

**ALGEBRA e LOGICA**  
**CdL in Ingegneria Informatica**  
*prof. Fabio GAVARINI*

*Sessione Estiva Anticipata 2014–2015 / Sessione Invernale 2013–2014 — II appello*  
Esame scritto del 23 Febbraio 2015 — COMPITO Q

.....

*N.B.: compilare il compito in modo sintetico ma **esauriente**, spiegando  
chiaramente quanto si fa, e scrivendo in corsivo con grafia leggibile.*

.....     $\mathbb{Q}$     .....

[1] Sia  $D_{250}$  l'insieme dei numeri naturali divisori di 250, dotato della relazione d'ordine di *divisibilità*, e sia  $\mathcal{P}(\{u, v, w\})$  l'insieme delle parti dell'insieme  $\{u, v, w\}$ , dotato della relazione d'ordine di *inclusione*; in particolare, entrambi sono insiemi ordinati.

(a)  $D_{250}$  è totalmente ordinato?  $\mathcal{P}(\{u, v, w\})$  è totalmente ordinato?

(b)  $D_{250}$  è limitato?  $\mathcal{P}(\{u, v, w\})$  è limitato? In entrambi i casi, se la risposta è negativa se ne spieghi il perché, se è affermativa si precisino i limiti.

(c)  $D_{250}$  è un *reticolo*?  $\mathcal{P}(\{u, v, w\})$  è un *reticolo*? Se sono entrambi reticoli, sono isomorfi l'uno all'altro?

(d)  $D_{250}$  è un'algebra di Boole?  $\mathcal{P}(\{u, v, w\})$  è un'algebra di Boole?

(e) Quali sono — se esistono — gli *atomi* di  $D_{250}$  e gli atomi di  $\mathcal{P}(\{u, v, w\})$ ?

[2] (a) Scrivere in base  $b' := \text{DIECI}$  il numero  $N$  che in base  $b := \text{CINQUE}$  è espresso dalla scrittura posizionale  $N := (4032)_b$ .

(b) Scrivere in base  $b := \text{CINQUE}$  il numero  $T$  che in base  $b' := \text{DIECI}$  è espresso dalla scrittura posizionale  $T := (387)_{b'}$ .

(c) Scrivere in base  $b' := \text{DIECI}$  il numero  $K$  che in base  $b'' = \text{DODICI}$ , tramite le dodici cifre (ordinate!) dell'insieme  $\{0, 1, 2, 3, \dots, 8, 9, \perp, \wedge\}$ , è espresso dalla scrittura posizionale  $K := (5\perp 7)_{b''}$ .

[3] Sia  $q \in \mathbb{Q}$ . Determinare — se esistono — tutte le successioni  $\underline{a}^{(q)} := \{a_n^{(q)}\}_{n \in \mathbb{N}} \in \mathbb{Q}^{\mathbb{N}}$  (dipendenti dal parametro  $q$ ), tali che

$$a_0^{(q)} = 2 - 5q \quad , \quad a_1^{(q)} = 5q - 4 \quad , \quad a_n^{(q)} = -4a_{n-1}^{(q)} - 3a_{n-2}^{(q)} \quad \forall n \geq 2 \quad .$$

[4] Determinare l'insieme di tutte le soluzioni del sistema di equazioni congruenziali

$$\circledast : \begin{cases} 138x \equiv -88 & (\text{mod } 10) \\ -65x \equiv 123 & (\text{mod } 7) \end{cases}$$

[5] Dati i due numeri interi  $a := 28$  e  $b := 70$ , calcolare  $\delta := \text{M.C.D.}(a, b)$ , calcolare  $\mu := \text{m.c.m.}(a, b)$ , e determinare una identità di Bézout per  $\text{M.C.D.}(a, b)$ .

[6] Si consideri il polinomio booleano  $Q(u, v, w)$ , nelle variabili  $u, v$  e  $w$ , dato da

$$Q(u, v, w) := (w \vee v'' \vee 0 \vee u')' \vee \left( (u' \vee (v \wedge 0' \wedge w''))' \wedge 1 \right)' \vee \\ \vee (u' \wedge w' \wedge 1 \wedge u) \vee \left( ((w' \vee 0 \vee u' \vee w') \wedge (u' \wedge 1 \wedge v''))' \vee w' \right)'$$

(a) Determinare la *forma normale disgiuntiva* di  $Q(u, v, w)$ .

(b) Determinare la *somma di tutti gli implicant primari* di  $Q(u, v, w)$ .

(c) Determinare una *forma minimale* di  $Q(u, v, w)$ .

— ★ —

## SOLUZIONI

[1] — (a) Un insieme ordinato  $(E; \preceq)$  è *totalmente* ordinato se per ogni  $e', e'' \in E$  si ha  $e' \preceq e''$  oppure  $e'' \preceq e'$  (in breve, “ $e'$  ed  $e''$  sono comparabili”). Nel caso in esame  $(D_{250}; |)$  non è totalmente ordinato, perché ad esempio si ha che per  $2, 5 \in D_{250}$  si verifica che  $2 \nmid 5$  (cioè “2 non divide 5”) e  $5 \nmid 2$  (cioè “5 non divide 2”). Analogamente,  $(\mathcal{P}(\{u, v, w\}); \subseteq)$  non è totalmente ordinato, perché ad esempio si ha che per  $\{u\}, \{v\} \in \mathcal{P}(\{u, v, w\})$  si verifica che  $\{u\} \not\subseteq \{v\}$  e  $\{v\} \not\subseteq \{u\}$ .

(b)  $D_{250}$  è limitato, con minimo  $\min(D_{250}) = 1$  e massimo  $\max(D_{250}) = 250$ . Analogamente anche  $\mathcal{P}(\{u, v, w\})$  è limitato, con minimo  $\min(\mathcal{P}(\{u, v, w\})) = \emptyset$  e massimo  $\max(\mathcal{P}(\{u, v, w\})) = \{u, v, w\}$ .

(c) Un insieme ordinato  $(E; \preceq)$  è un reticolo se per ogni  $e', e'' \in E$  esiste  $\inf(e', e'') \in E$  e  $\sup(e', e'') \in E$ . Nei casi in esame si ha che entrambi  $(D_{250}; |)$  e  $(\mathcal{P}(\{u, v, w\}); \subseteq)$  sono reticoli, in cui  $\inf(d', d'') = \text{M.C.D.}(d', d'')$  e  $\sup(d', d'') = \text{m.c.m.}(d', d'')$  per ogni  $d', d'' \in D_{250}$  mentre  $\inf(S', S'') = S' \cap S''$  e  $\sup(S', S'') = S' \cup S''$  per ogni  $S', S'' \in \mathcal{P}(\{u, v, w\})$ .

Infine, i due reticoli  $(D_{250}; |)$  e  $(\mathcal{P}(\{u, v, w\}); \subseteq)$  non sono isomorfi. Una possibile spiegazione è la seguente. Se i due reticoli fossero isomorfi, un qualunque isomorfismo da

$D_{250}$  a  $\mathcal{P}(\{u, v, w\})$  darebbe per restrizione una biiezione tra l'insieme degli atomi di  $D_{250}$  e l'insieme degli atomi di  $\mathcal{P}(\{u, v, w\})$ ; ma  $D_{250}$  ha esattamente *due* atomi — che sono 2 e 5 — mentre  $\mathcal{P}(\{u, v, w\})$  ha esattamente *tre* atomi — che sono i tre singoletti  $\{u\}$ ,  $\{v\}$  e  $\{w\}$ : quindi non ci può essere una biiezione tra i due insiemi di atomi (hanno cardinalità diverse...), e dunque i due reticoli considerati non sono isomorfi — sebbene abbiano la stessa cardinalità, precisamente  $|D_{250}| = 8 = |\mathcal{P}(\{u, v, w\})|$ .

(d) Ricordiamo che un'algebra di Boole è un reticolo limitato, distributivo e complementato. Ora, i reticoli  $D_{250}$  e  $\mathcal{P}(\{u, v, w\})$  sono entrambi limitati — vedasi (b) — e distributivi; però  $D_{250}$  *non* è complementato (perché, ad esempio, non esiste un complemento per 5) e quindi *non* è un'algebra di Boole, mentre invece  $\mathcal{P}(\{u, v, w\})$  è complementato (per ogni  $S \in \mathcal{P}(\{u, v, w\})$  come complemento in  $\mathcal{P}(\{u, v, w\})$  c'è il suo complementare  $\{u, v, w\} \setminus S$ ) e quindi è un'algebra di Boole.

N.B.: questo è anche un altro modo per provare che i due reticoli  $D_{250}$  e  $\mathcal{P}(\{u, v, w\})$  *non* sono isomorfi l'uno all'altro: infatti, se lo fossero allora sarebbero *entrambi* algebre di Boole oppure *entrambi* non lo sarebbero, e invece non è così (hanno proprietà opposte).

(e) Ricordiamo che in un insieme ordinato si dicono *atomi* gli elementi (se esistono...) che coprono il minimo. Nei casi in esame, gli atomi di  $D_{250}$  sono 2 e 5 — cioè gli unici fattori primi di 250 — mentre gli atomi di  $\mathcal{P}(\{u, v, w\})$  sono i tre singoletti  $\{u\}$ ,  $\{v\}$  e  $\{w\}$ .

- [2] — (a)  $N := (4032)_b = (517)_{b'}$  ;  
 (b)  $T := (387)_{b'} = (3022)_b$  ;  
 (c)  $K := (5 \perp 7)_{b''} = (859)_{b'}$  .

[3] — Il polinomio caratteristico associato alle successioni ricorsive cercate è della forma  $\Delta(x) = x^2 + 4x + 3$ , che ha radici  $r_+ = -1$  e  $r_- = -3$ ; pertanto le successioni cercate sono della forma  $\underline{a} = \{a_n = C_+ \cdot (-1)^n + C_- \cdot (-3)^n\}_{n \in \mathbb{N}}$ . Imponendo le condizioni iniziali si trova che dev'essere necessariamente  $C_+ = 1 - 5q$ ,  $C_- = 1$ : perciò esiste una e una sola successione del tipo richiesto, precisamente

$$\underline{a} = \{a_n = (1 - 5q) \cdot (-1)^n + 1 \cdot (-3)^n\}_{n \in \mathbb{N}}$$

- [4] —  $x \equiv 19 \equiv -16 \pmod{35}$ , o in altri termini  $x = 19 + 35z$ ,  $\forall z \in \mathbb{Z}$ .

- [5] — I numeri assegnati si fattorizzano univocamente in primi come segue:

$$a := 28 = 2^2 \cdot 7, \quad b := 70 = 2 \cdot 5 \cdot 7$$

Da questo otteniamo

$$\begin{aligned} \delta &:= \text{M.C.D.}(a, b) = \text{M.C.D.}(2^2 \cdot 7, 2 \cdot 5 \cdot 7) = 2 \cdot 7 = 14 \\ \mu &:= \text{m.c.m.}(a, b) = \text{m.c.m.}(2^2 \cdot 7, 2 \cdot 5 \cdot 7) = 2^2 \cdot 5 \cdot 7 = 140 \end{aligned}$$

Notiamo anche che basta ottenere uno dei due per poi ricavare l'altro tramite la relazione

$$\text{M.C.D.}(a, b) \cdot \text{m.c.m.}(a, b) = a \cdot b \tag{1}$$

Inoltre il M.C.D.( $a, b$ ) si può ottenere anche tramite l'algoritmo euclideo delle divisioni successive, che dà quanto segue:

$$\begin{aligned} 28 &= 70 \cdot 0 + 28 \\ 70 &= 28 \cdot 2 + \underline{14} \\ 28 &= 14 \cdot 2 + 0 \end{aligned} \tag{2}$$

L'ultimo resto non nullo è il M.C.D. cercato, dunque  $\text{M.C.D.}(28, 70) = 14$ . Inoltre, una volta che si sia calcolato in tal modo il M.C.D.(28,70) si può poi ottenere il m.c.m(28,70) tramite la formula in (1), per cui si trova

$$\text{m.c.m}(28, 70) = \frac{28 \cdot 70}{\text{M.C.D}(28, 70)} = \frac{1960}{14} = 140$$

Infine, dobbiamo trovare una identità di Bézout per  $\text{M.C.D.}(28, 70)$ , cioè un'espressione della forma  $\text{M.C.D.}(28, 70) = 28 \cdot r + 70 \cdot s$  per opportuni valori di  $r, s \in \mathbb{Z}$ . Una tale espressione si può ottenere invertendo le identità in (2): precisamente, così facendo si trova

$$\begin{aligned} 28 + 70 \cdot (-0) &= 28 \\ 70 + 28 \cdot (-2) &= \underline{14} \end{aligned}$$

da cui otteniamo

$$\begin{aligned} \text{M.C.D.}(28, 70) &= 14 = 70 + 28 \cdot (-2) = \\ &= 70 + (28 + 70 \cdot (-0)) \cdot (-2) = 28 \cdot (-2) + 70 \cdot 1 \end{aligned}$$

quindi una possibile identità di Bézout è

$$14 = 28 \cdot (-2) + 70 \cdot 1$$

in cui  $r = -2$  e  $s = 1$ .

- [6] — (a)  $F.N.D. = (u \wedge v \wedge w) \vee (u \wedge v' \wedge w) \vee (u \wedge v' \wedge w') \vee (u' \wedge v \wedge w)$   
 (c)  $s.t.i.p. = (u \wedge v') \vee (u \wedge w) \vee (v \wedge w)$   
 (d)  $f.m. = (u \wedge v') \vee (v \wedge w)$ , e questa è l'unica forma minimale possibile.

---

---