

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. Sia \mathbf{Z}_8 l'insieme delle classi resto modulo 8.
 - (a) Scrivere la tabella dell'addizione e della moltiplicazione in \mathbf{Z}_8 .
 - (b) Determinare \mathbf{Z}_8^* , il sottoinsieme degli elementi invertibili rispetto alla moltiplicazione in \mathbf{Z}_8 .
 - (c) Scrivere la tabella della moltiplicazione in \mathbf{Z}_8^* .
 - (d) Determinare le soluzioni in \mathbf{Z}_8 dell'equazione $\bar{x}^2 \equiv \bar{0}$.
 - (e) Determinare tutte le soluzioni intere della congruenza $4x \equiv 0 \pmod{8}$ e le soluzioni in \mathbf{Z}_8 dell'equazione $\bar{4}\bar{x} \equiv \bar{0}$.
 - (f) Determinare tutte le soluzioni intere della congruenza $2x \equiv 6 \pmod{8}$ e le soluzioni in \mathbf{Z}_8 dell'equazione $\bar{2}\bar{x} \equiv \bar{6}$.
 - (g) Determinare tutte le soluzioni intere della congruenza $3x \equiv 1 \pmod{8}$. Quante soluzioni in \mathbf{Z}_8 ha l'equazione $\bar{3}\bar{x} \equiv \bar{1}$?
3. 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 $\bar{x}^2 = \bar{1}$.
4. 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.
5. La funzione φ di Eulero è definita da $\varphi(n) = \#\mathbf{Z}_n^*$ (per $n \in \mathbf{N}$).
 - (a) Calcolare $\varphi(n)$ per ogni $n \leq 10$.
 - (b) In ognuno di tali casi enunciare il corrispondente Teorema di Lagrange per \mathbf{Z}_n^* .
6. Sia $n = 13$. Enunciare il Piccolo Teorema di Fermat per $G = \mathbf{Z}_{13}^*$. Usare tale risultato per calcolare

$$\overline{4^{24}}, \overline{4^{59}}, \overline{4^{26}}, \overline{4^{24001}} \in \mathbf{Z}_{13}.$$
7. 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} .
8. Calcolare $\bar{2}^{300}$ in \mathbf{Z}_6 . Possiamo usare il Teorema di Lagrange?
9. Calcolare

$$2^{1000} \pmod{5}, \quad 2^{1000} \pmod{7}, \quad 10^{1000} \pmod{3}, \quad 10^{1000} \pmod{5}.$$

10. Determinare l'ultima cifra decimale dei seguenti numeri

$$37^{37}, \quad 16^{16}, \quad 19^{19}.$$

11. Calcolare

$$5^{95} \pmod{70}, \quad 2^{1000} \pmod{110}.$$

12. (a) Determinare il resto delle divisioni per 5, per 7 e per 11 di 3^{302} ; determinare il resto della divisione per 385 di 3^{302} (si noti che $385 = 5 \cdot 7 \cdot 11$).

(b) Determinare il resto delle divisioni per 7, per 11 e per 13 di 5^{2003} ; determinare il resto della divisione per 1001 di 5^{2003} (si noti che $1001 = 7 \cdot 11 \cdot 13$).

13. Determinare il resto della divisione per 5 di $33213454^{27221447}$. Determinare il resto della divisione per 7 di $19^{19^{19}}$.

14. Calcolare il resto della divisione per 70 di 3^{302} .

15. Sia $n \in \mathbf{N}$. L'ordine $\text{ord}_n(x)$ di $x \in \mathbf{Z}_n^*$ è il più piccolo $r > 0$ tale che $x^r \equiv 1 \pmod{n}$.

(a) Sia $n = 7$. Calcolare $\text{ord}_n(x)$ per ogni $x \in \mathbf{Z}_n^*$.

(b) Sia n primo. Dimostrare che $\text{ord}_n(x)$ divide $n - 1$ per ogni $x \in \mathbf{Z}_n^*$.

(c) Sia $n \in \mathbf{N}$. Calcolare l'ordine di $-1 \pmod{n}$.

16. (a) Sia $p > 2$ un primo. Dimostrare che $\{x \in \mathbf{Z}_p : x^2 = 1\} = \{\pm 1\}$.

(b) Determinare tutti gli $x \in \mathbf{Z}_{15}^*$ per cui $x^2 = 1$. Stessa domanda per \mathbf{Z}_{21}^* .

(c) Sia $n = pq$ prodotto di due primi dispari. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?

(d) Determinare tutti gli $x \in \mathbf{Z}_9^*$ per cui $x^2 = 1$. Stessa domanda per \mathbf{Z}_{25}^* .

(e) Sia $n = p^2$ quadrato di un numero primo $p > 2$. Quanti sono gli elementi $x \in \mathbf{Z}_n^*$ con $x^2 = 1$?

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

18. 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.

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

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

21. Siano (G_1, e_1, \circ) e $(G_2, e_2, *)$ due gruppi. Sul prodotto cartesiano $G_1 \times G_2$ definiamo una operazione mediante

$$(g_1, g_2) \cdot (h_1, h_2) := (g_1 \circ h_1, g_2 * h_2).$$

(a) Dimostrare che con questa operazione $G_1 \times G_2$ è un gruppo.

(b) Siano $(G_1, e_1, \circ) = (G_2, e_2, *) = (\mathbf{Z}_2, \bar{0}, +)$, con la somma $\bar{x} + \bar{y} := \overline{x+y}$. Scrivere la tabella dell'operazione indotta su $\mathbf{Z}_2 \times \mathbf{Z}_2$.

(c) Siano $(G_1, e_1, \circ) = (\mathbf{Z}_2, \bar{0}, +)$ e $(G_2, e_2, *) = (\mathbf{Z}_3, \bar{0}, +)$. Scrivere la tabella dell'operazione indotta su $\mathbf{Z}_2 \times \mathbf{Z}_3$.

22. Sia G un gruppo tale che $g^2 = e$, per ogni $g \in G$. Dimostrare che G è abeliano.

23. Sia $G = \{M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{R}, \det M \neq 0\}$. Dimostrare che G col prodotto fra matrici usuale è un gruppo non commutativo.
24. Sia $A = \{M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \mid a, b, c, d \in \mathbf{R}\}$.
- Dimostrare che A con la somma fra matrici usuale è un gruppo abeliano.
 - Dimostrare che A con la somma e il prodotto fra matrici usuali è un anello non commutativo.
 - Far vedere che esistono matrici non nulle $M, N \in A$ il cui prodotto è la matrice nulla.
 - Chi sono le unità in A ?
25. Sia X un insieme e sia $P(X)$ l'insieme dei sottoinsiemi di X . Definiamo su $P(X)$ una “somma” ed un “prodotto” mediante

$$A \oplus B := (A \cup B) - (A \cap B), \quad A \otimes B := A \cap B.$$

- Verificare che $A \oplus B = (A - B) \cup (B - A)$.
- Dimostrare che $P(X)$ con l'operazione \oplus è un gruppo abeliano.
- Scrivere la tabella di composizione per un insieme X di due elementi. Confrontare con il gruppo di Klein V_4 .
- Dimostrare che $P(X)$ con le operazioni “ \oplus ” e “ \otimes ” è un anello commutativo.
- Chi sono le unità in $P(X)$?