CdS in Informatica — a.a. 2008/2009

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) mercoledì 17 giugno 2009

NOME E COGNOME	MATRICOLA

GRUPPO	☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME:	lunedì 22 giugno, ore 9, aula D, DMA

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

- Esiste un intero n multiplo di 15 tale che 3 non divida $7n$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $[11100^7 + 13]_{27}$ è invertibile in $\mathbb{Z}_{27}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(((p \Rightarrow q) \Rightarrow r) \Rightarrow s) \Rightarrow p$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\mathbb{R}, \cdot)$ è un gruppo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esiste un'algebra di Boole B tale che $100 < |B| < 200$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La permutazione $(1\,2\,3\,4\,5\,6)^{14}(1\,2\,3) \in \mathbb{S}_9$ ha classe pari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Per definizione, un albero è . . . .

. . . .

Esistono alberi con esattamente 10^{10} vertici? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

---

3 Sia $G = \{a, b, c, d, e, f\}$, con $|G| = 6$, e si considerino le due operazioni binarie $\otimes$ e $\star$ in G, definite dalle tavole di Cayley qui riportate:

$\otimes$	a	b	c	d	e	f
a	e	f	a	b	c	d
b	d	c	b	a	f	e
c	a	b	c	d	e	f
d	f	e	d	c	b	a
e	c	d	e	f	a	b
f	b	a	f	e	d	c

$\star$	a	b	c	d	e	f
a	b	a	d	d	a	b
b	a	b	d	d	b	a
c	d	d	c	d	c	c
d	d	d	d	d	d	d
e	a	b	c	d	e	f
f	b	a	c	d	f	e

$\otimes$ è commutativa? *sì* ☐ *no* ☐; $\star$ è commutativa? *sì* ☐ *no* ☐. Tenendo presente che sia $\otimes$ che $\star$ sono associative, si stabilisca: $(G, \otimes)$ è un monoide? *sì* ☐ *no* ☐, è un gruppo? *sì* ☐ *no* ☐; nel caso esista, se ne indichi l'elemento neutro: ☐ *non esiste*, oppure: ☐ *esiste*, è . . . $(G, \star)$ è un monoide? *sì* ☐ *no* ☐, è un gruppo? *sì* ☐ *no* ☐; nel caso esista, se ne indichi l'elemento neutro: ☐ *non esiste*, oppure: ☐ *esiste*, è . . .

Per ciascuna delle due operazioni, se esiste l'elemento neutro si indichino il periodo ed il simmetrico di ciascun elemento simmetrizzabile; o si indichi con una crocetta il fatto che l'elemento non è simmetrizzabile:

$\otimes$ a	b	c	d	e	f		a	b	c	d	e	f $\star$
						periodo						
						simmetrico						
						non simmetrizzabile						

---

4 Con $A = \{p \in \mathbb{P} \mid p < 25\}$ (dove $\mathbb{P}$ è l'insieme dei naturali primi) e $B = \{b \in \mathbb{N}^{\#} \mid b < 5\}$, sia $f\colon A \to B$ l'applicazione tale che, per ogni $a \in A$, a^f sia il numero di "1" nella rappresentazione binaria di a (ad esempio, poiché $13 = (1101)_2$, $13^f = 3$). Si ha $|A| =$ . . . , $|B| =$ . . . . f è ben definita? *sì* ☐ *no* ☐. Se lo è, si risponda alle domande seguenti. f è iniettiva? *sì* ☐ *no* ☐. f è suriettiva? *sì* ☐ *no* ☐. Esistono applicazioni $g\colon B \to A$ tali che $fg = \mathrm{id}_A$? *sì* ☐ *no* ☐. E ne esistono tali che $gf = \mathrm{id}_B$? *sì* ☐ *no* ☐. Elencare tutti gli elementi di $\operatorname{im} f = \{$. . . . . $\}$ e $\operatorname{coim} f = \{$. . . . . $\}$.

Calcolare $|A/{\sim_f}| =$ . . . . , dove $\sim_f$ è il nucleo di equivalenza di (o equivalenza associata a) f, $|[2]_{\sim_f}| =$ . . . , $|[3]_{\sim_f}| =$ . . . , $|[7]_{\sim_f}| =$ . . . , $|[19]_{\sim_f}| =$ . . . . Quante sono le applicazioni biettive $A/{\sim_f} \to \operatorname{coim} f$? . . . .

5 Si definisca in $\mathcal{P}(\mathbb{N}) \smallsetminus \{\varnothing\}$ una relazione binaria ρ ponendo, per ogni $X, Y \in \mathcal{P}(\mathbb{N}) \smallsetminus \{\varnothing\}$,

$$X \,\rho\, Y \iff (\exists\, x \in X)(\exists\, y \in Y)(x \mid y).$$

ρ è riflessiva? *sì* ☐ *no* ☐, è una relazione d'ordine largo? ☐ *sì*, oppure: ☐ *no, perché non verifica la proprietà* . . . . *, in quanto* . . . . Sia

$A = \{\{3\}, \{35\}, \{2, 5\}, \{7, 29\}, \{8, 9\}, \{16, 210\}, \{21, 37\}\}.$

ρ induce un ordinamento su A (di questo fatto non è richiesta verifica). Si disegni a lato 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* ☐.
$\min A =$ . . . . , oppure: ☐ $\min A$ *non esiste*;
$\max A =$ . . . . , oppure: ☐ $\max A$ *non esiste*. Esiste $X \in \mathcal{P}(\mathbb{N}) \smallsetminus \{\varnothing\}$ tale che ρ induca su $A \cup \{X\}$ un ordinamento che lo strutturi come reticolo booleano? ☐ *no*, oppure: ☐ *sì, ad esempio* $X =$ . . . .

---

6 Esistono grafi (semplici) G con (esattamente) 8 lati e 10 vertici, di cui uno di grado 7? *sì* ☐ *no* ☐. Nel caso, ne esiste uno connesso? *sì* ☐ *no* ☐. Si determinino il minimo, m, ed il massimo, M, numero possibile di componenti connesse di un tale grafo: $m =$ . . . ; $M =$ . . . . Quanti sono, a meno di isomorfismi, tali grafi? . . . Disegnare qui in basso due tali grafi, a sinistra uno con m componenti connesse, a destra uno con M componenti connesse.

---

7 Per ogni intero y sia $S(y) = \{x \in \mathbb{Z} \mid 1036x^2 - 42x + y^2 \equiv_{259} 0\}$. Determinare, se esiste, il minimo $m \in \mathbb{N}$ tale che $S(m) \neq \varnothing$ [*suggerimento:* $1036 = 4 \cdot 259$] e in tal caso descrivere esplicitamente $S(m)$: ☐ *tale m non esiste*, oppure: ☐ *m esiste, si ha* $m =$ . . . . *e* $S(m) =$ . . . . Calcolare $\left((-27)^{123456} + (-6)^{654321}\right)^2 \bmod 259 =$ . . . . , $|U(\mathbb{Z}_{259})| =$ . . . . .

---

8 Si considerino i polinomi $f := x^5 + 3x^4 - x^2 + 2x - 2$ e $g := x^4 + 5x^3 + 6x^2 - 2x - 4$ in $\mathbb{Q}[x]$. Dopo aver calcolato il massimo comun divisore monico $d =$ . . . . tra f e g in $\mathbb{Q}[x]$ si stabilisca: d è irriducible in $\mathbb{Q}[x]$? *sì* ☐ *no* ☐; d è irriducible in $\mathbb{R}[x]$? *sì* ☐ *no* ☐; d è irriducible in $\mathbb{C}[x]$? *sì* ☐ *no* ☐; $x^{100}d + 2$ è irriducible in $\mathbb{Q}[x]$? *sì* ☐ *no* ☐. Si scrivano f e g come prodotti di polinomi irriducibili monici in $\mathbb{Q}[x]$:

$f =$ . . . . ; $g =$ . . . .

Esistono numeri reali che siano radici sia di f che di g? *sì* ☐ *no* ☐. Esistono in $\mathbb{Q}[x]$ due polinomi non nulli che siano coprimi tra loro ed abbiano qualche radice (in $\mathbb{Q}$) comune? *sì* ☐ *no* ☐. Esistono in $\mathbb{Q}[x]$ due polinomi non nulli e di grado maggiore di 1 che non siano coprimi tra loro e non abbiano alcuna radice (in $\mathbb{Q}$) comune? *sì* ☐ *no* ☐.

Trovare il minimo primo naturale p tale che d, riguardato come polinomio a coefficienti in $\mathbb{Z}_p$, sia irriducibile: $p =$ . . . . Scrivere f_3, cioè f riguardato come polinomio a coefficienti in $\mathbb{Z}_3$, come prodotto di polinomi irriducibili in $\mathbb{Z}_3[x]$: $f_3 =$ . . . .
