ALGEBRA e LOGICA
CdL in Ingegneria Informatica

prof. Fabio GAVARINI

a.a. 2016–2017 — Sessione Estiva, I appello

Esame scritto del 5 Luglio 2017

. . . .

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] *(a)* Si consideri il seguente polinomio booleano

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

nelle quattro variabili booleane x, y, z, w.

(a) Calcolare la *Forma Normale Disgiuntiva* del polinomio $P(x,y,z,w)$.

(b) Calcolare la *somma di tutti gli implicanti primi* del polinomio $P(x,y,z,w)$.

(c) Calcolare una *forma minimale* del polinomio $P(x,y,z,w)$.

[2] Dimostrare per induzione che per ogni $n \in \mathbb{N}$, $n \geq 4$, vale la disuguaglianza

$$3^n - 5\,n \;>\; 2^n + 4\,n$$

[3] Si consideri in $\mathbb{Z}$ la relazione "$\sim$" definita da

$$u \sim v \quad \iff \quad 3\,u^2 + 7\,v^2 - 12 \equiv 8\,u + 2\,v + 28 \pmod{5} \qquad \forall\; u, v \in \mathbb{Z}$$

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

(b) Data la funzione $f : \mathbb{Z} \longrightarrow \mathbb{Z}_5$, $x \mapsto f(x) := \overline{x}\,\big(\overline{x} - \overline{1}\big)$, dimostrare che

$$u \sim v \iff f(u) = f(v) \qquad \forall\; u, v \in \mathbb{Z}$$

(c) Descrivere esplicitamente la classe di $\sim$–equivalenza di 1.

(d) Descrivere esplicitamente la classe di $\sim$–equivalenza di 3.

(e) Descrivere esplicitamente tutte le classi di $\sim$–equivalenza in $\mathbb{Z}$.

(continua...)

[4] Sia $\mathcal{P}\big(\{S,P,Q,R\}\big)$ l'insieme delle parti dell'insieme $\{S,P,Q,R\}$ e "$\supseteq$" la consueta relazione di "inclusione inversa" in $\mathcal{P}\big(\{S,P,Q,R\}\big)$, definita da $\mathcal{A} \supseteq \mathcal{B}$ se e soltanto se $\mathcal{A}$ contiene $\mathcal{B}$ — per ogni $\mathcal{A}\,,\mathcal{B} \in \mathcal{P}\big(\{S,P,Q,R\}\big)$.

Sia poi $D_{60} := \big\{\, d \in \mathbb{N} \,\big|\, d \text{ è divisore di } 60 \,\big\}$ l'insieme dei divisori di 60, e sia "$\big|$" la consueta relazione di divisibilità in D_{60}.

Nell'insieme $E := \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60}$ prodotto cartesiano di $\mathcal{P}\big(\{S,P,Q,R\}\big)$ con D_{60} consideriamo la relazione $\preceq$ definita da

$$\big(\mathcal{A}\,,d\,\big) \preceq \big(\mathcal{B}\,,q\,\big) \quad \Longleftrightarrow \quad \mathcal{A} \supseteq \mathcal{B}\ ,\ \ d\,\big|\,q$$

per ogni $\big(\mathcal{A}\,,d\,\big)\,,\big(\mathcal{B}\,,q\,\big) \in \mathcal{P}\big(\{S,P,Q,R\}\big) \times D_{60} =: E$.

(a) Dimostrare che $\preceq$ è una relazione d'ordine in E.

(b) Esiste un *minimo* nell'insieme ordinato $\big(E\,;\,\preceq\big)$? In caso negativo, spiegare perché; in caso affermativo, precisare quale sia tale minimo.

(c) Esiste un *massimo* nell'insieme ordinato $\big(E\,;\,\preceq\big)$? In caso negativo, spiegare perché; in caso affermativo, precisare quale sia tale massimo.

(d) Dimostrare che l'insieme ordinato $\big(E\,;\,\preceq\big)$ è un reticolo, *precisando come siano fatte le operazioni "$\vee := \sup$" e "$\wedge := \inf$"* in tale reticolo.

(e) Determinare se esista una $\vee$–fattorizzazione in $\vee$–irriducibili per l'elemento $\big(\{S,Q\}\,,30\big)$ nel reticolo $\big(E\,;\,\preceq\big)$. In caso negativo, si spieghi perché una tale $\vee$–fattorizzazione non esista; in caso affermativo, si determini esplicitamente una tale $\vee$–fattorizzazione.

[5] Siano $\mathbb{Z}_{11}$ e $\mathbb{Z}_{12}$ i consueti anelli di classi di congruenza modulo 11 e modulo 12 rispettivamente, con le consuete operazioni di somma e prodotto.

(a) Calcolare esplicitamente gli insiemi di elementi invertibili $U\big(\mathbb{Z}_{11}\big)$ e $U\big(\mathbb{Z}_{12}\big)$ in $\mathbb{Z}_{11}$ e in $\mathbb{Z}_{12}$ rispettivamente.

(b) Calcolare esplicitamente l'insieme di tutte le soluzioni in $\mathbb{Z}$ dell'equazione congruenziale $45\,x \equiv -135 \pmod{12}$.

(c) Per *entrambi* i valori $q = 11$ e $q = 12$, determinare se esista un elemento $\overline{z} \in \mathbb{Z}_q \setminus \big\{\,\overline{0}\,\big\}$ tale che $\overline{z}^{\,n} = \overline{0}$ per qualche esponente $n \in \mathbb{N}$. In caso negativo, si spieghi il perché; in caso affermativo, si determinino esplicitamente un tale elemento $\overline{z}$ e un esponente n tali che $\overline{z}^{\,n} = \overline{0}$.