CdS in Informatica — a.a. 2009/2010

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) mercoledì 15 settembre 2010

NOME E COGNOME	MATRICOLA

GRUPPO □ *I (Rao)* □ *rec. (Cutolo)*	ESAME: a causa dell'agitazione in corso, non sono state ancora fissate data e modalità dell'esame.

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

- L'operazione $(a, b) \in \mathbb{Z} \mapsto \max\{a, b\} \in \mathbb{Z}$ è associativa. *vero* □ *falso* □ *dati insufficienti* □
- $(\mathbb{Z}, \leq)$ (ordinamento usuale) è un reticolo. *vero* □ *falso* □ *dati insufficienti* □
- $\{X \in \mathcal{P}(\mathbb{Z}) \mid (\forall\, Y \in \mathcal{P}(\mathbb{N}))(X \cap Y = \varnothing)\} = \mathcal{P}(\mathbb{Z}) \smallsetminus \mathcal{P}(\mathbb{N})$. *vero* □ *falso* □ *dati insufficienti* □
- Per ogni scelta degli insiemi A, B, C si ha $(A \cap B) \cup (A \cup C) = (A \cup B \cup C) \smallsetminus (B \smallsetminus A)$. *vero* □ *falso* □ *dati insuff.* □
- È assegnato un intero n. Il numero $(n^2 + n + 1)^2\binom{n}{n-1}$ è pari. *vero* □ *falso* □ *dati insufficienti* □

---

2 Si enunci il teorema di Bézout per numeri interi: scelti comunque due interi n ed m ed un loro massimo comun divisore t, ...

....

---

3 Sia Φ la forma proposizionale $\big(p \vee r\big) \implies \big((q \wedge r) \Rightarrow p\big)$. Si completi la tabella a destra calcolando i valori di verità per Φ in funzione di quelli di p, q, r.

p	q	r	Φ
V	V	F	
F	F	V	
F	V	F	

La forma $p \implies \Phi$ è □ *una tautologia* □ *una contraddizione* □ *contingente.*

La forma $p \iff \Phi$ è □ *una tautologia* □ *una contraddizione* □ *contingente.*

La forma $\Phi \Rightarrow \Big(\big((q \Rightarrow r) \wedge (q \Rightarrow \neg r)\big) \Rightarrow \neg q\Big)$ è □ *una tautologia* □ *una contraddizione* □ *contingente.*

---

4 Sia $A = \{2, 3, 4\}$. Allora $|\mathcal{P}(A)| = \ldots$, $|\mathcal{P}_2(A)| = \ldots$, $|\mathcal{P}(\mathcal{P}_2(A))| = \ldots$ e $|\mathcal{P}_2(\mathcal{P}(A))| = \ldots$. Sia $f\colon \mathcal{P}(A) \to \{n \in \mathbb{N} \mid n < 6\}$ l'applicazione definita come segue: $\varnothing^f = 1$ e, per ogni $X \in \mathcal{P}(A) \smallsetminus \varnothing$, $X^f = \big(\prod_{x \in X} x\big) \bmod 6$ (il prodotto degli elementi di X modulo 6). f è iniettiva? □ *sì*, oppure: □ *no, perché* .... f è suriettiva? □ *sì*, oppure: □ *no, perché* .... Quante sezioni ha f? ..... Quante retrazioni ha f? .... Detto $\sim$ il nucleo di equivalenza di f, si descriva esplicitamente $\mathcal{P}(A)/\!\sim$, elencando gli elementi di ciascuna classe di equivalenza:

$$\mathcal{P}(A)/\!\sim\, = \{\{ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \}.$$

Siano poi σ e τ le relazioni binarie definite in $\mathcal{P}(A)$ ponendo, per ogni $X, Y \in \mathcal{P}(A)$,

$$X \;\sigma\; Y :\iff X^f \leq Y^f; \qquad \text{e} \qquad X \;\tau\; Y :\iff (X^f + 2) \bmod 6 < (Y^f + 2) \bmod 6.$$

σ è una relazione d'ordine? *sì* □ *no* □. τ è una relazione d'ordine? *sì* □ *no* □.

Se almeno una delle due lo è, detta questa ρ (dunque $\rho = \ldots$), si disegni a fianco il diagramma di Hasse di $(\mathcal{P}(A), \rho)$.

Questo ha minimo? □ *no*, oppure: □ *sì, esso è:* ...

ha massimo? □ *no*, oppure: □ *sì. esso è:* ...

$(\mathcal{P}(A), \rho)$è un reticolo? *sì* □ *no* □. Nel caso, è distributivo? *sì* □ *no* □, complementato? *sì* □ *no* □, booleano? *sì* □ *no* □.

---

5 Nel gruppo simmetrico $\mathbb{S}_9$ siano $\alpha = (2\,3)(1\,2\,3\,4)(1\,2\,5\,7)$ e β definita da $\binom{1\,2\,3\,4\,5\,6\,7\,8\,9}{9\,5\,3\,2\,4\,7\,8\,1\,6}$. α ha classe pari? *sì* □ *no* □; β ha classe pari? *sì* □ *no* □. Sia poi $\gamma = \alpha\beta$. Allora γ ha classe □ *pari*, □ *dispari*, □ *né pari né dispari*, □ *sia pari che dispari.* Si scriva γ come prodotto di cicli a due a due disgiunti:

$$\gamma = \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

γ ha periodo ... e si ha $\gamma^{2400014} = \ldots\ldots\ldots\ldots\ldots\ldots$ Esiste $\delta \in \mathbb{S}_9$ tale che $\gamma\delta^2 = \beta$? *sì* □ *no* □. Supponiamo assegnata (ma non specificata) un'applicazione σ di $\{1, 2, 3, 4, 5, 6, 7, 8, 9\}$ in sé che non sia iniettiva. σ è suriettiva? *sì* □ *no* □ *impossibile stabilirlo* □. $\sigma\gamma$ è suriettiva? *sì* □ *no* □ *impossibile stabilirlo* □.

6 Sia $V = \{n \in \mathbb{N} \mid n < 8\}$ e siano $A = \big\{\{a,b\} \mid (a,b \in V) \wedge (|a+b| \geq 4)\big\}$, $B = \big\{\{a,b\} \mid (a,b \in V) \wedge (0 < |a-b| < 3)\big\}$, $C = \big\{\{a,b\} \mid (a,b \in V) \wedge (\,(a-b)^2 \leq 6) \wedge (a \neq b)\big\}$. (V,A) è un grafo (semplice)? *sì* □ *no* □. (V,B) è un grafo (semplice)? *sì* □ *no* □. (V,C) è un grafo (semplice)? *sì* □ *no* □.
Se possibile, si scelga uno dei tre che sia un grafo e lo si chiami G (dunque $G = (V, \dots))$, lo si disegni a lato e si risponda alle seguenti domande. G è connesso? *sì* □ *no* □, è un albero? *sì* □ *no* □, è una foresta? *sì* □ *no* □, ha cammini euleriani? *sì* □ *no* □, ha circuiti euleriani? *sì* □ *no* □. Esiste in K_9 (il grafo completo su nove vertici) un sottografo isomorfo a G? *sì* □ *no* □. Quanti lati ha K_9 . . . . Sia $\bar{G}$ il grafo complementare di G. Quanti lati ha $\bar{G}$? . . . . E quante componenti connesse? . . .

---

7 Sia $R = \mathbb{Z}_{3^7}$, l'anello delle classi di resto modulo 3^7. R è commutativo? *sì* □ *no* □, unitario? *sì* □ *no* □, booleano? *sì* □ *no* □, integro? *sì* □ *no* □?, un campo? *sì* □ *no* □. Sia poi $U = \mathcal{U}(R)$. Si ha $|U| = \dots\dots$ U è stabile rispetto alla moltiplicazione in R? *sì* □ *no* □. E rispetto all'addizione? *sì* □ *no* □.

Sia $X = \{[a]_{3^7} \in \mathbb{Z}_{3^7} \mid a \equiv_3 1\}$. Allora $|X| = \dots.$ X è stabile rispetto alla moltiplicazione in R? *sì* □ *no* □. E rispetto all'addizione? *sì* □ *no* □. Si ha $X \subseteq U$? *sì* □ *no* □. $(X, \cdot)$ è un sottogruppo del gruppo degli invertibili di R? *sì* □ *no* □. Posto $g = [4]_{3^7}$, sapendo che $4^{3^5} \not\equiv_{3^7} 1$, possiamo concludere che il periodo di g è: . . . . . $(X, \cdot)$ è ciclico? *sì* □ *no* □.

---

8 Calcolare: $38^3 \bmod 67 = \dots\dots\dots\dots$ Qual è il minimo intero positivo m tale che $38^m \bmod 67 = 1$? □ *tale m non esiste*, oppure: □ *tale m esiste ed è* . . .
Posto $n = 66^{66} + 666(38^{662} + 38^{664} + 38^{666})$, calcolare $n \bmod 67 = \dots.$

Di ognuna delle seguenti equazioni congruenziali si determini l'insieme (risp. S_1, S_2, S_3, S_4) di tutte le soluzioni intere.

(1) $1140x \equiv_{2010} 30$ $(S_1 = \dots\dots\dots\dots\dots\dots)$ (2) $1110x \equiv_{2010} 30$ $(S_2 = \dots\dots\dots\dots\dots\dots)$

(3) $900x \equiv_{2010} 30$ $(S_3 = \dots\dots\dots\dots\dots\dots)$ (4) $870x \equiv_{2010} 30$ $(S_4 = \dots\dots\dots\dots\dots\dots)$

---

9 In $\mathbb{Q}[x]$, si calcoli il massimo comun divisore monico d tra i polinomi $a := 44(g+1)f$ e $b := 3g$, dove $f = x^5 + 3x^4 + 243$ e $g = x^5 + 2x^4 - x^3 + 9x^2 - 18x + 216$. $d = \dots\dots\dots\dots\dots\dots\dots\dots$ Si scrivano poi f e g come prodotti di polinomi irriducibili monici (sempre in $\mathbb{Q}[x]$):

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

Si indichi un minimo comune multiplo tra a e b: . . . .
Le radici (in $\mathbb{Q}$) di f sono: . . . . ; quelle di g sono: . . . . f ha radici in $\mathbb{R}$? *sì* □ *no* □. Esiste un intero positivo n tale che $f + n$ sia irriducibile in $\mathbb{Q}[x]$? □ *no*, oppure: □ *sì, un tale n è* . . . .

Si scrivano f_3 e f_5, cioè il polinomio f riguardato a coefficienti in $\mathbb{Z}_3$ e $\mathbb{Z}_5$ rispettivamente, come prodotti di polinomi irriducibili:

$f_3 = \dots\dots\dots\dots\dots\dots\dots\dots\dots$; $f_5 = \dots\dots\dots\dots\dots\dots\dots\dots\dots$
