

COGNOME ..... NOME .....

Inserire le risposte negli spazi predisposti, *accompagnandole con spiegazioni* chiare ed essenziali.

NON SI ACCETTANO RISPOSTE SCRITTE SU ALTRI FOGLI. Ogni esercizio vale 7.5 punti.

1. Costruire una biezione fra  $\{k \in \mathbf{Z} : k \equiv 1 \pmod{6}\}$  e l'insieme dei numeri naturali  $\mathbf{N}$ .

Sia  $A = \{k \in \mathbf{Z} : k \equiv 1 \pmod{6}\}$ . Si ha che  $A = \{\dots, -11, -5, 1, 7, 13, \dots\}$ . Esistono tante biezioni  $f : \mathbf{N} \rightarrow \mathbf{A}$ . Un esempio facile da descrivere è quello che fa corrispondere i numeri naturali *pari*  $2, 4, 6, \dots \in \mathbf{N}$  ai numeri *positivi* in  $A$  (cioè a  $1, 7, 13, \dots$ ) e che fa corrispondere i numeri naturali *dispari*  $1, 3, 5, \dots \in \mathbf{N}$  ai numeri *negativi* in  $A$  (cioè a  $-5, -11, -17, \dots$ ). Abbiamo quindi

$$\begin{aligned} f(1) &= -5, f(2) = 1, f(3) = -11, \\ f(4) &= 7, f(5) = -17, f(6) = 13, \text{ ecc.} \end{aligned}$$

Una formula per  $f$  è data da:  $f(n) = 2 - 3n$  se  $n \in \mathbf{N}$  è dispari, mentre  $f(n) = 3n - 5$  se  $n \in \mathbf{N}$  è pari.

2. Sia  $R$  la relazione su  $\mathbf{Z}_9 (= \mathbf{Z}/9\mathbf{Z})$  determinata da: “ $x$  è in relazione con  $y$  se e soltanto se  $x^2 \equiv y^2 \pmod{9}$ ”.
- (a) Dimostrare che  $R$  è una relazione di equivalenza.
- (b) Quante classi di equivalenza ci sono?

(a) Per ogni  $x \in \mathbf{Z}_9$  vale  $x^2 \equiv x^2 \pmod{9}$ ; se abbiamo che  $x^2 \equiv y^2 \pmod{9}$ , allora anche  $y^2 \equiv z^2 \pmod{9}$ ; se abbiamo che  $x^2 \equiv y^2 \pmod{9}$  e  $y^2 \equiv z^2 \pmod{9}$  allora anche  $x^2 \equiv z^2 \pmod{9}$ . Concludiamo che  $R$  è una relazione di equivalenza.

(b) I quadrati di  $0, 1, 2, 3, 4, 5, 6, 7, 8$  modulo 9 sono rispettivamente congrui a  $0, 1, 4, 0, 7, 7, 0, 4, 1$  modulo 9. Vediamo che ci sono quattro classi di equivalenza, vale a dire  $\{0, 3, 6\}$ ,  $\{1, 8\}$ ,  $\{2, 7\}$  e  $\{4, 5\}$ , cioè gli interi modulo 9 con quadrato rispettivamente uguale a  $0, 1, 4$  e  $7$  modulo 9.

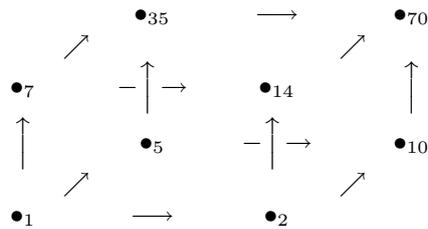
3. Calcolare il resto della divisione di  $7^{(7^7)}$  per 19.

Osserviamo che 19 è un numero primo e che dunque, grazie al piccolo teorema di Fermat, abbiamo  $7^{\phi(19)} = 1$ . Rimane quindi da calcolare la classe di congruenza di  $7^7$  modulo  $\phi(19) = 18$ . Ora,  $7^3 \equiv 1 \pmod{18}$ , quindi  $7^7 \equiv 7 \pmod{18}$ . Rimane da calcolare la classe di congruenza di  $7^7$  modulo 19. Ora,  $7^3 \equiv 1 \pmod{19}$ , quindi  $7^7 \equiv 7 \pmod{19}$ .

4. Sia  $X$  l'insieme  $X = \{2, 5, 7\}$ , e sia  $P$  il suo insieme delle parti.

- Scrivere esplicitamente  $P$ .
- Dimostrare che  $(P, \cup, \cap, ')$  è un'algebra di Boole.
- Disegnare il diagramma di Hasse di  $P$ .
- Sia  $(D_{70}, \mathbf{mcd}, \mathbf{mcm}, ')$  l'algebra di Boole dei divisori di 70. Scrivere esplicitamente un isomorfismo tra  $(P, \cup, \cap, ')$  e  $(D_{70}, \mathbf{mcd}, \mathbf{mcm}, ')$ . Giustificare la risposta.

- Abbiamo  $P = \{\emptyset, \{2\}, \{5\}, \{7\}, \{2, 5\}, \{2, 7\}, \{5, 7\}, \{2, 5, 7\}\}$ .
- Verifica esplicita del fatto che  $P$  è un reticolo limitato, complementato e distributivo (cf esercizi).
- Ecco il diagramma di Hasse



- Consideriamo ad esempio l'applicazione  $f$  che associa ad ogni elemento di  $P$  il prodotto dei numeri in esso contenuti (gli elementi di  $P$  sono a loro volta insiemi), e a  $\emptyset$  l'elemento 1 di  $D_{70}$ . Questa è chiaramente una biezione poiché ad ogni elemento di  $P$  essa associa uno ed un solo elemento di  $D_{70}$  (iniettività) ed i due insiemi hanno la stessa cardinalità (il che implica la suriettività); Si verifica inoltre che essa rispetta le operazioni di algebre di Boole.