CdS in Informatica — a.a. 2007/2008

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) martedì 17 giugno 2008

| NOME E COGNOME | MATRICOLA |
|---|---|
| | |

| GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)* | ESAME: venerdì 20 giugno, ore 9, aula G, DMA |
|---|---|

**1** Vero o falso? Oppure i dati non sono sufficienti per fornire alcuna delle due risposte?

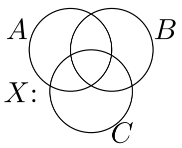
- Esistono in $\mathbb{S}_8$ tre permutazioni dispari $\alpha$, $\beta$ e $\gamma$ tali che $\alpha = \beta\gamma$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $[13 \cdot 78]_{15}$ è un elemento cancellabile nell'anello $\mathbb{Z}_{15}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La forma proposizionale $\big(p \Rightarrow (q \wedge r)\big) \vee \big(p \Rightarrow (\neg q)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\{X \in \mathcal{P}_5(\mathbb{Z}) \mid X \smallsetminus \{3\} \in \mathcal{P}_4(\mathbb{N})\} \subset \{X \in \mathcal{P}(\mathbb{N}) \mid 3 \in X\}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'applicazione $x \in \mathbb{Z} \longmapsto \begin{cases} 3x+2 & \text{se } x \text{ è pari} \\ 4x & \text{se } x \text{ è dispari} \end{cases} \in \mathbb{Z}$ è iniettiva. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

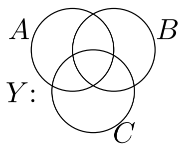
---

**2** Per definizione, un albero è . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

---

**3** Si completino i due diagrammi di Venn tratteggiando le aree corrispondenti a $X = (A \smallsetminus B) \cup (B \smallsetminus C)$ ed a $Y = (A \cup B) \smallsetminus C$. È vero che $X \subseteq Y$ per ogni scelta degli insiemi $A$, $B$, $C$? ☐ *sì*, oppure: ☐ *no, un controesempio è dato da* $A =$ . . . . . . . . . . . . . , $B =$ . . . . . . . . . . . . . , $C =$ . . . . . . . . . . . . . . È vero che $Y \subseteq X$ per ogni scelta degli insiemi $A$, $B$, $C$? ☐ *sì*, oppure: ☐ *no, un controesempio è dato da* $A =$ . . . . . . . . . . . . . , $B =$ . . . . . . . . . . . . . , $C =$ . . . . . . . . . . . . . .

$X$: 


$Y$: 


---

**4** Sia $S$ l'insieme costituito dalle nove stringhe aba, abe, acb, bdf, cef, dba, dbe, deb, def, formata ciascuna da tre caratteri. Definiamo due relazioni binarie $\rho$ e $\sigma$ in $S$ come segue. Se $c_1$ e $c_2$ sono due caratteri scriviamo $c_1 \preceq c_2$ per indicare che $c_1$ è uguale a $c_2$ o lo precede nell'usuale ordine alfabetico (ad esempio, a $\preceq$ d, b $\preceq$ b e f $\not\preceq$ c); poniamo poi, per ogni scelta degli elementi $x := c_1c_2c_3$ e $y := c_1'c_2'c_3'$ di $S$,

$$x \,\rho\, y :\iff \big((c_1 \preceq c_1') \wedge (c_2 \preceq c_2') \wedge (c_3 \preceq c_3')\big) \qquad \text{e} \qquad x \,\sigma\, y :\iff \big(\big((c_1 \preceq c_1') \wedge (c_2 \preceq c_2')\big) \vee (c_3 \preceq c_3')\big)$$

$\rho$ è un ordinamento? *sì* ☐ *no* ☐, $\sigma$ è un ordinamento? *sì* ☐ *no* ☐.

Se uno dei due lo è (specificare quale: . . . ), si consideri $S$ ordinato rispetto ad esso, se ne disegni accanto il diagramma di Hasse e si risponda alle domande che seguono.

$S$ è un reticolo? *sì* ☐ *no* ☐, nel caso è complementato? *sì* ☐ *no* ☐, distributivo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.

sup{abe, dba} è . . . . . . , oppure: ☐ *non esiste.*

sup{abe, acb, dba} è . . . . . . , oppure: ☐ *non esiste.*

Gli elementi massimali di $S$ sono: . . . . . . . . . . . . . , oppure: ☐ *non ne esistono.*

Gli elementi minimali di $S$ sono: . . . . . . . . . . . . . , oppure: ☐ *non ne esistono.*

$\min S =$ . . . . . . , oppure: ☐ *non esiste.* $\max S =$ . . . . . . , oppure: ☐ *non esiste.*

Esiste $x \in S$ tale che $S \smallsetminus \{x\}$, munito dell'ordinamento indotto da quello qui considerato, sia un reticolo booleano? ☐ *no*, oppure: ☐ *sì, un tale* $x$ *è* . . . . . . .

---

**5** Si completi la tabella, relativa alle relazioni binarie $\alpha$ e $\beta$ definite in $S := \{n \in \mathbb{Z} \mid -10 < n < 10\}$ ponendo, per ogni $a, b \in S$,

$a \,\alpha\, b :\iff (a \equiv_6 b \vee ab \text{ è dispari})$

$a \,\beta\, b :\iff (a \equiv_6 b \wedge ab \text{ è dispari})$

| | riflessiva | | antiriflessiva | | simmetrica | | antisimmetrica | | transitiva | |
|---|---|---|---|---|---|---|---|---|---|---|
| | *sì* | *no* | *sì* | *no* | *sì* | *no* | *sì* | *no* | *sì* | *no* |
| $\alpha$ è | | | | | | | | | | |
| $\beta$ è | | | | | | | | | | |

$\alpha$ è di equivalenza? *sì* ☐ *no* ☐. Se lo è, $|S/\alpha| =$ . . . , $[7]_\alpha = \{$ . . . . . . . . . . . . . . $\}$, $[8]_\alpha = \{$ . . . . . . . . . . . $\}$.

$\beta$ è di equivalenza? *sì* ☐ *no* ☐. Se lo è, $|S/\beta| =$ . . . , $[7]_\beta = \{$ . . . . . . . . . . . . . . $\}$, $[8]_\beta = \{$ . . . . . . . . . . . $\}$.

---

**6** Esistono grafi semplici con (esattamente) tre componenti connesse, dieci lati e dieci vertici, dei quali due siano isolati, due abbiano grado 4, quattro abbiano grado 2? *sì* ☐ *no* ☐. Nel caso ne esistano, quali sono i gradi dei rimanenti vertici? . . . e . . . , oppure: ☐ *non è possibile stabilirlo*. Se $G$ è un tale grafo, $G$ ha circuiti euleriani? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐, cammini euleriani? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐. Sempre se possibile, disegnare un grafo con le proprietà richieste, o due tali grafi, tra loro non isomorfi (oppure: ☐ *non ne esistono*), o tre tali grafi a due a due non isomorfi tra loro (oppure: ☐ *non ne esistono*).

---

**7** Si trovi l'insieme (rispettivamente $S_1$, $S_2$, $S_3$) di tutte le soluzioni intere di ciascuna delle seguenti equazioni congruenziali:

$2873x \equiv_{3757} 547$; $2873x \equiv_{3757} 1547$; $2873x \equiv_{3757} 2547$;

$S_1 = \dots\dots\dots\dots$; $S_2 = \dots\dots\dots\dots$; $S_3 = \dots\dots\dots\dots$;

Calcolare $905^2 \bmod 3757 =$ . . . . ; $905^{-1} \bmod 3757 =$ . . . . ;
$(905^{12345} + 905^{123456} + 905^{1234567}) \bmod 3757 =$ . . . . .

---

**8** Si trovi il massimo comun divisore monico $d$ in $\mathbb{Q}[x]$ tra $a = (5f + 33g^2)(5 + g^4)$ e $b = 18g$, dove $f = x^7 - 2x^6 - 2x^5 + 4x^4 + 3x^3 - 6x^2 + 6x - 12$ e $g = x^6 - 4x^5 + x^4 + 12x^3 - 6x^2 - 24x + 24$, e si scrivano poi $f$ e $g$ come prodotti di polinomi monici irriducibili in $\mathbb{Q}[x]$. $d = \dots\dots\dots\dots$

$f = \dots\dots\dots\dots$ $g = \dots\dots\dots\dots$

[*Suggerimento:* calcolare $d(1)$ e $d(2)$] Spiegare brevemente perché i fattori che appaiono qui sono irriducibili:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . .

Detti $f_5$ e $g_5$, rispettivamente, $f$ e $g$ riguardati come polinomi a coefficienti in $\mathbb{Z}_5$, si scrivano $f_5$ e $g_5$ come prodotti di polinomi monici irriducibili in $\mathbb{Z}_5[x]$ e si calcolino il massimo comun divisore monico $d_5$ ed il minimo comune multiplo $m_5$ tra $f_5$ e $g_5$ in $\mathbb{Z}_5[x]$. Quanti sono i massimi comuni divisori in $\mathbb{Z}_5[x]$ tra $f_5$ e $g_5$? . . . .

$f_5 = \dots\dots\dots\dots$ $g_5 = \dots\dots\dots\dots$

$d_5 = \dots\dots\dots\dots$ $m_5 = \dots\dots\dots\dots$

---

**9** In $S = \mathbb{Z}_4 \times \mathbb{Z}_6$ si definiscano le operazioni binarie $\oplus$ e $*$ ponendo, per ogni $a, c \in \mathbb{Z}_4$ e $b, d \in \mathbb{Z}_6$, $(a, b) \oplus (c, d) = (a + c + [2]_4, b + d - [2]_6)$ e $(a, b) * (c, d) = ([2]_4 + 2a + 2c - ac, bd - 2b - 2d)$.
$\oplus$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐; ammette elemento neutro? ☐ *no*, oppure: ☐ *sì, esso è* . . . . . . $*$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐; ammette elemento neutro? ☐ *no*, oppure: ☐ *sì, esso è* . . . . . . $(S, \oplus)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐. $(S, *)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐. $(S, \oplus, *)$ è un anello? *sì* ☐ *no* ☐, un anello unitario? *sì* ☐ *no* ☐, un anello booleano? *sì* ☐ *no* ☐, un dominio di integrità? *sì* ☐ *no* ☐. Nel caso $(S, *)$ abbia elemento neutro, determinare i suoi elementi simmetrizzabili:

. . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . . ,

i simmetrici di $([3]_4, [3]_6)$ rispetto a $\oplus$ (è . . . . . . , oppure: ☐ *non esiste*) e $*$ (è . . . . . . , oppure: ☐ *non esiste*) e i simmetrici di $([0]_4, [0]_6)$ rispetto a $\oplus$ (è . . . . . . , oppure: ☐ *non esiste*) e $*$ (è . . . . . . , oppure: ☐ *non esiste*). L'applicazione $n \in \mathbb{Z} \mapsto ([2]_4, [n + 2]_6) \in S$ è un omomorfismo da $(\mathbb{Z}, +)$ a $(S, \oplus)$? *sì* ☐ *no* ☐. E da $(\mathbb{Z}, \cdot)$ a $(S, *)$? *sì* ☐ *no* ☐.

---