COGNOME ..... **NOME** ..... Data di nascita.....

Risolvere gli esercizi negli spazi predisposti. Tutte le risposte devono essere motivate da spiegazioni *chiare ed essenziali*. Consegnare SOLO QUESTO FOGLIO. Ogni esercizio vale 6 punti.

1. Si consideri il reticolo $\mathbf{D}_{60}$. (a) Esibire esplicitamente (motivando) due elementi $h, k \in \mathbf{D}_{60}$ tali che h ha complemento e k non ha complemento.
(b) Stabilire (motivando) se qualcuno tra i seguenti sottoinsiemi di $\mathbf{D}_{60}$ è un sottoreticolo: (i) $A = \{1, 2, 4, 5, 20\}$; (ii) $B = \{1, 3, 4, 6, 12\}$; (iii) $C = \{1, 2, 3, 5, 30\}$.
(c) Stabilire se $\mathbf{D}_{60}$ è isomorfo a $\mathbf{D}_{90}$ e, in caso affermativo, esibire esplicitamente un isomorfismo e stabilire quanti sono gli isomorfismi di reticolo.

Soluzione. (a) L'elemento 3 ha complemento 20. Infatti $mcd(3, 20) = 1$ e $mcm(3, 20) = 60$.
L'elemento 2 non ha complemento. Infatti, se esistesse un complemento di 2, chimiamolo a, sarebbe $mcd(2, a) = 1$. Quindi a dovrebbe essere: 3, oppure 5, oppure 15. Ma $mcm(2, 3) = 6$, $mcm(2, 5) = 10$, $mcm(2, 15) = 30$.
(b) Nessuno dei tre sottoinsiemi è un sottoreticolo di $\mathbf{D}_{60}$. Infatti: $2 \vee 5 = mcm(2, 5) = 10 \notin A$. $4 \wedge 6 = mcd(4, 6) = 2 \notin B$. $2 \vee 3 = mcm(2, 3) = 6 \notin C$.
(c) Fattorizzando 60 e 90 in numeri primi, si ha che $60 = 2^2 \cdot 3 \cdot 5$ e $90 = 2 \cdot 3^2 \cdot 5$. Dunque entranbi sono della forma $p^2 \cdot q \cdot r$, con p, q, r primi distinti. Quindi sono isomorfi, perchè entranbi della forma $\{1, p, q, r, p^2, pq, pr, p^2q, p^2r, p^2qr\}$. Un isomorfismo dovrà mandare 2 in 3, 3 in 2 (oppure in 5) e 5 in 5 (oppure in 2). Gli altri valori sono determinati. Vi sono quindi due isomorfismi, coorsipondenti alla scelta $f(3) = 2$, $f(5) = 5$, oppure $f(3) = 5$, $f(5) = 2$. Il primo isomorfismo è:
$f : \mathbf{D}_{60} \to \mathbf{D}_{90}$, $f(1) = 1$, $f(2) = 3$, $f(3) = 2$, $f(5) = 5$, $f(6) = f(2 \vee 3) = f(2) \vee f(3) = 3 \vee 2 = 6$, $f(10) = f(2 \vee 5) = f(2) \vee f(5) = 3 \vee 5 = 15$, $f(15) = f(3 \vee 5) = f(3) \vee f(5) = 2 \vee 5 = 10$, $f(4) = 9$, $f(12) = f(4) \vee f(3) = 9 \vee 2 = 18$, $f(20) = f(4) \vee f(5) = 9 \vee 5 = 45$, $f(60) = 90$.

2. Nel sistema crittografico RSA di modulo $91 (= 7 \cdot 13)$ e esponente pubblico $D = 23$, si consideri il messaggio $m = 55$.
(a) Codificare il messaggio m. In altre parole, calcolare il resto di 55^{23} rispetto alla divisione per 91.
(b) Calcolare l'esponente di decodifica E. In altre parole: determinare $E > 0$ tale che $(a^{23})^E \equiv a \pmod{91}$ per ogni a tale che $mcd(a, 91) = 1$.

Soluzione. (a) Cerchiamo il numero intero x tale che $0 \leq x < 91$ e $x \equiv 55^{23} \pmod{91}$. Dunque $\begin{cases} x \equiv 55^{23} \pmod 7 \\ x \equiv 55^{23} \pmod{13} \end{cases}$.
Riduciamo 55^{23} modulo 7: $55 \equiv -1 \pmod 7$. Quindi $55^{23} \equiv -1 \pmod 7$.
Ora riduciamo 55^{23} modulo 13: $55 \equiv 3 \pmod{13}$. Dunque $55^{23} \equiv 3^{23} \pmod{13}$. Ora, usando le nota conseguenza del Teorema di Fermat, dobbiamo ridurre 23 modulo $12 (= 13 - 1)$. Si ha che

$$12 \equiv -1 \equiv 11 \pmod{12}$$

Dunque $3^{23} \equiv 3^{-1} \pmod{13}$, dove con $3^{-1} \pmod{13}$ si intende l'inverso di 3 modulo 13. Poichè l'inverso di 3 modulo 13 è 9 (infatti $3 \cdot 9 = 27 \equiv 1 \pmod{13}$), si ha, in definitiva, che

$$55^{23} \equiv 9 \pmod{13}.$$

Alternativamente, si può calcolare $3^2 = 9$, $3^3 = 27 \equiv 1 \pmod{13}$. Dunque $3^{11} = (3^3)^2 3^2 = 1 \cdot 9 = 9 \pmod{13}$. Dunque dobbiamo risolvere il sistema $\begin{cases} x \equiv -1 \pmod 7 \\ x \equiv 9 \pmod{13} \end{cases}$. Si vede facilmente che la più piccola soluzione positiva, cioè il resto cercato, è $r = 48$.
(b) Bisogna risolvere la congruenza $23x \equiv 1 \pmod{72} (= 6 \cdot 12)$. Con l'algoritmo euclideo si trova che $x \equiv -25 \equiv 47 \pmod{72}$. Dunque l'esponente cercato è $E = 47$.

3. Sia $A = \{n \in \mathbf{Z} \mid \exists k \in \mathbf{Z} \text{ tale che } k^3 = n\}$. (a) Determinare una funzione biettiva $f : \mathbf{N} \to A$.
(b) Stabilire per quali dei seguenti insiemi X esiste una funzione biettiva $g : X \to A$ (N.B: non si richiede di esibire esplicitamente una tale funzione g):
(i) $X = \mathbf{Q} \times \mathbf{Q}$; (ii) $X = \{x \in \mathbf{R} \mid 0 < x < 1\}$; (iii) $X = \{n \in \mathbf{Z} \mid n < 12\}$.

Soluzione. Si noti che A è l'insieme dei cubi dei numeri interi. Una funzione biettiva $f : \mathbf{N} \to A$ è, ad esempio, $f(n) = \begin{cases} (\frac{n}{2})^3 & \text{se } n \text{ è pari} \\ (-\frac{n-1}{2})^3 & \text{se } n \text{ è dispari} \end{cases}$.
(b) (i) Si ha che $\mathbf{Q} \times \mathbf{Q}$ è numerabile, in quanto prodotto cartesiano di due insiemi numerabili, Quindi una funzione biettiva $f : \mathbf{Q} \times \mathbf{Q} \to A$ esiste.
(ii) L'intervallo reale $(0, 1)$ non è numerabile. Quindi non esiste nessuna funzione biettiva $g : (0, 1) \to A$.
(iii) L'insieme dei numeri interi minori di 12 è numerabile, in quanto sottosinsieme infinito di un insieme numerabile. Quindi una funzione biettiva $g : \{n \in \mathbf{Z} \mid n < 12\} \to A$ esiste.

4. Sia $X = \{a, b\}$ e si denoti $\mathcal{A} = \mathcal{P}(X) \times \mathcal{P}(X)$. Si considerino le relazioni R ed S su $\mathcal{A}$ definite come segue. Dati (A, B) e (C, D) in $\mathcal{A}$:
(i) $(A, B)\, R\, (C, D)$ se $A \cap B = C \cap D$, (ii) $(A, B)\, S\, (C, D)$ se $A \cap B \subseteq C \cap D$.
(a) Stabilire se R o S sono relazioni di equivalenza o relazioni d'ordine.
(b) Nel caso di relazione di equivalenza, determinare le classi di equivalenza.

Soluzione. (a) R è di equivalenza. Infatti:
- R è riflessiva, perchè $A \cap B = A \cap B$ per ogni (A, B) in $\mathcal{A}$.
- R è simmetrica, perchè se $A \cap B = C \cap D$ allora $C \cap D = A \cap B$.
- R è transitiva, perchè se $A \cap B = C \cap D$ e $C \cap D = E \cap F$ allora $A \cap B = E \cap F$.

S non è di equivalenza, perchè non è simmetrica. Per esempio:
$(\emptyset, \emptyset)\, S\, (\{a\}, \{a\})$ (perchè $\emptyset \cap \emptyset = \emptyset \subseteq \{a\} \cap \{a\} = \{a\}$), però $(\{a\}, \{a\})\ \not S (\emptyset, \emptyset)$ (perchè $\{a\} \cap \{a\} = \{a\}$ non è contenuto in $\emptyset \cap \emptyset = \emptyset$).

S non è una relazione d'ordine, perchè non è antisimmetrica. Ad esempio:
$(\emptyset, \emptyset)\, S\, (\emptyset, \{a\})$ (perchè $\emptyset \cap \emptyset = \emptyset \subseteq \emptyset \cap \{a\} = \emptyset$) e anche $(\emptyset, \{a\})\, S\, (\emptyset, \emptyset)$ (per lo stesso motivo), ma $(\emptyset, \emptyset) \neq (\emptyset, \{a\})$.

(b) Poichè R è una relazione di equivalenza, determiniamone le classi di equivalenza. Esse sono quattro, e precisamente:
(1) l'insieme delle coppie (A, B) tali che $A \cap B = \emptyset$:

$$\big\{(\emptyset, \emptyset), (\emptyset, \{a\}), (\emptyset, \{b\}), (\emptyset, \{a, b\}), (\{a\}, \emptyset), (\{b\}, \emptyset), (\{a, b\}, \emptyset), (\{a\}, \{b\}), (\{b\}, \{a\})\big\}.$$

(2) l'insieme delle coppie (A, B) tali che $A \cap B = \{a\}$:

$$\big\{(\{a\}, \{a\}), (\{a\}, \{a, b\}), (\{a, b\}, \{a\})\big\}$$

(3) l'insieme delle coppie (A, B) tali che $A \cap B = \{b\}$:

$$\big\{(\{b\}, \{b\}), (\{b\}, \{a, b\}), (\{a, b\}, \{b\})\big\}$$

(4) l'insieme delle coppie (A, B) tali che $A \cap B = \{a, b\}$:

$$\big\{(\{a, b\}, \{a, b\})\big\}.$$

5. In un'algebra di Boole si consideri l'operazione $x \oplus y = x'y + xy'$. (a) Stabilire se le funzioni booleane $F(x, y, z) = (xz) \oplus (y \oplus x')$ e $E(x, y, z) = \big((xz) \oplus y\big) \oplus x'$ sono uguali o no.
(b) Scrivere $F(x, y, z)$ come somma di tutte le sue implicanti prime.

Soluzione. (b) Scriviamo $F(x,y,z)$ come some di prodotti. Si ha $F(x,y,z) = (xz)'(y \oplus x') + (xz)(y \oplus x')' = (xz)'(yx + y'x') + xz(yx + y'x')' = (x' + z')(yx + y'x') + xz((x' + y')(x + y)) = x'y' + xyz' + x'y'z' + xy'z = x'y' + xyz' + xy'z$.
Aggiungendo il consenso di $x'y'$ e $xy'z$, cioè $y'z$, si trova

$$F(x,y,z) = x'y' + xyz' + y'z.$$

Questa è la somma delle implicanti prime di $F(x,y,z)$.

(a) Scrivendo $E(x,y,z)$ come somma di prodotti, facendo passaggi analoghi al punto (b), risulta $E(x,y,z) = .. = x'y' + xyz' + xy'z$. Dunque $E(x,y,z) = F(x,y,z)$.