

1. Determinare la tabella additiva e la tabella moltiplicativa di  $\mathbb{Z}_6$ .
  - (a) Verificare dalla tabella moltiplicativa di  $\mathbb{Z}_6$  che esistono  $\bar{x}$  e  $\bar{y}$  non nulli in  $\mathbb{Z}_6$  tali che  $\bar{x} \cdot \bar{y} = \bar{0}$ .
  - (b) Verificare dalla tabella moltiplicativa di  $\mathbb{Z}_6$  che esiste  $\bar{x} \in \mathbb{Z}_6$  che non ammette inverso moltiplicativo.
2. Sia  $\mathbb{Z}_n$  l'anello degli interi modulo  $n$  e sia  $\mathbb{Z}_n^*$  il gruppo degli elementi invertibili di  $\mathbb{Z}_n$ . Determinare le tabelle moltiplicative di  $\mathbb{Z}_5^*$  e di  $\mathbb{Z}_{12}^*$  e confrontarle.
  - (a) Per ognuno degli elementi in  $\mathbb{Z}_5^*$  identificare il suo inverso.
  - (b) Determinare tutti gli  $\bar{x} \in \mathbb{Z}_5^*$  tali che  $\bar{x}^2 = \bar{1}$ .
  - (c) Per ognuno degli elementi in  $\mathbb{Z}_{12}^*$  identificare il suo inverso.
  - (d) Determinare tutti gli  $\bar{x} \in \mathbb{Z}_{12}^*$  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.
  - (a) Scrivere la tavola pitagorica di  $\mathbb{Z}_n^*$  per  $n = 5, 8, \text{ e } 12$ .
  - (b) Determinare gli interi positivi  $n$  che hanno la proprietà che  $\bar{x}^2 = \bar{1}$  per ogni  $\bar{x} \in \mathbb{Z}_n^*$ .
  - (c) Dimostrare che si ha  $\bar{x}^2 = \bar{1}$  per ogni  $\bar{x} \in \mathbb{Z}_{24}^*$ .
5. La funzione  $\varphi$  di Eulero è definita da  $\varphi(n) = \# \mathbb{Z}_n^*$  (per  $n \in \mathbb{N}$ ). Calcolare  $\varphi(n)$  per i seguenti numeri: 100, 10!, 101, 1001, 10001.
6. Si consideri la funzione  $\varphi$  di Eulero.
  - (a) Calcolare  $\varphi(n)$  per ogni  $n \leq 10$ .
  - (b) Calcolare  $\varphi(n)$  nei seguenti casi:  $n = 1729, 1100, 1313, 2^3 \cdot 5^3 \cdot 7^2$ .
  - (c) In ognuno di tali casi enunciare il corrispondente Teorema di Lagrange per  $\mathbb{Z}_n^*$ .
7. Siano dati  $\bar{x} = \overline{13^{35}}$  e  $\bar{y} = \overline{41^{35}}$  in  $\mathbb{Z}_{37}$ .
  - (a) Determinare  $\bar{x}^{-1}$ .
  - (b) Determinare  $\bar{y}^{-1}$ .
8. Calcolare
 
$$2^{1000} \pmod{5}, \quad 2^{1000} \pmod{7}, \quad 10^{1000} \pmod{3}, \quad 10^{1000} \pmod{5}.$$
9. Calcolare  $\bar{2}^{300}$  in  $\mathbb{Z}_6$ . Possiamo usare il Teorema di Lagrange?
10. Usando il Piccolo Teorema di Fermat verificare che i seguenti numeri non sono primi:  $n = 33, 45, 12$ .
11. Un numero di Carmichael è un numero che soddisfa il Piccolo Teorema di Fermat, ossia per ogni  $a \in \mathbb{Z}_n^*$ , vale  $a^{n-1} \equiv 1 \pmod{n}$ .
  - (a) *Criterio di Korselt*: Un intero  $n \in \mathbb{N}$  è un numero di Carmichael se e solo se è privo di fattori quadratici ed ha la proprietà che se un primo  $p$  divide  $n$ , allora anche  $p-1$  divide  $n-1$ .
  - (b) Dimostrare che un numero di Carmichael ha almeno tre divisori distinti.
  - (c) Dimostrare che  $561 = 3 \cdot 17 \cdot 11$  è un numero di Carmichael.
  - (d) Dimostrare che  $1729 = 7 \cdot 13 \cdot 19$  è un numero di Carmichael.
  - (e) Dimostrare che  $8911 = 7 \cdot 19 \cdot 67$  è un numero di Carmichael.
12. Sfruttando l'espressione binaria dell'esponente, calcolare
 
$$3^{200} \pmod{48}, \quad 45^{54} \pmod{91}, \quad 12^{256} \pmod{561}.$$
13. Fare il test di primalità di Miller-Rabin sui numeri  $n = 91, 101, 113, 221, 2465, 8911$ , con  $a = 2$ .
14. (RSA) Siano  $p$  e  $q$  numeri primi e sia  $n = pq$ . Siano  $E, D$  interi tali che  $E \cdot D \equiv 1 \pmod{(p-1)(q-1)}$ . Sia  $M \in \mathbb{Z}_n^*$ .

- (a) Verificare che  $M^{ED} \equiv M \pmod{n}$ .
- (b) Siano  $p = 7$ ,  $q = 11$  ed  $n = 77$ . Determinare una coppia  $E, D$  come sopra.
- (c) Sia  $M = 15$ . Per gli  $E, D$  determinati al punto precedente, calcolare  $M^E \pmod{n}$  e verificare che  $M^{ED} \equiv M \pmod{n}$ .
15. (a) Sia  $p > 2$  un primo. Dimostrare che  $\{x \in \mathbb{Z}_p : x^2 = 1\} = \{\pm 1\}$ .
- (b) Determinare tutte le soluzioni dell'equazione  $\bar{x}^2 = \bar{1}$  in  $\mathbb{Z}_{pq}$ , per  $p, q$  primi dispari.
- (c) Determinare tutti gli  $x \in \mathbb{Z}_{15}^*$  per cui  $x^2 = 1$ . Stessa domanda per  $\mathbb{Z}_{21}^*$ .
- (d) Sia  $n = p^2$  quadrato di un numero primo  $p > 2$ . Quanti sono gli elementi  $x \in \mathbb{Z}_n^*$  con  $x^2 = 1$ ?
- (e) Determinare tutti gli  $x \in \mathbb{Z}_9^*$  per cui  $x^2 = 1$ . Stessa domanda per  $\mathbb{Z}_{25}^*$ .
16. Dimostrare che  $4^{2n+1} + 3^{n+2}$  è divisibile per 13, per ogni  $n \in \mathbb{N}$  (suggerimento: calcolare in  $\mathbb{Z}_{13}$ ).
17. Sia  $p \in \mathbb{N}$  un numero primo. Verificare che in  $\mathbb{Z}_p$  vale l'uguaglianza  $(\bar{x} + \bar{y})^p = \bar{x}^p + \bar{y}^p$ , per ogni  $\bar{x}, \bar{y} \in \mathbb{Z}_p$  (suggerimento: usare la formula di Newton).  
Verificare che per  $n = 4$ , tale uguaglianza non vale.
18. Dimostrare che  $\sum_{\bar{x} \in \mathbb{Z}_n} \bar{x} = \bar{0}$  in  $\mathbb{Z}_n$ , per ogni  $n$  dispari.
19. (Teorema di Wilson) Calcolare  $(p-1)!$  in  $\mathbb{Z}_p$ , per  $p$  primo.
20. Sia  $n \in \mathbb{N}$ . L'ordine  $\text{ord}_n(x)$  di  $x \in \mathbb{Z}_n^*$  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  $x \in \mathbb{Z}_n^*$ .
- (b) Sia  $n \in \mathbb{N}$ . Calcolare l'ordine di  $-1 \pmod{n}$ .
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  $(G_1, e_1, \circ) = (G_2, e_2, *) = (\mathbb{Z}_2, \bar{0}, +)$ , con la somma  $\bar{x} + \bar{y} := \overline{x+y}$ . Scrivere la tabella dell'operazione indotta su  $\mathbb{Z}_2 \times \mathbb{Z}_2$ .
- (c) Siano  $(G_1, e_1, \circ) = (\mathbb{Z}_2, \bar{0}, +)$  e  $(G_2, e_2, *) = (\mathbb{Z}_3, \bar{0}, +)$ . Scrivere la tabella dell'operazione indotta su  $\mathbb{Z}_2 \times \mathbb{Z}_3$ .
22. Sia  $G$  un gruppo tale che  $g^2 = e$ , per ogni  $g \in G$ . Dimostrare che  $G$  è abeliano.
23. Sia  $G$  un gruppo abeliano finito di ordine  $|G| = n$ . Il gruppo si dice ciclico se esiste un elemento  $x \in G$  tale che  $G = \{e, x, x^2, \dots, x^{n-1}\}$ . L'ordine  $\text{ord}(x)$  di un elemento  $x \in G$  è il più piccolo  $r > 0$  tale che  $x^r = e$  in  $G$ . Dimostrare che:
- (a)  $\text{ord}(x)$  divide  $n$ .
- (b) Sia  $x^k$  una potenza di  $x$ . Allora  $\text{ord}(x^k)$  divide  $\text{ord}(x)$ .
- (c)  $\text{ord}(x^k) = \text{ord}(x)$  se e solo se  $\text{mcd}(k, \text{ord}(x)) = 1$ .
- (b) se  $G$  ha ordine  $n$  primo, allora  $G$  è ciclico.
24. Sia  $G$  un gruppo ciclico di ordine  $n$  e sia  $Q$  un divisore di  $n$ .
- (a) Sia  $G^Q = \{a^Q \mid a \in G\}$  l'insieme delle potenze  $Q$ -sime di  $G$ . Allora  $G^Q$  coincide con l'insieme degli elementi che soddisfano  $a^{n/Q} = 1$ .
- (b) Sia  $G_Q = \{a \in G \mid \text{ord}(a) \mid Q\}$  l'insieme degli elementi di  $G$  il cui ordine divide  $Q$ . Allora  $G_Q$  è un sottogruppo ciclico di  $G$  di ordine  $Q$ .