1. (a) Scrivere in base 2 e in base 8 i numeri 215 e 150.
   (b) Scrivere in base 7 i numeri 100 e 2400.

2. Per $n, b \in \mathbf{N}$, indichiamo con $(n)_b$ la scrittura di n in base b. Calcolare:
   (a) $(1011100)_2 + (11001)_2$; (b) $(11001)_2 \cdot (1110)_2$; (c) $(11011)_2 - (1100)_2$.

3. (a) Determinare il resto della divisione per 3 del numero $(1100110)_2$.
   (b) Determinare il resto della divisione per 4 del numero $(210211)_3$.

4. Stabilire se esiste l'inverso di a modulo n e, in caso affermativo, determinarlo, dove:
   (a) $a = 11$ e $n = 13$; (c) $a = 21$ e $n = 6$; (e) $a = -8$ e $n = 15$;
   (b) $a = 6$ e $n = 21$; (d) $a = 27$ e $n = 36$; (f) $a = 144$ e $n = 233$.

5. Per ogni intero $n > 1$ determinare il resto della divisone per n di $(n-1)!$.

6. 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) Dimostare 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 $\overline{x} + \overline{y} := \overline{x+y}$. 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 $\mathbf{Z}_2 \times \mathbf{Z}_3$.

7. 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 $\overline{x}^2 \equiv \overline{0}$. dell'equazione $\overline{2}\overline{x} \equiv \overline{6}$.
   (g) Determinare tutte le soluzioni intere della congruenza $3x \equiv 1 \pmod 8$. Quante soluzioni in $\mathbf{Z}_8$ ha l'equazione $\overline{3}\overline{x} \equiv \overline{1}$?

8. Sia $n = 23$. Enunciare il Piccolo Teorema di Fermat per $G = \mathbf{Z}_{13}^*$. Usare tale risultato per calcolare
$$\overline{4^{24}}, \quad \overline{4^{59}}, \quad \overline{4^{26}}, \quad \overline{4^{24001}} \quad \in \mathbf{Z}_{13}.$$

9. Sia X un insieme e sia $P(X)$ l'insieme dei sottoinsiemi di X. Definiamo su $P(X)$ una "somma" $\oplus$ ed un "prodotto" $\otimes$ mediante
$$A \oplus B := (A \cup B) - (A \cap B), \qquad A \otimes B := A \cap B.$$
   (a) Verificare che $A \oplus B = (A - B) \cup (B - A)$.
   (b) Dimostrare che $P(X)$ con l'operazione $\oplus$ è un gruppo abeliano.
   (c) Scrivere la tabella di composizione per un insieme X di due elementi. Confrontare con il gruppo dell'Eserc. 6 (b).
   (d) Dimostrare che $P(X)$ con le operazioni "$\oplus$" e "$\otimes$" è un anello commutativo.
   (e) Chi sono gli elementi invertibili in $P(X)$?

10. 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 $x^r \equiv 1 \pmod n$.
   (a) Sia $n = 7$. Calcolare $\mathrm{ord}_n(x)$ per ogni $x \in \mathbf{Z}_n^*$.
   (b) Sia n primo. Dimostrare che $\mathrm{ord}_n(x)$ divide $n - 1$ per ogni $x \in \mathbf{Z}_n^*$.
   (c) Sia $n \in \mathbf{N}$. Calcolare l'ordine di $-1 \pmod n$.

11. La *funzione φ di Eulero* è definita da $\varphi(n) = \#\mathbf{Z}_n^*$ (per $n \in \mathbf{N}$).
   (a) Dimostrare: $\varphi(n) = \#\{a \in \mathbf{N} : 0 \le a < n \text{ e } \mathrm{mcd}(a, n) = 1\}$.
   (b) Calcolare $\varphi(n)$ per ogni $n \le 10$.
   (c) Dimostrare che $\varphi(n) = n - 1$ quando n è primo.
   (d) Sia $n = pq$ per due primi p e q. Dimostrare che $\varphi(n) = (p-1)(q-1)$.
   (e) Sia p un primo. Calcolare $\varphi(p^2)$. Calcolare $\varphi(p^k)$ per ogni $k \ge 1$.