Elementi di Algebra e Logica — Secondo Esonero — 22 febbraio 2007

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) $C = \{1, 2, 3, 5, 30\}$.

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, chiamiamolo 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: $2 \vee 5 = mcm(2, 5) = 10 \notin A$. $4 \wedge 6 = mcd(4, 6) = 2 \notin B$. $2 \vee 3 = mcm(2, 3) = 6 \notin C$.

2. Si consideri il reticolo $L = \mathcal{P}(\{0\}) \times \mathcal{P}(\{a, b\})$, ordinato mediante la relazione $(A, B) \leq (C, D)$ se $A \subseteq C$ e $B \subseteq D$. Si consideri anche il reticolo $M = \{1, 2, 3, 4, 9, 15, 60, 180\}$, ordinato mediante la divisibilità.
(a) Stabilire se L o M è isomorfo a $\mathcal{P}(\{a, b, c\})$ e, in tal caso, esibire esplicitamente un isomorfismo e determinare quanti sono gli isomorfismi.
(b) Stabilire (motivando) L è un'algebra di Boole o no. Stabilire (motivando) se M è un'algebra di Boole o no.

Soluzione. Innanzitutto è utile elencare esplicitamente gli elementi di L:

$$L = \{(\emptyset, \emptyset), (\emptyset, \{a\}), (\emptyset, \{b\}), (\emptyset, \{a, b\}), (\{0\}, \emptyset), (\{0\}, \{a\}), (\{0\}, \{b\}), (\{0\}, \{a, b\})$$

Si vede che L è isomorfo a $\mathcal{P}(a, b, c)$. Un isomorfismo è $f : L \to \mathcal{P}(\{a, b, c\})$, così definito: $f((\emptyset, \emptyset)) = \emptyset$, $f((\emptyset, \{a\})) = \{a\}$, $f((\emptyset, \{b\})) = \{b\}$, $f((\{0\}, \emptyset)) = \{c\}$, $f((\emptyset, \{a, b\})) = \{a, b\}$, $f((\{0\}, \{a\})) = \{a, c\}$, $f((\{0\}, \{b\})) = \{b, c\}$, $f((\{0\}, \{a, b\})) = \{a, b, c\}$. Gli isomorfismi devono mandare biettivamente gli atomi in atomi. Poichè gli atomi sono tre, ci sono $3! = 6$ modi di fare ciò. Dunque gli isomorfismi tra L e $\mathcal{P}(\{a, b, c\})$ sono sei.
Il reticolo M non è isomorfo a $\mathcal{P}(\{a, b, c\})$ (ad esempio, M ha solamente due atomi).
(b) L è un'algebra di Boole, perchè isomorfo a $\mathcal{P}(\{a, b, c\})$, che è un'algebra di Boole.
M non è un'algebra di Boole perchè, avendo otto elementi, per il Teorema di Rappresentazione, se fosse un'algebra di Boole, dovrebbe essere isomorfo a $\mathcal{P}(\{a, b, c\})$.

3. 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 r di 55^{23} rispetto alla divisione per 91.
(b) Stabilire (motivando) se si sarebbe potuto usare il messaggio $m' = 39$. Stabilire (motivando) se si sarebbe potuto usare l'esponente $D' = 27$.

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) NON si sarebbe potuto usare il messaggio $m' = 39$, perchè $mcd(39, 91) > 1$.
NON si sarebbe potuto usare l'esponente $D' = 27$ perché $mcd(27, 72) > 1$ (dove $72 = (7-1)(13-1)$).

4. (a) Continuando con il sistema RSA dell'esercizio precedente, 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 $mcd(a, 91) = 1$.
(b) Continuando con la notazione del punto (a) dell'esercizio precedente, decodificare il messaggio in codice r. In altre parole, verificare che $r^E \equiv 55 \pmod{91}$

Soluzione.
(a) 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 $E = 47$.
(b) Dobbiamo verificare che $48^{47} \equiv 55 \pmod{91}$. Per il Teorema cinese dei resti, è sufficiente verificare che: (i) $48^{47} \equiv 55 \pmod{7}$ e (ii) $48^{47} \equiv 55 \pmod{13}$.) Per fare cioò usiamo (dal primo esercizio), che $48 \equiv -1 \pmod{7}$ e $48 \equiv 9 \pmod{13}$.
(i) Poichè $55 \equiv -1 \pmod{7}$ e $48^{23} \equiv (-1)^{23} \pmod{13}$ la (i) è verificata.
(ii) Si ha che $55 \equiv 3 \pmod{13}$. Inoltre $48^{47} \equiv 9^{47} \equiv 9^{-1} \pmod{13}$ (dove, come sopra, con $9^{-1} \pmod{13}$ si intende l'inverso di 9 modulo 13. Come dall'esercizio precedente, tale inverso è 3. Dunque anche (ii) è verificata.

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 $E(x, y, z) = F(x, y, z)$.