

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 R

.....

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

..... R

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

$$a_0 = 3 \quad , \quad a_1 = -1 \quad , \quad a_n = a_{n-1} + 6 a_{n-2} \quad \forall \quad n \geq 2$$

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

$$b_0 = 4 \quad , \quad b_2 = 21 \quad , \quad b_3 = 3 \quad , \quad b_n = b_{n-1} + 6 b_{n-2} \quad \forall \quad n \geq 2 \quad .$$

[2] Calcolare la *Forma Normale Disgiuntiva* del polinomio booleano — nelle tre variabili h, k e ℓ — dato da

$$R(h, k, \ell) := \left(\ell \vee \left((h'' \vee k' \vee h) \wedge (h \wedge 0' \wedge k')' \right)' \vee 0 \right)' \vee \\ \vee \left(((\ell' \vee h' \vee \ell') \vee (h' \wedge 1 \wedge \ell''))' \right)' \wedge k')$$

[3] Sia D_{360} l'insieme dei numeri naturali divisori di 360, e si consideri in esso la relazione (d'ordine) di divisibilità, indicata con δ , così che $(D_{360}; \delta)$ è un insieme ordinato.

Sia inoltre $D' := \{2, 8, 3, 9, 5, 10, 18, 40, 30\}$ il sottoinsieme di D_{360} , dotato della relazione d'ordine δ' indotta da δ .

(a) $(D_{360}; \delta)$ è un *reticolo*?

(b) $(D_{360}; \delta)$ è un'algebra di Boole?

(c) Quali sono — se esistono — gli *atomi* di $(D_{360}; \delta)$?

(d) Quali sono — se esistono — gli elementi \vee -irriducibili di $(D_{360}; \delta)$?

(e) Determinare (se esiste) una \vee -fattorizzazione non ridondante in elementi \vee -irriducibili per ciascuno degli elementi 60, 30, 180 in D_{360} .

(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 ψ definita da

$$n' \psi n'' \iff \left| \{ p \in \{3, 7\} \mid p \text{ divide } n' \} \right| = \left| \{ q \in \{3, 7\} \mid q \text{ divide } n'' \} \right|$$

(a) Dimostrare che ψ è una relazione di *equivalenza*.

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

(c) Calcolare le classi di ψ -equivalenza $[17]_\psi$, $[42]_\psi$, $[126]_\psi$, $[15]_\psi$, $[3]_\psi$ e $[77]_\psi$.

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

[5] Calcolare il resto r del numero naturale 2769^{55121} nella divisione euclidea per 14.

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

$$(*) : \begin{cases} 89x \equiv 64 & (\text{mod } 7) \\ -92x \equiv 217 & (\text{mod } 5) \end{cases}$$

— ★ —

SOLUZIONI

[1] — (a) Il polinomio caratteristico associato alle successioni ricorsive cercate è della forma $\Delta(x) = x^2 - x - 6$, che ha radici $r_+ = 3$ e $r_- = -2$; pertanto le successioni cercate sono della forma $\underline{a} = \{ a_n = C_+ \cdot 3^n + C_- \cdot (-2)^n \}_{n \in \mathbb{N}}$. Imponendo le condizioni iniziali si trova che dev'essere necessariamente $C_+ = 1$, $C_- = 2$: perciò esiste una e una sola successione del tipo richiesto, precisamente

$$\underline{a} = \{ a_n = 1 \cdot 3^n + 2 \cdot (-2)^n \}_{n \in \mathbb{N}}$$

(b) In questo caso le successioni cercate soddisfanno la stessa legge di ricorsività che in (a), in particolare il polinomio caratteristico è di nuovo $\Delta(x) = x^2 - x - 6$, sempre con radici $r_+ = 3$ e $r_- = -2$; dunque le successioni cercate (se esistono) sono ancora della forma $\underline{b} = \{ b_n = \kappa_+ \cdot 3^n + \kappa_- \cdot (-2)^n \}_{n \in \mathbb{N}}$. Quando poi si impongono le tre condizioni $b_0 = 4$, $b_2 = 21$ e $b_3 = 3$ si richiede che i due coefficienti incogniti κ_+ e κ_- siano soluzioni di un sistema di tre equazioni lineari (in tali incognite), precisamente

$$\begin{cases} \kappa_+ \cdot 3^0 + \kappa_- \cdot (-2)^0 = 4 \\ \kappa_+ \cdot 3^2 + \kappa_- \cdot (-2)^2 = 21 \\ \kappa_+ \cdot 3^3 + \kappa_- \cdot (-2)^3 = 3 \end{cases}, \quad \text{cioè} \quad \begin{cases} 1 \cdot \kappa_+ + 1 \cdot \kappa_- = 4 \\ 9 \cdot \kappa_+ + 4 \cdot \kappa_- = 21 \\ 27 \cdot \kappa_+ + (-8) \cdot \kappa_- = 3 \end{cases}$$

Tale sistema ha una e una sola soluzione, precisamente $\kappa_+ = 1$, $\kappa_- = 3$: perciò esiste una e una sola successione del tipo richiesto, che è

$$\underline{b} = \{ b_n = 1 \cdot 3^n + 3 \cdot (-2)^n \}_{n \in \mathbb{N}}$$

$$[2] \quad \text{---} \quad F.N.D. = (h \wedge k' \wedge \ell') \vee (h' \wedge k \wedge \ell')$$

[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 $(D_{360}; |)$ è un reticolo, in cui $\inf(d', d'') = M.C.D.(d', d'')$ e $\sup(d', d'') = m.c.m.(d', d'')$ per ogni $d', d'' \in D_{360}$.

(b) Ricordiamo che un'algebra di Boole è un reticolo limitato, distributivo e complementato. Ora, il reticolo D_{360} è limitato — con $\min(D_{360}) = 1$ e $\max(D_{360}) = 360$ — e distributivo (come tutti i reticoli del tipo $(D_n; |)$; però D_{360} non è complementato (perché, ad esempio, non esiste un complemento per 2, né uno per 4) e quindi non è un'algebra di Boole. Oppure, possiamo affermare che D_{360} non è algebra di Boole perché ha cardinalità

$$|D_{360}| = |D_{2^3 \cdot 3^2 \cdot 5}| = (3+1) \cdot (2+1) \cdot (1+1) = 4 \cdot 3 \cdot 2 \notin \{2^n \mid n \in \mathbb{N}\}$$

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_{360} 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_{360} il minimo è 1, e gli atomi sono tutti e soli i fattori primi di 360, 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_{360} allora gli elementi \vee -irriducibili sono esattamente

$$1, 2, 2^2 = 4, 2^3 = 8, 3, 3^2 = 9, 5.$$

$$(e) \quad 60 = 4 \vee 3 \vee 5, \quad 30 = 2 \vee 3 \vee 5, \quad 180 = 4 \vee 9 \vee 5$$

(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 18, 30 e 40.

(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

$$f(n) := \left| \{ p \in \{3, 7\} \mid p \text{ divide } n \} \right|$$

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

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

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

(b) Ricordiamo che l'insieme quoziente \mathbb{N}_+ / ψ non è altro che l'insieme di tutte le classi di equivalenza di ψ . Usando la caratterizzazione di ψ 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 ψ -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}_+ / ψ , cioè il numero delle classi di equivalenza di ψ , è appunto tre.

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

$$3 \nmid 17, 7 \nmid 17 \implies f(17) := \left| \{ p \in \{3, 7\} \mid p \text{ divide } 17 \} \right| = |\emptyset| = 0$$

e quindi, usando la caratterizzazione di ψ data in (1), abbiamo

$$\begin{aligned} [17]_\psi &:= \{ n \in \mathbb{N}_+ \mid n \psi 17 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(17) = 0 \} = \\ &= \{ n \in \mathbb{N}_+ \mid 3 \nmid n, 7 \nmid n \} = (\mathbb{N}_+ \setminus 3\mathbb{N}_+) \cap (\mathbb{N}_+ \setminus 7\mathbb{N}_+) = \mathbb{N}_+ \setminus (3\mathbb{N}_+ \cup 7\mathbb{N}_+) \end{aligned}$$

Analogamente si trova

$$3 \mid 42, 7 \mid 42 \implies f(42) := \left| \{ p \in \{3, 7\} \mid p \text{ divide } 42 \} \right| = \left| \{3, 7\} \right| = 2$$

e quindi

$$\begin{aligned} [42]_\psi &:= \{ n \in \mathbb{N}_+ \mid n \psi 42 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(42) = 2 \} = \\ &= \{ n \in \mathbb{N}_+ \mid 3 \mid n, 7 \mid n \} = 3\mathbb{N}_+ \cap 7\mathbb{N}_+ = \text{m.c.m.}(3, 7)\mathbb{N}_+ = 21\mathbb{N}_+ \end{aligned}$$

Poi

$$3 \mid 126, 7 \mid 126 \implies f(126) := \left| \{ p \in \{3, 7\} \mid p \text{ divide } 126 \} \right| = \left| \{3, 7\} \right| = 2$$

e quindi come prima abbiamo di nuovo

$$[126]_\psi := \{ n \in \mathbb{N}_+ \mid n \psi 126 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(126) = 2 \} = 21\mathbb{N}_+$$

Allo stesso modo, si ha

$$3 \mid 15, \quad 7 \nmid 15 \quad \Longrightarrow \quad f(15) := \left| \{ p \in \{3, 7\} \mid p \text{ divide } 15 \} \right| = \left| \{3\} \right| = 1$$

e quindi

$$\begin{aligned} [15]_\psi &:= \{ n \in \mathbb{N}_+ \mid n \psi 15 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(15) = 1 \} = \\ &= \{ n \in \mathbb{N}_+ \mid 3 \mid n, \quad 7 \nmid n \text{ oppure } 3 \nmid n, \quad 7 \mid n \} = \\ &= \{ n \in \mathbb{N}_+ \mid 3 \mid n, \quad 7 \nmid n \} \cup \{ n \in \mathbb{N}_+ \mid 3 \nmid n, \quad 7 \mid n \} = (3\mathbb{N}_+ \setminus 7\mathbb{N}_+) \cup (7\mathbb{N}_+ \setminus 3\mathbb{N}_+) = \\ &= (3\mathbb{N}_+ \cup 7\mathbb{N}_+) \setminus (7\mathbb{N}_+ \cap 3\mathbb{N}_+) = 3\mathbb{N}_+ \oplus 7\mathbb{N}_+ \end{aligned}$$

come anche

$$3 \mid 3, \quad 7 \nmid 3 \quad \Longrightarrow \quad f(3) := \left| \{ p \in \{3, 7\} \mid p \text{ divide } 3 \} \right| = \left| \{3\} \right| = 1$$

da cui segue di nuovo

$$[3]_\psi := \{ n \in \mathbb{N}_+ \mid n \psi 3 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(3) = 1 \} = 3\mathbb{N}_+ \oplus 7\mathbb{N}_+$$

e allo stesso modo

$$3 \nmid 77, \quad 7 \mid 77 \quad \Longrightarrow \quad f(77) := \left| \{ p \in \{3, 7\} \mid p \text{ divide } 77 \} \right| = \left| \{7\} \right| = 1$$

da cui segue ancora una volta

$$[77]_\psi := \{ n \in \mathbb{N}_+ \mid n \psi 77 \} = \{ n \in \mathbb{N}_+ \mid f(n) = f(77) = 1 \} = 3\mathbb{N}_+ \oplus 7\mathbb{N}_+$$

(d) Abbiamo già descritto in (b) le classi di ψ -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

$$\begin{aligned} C_0 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 0 \} = \{ n \in \mathbb{N}_+ \mid 3 \nmid n, \quad 7 \nmid n \} = \mathbb{N}_+ \setminus (3\mathbb{N}_+ \cup 7\mathbb{N}_+) \\ C_1 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 1 \} = \{ n \in \mathbb{N}_+ \mid 3 \mid n, \quad 7 \nmid n \text{ oppure } 3 \nmid n, \quad 7 \mid n \} = 3\mathbb{N}_+ \oplus 7\mathbb{N}_+ \\ C_2 &:= \{ n \in \mathbb{N}_+ \mid f(n) = 2 \} = \{ n \in \mathbb{N}_+ \mid 3 \mid n, \quad 7 \mid n \} = 3\mathbb{N}_+ \cap 7\mathbb{N}_+ = 21\mathbb{N}_+ \end{aligned}$$

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

$$0 \leq r \leq 13 \quad \text{e} \quad 2769^{55121} \equiv r \pmod{14}$$

Queste condizioni poi equivalgono anche a

$$0 \leq r \leq 13 \quad \text{e} \quad \overline{2769^{55121}} = \bar{r} \in \mathbb{Z}_{14}$$

Ora, notiamo prima di tutto che $\overline{2769^{55121}} = \overline{2769}^{55121}$ in \mathbb{Z}_{14} ; inoltre abbiamo che $2769 \equiv 11 \pmod{14}$, quindi $\overline{2769} = \overline{11}$ in \mathbb{Z}_{14} , e così anche

$$\overline{2769^{55121}} = \overline{2769}^{55121} = \overline{11}^{55121} \quad \text{in} \quad \mathbb{Z}_{14}.$$

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 φ 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 55121 per $\varphi(14) = 6$: troviamo $55121 = 6 \cdot q + 5$ per un certo quoziente q ; in altre parole, abbiamo $55121 \equiv 5 \pmod{6}$. Allora

$$\overline{11}^{55121} = \overline{11}^{6 \cdot q + 5} = \left(\overline{11}^6\right)^q \cdot \overline{11}^5 = \left(\bar{1}^6\right)^q \cdot \overline{11}^5 = \overline{11}^5$$

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

$$\overline{2769^{55121}} = \overline{2769}^{55121} = \overline{11}^{55121} = \overline{11}^5 = \bar{9} \in \mathbb{Z}_{14}$$

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

[6] — $x \equiv 24 \equiv -11 \pmod{35}$, o in altri termini $x = 24 + 35z$, $\forall z \in \mathbb{Z}$.