

1. Nell'anello degli interi di Gauss $\mathbf{Z}[i]$, determinare il resto della divisione di $5 + 14i$ per $3 + 5i$. (Sarebbe meglio dire: "un" resto ...). Determinare $\text{mcd}(5 + 14i, 3 + 5i)$.
2. Dimostrare che gli ideali $(5, X - 2)$, $(5, 2X + 1)$ e $(X - 2, X^2 + 1)$ di $\mathbf{Z}[X]$ sono tutti uguali. Quanti elementi ha l'anello quoziente?
3. Sia A l'anello $\mathbf{Z}[X]/(X^2 + 2)$.
 - (a) Dimostrare che l'applicazione $\phi : A \longrightarrow \mathbf{C}$ data da $\phi(\bar{g}) = g(\sqrt{-2})$, per $g \in \mathbf{Z}[X]$, è un omomorfismo di anelli ben definito.
 - (b) Dimostrare che A è isomorfo al sottoanello $\mathbf{Z}[\sqrt{-2}] = \{a + b\sqrt{-2} : a, b \in \mathbf{Z}\}$ di $\mathbf{C}$.
 - (c) Dimostrare che per ogni $x \in \mathbf{C}$ esiste $y \in \mathbf{Z}[\sqrt{-2}]$ tale che $|x - y|^2 \leq \frac{3}{4}$.
 - (d) Dimostrare che l'anello $\mathbf{Z}[\sqrt{-2}]$ è un dominio Euclideo rispetto alla funzione $N(a + b\sqrt{-2}) = a^2 + 2b^2$.
 - (e)* Indovinare chi sono i primi p della forma $a^2 + 2b^2$, con $a, b \in \mathbf{Z}$.
4. Sia B l'anello $\mathbf{Z}[X]/(X^2 - 2)$.
 - (a) Dimostrare che l'applicazione $\phi : B \longrightarrow \mathbf{R}$ data da $\phi(\bar{g}) = g(\sqrt{2})$ per $g \in \mathbf{Z}[X]$, è un omomorfismo di anelli ben definito.
 - (b) Dimostrare che B è isomorfo al sottoanello $\mathbf{Z}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Z}\}$ di $\mathbf{R}$.
 - (c) Dimostrare che il sottocampo $\mathbf{Q}[\sqrt{2}] = \{a + b\sqrt{2} : a, b \in \mathbf{Q}\}$ di $\mathbf{R}$ è il campo delle frazioni di $\mathbf{Z}[\sqrt{2}]$.
Sia $N : \mathbf{Q}[\sqrt{2}] \longrightarrow \mathbf{N}$ l'applicazione data da $N(a + b\sqrt{2}) = |(a + b\sqrt{2})(a - b\sqrt{2})| = |a^2 - 2b^2|$.
 - (d) Dimostrare che per ogni $x \in \mathbf{Q}[\sqrt{2}]$ esiste $y \in \mathbf{Z}[\sqrt{2}]$ tale che $|N(x - y)| \leq \frac{1}{2}$.
 - (e) Dimostrare che l'anello $\mathbf{Z}[\sqrt{2}]$ è un dominio Euclideo rispetto alla funzione N .
5. Scrivere ogni intero $n = 22, 23, \dots, 30$ 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.
6. Sia $p = 71$ e sia z il quaternione $1 + 14i + 4j$. Fattorizzare $N(p)$ e $N(z)$. Esibire un quaternione intero y più vicino possibile al quaternione pz^{-1} . Calcolare la norma $N(p - yz)$.
7. Sia I l'ideale di $\mathbf{Z}[X]$ generato da 3 e X . Sia J l'ideale I^2 (cioè $J = I \cdot I$). Quanti elementi ha l'anello R/J ? Stessa domanda per l'ideale $I = (3, X^2)$.
8. 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 ϕ è suriettivo.
 - (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? (Sugg: la risposta dipende solo da p e non da t).