CdS in Informatica — a.a. 2009/2010

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 8 ottobre 2010

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: martedì 12 ottobre, ore 9, studio 88, DMA

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

- Sono dati tre insiemi, A, B, C. Esiste $x \in B$ tale che $x \notin (A \cap C)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La permutazione $\prod_{i=2}^{100}(1\, i) \in \mathbb{S}_{100}$ è un ciclo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La (stessa) permutazione $\prod_{i=2}^{100}(1\, i) \in \mathbb{S}_{100}$ ha classe pari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esiste un'algebra di Boole di cardinalità $2^{50} + 2^{100}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esiste un numero naturale multiplo di 123^{12+71} e maggiore di $\binom{234}{47}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esiste un numero primo multiplo di 38. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Per definizione, un *campo* è un anello $(A, +, \cdot)$ che sia ....

....

Si forniscano, ove possibile, esempi di:

un anello che non sia un campo: ...., oppure: ☐ *non ne esistono;*

un campo finito: ...., oppure: ☐ *non ne esistono;*

un campo infinito: ...., oppure: ☐ *non ne esistono.*

---

3 Sia Φ la forma proposizionale $\big((q \vee r) \Rightarrow (p \vee s)\big) \Longrightarrow \big(q \Rightarrow (p \vee r)\big)$. Φ è ☐ *una tautologia* ☐ *una contraddizione* ☐ *contingente.*

Se possibile, indicare valori di verità (V/F) per p, q, r, s che rendano Φ vera: p . . . , q . . . , r . . . , s . . . .

Se possibile, indicare valori di verità (V/F) per p, q, r, s che rendano Φ falsa: p . . . , q . . . , r . . . , s . . . .

La forma $q \Longrightarrow \Phi$ è ☐ *una tautologia* ☐ *una contraddizione* ☐ *contingente.*

La forma $r \Longrightarrow \Phi$ è ☐ *una tautologia* ☐ *una contraddizione* ☐ *contingente.*

La forma $\Phi \vee p \vee s$ è ☐ *una tautologia* ☐ *una contraddizione* ☐ *contingente.*

---

4 Quanti sono, a meno di isomorfismi, i grafi (semplici) con esattamente 5 vertici e tre componenti connesse? . . . Quanti tra questi sono foreste? . . . Disegnarli tutti, segnalando tra essi le foreste:

---

5 In $S = \mathrm{Map}(\mathbb{N}, \mathbb{N})$ si consideri l'operazione binaria $*$ definita ponendo, per ogni $f, g \in S$,

$$f * g : n \in \mathbb{N} \longmapsto n^f n^g \in \mathbb{N}.$$

$*$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐, ha elemento neutro? ☐ *no*, oppure: ☐ *sì, l'applicazione:*

$$n \in \mathbb{N} \longmapsto \;\ldots\ldots\ldots\ldots\ldots\;\in \mathbb{N}.$$

$(S, *)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐. L'applicazione identica $\mathrm{id}_{\mathbb{N}}$ in $\mathbb{N}$ è simmetrizzabile in $(S, *)$? ☐ *no*, oppure: ☐ *sì il suo simmetrico è l'applicazione:*

$$n \in \mathbb{N} \longmapsto \;\ldots\ldots\ldots\ldots\ldots\;\in \mathbb{N}.$$

---

6 Sia $A = \{n \in \mathbb{N} \mid n < 10\}$, dunque $|A| = \ldots .$ Indicare il numero delle applicazioni da $A \times A$ a $\mathcal{P}_3(A)$: questo numero è .... Stabilire quante sono le relazioni di equivalenza σ in A tali che:

(1) Per ogni a e b in A, se a e b sono entrambi pari allora $a\ \sigma\ b$;

(2) $(\forall\, a \in A)\big((3 \mid a) \Rightarrow (a\ \sigma\ 0)\big)$;

(3) $(\exists\, a \in A)(|[a]_\sigma| = 2)$.

[Risposta: il loro numero è ....]. Se possibile, si scelga una tra queste relazioni di equivalenza e si descriva A/σ, elencando esplicitamente gli elementi di ogni classe di equivalenza:

$$A/\sigma = \big\{\{0, 2, \ldots\ldots\ldots\ldots \}, \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \big\}; \quad \text{dunque } |A/\sigma| = \ldots .$$

Per questa scelta di σ, quante sono le sezioni della proiezione canonica $A \twoheadrightarrow A/\sigma$? ...

Quante sono, invece, le relazioni di equivalenza σ in A che verificano le proprietà (1) e (2)? ...

---

7 Si definiscano in $\mathbb{Z}$ le relazioni binarie α, β, γ e δ ponendo, per ogni $a, b \in \mathbb{Z}$,

$a\ \alpha\ b :\iff \big((a \mid b) \wedge ((b \mid a) \Rightarrow (a \le b))\big)$; $\qquad a\ \gamma\ b :\iff a \mid b$;

$a\ \beta\ b :\iff \big((a \mid b) \wedge (a + b \ge 0)\big)$; $\qquad a\ \delta\ b :\iff \big((a \mid b) \wedge ((|a| = |b|) \Rightarrow (a \le b))\big)$.

Tra queste, si dica quali sono relazioni di ordine stretto: ...., quali sono relazioni di ordine largo: .... e quali non sono relazioni d'ordine: .... Se possibile, se ne scelga una che sia una relazione d'ordine e la si chiami ρ (dunque, $\rho = \ldots$) e si consideri l'insieme $S = \{-60, -6, -5, -3, 1, 2, 5, 6, 10, 15\}$ ordinato dall'ordinamento indotto da ρ. Se ne disegni a fianco il diagramma di Hasse. Rispetto a questo ordinamento, $\min S = \ldots$, oppure: ☐ $\min S$ *non esiste*;

$\max S = \ldots$, oppure: ☐ $\max S$ *non esiste*;

$\sup\{-5, 2\} = \ldots$, oppure: ☐ $\sup\{-5, 2\}$ *non esiste*.

S è un reticolo? *sì* ☐ *no* ☐. Nel caso, è complementato? *sì* ☐ *no* ☐; distributivo? *sì* ☐ *no* ☐; booleano? *sì* ☐ *no* ☐.

---

8 Sapendo che: 337 è primo; nel gruppo $\mathcal{U}(\mathbb{Z}_{337})$, $[10]_{337}$ ha periodo $336 = 2^4 \cdot 3 \cdot 7$;

$$128 \equiv_{337} 10^{112}, \qquad 148 \equiv_{337} 10^{84}, \qquad 72 \equiv_{337} 128 \cdot 148,$$

si ha: $|\mathcal{U}(\mathbb{Z}_{337})| = \ldots .$, $[128]_{337}$ ha periodo ... , $[148]_{337}$ ha periodo ... , quindi $[72]_{337}$, ha periodo ... e $72^{72} \bmod 337 = \ldots .$ Sapendo inoltre che $72^{11} \equiv_{337} 220$, calcolare il minimo intero non negativo m tale che $-5 + 72m$ sia multiplo di 337: $m = \ldots .$, oppure: ☐ *tale intero non esiste*.

---

9 In $\mathbb{Q}[x]$, si calcoli il massimo comun divisore monico d tra i polinomi $f := 12(x^7 - x^6 + x^4 - x^3 + x^2 - 1)$ e $g := 8(x^6 - x^5 + x^2 - 1)$. $d = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$. Si scrivano poi d, f e g come prodotti di un invertibile e di polinomi irriducibili monici (sempre in $\mathbb{Q}[x]$):

$d = \ldots\ldots\ldots\ldots\ldots\ldots$; $\quad f = \ldots\ldots\ldots\ldots\ldots\ldots$; $\quad g = \ldots\ldots\ldots\ldots\ldots\ldots$

Le radici comuni a f e g in $\mathbb{Q}$ sono: ....

Si determini il minimo numero primo p tale che f_p, cioè f riguardato come polinomio a coefficienti in $\mathbb{Z}_p$, non abbia divisori irriducibili di grado maggiore di 2. $p = \ldots .$
