1. Scrivere ogni intero $n = 22, 23, ..., 33$ come somma di quattro quadrati di numeri interi. Se possibile scrivere n come somma di tre quadrati. Se possibile scrivere n come somma di due quadrati.

2. Sia m un intero congruo a 7 (mod 8). Dimostrare che m non è una somma di tre quadrati di numeri interi. Dimostrare che $4^k m$ non è somma di tre quadrati di numeri interi per alcun $k \in \mathbf{Z}_{\geq 0}$.

3. Scrivere $x = \frac{1+3i-j+5k}{2}$ come prodotto di un elemento del tipo $\frac{\pm 1 \pm i \pm j \pm k}{2}$ per un quaternione $a + bi + cj + dk$, con $a, b, c, d \in \mathbf{Z}$.

4. Sia $n \geq 1$. Un elemento $x \in \mathbf{Z}_n^*$ si dice *quadrato* se esiste $y \in \mathbf{Z}_n^*$ tale che $x = y^2$. Enumerare i quadrati e i non quadrati di $\mathbf{Z}_{13}^*$ e di $\mathbf{Z}_{15}^*$.

5. Sia p un primo e sia $k > 0$ un divisore di $p - 1$. Un elemento $x \in \mathbf{Z}_p^*$ si dice k-esima potenza se esiste $y \in \mathbf{Z}_p^*$ tale che $x = y^k$.
   (a) Dimostrare che $x \in \mathbf{Z}_p^*$ è k-esima potenza se e solo se $x^{(p-1)/k} = 1$ in $\mathbf{Z}_p^*$.
   (b) Dimostrare che $\{x^k : x \in \mathbf{Z}_p^*\}$ è un sottogruppo di $\mathbf{Z}_p^*$ di cardinalità $(p-1)/k$.
   (c) Generalizzare le affermazioni delle parti (a) e (b) al caso: k non divide $p - 1$.

6. Sia k un campo. Un polinomio $f \in k[X]$ si dice irriducibile, se non è costante e se non è prodotto di due polinomi non costanti.
   (a) Supponiamo che f abbia grado ≤ 3. Dimostrare che f è irriducibile se e solo se non ha zeri in k.
   (b) Esibire un polinomio riducibile di grado 4 in $\mathbf{R}[X]$ senza zeri reali.

7. Sia $p > 2$ un primo. Sia R l'anello $\mathbf{Z}_p[X]/(X^2 + 1)$.
   (a) Determinare $\#R^*$ (la risposta dipende dalla classe di p (mod 4)).
   (b) Dimostrare che l'applicazione $\phi : R^* \to \mathbf{Z}_p^*$ data da $a + bX \mapsto a^2 + b^2$ è un omomorfsimo di gruppi.
   (c) Dimostrare che ϕ è suriettiva.
   (d) Dato $t \in \mathbf{Z}_p^*$, quante copie $(a, b) \in \mathbf{Z}_p \times \mathbf{Z}_p$ con $a^2 + b^2 = t$ ci sono?

8. Sia R un anello non necessariamente commutativo e supponiamo che l'applicazione $f : R \longrightarrow R$ data da $f(x) = x^2$ sia un omomorfismo di anelli.
   (a) Dimostrare che R è un anello commutativo.
   (b) Dimostrare che per ogni $x \in R$ si ha $x + x = 0$.
   (c) Dimostrare che se $x \in \ker(f)$, allora $1 + x \in R^*$.

9. Sia $n > 1$ un intero senza fattori quadrati.
   (a) Dimostrare che ogni gruppo abeliano di cardinalità n è ciclico. (Sugg: sia $x \in G$ diverso dall'elemento neutro. Se x non ha ordine n, allora considerare il sottogruppo $H = \langle x \rangle$ e il quoziente G/H e procedere per induzione)
   (b) Dimostrare che ogni anello (commutativo con 1) di cardinalità n è isomorfo all'anello $\mathbf{Z}_n$.