ALGEBRA e LOGICA
CdL in Ingegneria Informatica

prof. Fabio GAVARINI

a.a. 2013–2014 — Sessione Autunnale, II appello

Esame scritto del 18 Settembre 2014

. . . .

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

. . . . ⋆ . . . .

[1] Determinare tutti i valori di $x \in \mathbb{Z}$ che siano soluzioni *simultaneamente* delle due equazioni congruenziali seguenti:

$$\circledast : \begin{cases} [381]_{15}\,[x]_{15} \;=\; -[132]_{15} & \text{in } \mathbb{Z}_{15} \\ [95]_7\,[x]_7 \;=\; [47]_7 & \text{in } \mathbb{Z}_7 \end{cases}$$

[2] Sia $D^*_{140} := D_{140} \setminus \{1\}$ l'insieme dei numeri naturali divisori di 140 privato dell'elemento 1. Si consideri in D^*_{140} la relazione (d'ordine) di divisibilità, indicata con δ, così che $\big(D^*_{140}\,;\delta\big)$ è un insieme ordinato.

(a) $\big(D^*_{140}\,;\delta\big)$ è *totalmente* ordinato?

(b) $\big(D^*_{140}\,;\delta\big)$ è un reticolo?

(c) Quali sono gli elementi *massimali* in $\big(D^*_{140}\,;\delta\big)$?

(d) Esiste un *massimo* in $\big(D^*_{140}\,;\delta\big)$? Se sì, qual è? Se no, perché non esiste?

(e) Quali sono gli elementi *minimali* in $\big(D^*_{140}\,;\delta\big)$?

(f) Esiste un *minimo* in $\big(D^*_{140}\,;\delta\big)$? Se sì, qual è? Se no, perché non esiste?

[3] Si considerino i polinomio booleani $h(x,y,z)$ ed $\ell(x,y,z)$, nelle variabili x, y e z, dati da

$$h(x,y,z) \;:=\; \Big(y' \vee \big(z' \wedge 1 \wedge x'\big)'\Big)' \vee \Big(\big(\big(y' \wedge z\big) \vee \big(z \wedge 1 \wedge x'\big)\big) \wedge \big(z' \vee y\big)'\Big)$$

$$\ell(x,y,z) \;:=\; \Big(x \vee \big(\big(y' \wedge z\big)' \wedge \big(z \vee y'\big)\big) \vee 0\Big)' \vee \Big(\big(y' \wedge z\big) \wedge \big(x' \vee y\big)'\Big)$$

(a) Dimostrare che $h \sim \ell$, cioè i due polinomi sono equivalenti.

(b) Determinare la *forma normale disgiuntiva* del polinomio h.

(c) Determinare la *forma normale disgiuntiva* del polinomio ℓ.

(continua...)

[4] *(a)* Dimostrare che per ogni $n \in \mathbb{N}$ il numero
$$C_n \;:=\; 5 \cdot 2^{1+3\,n} \;-\; 6^n \cdot 4 \cdot (-1)^{n^2+1}$$
è divisibile per 7.

(b) Calcolare il resto di B^E nella divisione per 12 per i valori

(b.1) $\quad B := 4517 \;, \quad E := 1895 \;,$

(b.2) $\quad B := 4515 \;, \quad E := 96 \;.$

[5] *(a)* Determinare tutte le successioni reali $\underline{a} := \big\{a_n\big\}_{n\in\mathbb{N}} \in \mathbb{R}^{\mathbb{N}}$ tali che
$$a_0 \;=\; 4 \quad , \quad a_1 \;=\; -1 \quad , \qquad a_n \;=\; a_{n-1} + 2\,a_{n-2} \qquad \forall\;\; n \geq 2 \;\; .$$

(b) Per ciascuna delle successioni trovate al punto *(a)*, calcolare il valore a_3.

— ⋆ —

SOLUZIONI

[1] — $\quad x \equiv 3 \pmod{35}$, o in altri termini $\quad x \;=\; 3 + 35\,z\,,\;\; \forall\; z \in \mathbb{Z}$.

[2] — *(a)* No, ad esempio perché non sono comparabili — per la relazione d'ordine δ — i due elementi 2 e 5, in quanto $2 \not| \, 5$ (cioè "2 non divide 5") e $5 \not| \, 2$ (cioè "5 non divide 2").

(b) No, ad esempio perché non esiste $\inf(2,5)$.

(c) Esiste un unico elemento massimale (cioè tale che nessun altro elemento sia pi'u grande di lui), ed è 140.

(d) Dato che esiste un unico elemento massimale, in questo caso 140, esso 'e anche il massimo.

(e) Gli elementi minimali (cioè tali che nessun altro elemento sia pi'u piccolo) sono 2, 5 e 7.

(f) Dato che esiste più di un elemento minimale, necessariamente non esiste un minimo.

[3] — Le F.N.D. di $h(x,y,z)$ e $\ell(x,y,z)$ sono date entrambe da
$$(\,x \wedge y' \wedge z\,) \vee \big(x' \wedge y \wedge z'\big) \vee \big(x' \wedge y' \wedge z\big)$$
Poiché coincidono, ne segue anche che h ed ℓ sono equivalenti.

[4] — *(a)* Dimostrare che C_n è divisibile per 7 (per ogni $\in \mathbb{N}$) equivale a dimostrare che $C_n \equiv 0 \pmod{7}$ (per ogni $n \in \mathbb{N}$). Questo si può fare per induzione su n.

<u>Base dell'induzione $(n=0)$</u>: il calcolo esplicito dà

$$C_0 \;:=\; 5\cdot 2^{1+3\cdot 0} \;-\; 6^0\cdot 4\cdot (-1)^{0^2+1} \;=\; 5\cdot 2 \;-\; 1\cdot 4\cdot(-1) \;=\; 10+4 \;=\; 14$$

dunque $C_0 = 14$, che è congruente a 0 modulo 7, cioè è divisibile per 7.

<u>Passo induttivo $(n \Longrightarrow n+1)$</u>: dato un qualsiasi $n\in\mathbb{N}$, facciamo l'ipotesi induttiva che $C_n \equiv 0 \pmod{7}$, e dimostriamo che allora $C_{n+1} \equiv 0 \pmod{7}$. Il calcolo esplicito dà

$$\begin{aligned} C_{n+1} \;:=\; & 5\cdot 2^{1+3\cdot(n+1)} \;-\; 6^{n+1}\cdot 4\cdot (-1)^{(n+1)^2+1} \;= \\ =\; & 5\cdot 2^{1+3\,n}\cdot 2^3 \;-\; 6^n\cdot 6\cdot 4\cdot (-1)^{n^2+1}\cdot (-1)^{2n+1} \;\overset{\circledast}{\equiv} \\ & \overset{\circledast}{\equiv}\; 5\cdot 2^{1+3\,n}\cdot 1 \;-\; 6^n\cdot(-1)\cdot 4\cdot(-1)^{n^2+1} \;= \\ & =\; 5\cdot 2^{1+3\,n} \;-\; 6^n\cdot 4\cdot(-1)^{n^2+1}\cdot(-1)^{2n+1} \;=\; C_n \end{aligned}$$

dove la congruenza $\overset{\circledast}{\equiv}$ è dovuta al fatto che

$$2^3 = 8 \equiv 1 \pmod{7} \qquad \text{e} \qquad 6 \equiv -1 \pmod{7}$$

e poi la penultima uguaglianza al fatto che $(-1)\cdot(-1)^{2n+1} = 1$ per ogni n. Allora $C_{n+1} \equiv C_n \pmod{7}$ e per ipotesi induttiva si ha $C_n \equiv 0 \pmod{7}$, quindi per transitività segue anche che $C_{n+1} \equiv 0 \pmod{7}$.

(b) Sia per *(b.1)* che per *(b.2)* si tratta di trovare l'unico intero r compreso tra 0 e 11 (inclusi) tale che $\overline{B^E} = \overline{r}$ in $\mathbb{Z}_{12}$. Inoltre, osserviamo che nell'anello $\mathbb{Z}_{12}$ si ha $\overline{B^E} = \overline{B}^{\,E}$.

Nel caso *(b.1)* si ha $\overline{B} = \overline{4517} = \overline{5}$ in $\mathbb{Z}_{12}$, quindi $\overline{B^E} = \overline{B}^{\,E} = \overline{4517}^{\,1895} = \overline{5}^{\,1895}$. Ora osserviamo che M.C.D.$(5,12) = 1$, e quindi per il Teorema di Fermat si ha $5^{\varphi(12)} \equiv 1 \pmod{12}$, cioè $\overline{5}^{\,\varphi(12)} = \overline{1}$ nell'anello $\mathbb{Z}_{12}$. Qui φ indica la funzione di Eulero, per la quale abbiamo $\varphi(12) = \varphi\big(2^2 3\big) = 2^{2-1}\,(2-1)\,(3-1) = 4$. Pertanto abbiamo $\overline{5}^{\,4} = \overline{1}$ in $\mathbb{Z}_{12}$.

A questo punto osserviamo che $1895 = 4\cdot q + 1$ (e non è necessario sapere il quoziente esatto in questa divisione per 4, basta conoscere il resto...) per cui otteniamo

$$\overline{B^E} \;=\; \overline{4517}^{\,1895} \;=\; \overline{5}^{\,1895} \;=\; \overline{5}^{\,4\cdot q+1} \;=\; \Big(\overline{5}^{\,4}\Big)^{q}\cdot\overline{5}^{\,1} \;=\; \overline{1}^{\,q}\cdot\overline{5}^{\,1} \;=\; \overline{5}$$

e concludiamo che il resto cercato è $r_1 = 5$.

In alternativa (anche senza sapere il Teorema di Fermat...), il calcolo diretto dà $\overline{5}^{\,\varphi(12)} = \overline{25} = \overline{1}$ in $\mathbb{Z}_{12}$: allora dividendo l'esponente 1895 per 2 abbiamo $1895 = 2\cdot k + 1$ da cui otteniamo

$$\overline{B^E} \;=\; \overline{4517}^{\,1895} \;=\; \overline{5}^{\,1895} \;=\; \overline{5}^{\,2\cdot k+1} \;=\; \Big(\overline{5}^{\,2}\Big)^{k}\cdot\overline{5}^{\,1} \;=\; \overline{1}^{\,k}\cdot\overline{5}^{\,1} \;=\; \overline{5}$$

e concludiamo comunque che il resto cercato è $r_1 = 5$.

Nel caso *(b.2)* si ha $\overline{B} = \overline{4515} = \overline{3}$ in $\mathbb{Z}_{12}$, quindi $\overline{B^E} = \overline{B}^{\,E} = \overline{4515}^{\,96} = \overline{3}^{\,96}$. Adesso si ha M.C.D.$(3,12) = 3 \neq 1$, quindi NON si può applicare il Teorema di

Fermat! Tuttavia il calcolo diretto delle prime potenze di $\overline{3}$ ci porta a trovare che $\overline{3}^{\,3} = \overline{27} = \overline{3}$ in $\mathbb{Z}_{12}$. A questo punto osserviamo che se $E = 3 \cdot q' + r'$ allora

$$\overline{3}^{\,E} = \overline{3}^{\,3 \cdot q' + r'} = \left(\overline{3}^{\,3}\right)^{q'} \cdot \overline{3}^{\,r'} = \overline{3}^{\,q'} \cdot \overline{3}^{\,r'} = \overline{3}^{\,q'} = \overline{3}^{\,E'} \tag{1}$$

e così $\overline{3}^{\,E} = \overline{3}^{\,E'}$ che è una semplificazione perché la potenza iniziale di $\overline{3}$ è stata uguagliata ad una analoga potenza (la base è la stessa) con esponente $E' := q' + r'$ *più piccolo* dell'esponente iniziale $E := 3\,q' + r'$. Applicando dunque più volte questa idea (cioè svolgendo vari passaggi come in (1) qui sopra si ottiene

$$\begin{aligned} \overline{B^E} = \overline{4515}^{\,96} = \overline{3}^{\,96} = \overline{3}^{\,3\cdot 32+0} = \overline{3}^{\,32+0} = \overline{3}^{\,32} &= \\ = \overline{3}^{\,3\cdot 10+2} = \overline{3}^{\,10+2} = \overline{3}^{\,12} &= \\ = \overline{3}^{\,3\cdot 4+0} = \overline{3}^{\,4+0} = \overline{3}^{\,4} &= \\ = \overline{3}^{\,3\cdot 1+1} = \overline{3}^{\,1+1} = \overline{3}^{\,2} &= \overline{9} \end{aligned}$$

e così concludiamo che il resto cercato è $r_2 = 9$.

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

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

(b) Il valore a_3 può essere calcolato *senza* conoscere la forma esplicita — data in (2) — delle successioni ricorsive considerate. Infatti, dalla conoscenza dei dati iniziali a_0 e a_1 e dalla formula ricorsiva otteniamo facilmente

$$a_0 := 4\,, \qquad a_1 := -1\,, \qquad a_2 := a_1 + 2\,a_0 = -1 + 2 \cdot 4 = 7$$
$$a_3 = a_2 + 2\,a_1 = 7 + 2 \cdot (-1) = 5$$

così che $a_3 = 5$.

In alternativa (ma è "peggio", perché è vincolato ad un lavoro precedente), il valore a_3 può essere calcolato dalla formula (2), e quindi sarà dato da

$$a_3 = 2^3 + 3 \cdot (-1)^3 = 8 - 3 = 5$$

cioè $a_3 = 5$ come già osservato (indipendentemente) in precedenza.