

1. Scrivere ogni intero  $n = 22, 23, \dots, 33$  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  $7 \pmod{8}$ . 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 quaternionione  $a + bi + cj + dk$ , 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) Dimostrare che ogni polinomio di grado 1 è irriducibile.
  - (b) Dimostrare che  $X^2 + 1 \in \mathbf{R}[X]$  è irriducibile.
  - (c) Dimostrare che se  $f$  è irriducibile, allora l'anello quoziente  $k[X]/(f)$  è un campo.
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  $p \pmod{4}$ ).
  - (b) Dimostrare che l'applicazione  $\phi : R^* \rightarrow \mathbf{Z}_p^*$  data da  $a + bX \mapsto a^2 + b^2$  è un omomorfismo di gruppi.
  - (c) Dimostrare che  $\phi$  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  $n$  un intero senza fattori quadrati.
  - (a) Dimostrare che ogni gruppo abeliano di cardinalità  $n$  è ciclico.
  - (b) Dimostrare che ogni anello di cardinalità  $n$  è isomorfo all'anello  $\mathbf{Z}_n$ .
9. Una successione  $(a_1, a_2, a_3, \dots)$  con  $a_i \in \mathbf{Q}$  si dice *di Cauchy* se per ogni  $\epsilon \in \mathbf{Q}_{>0}$  esiste  $n_0$  tale che  $|a_n - a_m| < \epsilon$  per  $n, m > n_0$ . Sia  $R$  l'insieme delle successioni di Cauchy e definiamo la somma ed il prodotto di due successioni  $(a_1, a_2, \dots)$  e  $(b_1, b_2, \dots)$  in  $R$  coordinata per coordinata. Una successione  $(a_1, a_2, a_3, \dots)$  si dice una *successione nulla* se converge a zero. In altre parole, se per ogni  $\epsilon \in \mathbf{Q}_{>0}$  esiste  $n_0$  tale che  $|a_n| < \epsilon$  per  $n > n_0$ .
  - (a) Dimostrare che  $R$  è un anello commutativo.
  - (b) Dimostrare che le successioni nulle formano un ideale  $I$  di  $R$ .
  - (c) Dimostrare che l'anello quoziente  $R/I$  è un campo.
  - (d) Esibire un isomorfismo  $R/I \cong \mathbf{R}$ .