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

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

4. Sia R l'anello $\mathbf{Z}[X]/(X^2+2)$.
   (a) Dimostrare che l'applicazione $\phi : R \longrightarrow \mathbf{C}$ data da $\phi(\overline{g}) = g(\sqrt{-2})$ per $g \in \mathbf{Z}[X]$, è un omomorfismo di anelli ben definito.
   (b) Dimostrare che R 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 $|x-y|^2 \le \frac{3}{4}$.
   (d) Dimostrare che l'anello $R = \mathbf{Z}[\sqrt{-2}]$ è un dominio Euclideo rispetto alla funzione $N(a+b\sqrt{-2}) = a^2+2b^2$.

5. Siano R e K i sottoanelli del campo $\mathbf{R}$ dei numeri reali, dati rispettivamente da $R = \mathbf{Z}[\sqrt{2}] = \{a+b\sqrt{2} : a,b \in \mathbf{Z}\}$ e $K = \{a+b\sqrt{2} : a,b \in \mathbf{Q}\}$. Sia $N : K \longrightarrow \mathbf{Q}$ l'applicazione data da $N(a+b\sqrt{2}) = |(a+b\sqrt{2})(a-b\sqrt{2})| = |a^2-2b^2|$.
   (a) Dimostrare che se $a+b\sqrt{2} = a'+b'\sqrt{2}$ per certi $a,b,a',b' \in \mathbf{Q}$, allora $a=a'$ e $b=b'$.
   (b) Dimostrare che K è isomorfo al campo quoziente di R.
   (c) Dimostrare che $N(xy) = N(x)N(y)$ per ogni $x,y \in K$.
   (d) Dimostrare che per ogni $x \in K$ esiste $y \in R$ tale che $N(x-y) \le \frac{1}{2}$.
   (e) Dimostrare che $R = \mathbf{Z}[\sqrt{2}]$ è un dominio Euclideo rispetto alla funzione N.

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 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 $\operatorname{mcd}(f,g)=1$, 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.

7. 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.

8. Sia $\zeta = \frac{-1+\sqrt{-3}}{2} \in \mathbf{C}$. Allora si ha che $\zeta^2+\zeta+1=0$. Sia R l'anello dato da $\mathbf{Z}[\zeta] = \{a+b\zeta : a,b \in \mathbf{Z}\}$.
   (a) Dimostrare che R è un anello Euclideo rispetto alla funzione $N : (R-\{0\}) \longrightarrow \mathbf{Z}_{\ge 1}$ data da $N(x) = x\overline{x}$.
   (b) Sia p un numero primo diverso da 3. Dimostrare che $p = x^2+xy+y^2$ per certi $x,y \in \mathbf{Z}$ se e solo se $p \equiv 1 \pmod 3$.