1. Determinare la tabella additiva e la tabella moltiplicativa di $\mathbf{Z}_6$.
   (a) Verificare dalla tabella moltiplicativa di $\mathbf{Z}_6$ che esistono $\bar{x}$ e $\bar{y}$ non nulli in $\mathbf{Z}_6$ tali che $\bar{x} \cdot \bar{y} = \bar{0}$.
   (b) Verificare dalla tabella moltiplicativa di $\mathbf{Z}_6$ che esiste $\bar{x} \in \mathbf{Z}_6$ che non ammette inverso moltiplicativo.

2. Determinare le tabelle moltiplicative di $\mathbf{Z}_5^*$ e di $\mathbf{Z}_{12}^*$ e confrontarle.
   (a) Per ognuno degli elementi in $\mathbf{Z}_5^*$ identificare il suo inverso.
   (b) Determinare tutti gli $\bar{x} \in \mathbf{Z}_5^*$ tali che $\bar{x}^2 = \bar{1}$.
   (c) Per ognuno degli elementi in $\mathbf{Z}_{12}^*$ identificare il suo inverso.
   (d) Determinare tutti gli $\bar{x} \in \mathbf{Z}_{12}^*$ tali che $\bar{x}^2 = \bar{1}$.

3. Sia dato l'insieme $A = \{1, -1, i, -i\}$ con l'operazione data dalla moltiplicazione fra numeri complessi.
   (a) Verificare che A è un gruppo abeliano.
   (b) Determinare i^{-1} e $(-i)^{-1}$.
   (c) Scrivere la tabella della moltiplicazione su A. Confrontarla con quelle dell'esercizio precedente.

4. Siano dati $\bar{x} = \overline{13^{35}}$ e $\bar{y} = \overline{41^{35}}$ in $\mathbf{Z}_{37}$.
   (a) Determinare $\bar{x}^{-1}$.
   (b) Determinare $\bar{y}^{-1}$.

5. Sia $p \in \mathbf{N}$ un numero primo. Verificare che in $\mathbf{Z}_p$ vale l'uguaglianza $(\bar{x} + \bar{y})^p = \bar{x}^p + \bar{y}^p$, per ogni $\bar{x},\ \bar{y} \in \mathbf{Z}_p$ (suggerimento: usare la formula di Newton).
   Verificare che per $n = 4$, tale uguaglianza non vale.

6. Calcolare
$$2^{1000} \bmod 5, \qquad 2^{1000} \bmod 7, \qquad 10^{1000} \bmod 3, \qquad 10^{1000} \bmod 5.$$

7. Determinare l'ultima cifra decimale dei seguenti numeri
$$37^{37}, \qquad 16^{16}, \qquad 19^{19}.$$

8. Dimostrare che $4^{2n+1} + 3^{n+2}$ è divisibile per 13, per ogni $n \in \mathbf{N}$ (suggerimento: calcolare in $\mathbf{Z}_{13}$).

9. Dimostrare che $\sum_{\bar{x} \in \mathbf{Z}_n} \bar{x} = \bar{0}$ in $\mathbf{Z}_n$, per ogni n dispari.

10. Calcolare $(p-1)!$ in $\mathbf{Z}_p$, per p primo.

11. Sia $n \in \mathbf{N}$. L'ordine $\mathrm{ord}_n(x)$ di $x \in \mathbf{Z}_n^*$ è il più piccolo $r > 0$ tale che $x^r \equiv 1 \bmod n$.
   (a) Sia $n = 7$. Calcolare $\mathrm{ord}_n(x)$ per ogni $x \in \mathbf{Z}_n^*$.
   (b) Sia $n \in \mathbf{N}$. Calcolare l'ordine di $-1 \bmod n$.
   (c) Sia p primo. Dimostrare che $\mathrm{ord}_p(x)$ divide $p - 1$ per ogni $x \in \mathbf{Z}_p^*$.