

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 $R[X] \rightarrow R$ che manda un polinomio $f(X)$ in $f(a)$, è un omomorfismo di anelli.
3. Sia $\mathbf{H}$ il corpo dei quaternioni.
 - (a) Siano $x, y \in \mathbf{H}$ dati da $x = 1 + i + j - k$ e $y = -2 - j + k$. Calcolare $x + y$, $x\bar{y}$, $1/x$ e $\bar{y}^2$.
 - (b) Dimostrare che $x \in \mathbf{H}$ ha la proprietà che $xy = yx$ per ogni $y \in \mathbf{H}$ se e solo se $x \in \mathbf{R}$.
4. Un quaternione "puro" è un quaternione della forma $bi + cj + dk$ con $b, c, d \in \mathbf{R}$.
 - (a) Dimostrare x è un quaternione puro se e solo se $\bar{x} = -x$.
 - (b) Dimostrare che i quaternioni puri formano un $\mathbf{R}$ -spazio vettoriale $\mathbf{H}_0$ di dimensione 3.
 - (c) Dimostrare che ogni quaternione puro x di norma $x\bar{x} = 1$ soddisfa $x^2 = -1$.
 - (d) Dimostrare che gli zeri del polinomio $X^2 + 1$ in $\mathbf{H}$ formano una sfera in $\mathbf{H}_0$. In particolare, sono infiniti.
5. Sia Q_4 il gruppo $\{\pm 1, \pm i, \pm j, \pm k\}$ dei quaternioni.
 - (a) Determinare il centro di Q_4 .
 - (b) Dimostrare che ogni sottogruppo di Q_4 è normale.
 - (c) Dimostrare che il gruppo quoziente $Q_4/\{\pm 1\}$ è isomorfo al gruppo di Klein.
6. Il numero 2011 è primo. Quante radici primitive ci sono in $\mathbf{Z}_{2011}^*$?
7. Sia G un gruppo ciclico finito di cardinalità n e sia $g \in G$ un generatore.
 - (a) Dimostrare che x è un generatore di G se e solo se $x = g^i$ per un esponente $i \in \mathbf{Z}$ che soddisfa $\text{mcd}(i, n) = 1$.
 - (b) Dimostrare che x è un quadrato in G se e solo se $x = g^i$ per un $i \in \mathbf{Z}$ pari.
8. (a) Determinare una radice primitiva $\bar{g}$ in $\mathbf{Z}_{13}^*$.
 (b) Sia g la radice primitiva modulo 13 calcolata nella parte (a). Calcolare $m \in \mathbf{Z}$ tale che $\bar{10} = \bar{g}^m$ in $\mathbf{Z}_{13}^*$.
 (c) Stesse domande per il primo 41 invece di 13.
9. 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 $\mathbf{Z}_{pq}^*$.
10. 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 $\bar{10} \in \mathbf{Z}_p^*$ è una radice primitiva.
 - (b) Dimostrare che il periodo della frazione *esadecimale* (cioè in base 16) di $1/p$ non ha mai lunghezza $p - 1$.
11. 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).
12. (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 $\mathbf{Z}_n$?
13. Sia $n = 72263$. Verificare che 43814 è uno zero del polinomio $X^2 - 1$ in $\mathbf{Z}_n$. Dedurre che n non è primo. Sfruttare lo zero dato per fattorizzare n .