z}_{13}^*$.
   (c) Stesse domande per il primo 41 invece di 13.

4. Sia p un numero primo e sia e g una radice primitiva modulo p. Calcolare il logaritmo discreto di $-1 \in \mathbf{Z}_p^*$. In altre parole, determinare $i \in \mathbf{Z}$ tale che $\overline{g}^i = -\overline{1}$ in $\mathbf{Z}_p^*$.

5. Siano p, q due primi dispari distinti. Dimostrare che esiste $g \in \mathbf{Z}$ tale che g è radice primitiva sia modulo p che modulo q. Dimostrare che un tale elemento g *non* genera $\mathbf{Z}_{pq}^*$.

6. Sia $p > 5$ un primo. Dimostrare che il periodo della frazione decimale di $1/p$ è uguale a $p-1$ se e solo se $\overline{10} \in \mathbf{Z}_p^*$ è una radice primitiva.

7. Sia $p > 2$ un primo. Dimostrare che il periodo della frazione *esadecimale* (cioè in base 16) di $1/p$ non ha mai lunghezza $p-1$.

8. Determinare gli zeri del polinomio $X^3 - 1$ negli anelli $\mathbf{Z}_7$, in $\mathbf{Z}_9$ e in $\mathbf{Z}_{63}$. (Sugg: per $\mathbf{Z}_{63}$ usare il teorema cinese del resto).

9. (a) Sia $p > 2$ un primo e sia $k \geq 1$. Dimostrare che il polinomio $X^2 - 1$ ha esattamente due zeri in $\mathbf{Z}_{p^k}$.
   (b) Sia n un numero dispari. Il polinomio $X^2 - 1$, quanti zeri ha in $\mathbf{Z}_n$?

10. Sia R un anello commutativo. Un sottoinsieme $S \subset R$ si dice *moltiplicativo* se $1 \in S$ e se per ogni $x, y \in S$ anche $xy \in S$.
    (a) Dimostrare che se R è un dominio, allora $R - \{0\}$ è un sottoinsieme moltiplicativo.
    (b) Sia $a \in R$, allora $\{a^k : k \in \mathbf{Z}_{\geq 0}\}$ è un sottoinsieme moltiplicativo.
    (c) Sia p un numero primo. Dimostrare che $S = \{n \in \mathbf{Z} : n \not\equiv 0 \pmod{p}\}$ è un sottoinsieme moltiplicativo di $\mathbf{Z}$.

11. (Localizzazione.) Sia R un anello commutativo e sia $S \subset R$ un sottoinsieme moltiplicativo. Definiamo sull'insieme $R \times S$ la seguente relazione: si ha che $(r, s) \sim (r', s')$ se e solo se esiste un elemento $t \in S$ con $(rs' - r's)t = 0$.
    (a) Dimostrare che si tratta di una relazione di equivalenza. Scriviamo $S^{-1}R$ per l'insieme delle classi di equivalenza e $\frac{r}{s}$ per la classe di una coppia $(r, s) \in R \times S$.
    (b) Definire un'addizione e moltiplicazione su $S^{-1}R$ usando le solite formule per addizionare e moltiplicare le frazioni. Dimostrare che $S^{-1}R$ diventa un anello commutativo.
    (c) Dimostrare che la mappa $R \longrightarrow S^{-1}R$ data da $r \mapsto \frac{r}{1}$ diventa un omomorfismo di anelli. Dimostrare che se $r \in S$, allora $\frac{r}{1}$ è invertibile in $S^{-1}R$.
    (d) Dimostrare che $S^{-1}R$ è l'anello zero se e solo se $0 \in S$.
    (e) Esibire un anello R e un sottoinsieme moltiplicativo $S \subset R$ che non contiene 0, tale che la mappa $R \longrightarrow S^{-1}R$ *non* è iniettiva.