

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

*Sessione Estiva Anticipata 2014–2015 / Sessione Invernale 2013–2014 — I appello*

Esame scritto del 9 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] Determinare — se esistono — tutte le successioni  $\underline{a} := \{a_n\}_{n \in \mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$  tali che

$$a_0 = 9 \quad , \quad a_1 = 5 \quad , \quad a_n = -2a_{n-1} + 3a_{n-2} \quad \forall n \geq 2$$

e tutte le successioni  $\underline{b} := \{b_n\}_{n \in \mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$  tali che

$$b_0 = 1 \quad , \quad b_2 = 5 \quad , \quad b_3 = -7 \quad , \quad b_n = -2b_{n-1} + 3b_{n-2} \quad \forall n \geq 2 \quad .$$

[2] Calcolare la *Forma Normale Disgiuntiva* del polinomio booleano — nelle tre variabili  $u, v$  e  $w$  — dato da

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

[3] Sia  $D_{540}$  l'insieme dei numeri naturali divisori di 540, e si consideri in esso la relazione (d'ordine) di divisibilità, indicata con  $\delta$ , così che  $(D_{540}; \delta)$  è un insieme ordinato.

Sia inoltre  $D' := \{3, 27, 2, 4, 5, 6, 12, 135, 30\}$  il sottoinsieme di  $D_{540}$ , dotato della relazione d'ordine  $\delta'$  indotta da  $\delta$ .

(a)  $(D_{540}; \delta)$  è un *reticolo*?

(b)  $(D_{540}; \delta)$  è un'algebra di Boole?

(c) Quali sono — se esistono — gli *atomi* di  $(D_{540}; \delta)$ ?

(d) Quali sono — se esistono — gli elementi  $\vee$ -irriducibili di  $(D_{540}; \delta)$ ?

(e) Determinare (se esiste) una  $\vee$ -fattorizzazione non ridondante in elementi  $\vee$ -irriducibili per ciascuno degli elementi 90, 30, 60 in  $D_{540}$ .

(f) Determinare gli *elementi minimali* e gli *elementi massimali* di  $(D'; \delta')$ .

(g) Esiste un *minimo* in  $(D'; \delta')$ ? Se sì, qual è? Se no, perché non esiste?

(h) Esiste un *massimo* in  $(D'; \delta')$ ? Se sì, qual è? Se no, perché non esiste?

[4] Nell'insieme  $\mathbb{N}_+$  dei numeri naturali positivi si consideri la relazione  $\phi$  definita da

$$n' \phi n'' \iff \left| \{ p \in \{2, 7\} \mid p \text{ divide } n' \} \right| = \left| \{ q \in \{2, 7\} \mid q \text{ divide } n'' \} \right|$$

(a) Dimostrare che  $\phi$  è una relazione di *equivalenza*.

(b) Determinare la cardinalità dell'insieme quoziente  $\mathbb{N}_+ / \phi$ .

(c) Calcolare le classi di  $\phi$ -equivalenza  $[17]_\phi$ ,  $[70]_\phi$ ,  $[84]_\phi$ ,  $[35]_\phi$ ,  $[7]_\phi$  e  $[34]_\phi$ .

(d) Calcolare tutte le classi di  $\phi$ -equivalenza in  $\mathbb{N}_+$ .

[5] Calcolare il resto  $r$  del numero naturale  $3021^{55841}$  nella divisione euclidea per 14.

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

$$(*) : \begin{cases} -82x \equiv 238 & (\text{mod } 5) \\ 95x \equiv -64 & (\text{mod } 7) \end{cases}$$

— ★ —

## SOLUZIONI

[1] — (a) Il polinomio caratteristico associato alle successioni ricorsive cercate è della forma  $\Delta(x) = x^2 + 2x - 3$ , 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  $C_+ = 8$ ,  $C_- = 1$ : perciò esiste una e una sola successione del tipo richiesto, precisamente

$$\underline{a} = \{ a_n = 8 \cdot 1^n + 1 \cdot (-3)^n \}_{n \in \mathbb{N}}$$

(b) In questo caso le successioni cercate soddisfanno la stessa legge di ricorsività che in (a), in particolare il polinomio caratteristico è di nuovo  $\Delta(x) = x^2 + 2x - 3$ , sempre con radici  $r_+ = 1$  e  $r_- = -3$ ; dunque le successioni cercate (se esistono) sono ancora della forma  $\underline{b} = \{ b_n = \kappa_+ \cdot 1^n + \kappa_- \cdot (-3)^n \}_{n \in \mathbb{N}}$ . Quando poi si impongono le tre condizioni  $b_0 = 1$ ,  $b_2 = 5$  e  $b_3 = -7$  si richiede che i due coefficienti incogniti  $\kappa_+$  e  $\kappa_-$  siano soluzioni di un sistema di tre equazioni lineari (in tali incognite), precisamente

$$\begin{cases} \kappa_+ \cdot 1^0 + \kappa_- \cdot (-3)^0 = 1 \\ \kappa_+ \cdot 1^2 + \kappa_- \cdot (-3)^2 = 5 \\ \kappa_+ \cdot 1^3 + \kappa_- \cdot (-3)^3 = -7 \end{cases}, \quad \text{cioè} \quad \begin{cases} 1 \cdot \kappa_+ + 1 \cdot \kappa_- = 1 \\ 1 \cdot \kappa_+ + 9 \cdot \kappa_- = 5 \\ 1 \cdot \kappa_+ + (-27) \cdot \kappa_- = -7 \end{cases}$$

Tale sistema *non* ha soluzioni, perciò non esiste nessuna successione del tipo richiesto.

$$[2] \quad \text{---} \quad F.N.D. = (u \wedge v' \wedge w) \vee (u' \wedge v' \wedge w')$$

[3] — (a) Un insieme ordinato  $(E; \preceq)$  è un reticolo se per ogni  $e', e'' \in E$  esiste  $\inf(e', e'') \in E$  e  $\sup(e', e'') \in E$ . Nel caso in esame si ha che  $(D_{540}; |)$  è un reticolo, in cui  $\inf(d', d'') = M.C.D.(d', d'')$  e  $\sup(d', d'') = m.c.m.(d', d'')$  per ogni  $d', d'' \in D_{540}$ .

(b) Ricordiamo che un'algebra di Boole è un reticolo limitato, distributivo e complementato. Ora, il reticolo  $D_{540}$  è limitato — con  $\min(D_{540}) = 1$  e  $\max(D_{540}) = 540$  — e distributivo (come tutti i reticoli del tipo  $(D_n; |)$ ; però  $D_{540}$  non è complementato (perché, ad esempio, non esiste un complemento per 3, né uno per 9) e quindi non è un'algebra di Boole. Oppure, possiamo affermare che  $D_{540}$  non è algebra di Boole perché ha cardinalità

$$|D_{540}| = |D_{2^2 \cdot 3^3 \cdot 5}| = (2+1) \cdot (3+1) \cdot (1+1) = 3 \cdot 4 \cdot 2 \notin \{2^n \mid n \in \mathbb{N}\}$$

cioè una cardinalità finita che non potenza di 2: siccome sappiamo che ogni algebra di Boole finita ha necessariamente per cardinalità una potenza di 2 (per il Teorema di Stone) possiamo dedurre che  $D_{540}$  non è un'algebra di Boole.

(c) Ricordiamo che in un insieme ordinato si dicono *atomi* gli elementi (se esistono...) che coprono il minimo. Nel caso di  $D_{540}$  il minimo è 1, e gli atomi sono tutti e soli i fattori primi di 540, cioè sono 2, 3 e 5.

(d) Ricordiamo che in un reticolo del tipo  $(D_n; |)$  sono  $\vee$ -irriducibili tutti i divisori di  $n$  che siano della forma  $p^e$  con  $p$  primo (dunque  $p$  deve comparire nella fattorizzazione in primi di  $n$  con un esponente maggiore o uguale a  $e$ ). Nel caso di  $D_{540}$  allora gli elementi  $\vee$ -irriducibili sono esattamente

$$1, 2, 2^2 = 4, 3, 3^2 = 9, 3^3 = 27, 5.$$

$$(e) \quad 90 = 2 \vee 9 \vee 5, \quad 30 = 2 \vee 3 \vee 5, \quad 60 = 4 \vee 3 \vee 5$$

(f) Ricordiamo che in un insieme ordinato si dice *minimale* ogni elemento (se esiste...) per il quale non esista nessun altro elemento che ne sia (strettamente) minore; si dice invece *massimale* ogni elemento (se esiste...) per il quale non esista nessun altro elemento che ne sia (strettamente) maggiore.

Nel caso di  $D'$  i suoi elementi minimali sono 2, 3 e 5, mentre i suoi elementi massimali sono 12, 30 e 135.

(g) Ricordiamo che in un insieme ordinato si dice *minimo* un elemento (necessariamente unico, se esiste...) per il quale ogni altro elemento sia maggiore o uguale. In generale, esiste minimo se e soltanto se esso è l'unico elemento minimale dell'insieme ordinato considerato.

Nel caso di  $D'$  non esiste minimo, in quanto ci sono tre elementi minimali.

(h) Ricordiamo che in un insieme ordinato si dice *massimo* un elemento (necessariamente unico, se esiste...) per il quale ogni altro elemento sia minore o uguale. In generale, esiste massimo se e soltanto se esso è l'unico elemento massimale dell'insieme ordinato considerato.

Nel caso di  $D'$  non esiste massimo, in quanto ci sono tre elementi massimali.

[4] — (a) Si consideri la funzione  $\mathbb{N}_+ \longrightarrow \mathbb{N}$  definita da

$$f(n) := \left| \{ p \in \{2, 7\} \mid p \text{ divide } n \} \right|$$

Usando tale  $f$ , relazione  $\phi$  assegnata in  $\mathbb{N}_+$  è caratterizzata ( $\forall n', n'' \in \mathbb{N}_+$ ) da

$$n' \phi n'' \iff f(n') = f(n'') \quad (1)$$

Da questa caratterizzazione è facile verificare che la relazione  $\phi$  è riflessiva, transitiva e simmetrica, e dunque è una equivalenza.

(b) Ricordiamo che l'insieme quoziente  $\mathbb{N}_+ / \phi$  non è altro che l'insieme di tutte le classi di equivalenza di  $\phi$ . Usando la caratterizzazione di  $\phi$  data in (a), è chiaro che le classi di equivalenza sono esattamente una per ogni possibile valore della funzione  $f$ : tali possibili valori sono 0, 1 e 2, quindi le classi di  $\phi$ -equivalenza sono i sottoinsiemi

$$\begin{aligned} C_0 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 0 \} & \left( = f^{-1}(0) \right) \\ C_1 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 1 \} & \left( = f^{-1}(1) \right) \\ C_2 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 2 \} & \left( = f^{-1}(2) \right) \end{aligned}$$

in particolare sono in tutto *tre* classi. Dunque la cardinalità dell'insieme quoziente  $\mathbb{N}_+ / \phi$ , cioè il numero delle classi di equivalenza di  $\phi$ , è appunto tre.

(c) Ricordiamo che la classe di  $\phi$ -equivalenza  $[n_0]_\phi$  di un dato numero  $n_0 \in \mathbb{N}_+$  non è altro che il sottoinsieme  $[n_0]_\phi := \{ n \in \mathbb{N}_+ \mid n \phi n_0 \}$  di tutti gli elementi di  $\mathbb{N}_+$  che sono equivalenti a  $n_0$ . Per il primo dei casi in esame allora abbiamo

$$2 \nmid 17, \quad 7 \nmid 17 \implies f(17) := \left| \{ p \in \{2, 7\} \mid p \text{ divide } 17 \} \right| = |\emptyset| = 0$$

e quindi, usando la caratterizzazione di  $\phi$  data in (1), abbiamo

$$\begin{aligned} [17]_\phi &:= \{ n \in \mathbb{N}_+ \mid n \phi 17 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(17) = 0 \} = \\ &= \{ n \in \mathbb{N}_+ \mid 2 \nmid n, \quad 7 \nmid n \} = (\mathbb{N}_+ \setminus 2\mathbb{N}_+) \cap (\mathbb{N}_+ \setminus 7\mathbb{N}_+) = \mathbb{N}_+ \setminus (2\mathbb{N}_+ \cup 7\mathbb{N}_+) \end{aligned}$$

Analogamente si trova

$$2 \mid 70, \quad 7 \mid 70 \implies f(70) := \left| \{ p \in \{2, 7\} \mid p \text{ divide } 70 \} \right| = \left| \{2, 7\} \right| = 2$$

e quindi

$$\begin{aligned} [70]_\phi &:= \{ n \in \mathbb{N}_+ \mid n \phi 70 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(70) = 2 \} = \\ &= \{ n \in \mathbb{N}_+ \mid 2 \mid n, \quad 7 \mid n \} = 2\mathbb{N}_+ \cap 7\mathbb{N}_+ = \text{m.c.m.}(2, 7)\mathbb{N}_+ = 14\mathbb{N}_+ \end{aligned}$$

Poi

$$2 \mid 84, \quad 7 \mid 84 \implies f(84) := \left| \{ p \in \{2, 7\} \mid p \text{ divide } 84 \} \right| = \left| \{2, 7\} \right| = 2$$

e quindi come prima abbiamo di nuovo

$$[84]_\phi := \{ n \in \mathbb{N}_+ \mid n \phi 84 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(84) = 2 \} = 14\mathbb{N}_+$$

Allo stesso modo, si ha

$$2 \nmid 35, 7 \mid 35 \implies f(35) := \left| \{ p \in \{2, 7\} \mid p \text{ divide } 35 \} \right| = \left| \{7\} \right| = 1$$

e quindi

$$\begin{aligned} [35]_\phi &:= \{ n \in \mathbb{N}_+ \mid n \not\mid 35 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(35) = 1 \} = \\ &= \{ n \in \mathbb{N}_+ \mid 2 \mid n, 7 \nmid n \text{ oppure } 2 \nmid n, 7 \mid n \} = \\ &= \{ n \in \mathbb{N}_+ \mid 2 \mid n, 7 \nmid n \} \cup \{ n \in \mathbb{N}_+ \mid 2 \nmid n, 7 \mid n \} = (2\mathbb{N}_+ \setminus 7\mathbb{N}_+) \cup (7\mathbb{N}_+ \setminus 2\mathbb{N}_+) = \\ &= (2\mathbb{N}_+ \cup 7\mathbb{N}_+) \setminus (7\mathbb{N}_+ \cap 2\mathbb{N}_+) = 2\mathbb{N}_+ \oplus 7\mathbb{N}_+ \end{aligned}$$

come anche

$$2 \nmid 7, 7 \mid 7 \implies f(7) := \left| \{ p \in \{2, 7\} \mid p \text{ divide } 7 \} \right| = \left| \{7\} \right| = 1$$

da cui segue di nuovo

$$[7]_\phi := \{ n \in \mathbb{N}_+ \mid n \not\mid 7 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(7) = 1 \} = 2\mathbb{N}_+ \oplus 7\mathbb{N}_+$$

e allo stesso modo

$$2 \mid 34, 7 \nmid 34 \implies f(34) := \left| \{ p \in \{2, 7\} \mid p \text{ divide } 34 \} \right| = \left| \{2\} \right| = 1$$

da cui segue ancora una volta

$$[34]_\phi := \{ n \in \mathbb{N}_+ \mid n \not\mid 34 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(34) = 1 \} = 2\mathbb{N}_+ \oplus 7\mathbb{N}_+$$

(d) Abbiamo già descritto in (b) le classi di  $\phi$ -equivalenza, che sono i tre sottoinsiemi

$$\begin{aligned} C_0 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 0 \} & \left( = f^{-1}(0) \right) \\ C_1 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 1 \} & \left( = f^{-1}(1) \right) \\ C_2 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 2 \} & \left( = f^{-1}(2) \right) \end{aligned}$$

Gli esempi considerati in (c) hanno già permesso di trovare *tutti* e tre i casi possibili, cioè tutte e tre le classi in causa. Riassumendo, esse sono

$$\begin{aligned} C_0 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 0 \} = \{ n \in \mathbb{N}_+ \mid 2 \nmid n, 7 \nmid n \} = \mathbb{N}_+ \setminus (2\mathbb{N}_+ \cup 7\mathbb{N}_+) \\ C_1 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 1 \} = \{ n \in \mathbb{N}_+ \mid 2 \mid n, 7 \nmid n \text{ oppure } 2 \nmid n, 7 \mid n \} = 2\mathbb{N}_+ \oplus 7\mathbb{N}_+ \\ C_2 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 2 \} = \{ n \in \mathbb{N}_+ \mid 2 \mid n, 7 \mid n \} = 2\mathbb{N}_+ \cap 7\mathbb{N}_+ = 14\mathbb{N}_+ \end{aligned}$$

[5] — Il resto cercato è l'unico  $r \in \mathbb{N}$  tale che

$$0 \leq r \leq 13 \quad \text{e} \quad 3021^{55841} \equiv r \pmod{14}$$

Queste condizioni poi equivalgono anche a

$$0 \leq r \leq 13 \quad \text{e} \quad \overline{3021^{55841}} = \bar{r} \in \mathbb{Z}_{14}$$

Ora, notiamo prima di tutto che  $\overline{3021^{55841}} = \overline{3021}^{55841}$  in  $\mathbb{Z}_{14}$ ; inoltre abbiamo che  $3021 \equiv 11 \pmod{14}$ , quindi  $\overline{3021} = \overline{11}$  in  $\mathbb{Z}_{14}$ , e così anche

$$\overline{3021^{55841}} = \overline{3021}^{55841} = \overline{11}^{55841} \quad \text{in} \quad \mathbb{Z}_{14}.$$

A questo punto, osserviamo che  $\text{M.C.D.}(11, 14) = 1$ ; allora si può applicare il Teorema di Eulero, che ci assicura che  $11^{\varphi(14)} \equiv 1 \pmod{14}$ , cioè  $\overline{11}^{\varphi(14)} = \bar{1}$  nell'anello  $\mathbb{Z}_{14}$ : qui  $\varphi$  è la funzione di Eulero, per cui abbiamo

$$\varphi(14) = \varphi(7 \cdot 2) = \varphi(7) \cdot \varphi(2) = (7-1) \cdot (2-1) = 6 \cdot 1 = 6$$

e dunque  $\overline{11}^{\varphi(14)} = \bar{1}$  si legge  $\overline{11}^6 = \bar{1}$ . Facciamo adesso la divisione con resto di 55841 per  $\varphi(14) = 6$ : troviamo  $55841 = 6 \cdot q + 5$  per un certo quoziente  $q$ ; in altre parole, abbiamo  $55841 \equiv 5 \pmod{6}$ . Allora

$$\overline{11}^{55841} = \overline{11}^{6 \cdot q + 5} = \left(\overline{11}^6\right)^q \cdot \overline{11}^5 = \left(\bar{1}^6\right)^q \cdot \overline{11}^5 = \overline{11}^5$$

e dunque ci basta calcolare  $\overline{11}^5$  in  $\mathbb{Z}_{14}$ . Osservando che  $\overline{11} = \overline{-3}$  in  $\mathbb{Z}_{14}$ , con un calcolo diretto otteniamo

$$\overline{11}^5 = (\overline{-3})^5 = (\overline{-3})^3 \cdot (\overline{-3})^2 = (\overline{-27}) \cdot \bar{9} = \bar{1} \cdot \bar{9} = \bar{9} \in \mathbb{Z}_{14}$$

Quindi, ricapitolando tutto, abbiamo

$$\overline{3021^{55841}} = \overline{3021}^{55841} = \overline{11}^{55841} = \overline{11}^5 = \bar{9} \in \mathbb{Z}_{14}$$

con  $0 \leq 9 \leq 13$ ; pertanto il resto cercato è  $r = 9$ .

[6] —  $x \equiv 26 \equiv -9 \pmod{35}$ , o in altri termini  $x = 26 + 35z$ ,  $\forall z \in \mathbb{Z}$ .