

1. Siano  $n, m$  due numeri naturali.
  - (a) Dimostrare che  $\text{mcm}(n, m) \cdot \text{mcd}(n, m) = nm$ .
  - (b) Disegnare un algoritmo per calcolare il  $\text{mcm}(n, m)$  usando l'algoritmo Euclideo. Analizzare la complessità.
2. Disegnare un algoritmo che, dato  $n \in \mathbf{N}$ , calcola  $n! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot n$ . Stimare la lunghezza dell'output. Analizzare la complessità dell'algoritmo.
3. Fattorizzare i seguenti numeri in fattori primi.

|             |                    |                    |
|-------------|--------------------|--------------------|
| (a) 91;     | (d) $15^2 - 2^2$ ; | (g) $2^{11} - 1$ ; |
| (b) 210;    | (e) $10!$ ;        | (h) 10001;         |
| (c) $6^6$ ; | (f) $2^{10} - 1$ ; | (i) 100000003.     |
4. Per i seguenti numeri  $n$  e  $m$ , determinare  $a, b \in \mathbf{Z}$  tali che  $an + bm = \text{mcd}(n, m)$ .

|                           |                             |                                |
|---------------------------|-----------------------------|--------------------------------|
| (a) $n = 4$ e $m = 30$ ;  | (c) $n = 103$ e $m = 101$ ; | (e) $n = 221$ e $m = 169$ ;    |
| (b) $n = 14$ e $m = 40$ ; | (d) $n = 91$ e $m = 0$ ;    | (g) $n = 10001$ e $m = 9999$ . |
5.
  - (a) Scrivere in base 2 e in base 8 i numeri 215 e 150.
  - (b) Scrivere in base 7 i numeri 100 e 2400.
6. 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)  $(11011)_2 - (1100)_2$ .
7. Determinare il resto delle divisioni per 3, 9, 4, 11 del numero 3548917.
8.
  - (a) Determinare il resto della divisione per 3 del numero  $(1100110)_2$ .
  - (b) Determinare il resto della divisione per 4 del numero  $(210211)_3$ .
9.
  - (a) Stabilire se esistono  $s, t \in \mathbf{Z}$  tali che  $24s + 18t = 20$ ;
  - (b) Stabilire se esistono  $s, t \in \mathbf{Z}$  tali che  $24s + 18t = -12$ ;
  - (c) Stabilire se esistono  $s, t \in \mathbf{Z}$  tali che  $24s + 18t = 3$ .
10. Per ogni intero  $n > 1$  determinare il resto della divisione per  $n$  di  $(n-1)!$ .
11. Sia  $n \in \mathbf{N}$ . Dimostrare
  - (a) Se  $2^n - 1$  è primo, allora  $n$  è primo.
  - (b) Se  $2^n + 1$  è primo, allora  $n$  è una potenza di 2.
  - (c) Valgono le affermazioni inverse di (a) e (b)?
12. 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 $n = 233$ . |
13. Stabilire se per le seguenti congruenze esistono soluzioni intere  $x \in \mathbf{Z}$ . In caso affermativo, determinarle tutte.

|                               |                                |                                |
|-------------------------------|--------------------------------|--------------------------------|
| (a) $5x \equiv 8 \pmod{17}$ ; | (b) $9x \equiv 26 \pmod{30}$ ; | (c) $9x \equiv 24 \pmod{30}$ . |
|-------------------------------|--------------------------------|--------------------------------|