CdL e CdD in Informatica — a.a. 2002/2003

Esercitazione scritta di **ALGEBRA** (Prof. Rao) giovedì 8 gennaio 2004

NOME E COGNOME	MATRICOLA

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

- $p \Rightarrow \big((q \wedge r) \Rightarrow r\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\big((p \wedge q) \Rightarrow p\big) \Rightarrow r$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esiste almeno un reticolo di Boole B tale che $800 < |B| < 1000$ *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Un intero n tale che $400 < n < 450$ è primo se e solo se non è divisibile per nessuno dei primi otto numeri primi. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Ogni albero è una foresta, ma esistono foreste che non sono alberi. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Ogni corpo ha esattamente due ideali sinistri. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Nell'anello $\mathbb{Z}_{12}$ l'elemento $[4]_{12}$ è nilpotente. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Siano A e B insiemi tali che $|A| = 10$, $|B| = 20$ e $|A \cup B| = 22$. Allora esiste almeno un'applicazione iniettiva di $\mathbb{Z}_9$ in $A \cap B$. *vero* ☐ *falso* ☐ *dati insuff.* ☐

---

2 [*Riportare i calcoli relativi a questo esercizio e le motivazioni alle risposte sul retro di questo foglio*]
Dati in $\mathbb{Q}[x]$ i polinomi $f = x^6 - 10x^4 + x^3 + 30x^2 - 4x - 24$ e $g = x^4 - 6x^2 + 8$, con l'algoritmo euclideo si trovino: il massimo comun divisore *monico* d di f e g e quindi dei polinomi u_0, $v_0 \in \mathbb{Q}[x]$ tali che $d = u_0 f + v_0 g$. Si trovino poi l'insieme C delle radici razionali comuni a f e g e si calcolino i quozienti $g_1 = g/d$ e $f_1 = f/d$.

[Risposte: $d =$ . . . .

$u_0 =$ . . . . $v_0 =$ . . . .

$C = \{c \in \mathbb{Q} \mid f(c) = 0 = g(c)\} =$ . . . .

$g_1 =$ . . . . $f_1 =$ . . . .]

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* ☐

Qual è il massimo comun divisore *monico* dei polinomi ff_1^2 e gg_1^2? [*non occorre fare calcoli!*] . . . .
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 $\mathbb{Z}_3[x]$:

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

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

Quali sono le radici comuni a f_3 e g_3 in $\mathbb{Z}_3$? $C_3 = \{c \in \mathbb{Z}_3 \mid f_3(c) = 0 = g_3(c)\} =$ . . . .

---

3 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 $a \not\sim b$. Definiamo un grafo G che abbia come vertici gli elementi di S e tale che due qualunque vertici distinti x e y siano adiacenti se e solo se $x \sim y$. 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 $|S| \leq 5$, G è planare? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

---

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

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

Allora:

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

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 sono le applicazioni $k\colon B \to A$ tali che $kf = \mathrm{id}_B$? . . . .

Quante sono le applicazioni $s\colon A \to B$ tali che $sg = \mathrm{id}_A$? . . . .

Quante sono le applicazioni $t\colon A \to B$ tali che $gt = \mathrm{id}_B$? . . . .

Se esistono, se ne diano degli esempi:

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

Quante sono le applicazioni di $\mathcal{P}_2(A)$ in B? . . . . Di queste, quante sono inettive? . . . . E quante sono suriettive e non iniettive? . . . . Il numero delle applicazioni non biettive di A in A è . . . . Inoltre, $|\mathcal{P}_4(B)| =$ . . . . .

---

5 Calcolare $|\mathcal{U}(\mathbb{Z}_{25})| =$ . . . . Qual è il periodo di $u := [7]_{25}$ nel gruppo $\mathcal{U}(\mathbb{Z}_{25})$? . . . . E qual è l'inverso di u? $u^{-1} =$ . . . .

Calcolare il resto di $n := 7^{5620}(7^{1001} + 7^{1002}) + 7^{5621}(5^{1001} + 5^{1002})$ modulo 25. $n \bmod 25 =$ . . . . .

Determinare l'insieme delle soluzioni in $\mathbb{Z}$ di ciascuna delle seguenti equazioni congruenziali. *[Trascrivere il procedimento effettuato sul retro di questo foglio.]*

$630x \equiv 180 \pmod{250}$ *insieme delle soluzioni:* . . . .

$450x \equiv 180 \pmod{250}$ *insieme delle soluzioni:* . . . .

$630x \equiv 1260 \pmod{250}$ *insieme delle soluzioni:* . . . .

---

6 Sia $\big(D(20), |\,\big)$ l'insieme dei numeri naturali divisori di 20, ordinato per divisibilità. Disegnarne qui a fianco il diagramma di Hasse e stabilire quanto segue:
$\big(D(20), |\,\big)$ è un reticolo? *sì* ☐ *no* ☐ è una catena? *sì* ☐ *no* ☐
è un reticolo distributivo? *sì* ☐ *no* ☐ è un reticolo complementato? *sì* ☐ *no* ☐
è un reticolo booleano? *sì* ☐ *no* ☐
In $\big(D(20), |\,\big)$ l'elemento 5 ha:
nessun complemento *sì* ☐ *no* ☐
un unico complemento *sì* ☐ *no* ☐, esso è . . .
più di un complemento *sì* ☐ *no* ☐, essi sono . . . .
$\sup\{2, 4, 5\}$ non esiste ☐, oppure è . . . $\inf\{4, 5\}$ non esiste ☐, oppure è . . .
