1. In questo esercizio i calcoli vanno fatti nell'anello $\mathbf{Z}[X]$.
   (a) Determinare il resto della divisione di $f = 2X^3 - 3X + 2$ per $g = X^2 - 2X + 5$.
   (b) Dimostrare che non è possibile dividere $f = 2X^3 - 3X + 2$ per $h = 3X + 1$ con resto zero o di grado $< \deg(h)$.

2. Sia R un anello commutativo e sia $a \in R$. Dimostrare che l'applicazione $R[X] \longrightarrow R$ che manda un polinomio $f(X)$ in $f(a)$, è un omomorfismo di anelli.

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

4. (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 $\overline{10} = \overline{g}^m$ in $\mathbf{Z}^*_{13}$.
   (c) Stesse domande per il primo 41 invece di 13.

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.
   (a) 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.
   (b) Dimostrare che il periodo della frazione *esadecimale* (cioè in base 16) di $1/p$ non ha mai lunghezza $p - 1$.

7. 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).

8. (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 con esattamente t fattori primi distinti. Il polinomio $X^2 - 1$, quanti zeri ha in $\mathbf{Z}_n$?

9. Sia $n = 72263$. Verificare che 43814 è uno zero del polinomio $X^2 - 1$ in $\mathbf{Z}_n$. Dedurne che n non è primo. Sfruttare lo zero dato per fattorizzare n.

10. Sia R un anello commutativo. Un elemento $a \in R$ si dice *divisore di zero* se $a \neq 0$ e se esiste $b \in R$ diverso da zero con $ab = 0$.
    (a) dimostrare che un campo non possiede divisori di zero.
    (b) Determinare i divisori di zero di $\mathbf{Z}_{12}$.
    (c) Se R è finito, dimostrare che ogni $x \in R$ o è 0, o è un divisore di zero oppure è invertibile.

11. Siano R_1 ed R_2 due anelli commutativi.
    (a) Siano $I_1 \subset R_1$ e $I_2 \subset R_2$ ideali. Dimostrare che $I_1 \times I_2$ è un ideale di $R_1 \times R_2$.
    (b) Dimostrare che ogni ideale $I \subset R_1 \times R_2$ ha la forma $I = I_1 \times I_2$ dove $I_1 \subset R_1$ e $I_2 \subset R_2$ sono ideali.

12. Sia R un anello e siano $I, J \subset R$ due ideali di R. Dimostrare che $I \cup J$ è un ideale se e soltanto se $I \subset J$ oppure $J \subset I$.

13. Dimostrare che per nessun anello (commutativo con 1) il gruppo addittivo è isomorfo a $\mathbf{Q}/\mathbf{Z}$.