1. Per i seguenti insiemi $G$ e "composizioni" $*$, indicare, se esiste, un elemento neutro. Dire quando si tratta di un gruppo:
   (a) $G = \mathbf{Z}_{>0}$ con $a * b = a^b$.
   (b) $G = \mathbf{R}$ con $a * b = a + b + 3$,
   (c) $G = \mathbf{R}_{>1}$ con $a * b = a^{\log(b)}$.
   (d) $G = \{-1, 0, 1\}$ con $a * b = a + b$.
   (e) $G = \{1, 2, 3, 4, \ldots\}$ con $a * b = \max(a, b)$.
   (f) $G = \mathbf{R}^2$ con $\binom{a}{b} * \binom{c}{d} = \binom{c+ad}{bd}$.

2. Sia $G$ un gruppo. Usiamo notazione moltiplicativa. In particolare, scriviamo $x^{-1}$ per l'inverso di un elemento $x$ di $G$.
   (a) Siano $a, b \in G$. Dimostrare che l'equazione
   $$ax = b$$
   ha una unica soluzione $x \in G$. Questa soluzione è $x = a^{-1}b$. Similmente, dimostare che esiste una unica soluzione $x \in G$ di $xa = b$, vale a dire $x = ba^{-1}$.
   (b) (Proprietà Sudoku) Provare che, nella tabella di composizione di un gruppo finito, ogni elemento compare esattamente una volta in ogni riga ed ogni colonna.

3. Sia $X$ un insieme e sia $P(X)$ l'insieme delle parti di $X$. *La differenza simmetrica* $A \triangle B$ di due sottoinsiemi $A$ e $B$ di $X$ è definita da
   $$A \triangle B = (A \cup B) - (A \cap B).$$
   (a) Dimostrare che $A \triangle \emptyset = A$ e che $A \triangle A = \emptyset$ per ogni $A \in P(X)$ Dimostrare che $P(X)$ con la composizione $\triangle$ en elemento neutro $\emptyset$ è un gruppo abeliano. Scrivere la tabella di composizione per l'insieme $X = \{0, 1\}$.

4. Una trasformazione *affine* di $\mathbf{R}$ è una applicazione $A : \mathbf{R} \longrightarrow \mathbf{R}$ data da
   $$x \mapsto ax + b$$
   con $a \in \mathbf{R}^*$ e $b \in \mathbf{R}$. Dimostrare che le trasformazioni affini di $\mathbf{R}$ formano un gruppo con la composizione. Si tratta di un gruppo commutativo?

5. Sia $n \in \mathbf{N}$. L'ordine $\mathrm{ord}_n(\overline{x})$ di $\overline{x} \in \mathbf{Z}_n^*$ è il più piccolo intero $r > 0$ tale che $\overline{x}^r = \overline{1}$ in $\mathbf{Z}_n^*$.
   (a) Sia $n = 13$. Calcolare $\mathrm{ord}_n(x)$ per ogni $x \in \mathbf{Z}_n^*$.
   (b) Sia $n \in \mathbf{N}$ arbitrario. Calcolare l'ordine di $\overline{-1} \in \mathbf{Z}_n^*$.

6. (a) Determinare tutti gli $x \in \mathbf{Z}_9^*$ per cui $\overline{x}^2 = \overline{1}$. Stessa domanda per $\mathbf{Z}_{25}^*$.
   (b) Determinare tutti gli $\overline{x} \in \mathbf{Z}_{15}^*$ per cui $\overline{x}^2 = \overline{1}$. Stessa domanda per $\mathbf{Z}_{21}^*$.
   (c) Sia $n$ quadrato di un numero primo $p > 2$. Quanti sono gli elementi $\overline{x} \in \mathbf{Z}_n^*$ con $\overline{x}^2 = \overline{1}$?
   (d) Sia $n$ prodotto di due primi dispari. Quanti sono gli elementi $\overline{x} \in \mathbf{Z}_n^*$ con $\overline{x}^2 = \overline{1}$?