Algebra I. 11. Anelli quozienti, CRT, PID, domini euclidei. Roma, 11 dicembre 2019.

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 $\mathrm{mcd}(5+14i, 3+5i)$.

2. Sia $p > 2$ un primo.
   (a) Dimostrare che l'anello $\mathbf{Z}_p[X]/(X^2-1)$ è isomorfo a $\mathbf{Z}_p \times \mathbf{Z}_p$.
   (b) Dimostrare che l'affermazione della parte (a) è falsa per $p = 2$.

3. (a) Dimostrare che la mappa $\Psi : \mathbf{Z}[X] \longrightarrow \mathbf{Z}_2$ data da $\Psi(f) = f(0) \pmod 2$ è un omomorfismo suriettivo di anelli.
   (b) Dimostrare che $\ker(\Psi)$ è l'ideale $(2, X)$ (l'ideale generato da 2 e da X).
   (c) Dimostrare che l'anello $\mathbf{Z}[X]/(2, X)$ è isomorfo a $\mathbf{Z}_2$.

4. Dimostrare che ognuno degli anelli quozienti $\mathbf{Z}[X]/(5, X-2)$, $\mathbf{Z}[X]/(5, 2X-2)$ e $\mathbf{Z}[X]/(X-2, X^2+1)$ è un campo di 5 elementi.

5. 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 in $k[X]$.
   (a) Dimostrare che ogni polinomio di grado 1 è irriducibile.
   (b) Sia $f \in k[X]$ irriducibile e sia $g \in k[X]$. Dimostrare che se f non divide g, allora $\mathrm{mcd}(f, g) = 1$, cioé l'ideale generato da f e g è uguale a $k[X]$.
   (c) Dimostrare che se f è irriducibile, allora l'anello quoziente $k[X]/(f)$ è un campo.

6. Sia $p > 2$ un primo. Sia R l'anello $\mathbf{Z}_p[X]/(X^2+1)$. Determinare $\#R^*$ (la risposta dipende dalla classe di $p \pmod 4$).

7. Sia A l'anello $\mathbf{Z}[X]/(X^2+2)$.
   (a) Dimostrare che l'applicazione $\phi : A \longrightarrow \mathbf{C}$ data da $\phi(\overline{g}) = g(\sqrt{-2})$ 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 per qualche $a, b \in \mathbf{Z}$.

8. Sia B l'anello $\mathbf{Z}[X]/(X^2-2)$.
   (a) Dimostrare che l'applicazione $\phi : B \longrightarrow \mathbf{R}$ data da $\phi(\overline{g}) = g(\sqrt{2})$ 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.