1. Determinare quali sottoinsiemi sono sottogruppi:
 - (a) $\mathbf{Q}_{>0} \subset \mathbf{Q}^*$,
 - (b) $\{x \in \mathbf{R} : x > 1\} \subset \mathbf{R}^*$,
 - (c) $\{\pm 1, \pm i\} \subset \mathbf{C}^*$,
 - (d) $\{\bar{x} \in \mathbf{Z}_n^* : x \equiv 1 \pmod{d}\} \subset \mathbf{Z}_n^*$ per d un divisore di n ,
 - (e) $D_d \subset D_n$ per d un divisore di $n \in \mathbf{Z}_{>0}$,
 - (f) $\{x \in \mathbf{Q}^* : \text{esistono } a, b \in \mathbf{Q} \text{ tali che } x = a^2 + b^2\} \subset \mathbf{Q}^*$.
2. Dimostrare che un sottogruppo di un gruppo abeliano è abeliano. Dare un esempio di un gruppo non abeliano con sottogruppo abeliano non banale.
3. (a) Sia G un gruppo e sia $\{H_\alpha : \alpha \in A\}$ una famiglia di sottogruppi di G . Dimostrare che $\cap_\alpha H_\alpha = \{h : h \in H_\alpha \text{ per ogni } \alpha \in A\}$ è un sottogruppo di G .
 (b) Sia G un gruppo e siano $H \subset G$ e $H' \subset G$ due sottogruppi. Dimostrare: se $G = H \cup H'$ allora $G = H$ oppure $G = H'$.
 (c) Provare che il gruppo $G = \mathbf{Z}_{12}^*$ ha *tre* sottogruppi H_1, H_2 e H_3 diversi da G ma con $H_1 \cup H_2 \cup H_3 = G$.
4. Esprimere le seguenti permutazioni in S_9 come prodotti di cicli disgiunti. Calcolare gli inversi.
 - (a) $\sigma : \begin{cases} 1 \mapsto 9, & 4 \mapsto 1, & 7 \mapsto 2, \\ 2 \mapsto 7, & 5 \mapsto 3, & 8 \mapsto 5, \\ 3 \mapsto 8, & 6 \mapsto 4, & 9 \mapsto 6. \end{cases}$
 - (b) $\tau : \begin{cases} 1 \mapsto 8, & 4 \mapsto 6, & 7 \mapsto 9, \\ 2 \mapsto 2, & 5 \mapsto 5, & 8 \mapsto 1, \\ 3 \mapsto 3, & 6 \mapsto 4, & 9 \mapsto 7. \end{cases}$
5. Scrivere la permutazione $(1964387)(1374862)(271)$ come prodotto di cicli disgiunti.
6. Sia n un intero positivo e sia p un numero primo. Provare: se $\sigma \in S_n$ ha ordine p , allora σ è un prodotto di un certo numero di p -cicli disgiunti.
7. Sia $n \in \mathbf{Z}_{>1}$.
 - (a) Per $n = 2, 3, 4, 5$ fattorizzare $n^4 + 1$ in fattori primi.
 - (b) Sia $m = n^4 + 1$. Dimostrare che $\bar{n} \in \mathbf{Z}_m^*$ ha ordine 8.
 - (c) Dimostrare che ogni divisore primo $q > 2$ di $n^4 + 1$ soddisfa $q \equiv 1 \pmod{8}$.
8. Sia p un numero primo e sia $M_p = 2^p - 1$ il p -esimo numero di Mersenne. Sia q un divisore primo di M_p .
 - (a) Dimostrare che $\bar{2} \in \mathbf{Z}_q^*$ ha ordine p .
 - (b) Dimostrare che $q \equiv 1 \pmod{p}$.
 - (c) Dimostrare che M_p è primo per ogni primo $p < 11$, ma che $M_{11} = 2047$ non è primo.
9. Sia $k \in \mathbf{Z}_{\geq 0}$ e sia $F_k = 2^{2^k} + 1$ il k -esimo numero di Fermat. Sia q un divisore primo di F_k .
 - (a) Dimostrare che $\bar{2} \in \mathbf{Z}_q^*$ ha ordine 2^{k+1} .
 - (b) Dimostrare che $q \equiv 1 \pmod{2^{k+1}}$.