CdS in Informatica — a.a. 2009/2010
Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 19 novembre 2010

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: martedì 23 novembre, ore 9, aula D, DMA

1 Vero o falso? Oppure i dati non sono sufficienti per fornire alcuna delle due risposte?
- Nell'anello $\mathbb{Z}_{12}$ l'elemento $[6]_{12}$ è invertibile. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Nell'anello $\mathbb{Z}_{12}$ l'elemento $[6]_{12}$ è idempotente. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esiste almeno un anello booleano B tale che $1000 < |B| < 2000$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\{a \in \mathbb{Z} \mid a \equiv_{30} 18\} \subseteq \{n \in \mathbb{Z} \mid n \equiv_{10} -2\}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'operazione $(u, v) \in \mathbb{R} \times \mathbb{R} \mapsto u + v - 1 \in \mathbb{R}$ è associativa. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Siano A e B insiemi tali che $|A| = 12$, $|B| = 20$ e $|A \cup B| = 25$. Esiste almeno un'applicazione iniettiva da $\mathbb{Z}_8$ a $A \cap B$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Se A è un anello commutativo unitario e f un polinomio in $A[x]$, per definizione, f è *irriducibile* in $A[x]$ se e solo se ....

....

---

3 Sia Φ la forma proposizionale $\big((p \wedge q) \iff (p \vee q)\big) \implies \big((p \Rightarrow r) \Rightarrow (r \Rightarrow q)\big)$. Si completi la tabella a destra calcolando i valori di verità per Φ in funzione di quelli di p, q, r.
Φ è ☐ *una tautologia* ☐ *una contraddizione* ☐ *contingente*.
La forma $p \implies \Phi$ è ☐ *una tautologia* ☐ *una contraddizione* ☐ *contingente*.
La forma $q \iff \Phi$ è ☐ *una tautologia* ☐ *una contraddizione* ☐ *contingente*.

p	q	r	Φ
V	V	F	
F	V	V	
F	F	V	

---

4 Dati $A = \{n \in \mathbb{N} \mid 1 \le n \le 6\}$ e $B = \{n \in \mathbb{N} \mid 1 \le n \le 4\}$, siano $f\colon A \to B$ e $g\colon B \to A$ definite da:

$$f = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 1 & 2 & 1 & 3 & 2 & 4 \end{pmatrix} \qquad g = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 3 & 6 & 5 \end{pmatrix}$$

Allora:

$$fg = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ - & - & - & - & - & - \end{pmatrix} \qquad gf = \begin{pmatrix} 1 & 2 & 3 & 4 \\ - & - & - & - \end{pmatrix}$$

f è iniettiva *sì* ☐ *no* ☐, suriettiva *sì* ☐ *no* ☐; g è iniettiva *sì* ☐ *no* ☐, suriettiva *sì* ☐ *no* ☐;
fg è iniettiva *sì* ☐ *no* ☐, suriettiva *sì* ☐ *no* ☐, una permutazione *sì* ☐ *no* ☐;
gf è iniettiva *sì* ☐ *no* ☐, suriettiva *sì* ☐ *no* ☐, una permutazione *sì* ☐ *no* ☐.
Quante sono le applicazioni $h\colon B \to A$ tali che $fh = \mathrm{id}_A$? . . . Quante quelle $k\colon B \to A$ tali che $kf = \mathrm{id}_B$? . . .
Quante quelle $s\colon A \to B$ tali che $sg = \mathrm{id}_A$? . . . . Quante quelle $t\colon A \to B$ tali che $gt = \mathrm{id}_B$? . . . .
Laddove ne esistano, se ne diano degli esempi:

$$h = \begin{pmatrix} 1 & 2 & 3 & 4 \\ - & - & - & - \end{pmatrix}, \quad k = \begin{pmatrix} 1 & 2 & 3 & 4 \\ - & - & - & - \end{pmatrix}, \quad s = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ - & - & - & - & - & - \end{pmatrix}, \quad t = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ - & - & - & - & - & - \end{pmatrix}.$$

Indicare, senza calcolare, i numeri richiesti. Quante sono le applicazioni da $\mathcal{P}_2(B)$ a A? . . . . Di queste, quante sono inettive? . . . . E quante sono suriettive e non iniettive? . . . . Il numero delle applicazioni non biettive da A a A è . . . . . . Inoltre, $|\mathcal{P}_4(A)| =$ . . . . .

---

5 Nel gruppo $\mathbb{S}_9$, sia $\alpha = (1\,4\,8\,6\,7)(2\,5\,9)(1\,6\,4\,3)$. Si scriva α come prodotto di cicli a due a due disgiunti: $\alpha =$ . . . . Il periodo di α è . . . ; α ha classe ☐ *pari*, ☐ *dispari*. $\alpha^{100000000000000000000}$ ha classe ☐ *pari*, ☐ *dispari*. $\alpha^{300000000000000000000} =$ . . . .

---

6 Sia $(X, |)$ l'insieme dei numeri naturali pari divisori di 100, ordinato per divisibilità (in $\mathbb{N}$). Dunque, $|X| =$ . . . . . Disegnarne qui a fianco il diagramma di Hasse e stabilire quanto segue:
$(X, |)$ è un reticolo? *sì* ☐ *no* ☐, una catena? *sì* ☐ *no* ☐, un reticolo distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐, un sottoreticolo di $(\mathbb{N}, |)$? *sì* ☐ *no* ☐. In $(X, |)$ l'elemento 10 ha:
☐ *nessun complemento*, ☐ *un unico complemento*: esso è . . . ,
☐ *più di un complemento*: essi sono . . . . ;
$\sup\{4, 10, 50\}$ ☐ *non esiste*, oppure: ☐ *esiste* ed è . . . ;
$\inf\{20, 50\}$ non esiste ☐, oppure: ☐ *esiste* ed è . . . .

---

7 Sia S un insieme e sia $\sim$ una relazione di equivalenza in S. Supponiamo che in S esistano due elementi distinti a e b tali che $a \sim b$. Definiamo un grafo G che abbia come vertici gli elementi di S ed in cui due qualunque vertici x e y siano adiacenti se e solo se $x \not\sim y$. Allora:

- G è connesso? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐
- il grafo complementare di G è connesso? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐
- G è una foresta? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐
- se S ha almeno due $\sim$-classi di equivalenza con più di due elementi, G è planare? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

---

8 Calcolare $|\mathcal{U}(\mathbb{Z}_{25})| =$ . . . . Nel gruppo $\mathcal{U}(\mathbb{Z}_{25})$ il periodo di $u := [7]_{25}$ è. . . , l'inverso è $u^{-1} =$ . . . . . Calcolare il resto di $n := 7^{5620}(7^{1001}+7^{1002})+7^{5621}(5^{1001}+5^{1002})$ modulo 25. $n \bmod 25 =$. . . .
Determinare gli insiemi (risp. S_1, S_2, S_3) di tutte le soluzioni intere delle seguenti equazioni conguenziali:

$$630x \equiv_{250} 180 \qquad 450x \equiv_{250} 180 \qquad 630x \equiv_{250} 1260$$

$S_1 =$. . . . . $S_2 =$. . . . . $S_3 =$. . . . .

---

9 Dati in $\mathbb{Q}[x]$ i polinomi $f = x^6 - 10x^4 - x^3 + 30x^2 + 4x - 24$ e $g = x^4 - 6x^2 + 8$, il massimo comun divisore *monico* tra f e g è $d =$ . . . . L'insieme delle radici razionali comuni a f e g è poi $C = \{c \in \mathbb{Q} \mid f(c) = 0 = g(c)\} =$ . . . .
Si decompongano i polinomi d, g ed f nel prodotto di polinomi *monici irriducibili* in $\mathbb{Q}[x]$:

$d =$ . . . . $g =$ . . . .

$f =$ . . . .

Esistono in $\mathbb{Q}[x]$ dei polinomi h e k tali che $(x-4)^2(x+4)^3(x-2)^2 = hf + kg$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐. Ed esistono in $\mathbb{Q}[x]$ dei polinomi u e v tali che $(x-2)^2(x+2)^3(x-4)^2 = uf + vg$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐
Se $f_1 = f/d$ e $g_1 = g/d$, il massimo comun divisore *monico* tra i polinomi ff_1^2 e gg_1^2 è . . . .

Siano f_3 e g_3, rispettivamente, i polinomi f e g riguardati come polinomi in $\mathbb{Z}_3[x]$, e sia $\bar{d}$ il loro massimo comun divisore monico in $\mathbb{Z}_3[x]$. Si decompongano (nell'ordine) f_3, g_3 e $\bar{d}$ nel prodotto di polinomi monici irriducibili in $\mathbb{Z}_3[x]$:

$f_3 =$ . . . . $g_3 =$ . . . .

$\bar{d} =$ . . . .

L'insieme delle radici comuni a f_3 e g_3 in $\mathbb{Z}_3$ è $C_3 = \{c \in \mathbb{Z}_3 \mid f_3(c) = 0 = g_3(c)\} =$ . . . .
