

1. Quali dei seguenti insiemi sono uguali?

$$A = \emptyset, \quad B = \{\emptyset\}, \quad C = \{0\}.$$

2. Sia  $X = \{1, 3, 4, 5\}$  e sia  $\mathcal{P}(X)$  l'insieme delle parti di  $X$ . Quali dei seguenti insiemi sono elementi di  $\mathcal{P}(X)$ ?

$$A = \{1, 3, 5\}, \quad B = \{\{1\}, 3\}, \quad C = \emptyset, \quad D = \{\emptyset\}, \quad E = \{\{1, 3\}, \{5\}\}, \quad F = \{1, 4\}.$$

3. Siano dati  $A = \{1, 2, 3\}$  e  $B = \{x, y, z\}$ . Determinare  $A \times A$ ,  $A \times B$  e  $B \times A$ . A chi appartengono gli elementi  $(1, 2)$ ,  $(1, x)$ ,  $(z, 3)$ ?

4. Sia  $A = \{x, y, z\}$ . Determinare la cardinalità dei seguenti insiemi:

$$A \cap (A \setminus A), \quad A \cup (A \cap A), \quad A \cup \mathcal{P}(A), \quad \mathcal{P}(A) \times \mathcal{P}(A), \quad \mathcal{P}(A \times A).$$

5. Sia data la funzione  $f: \mathbf{R} \rightarrow \mathbf{R}$ ,  $f(x) = \cos x + 1$ .

- (a) Determinare sottoinsiemi  $A$  e  $B$  di  $\mathbf{R}$  tali che  $f: A \rightarrow B$  sia iniettiva ma non suriettiva.  
 (b) Determinare sottoinsiemi  $C$  e  $D$  di  $\mathbf{R}$  tali che  $f: C \rightarrow D$  sia suriettiva ma non iniettiva.  
 (b) Determinare sottoinsiemi  $E$  e  $F$  di  $\mathbf{R}$  tali che  $f: E \rightarrow F$  sia biiettiva.

6. Sia  $A = \{1, 2, 5, 20, 50, 100\}$ .

- (a) Disegnare il diagramma di Hasse di  $(A, \leq)$ , dove  $\leq$  è l'ordinamento standard.  
 (b) Disegnare il diagramma di Hasse di  $(A, |)$ , dove  $|$  è l'ordinamento dato dalla "divisibilità" (ossia  $mRn$  se  $m|n$ ).

Che differenza c'è tra i due ordinamenti?

7. Sia  $A = \{1, 2, 3\}$ .

- (a) Quante relazioni simmetriche si possono definire su  $A$ ?  
 (b) Quante relazioni riflessive e simmetriche si possono definire su  $A$ ?

8. Verificare che 5 divide  $n^5 - n$ , per ogni  $n \in \mathbf{N}$ .

9. Determinare tutti gli interi che soddisfano il sistema di congruenze

$$\begin{cases} x \equiv 0 \pmod{2} \\ x \equiv 3 \pmod{7} \\ x \equiv 6 \pmod{11}. \end{cases}$$

Quanti ce ne sono nell'intervallo  $[0, 200]$ ? Determinarli tutti.

10. Calcolare  $\varphi(36)$ ,  $\varphi(37)$ ,  $\varphi(81)$ ,  $\varphi(1024)$ , dove  $\varphi$  indica la funzione di Eulero. Spiegare quali proprietà di  $\varphi$  avete usato.

11. Calcolare  $81^{-1}$  in  $\mathbf{Z}_{250}^*$ .

12. Calcolare  $111111^{33333333} \pmod{11}$  e  $33333333^{33333333} \pmod{11}$ . Giustificare bene ogni passaggio.

13. Sia Rossi un utente con chiavi pubbliche  $N = 221$  ed  $E = 7$ .

- (a) Spedirgli il messaggio  $m = 10$  dopo averlo criptato.

14. Preparare un kit RSA funzionante con chiavi pubbliche  $N$  ed  $E$  e chiave segreta  $D$ .