0. Sia G un gruppo e sia $x \in G$ un elemento di ordine n. Dimostrare che per ogni $a \in \mathbf{Z}$ l'ordine dell'elemento x^a è uguale a $n/\mathrm{mcd}(a, n)$.

1. (a) Determinare radici primitive per i numeri primi 11, 23, 29 e 41.
   (b) Quanti radici primitive ci sono in $\mathbf{Z}_p^*$ per un numero primo dato p?

2. Un anello commutativo R si dice *Noetheriano* se ogni successione di ideali di R

$$I_1 \underset{\neq}{\subset} I_2 \underset{\neq}{\subset} I_3 \underset{\neq}{\subset} I_4 \underset{\neq}{\subset} \dots$$

   si stabilizza. Dimostrare che R è Noetheriano se e solo se ogni ideale di R è generato da un insieme finito di elementi.

3. Sia R un dominio.
   (a) Dimostrare che $R[X]$ è un dominio;
   (b) Dimostrare che $R[X]^* = R^*$.

4. Sia R un anello commutativo. Un sottoinsieme $S \subset R$ si dice *moltiplicativamente chiuso* se $1 \in S$ e se per ogni $x, y \in S$ si ha che $xy \in S$.
   (a) Dimostrare: se R è un dominio, allora $S = R - \{0\}$ è moltiplicativamente chiuso.
   (b) Sull'insieme $R \times S$ definiamo $(x, s) \sim (y, t)$ se esiste $u \in S$ tale che $u(xt - ys) = 0$. Far vedere che si tratta di una relazione di equivalenza. Scriviamo $\frac{x}{s}$ per la classe di (x, s).
   (c) Sia R_S l'insieme delle classi di equivalenza della parte (b). Dimostrare che le operazioni $\frac{x}{s} + \frac{y}{t} = \frac{xt+ys}{st}$ e $\frac{x}{s} \cdot \frac{y}{t} = \frac{xy}{st}$ danno ad R_S la struttura di un anello commutativo.
   (d) Far vedere che la mappa $R \longrightarrow R_S$ che manda x in $\frac{x}{1}$ è un morfismo di anelli.

5. Sia $\mathbf{Z}[i]$ l'anello degli interi di Gauss.
   (a) Verificare che $\mathbf{Z}[i]$ è un dominio ad ideali principali.
   (b) Fattorizzare gli elementi $5 + i$ e $239 + i$ come prodotto di elementi irriducibili di $\mathbf{Z}[i]$.
   (c) Dedurre la formula classica che John Machin ha usato nel 1706 per calcolare a mano i primi 100 decimali di π:

$$\pi = 16 \arctan\frac{1}{5} - 4 \arctan\frac{1}{239}, \qquad \text{con} \quad \arctan x = \sum_{k=0}^{\infty} (-1)^k \frac{x^{2k+1}}{2k+1}.$$

6. Determinare le soluzioni in $\mathbf{Z}$ dell'equazione $X^2 + 1 = Y^3$. Sia (x, y) una soluzione.
   (a) Dimostrare che x è un intero *pari*;
   (b) Dimostrare che gli elementi $x + i$ e $x - i$ di $\mathbf{Z}[i]$ hanno mcd uguale a 1;
   (c) Far vedere che $x + i$ è il cubo di un elemento $a + bi \in \mathbf{Z}[i]$;
   (d) Concludere che $(x, y) = (0, 1)$.