

1. 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 $\mathbf{Z}_2 \times \mathbf{Z}_3$.
2. 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: $A \oplus B := (A \cup B) - (A \cap B)$, $A \otimes B := A \cap B$.
 - (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. 1 (b).
 - (d) Dimostrare che $P(X)$ con le operazioni " $\oplus$ " e " $\otimes$ " è un anello commutativo.
 - (e) Chi sono gli elementi invertibili in $P(X)$?
3. (a) Stabilire se esiste l'inverso di a modulo n e, in caso affermativo, determinarlo, dove:
 - (i) $a = 11$ e $n = 13$; (ii) $a = 6$ e $n = 21$; (iii) $a = 21$ e $n = 6$; (iv) $a = 27$ e $n = 36$;
 - (b) Stabilire se $\bar{a} \in \mathbf{Z}_n^*$ e, in caso affermativo, determinare l'inverso di $\bar{a}$ in $\mathbf{Z}_n^*$ dove:
 - (i) $a = -8$ e $n = 15$; (ii) $a = 144$ e $n = 233$; (iii) $a = 7$ e $n = 91$; (iv) $a = 8$ e $n = 91$.
4. 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 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 $\bar{3}\bar{x} \equiv \bar{1}$?
5. 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 $-1 \pmod{n}$.
6. Sia $n = 23$. 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. (a) Determinare il resto della divisione per 55 del numero 3^{193} .
- (b) Determinare il resto della divisione per 91 del numero 5^{193} .
(Sugg. fattorizzare 55 e 91 ed usare il Teorema Cinese del resto).
9. (a) Determinare il resto della divisione per 385 ($= 5 \cdot 7 \cdot 11$) del numero 2^{677} .
- (b) Determinare il resto della divisione per 55 del numero 2238^{2142} .
- (c) Determinare il resto della divisione per 11 del numero $8^{11^{11}}$.
- (d) Determinare l'ultima cifra decimale dei numeri 5^{6^7} e 7^{6^5} .