CdS in Informatica — a.a. 2007/2008

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) giovedì 8 maggio 2008

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)*

ESAME: venerdì 9 maggio, ore 15, aula C, DMA

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

- Ogni insieme ordinato finito non vuoto ha elementi massimali. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\{X \in \mathcal{P}(\mathbb{Z}) \mid X \smallsetminus \mathbb{N} = X\} = \{A \in \mathcal{P}(\mathbb{Z}) \mid A \cap \mathbb{N} = \varnothing\}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Ogni permutazione su un insieme finito è prodotto di trasposizioni. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Ogni permutazione su un insieme finito è prodotto di trasposizioni tra loro disgiunte. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $\{f \in T(\mathbb{Z}) \mid (\forall x \in \mathbb{Z})(x^f > x)\}$ è una parte stabile di $T(\mathbb{Z})$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\{f \in T(\mathbb{Z}) \mid (\forall x \in \mathbb{Z})(x^f \neq x)\}$ è una parte stabile di $T(\mathbb{Z})$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- È dato un intero $n > 23$. Il coefficiente binomiale $\binom{n}{3}$ è pari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Per definizione, un anello $(R, +, \cdot)$ è *booleano* se e solo se ....

....

Si fornisca, se possibile, un esempio di:

anello booleano di cardinalità 15: ...., oppure: ☐ *non ne esistono*

anello booleano di cardinalità 16: ...., oppure: ☐ *non ne esistono*

anello booleano di cardinalità 16 non isomorfo al precedente: ...., oppure: ☐ *non ne esistono*

anello non booleano di cardinalità 16: ...., oppure: ☐ *non ne esistono*

anello booleano infinito: ...., oppure: ☐ *non ne esistono*

anello booleano non commutativo: ...., oppure: ☐ *non ne esistono*

anello booleano ed un suo elemento a tale che $a \neq -a$: ...., oppure: ☐ *non ne esistono*

---

3 Si consideri l'applicazione $\theta\colon n \in A \mapsto \{p \in B \mid p \text{ divide } n\} \in \mathcal{P}(B)$, dove $A = \{n \in \mathbb{N}^\# \mid n \leq 20\}$ e $B = \{p \in A \mid p \text{ è primo}\}$. θ è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐. Quante sezioni ha θ? . . . E quante retrazioni? . . . Indicare $|A| = \ldots$, $|B| = \ldots$, $|\mathcal{P}(B)| = \ldots$, $|\operatorname{Map}(A, \mathcal{P}(B))| = \ldots$ $|\operatorname{im}\theta| = \ldots$

Si ha: $\mathcal{P}(\{2,3\}) \subseteq \operatorname{im}\theta$? *sì* ☐ *no* ☐, $\mathcal{P}(\{3,5\}) \subseteq \operatorname{im}\theta$? *sì* ☐ *no* ☐, $\mathcal{P}(\{2,3,5\}) \subseteq \operatorname{im}\theta$? *sì* ☐ *no* ☐.

Si considerino le relazioni binarie α, β, γ, δ definite in A ponendo, per ogni $x, y \in A$,

$$x \;\alpha\; y :\iff x^\theta = y^\theta; \qquad x \;\beta\; y :\iff |x^\theta| = |y^\theta|; \qquad x \;\gamma\; y :\iff |x^\theta| \leq |y^\theta|;$$

$$x \;\delta\; y :\iff (\exists \max x^\theta \wedge \exists \max y^\theta \wedge \max x^\theta < \max y^\theta).$$

α è di equivalenza? *sì* ☐ *no* ☐. Se sì, $|A/\alpha| = \ldots$, $[1]_\alpha = \{\ldots\ldots\ldots\}$ e $[2]_\alpha = \{\ldots\ldots\ldots\}$

β è di equivalenza? *sì* ☐ *no* ☐. Se sì, $|A/\beta| = \ldots$, $[2]_\beta = \{\ldots\ldots\ldots\}$ e $[6]_\beta = \{\ldots\ldots\ldots\}$

γ è di equivalenza? *sì* ☐ *no* ☐. Se sì, $|A/\gamma| = \ldots$, $[3]_\gamma = \{\ldots\ldots\ldots\}$ e $[4]_\gamma = \{\ldots\ldots\ldots\}$

δ è di equivalenza? *sì* ☐ *no* ☐. Se sì, $|A/\delta| = \ldots$, $[4]_\delta = \{\ldots\ldots\ldots\}$ e $[5]_\delta = \{\ldots\ldots\ldots\}$.

Quali tra α, β, γ e δ sono: . . . . e quali non sono: . . . . ordinamenti (stretti o larghi)? Se possibile se ne scelga uno, lo si chiami ρ (dunque $\rho = \ldots$) e si disegni il diagramma di Hasse di (A, ρ). (A, ρ) è un reticolo? *sì* ☐ *no* ☐, nel caso è complementato *sì* ☐ *no* ☐?, distributivo *sì* ☐ *no* ☐?, booleano *sì* ☐ *no* ☐?.

Gli elementi massimali di (A, ρ) sono: . . . . , oppure: ☐ *non ne esistono*. Gli elementi minimali di (A, ρ) sono: . . . . , oppure: ☐ *non ne esistono*.

Sempre rispetto a ρ, $\min A = \ldots$, oppure: ☐ $\min A$ *non esiste.*;

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

$\sup\{5, 9\} = \ldots$, oppure: ☐ $\sup\{5, 9\}$ *non esiste.*;

$\inf\{10, 20\} = \ldots$, oppure: ☐ $\inf\{10, 20\}$ *non esiste.*;

Tra le seguenti parti di A stabilire quali, con l'ordinamento indotto da ρ costituiscono un reticolo e quali un reticolo booleano:

$\{2, 3, 4, 5\}$: reticolo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐?

$\{3, 4, 5, 6\}$: reticolo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐?

$\{3, 4, 5, 7\}$: reticolo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐?

$\{2, 3, 4, 5, 6, 7\}$: reticolo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐?

4 Il periodo di $[15]_{211}$ nel gruppo $\mathcal{U}(\mathbb{Z}_{211})$ è . . . . . Calcolare $15^2 \bmod 211 =$ . . . . ; $(15^{123456789} + 14^{123456789}) \bmod 211 =$ . . . . . Si trovi l'insieme (rispettivamente S_1, S_2, S_3) di tutte le soluzioni intere di ciascuna delle seguenti equazioni congruenziali:

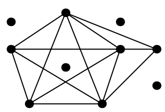
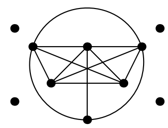
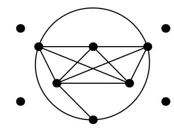
$15x \equiv_{211} 14$; $\qquad$ $14x \equiv_{211} 15$; $\qquad$ $(14 \cdot 15)x \equiv_{211} 1$;

$S_1 =$ . . . . ; $\quad S_2 =$ . . . . ; $\quad S_3 =$ . . . . ;

Trovare, se esiste, $n \in \mathbb{N}$ tale che $2^{10} - 2^6 < n < 2^{10} + 2^6$ e $211 \mid (3^5 n - 2^5)$. ☐ *Tale n non esiste*, oppure: ☐ *n esiste, si ha $n =$* . . . . .

---

5 Sia G il grafo il cui insieme di vertici è $\{n \in \mathbb{N} \mid 10 \leq n < 20\}$ e due qualsiasi vertici tra loro distinti sono adiacenti se e solo se non sono coprimi. Indicare quali tra i tre vertici qui disegnati sono . . . . e quali non sono . . . . isomorfi a G. G ha cammini euleriani? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

A:  $\quad B$:  $\quad C$: 

---

6 Si stabiliscano i valori di verità assunti dalla forma proposizionale $\Phi\colon p \Rightarrow (q \vee r)$ in corrispondenza dei valori indicati per p, q, r. Nel caso in cui p vale vero, q falso, r vero, Φ vale ☐ *vero* ☐ *falso.* Nel caso in cui p vale falso, q falso, r falso: Φ vale ☐ *vero* ☐ *falso.* Φ è ☐ *una tautologia*, ☐ *contingente*, ☐ *una contraddizione.*
La forma $\big(p \Rightarrow (q \vee r)\big) \Longrightarrow \big((p \wedge \neg q) \Rightarrow r\big)$ è ☐ *una tautologia*, ☐ *contingente*, ☐ *una contraddizione.*
La forma $\big(p \Rightarrow (q \vee r)\big) \Longleftarrow \big((p \wedge \neg q) \Rightarrow r\big)$ è ☐ *una tautologia*, ☐ *contingente*, ☐ *una contraddizione.*

---

7 Si calcoli in $\mathbb{Q}[x]$ il massimo comun divisore monico d tra i polinomi
$f = 4x^8 + 2x^7 + 2x^6 - 48x^5 - 11x^4 - 3x^3 + 141x^2 - 27x - 42$ e $g = 2x^7 - 25x^4 + 6x^3 + 72x - 48$:

$d =$ . . . .

Quante . . . e quali . . . . sono le radici comuni a g e $f + g$ in $\mathbb{Q}$?

d è irriducibile in $\mathbb{Q}[x]$? ☐ *sì, perché:* . . . . ☐ *no, perché:* . . . .

d è irriducibile in $\mathbb{R}[x]$? ☐ *sì, perché:* . . . . ☐ *no, perché:* . . . .

Si scomponga g nel prodotto di un polinomio invertibile e polinomi irriducibili monici in $\mathbb{Q}[x]$:

$g =$ . . . .

Sia $f_1 = f/d$. Sapendo che nessun numero razionale della forma $n/4$, con $n \in \mathbb{Z}$ e $|n| < 200$, è radice di f e che f non è divisibile in $\mathbb{Q}[x]$ per alcun polinomio irriducibile di secondo grado, si può stabilire se f_1 è irriducibile in $\mathbb{Q}[x]$? ☐ *no, è impossibile stabilirlo senza calcolare f_1*, oppure: ☐ *sì, f_1 è certamente riducibile*, oppure: ☐ *sì, f_1 è certamente irriducibile.*

Si scomponga g_3, cioè g riguardato come polinomio a coefficienti in $\mathbb{Z}_3$, nel prodotto di un polinomio invertibile e polinomi irriducibili monici in $\mathbb{Z}_3[x]$:

$g_3 =$ . . . .
