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

Esercitazione scritta di **ALGEBRA** (Prof. Rao) mercoledì 23 luglio 2003

NOME E COGNOME	MATRICOLA

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

- Se $+$ e $\cdot$ indicano le usuali operazioni di addizione e moltiplicazione, $(\mathbb{N}, +, \cdot)$ è un anello commutativo. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- $\big(\neg(p \wedge q) \iff (\neg q \vee \neg p)\big) \iff \big(q \vee \neg q\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Sia α una permutazione di un insieme finito. Allora α^2 è di classe pari. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Siano A e B insiemi tali che $|A| = 16$, $|B| = 17$ e $|A \cap B| = 8$. Esistono applicazioni suriettive da $A \cup B$ a $\mathbb{Z}_{20}$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Sia B reticolo booleano, e sia $x \in B$. x ha uno ed un solo complemento in B. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Siano p e q due numeri primi distinti. p^q divide q^p. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Per definizione, un corpo è un anello in cui ogni elemento diverso da zero è invertibile. *vero* ☐ *falso* ☐
- $[3]_6$ è idempotente in $\mathbb{Z}_6$. *vero* ☐ *falso* ☐ *dati insuff.* ☐

---

2 Calcolare $|\mathcal{U}(\mathbb{Z}_{165})| = \ldots\ldots\ldots$ Qual è il periodo di $u := [2^5]_{165}$ nel gruppo $\mathcal{U}(\mathbb{Z}_{165})$? . . . . E qual è l'inverso di u? $u^{-1} = \ldots\ldots\ldots$

Calcolare il resto di $n := 32^{4320} + 32^{4321} + 32^{4322} + 32^{4323} + 3^{10}5^{100}11^{1000}$ modulo 165. $n \bmod 165 = \ldots\ldots$

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

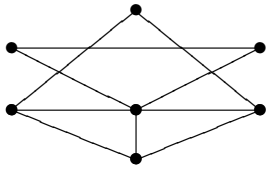
$2^{105}x \equiv 2^{100} \pmod{165}$ *insieme delle soluzioni:* $\ldots\ldots\ldots$

$2^{100}x \equiv 2^{105} \pmod{165}$ *insieme delle soluzioni:* $\ldots\ldots\ldots$

$2^{105}x \equiv 2^{100} \cdot 3 \pmod{165}$ *insieme delle soluzioni:* $\ldots\ldots\ldots$

---

3 Sia $G = (V, L)$ il grafo disegnato qui a destra. G ha un sottoalbero massimale? *sì* ☐ *no* ☐. Nel caso, quanti vertici (: . . . .) e quanti lati (: . . . .) ha questo sottoalbero?, oppure: non è possibile stabilirlo ☐



G ha un circuito euleriano? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

G ha un cammino euleriano? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

Esiste $l \in L$ tale che il sottografo $(V, L \setminus \{l\})$ di G (cioè quello ottenuto da G cancellando il lato l) abbia un circuito euleriano? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐ Nel caso, quanti tali lati l esistono? . . . .

Esiste $l \in L$ tale che il sottografo $(V, L \setminus \{l\})$ abbia un cammino euleriano? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐. Nel caso, quanti tali lati l esistono? . . . .

---

4 Siano $f : (x, y) \in \mathbb{Z} \times \mathbb{Z} \mapsto (-x, y) \in \mathbb{Z} \times \mathbb{Z}$ e $g : (x, y) \in \mathbb{Z} \times \mathbb{Z} \mapsto (x, -y) \in \mathbb{Z} \times \mathbb{Z}$. Allora:

$$fg : (u, v) \in \ldots\ldots\ldots \longmapsto \ldots\ldots\ldots \in \ldots\ldots\ldots .$$

f è: iniettiva *sì* ☐ *no* ☐, suriettiva *sì* ☐ *no* ☐, biettiva *sì* ☐ *no* ☐

g è una permutazione di $\mathbb{Z} \times \mathbb{Z}$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

È vero che l'insieme $S := \{f, g, fg\}$, munito dell'operazione di prodotto operativo, costituisce un gruppo? *sì* ☐ *no* ☐

Detta id l'applicazione identica di $\mathbb{Z} \times \mathbb{Z}$, l'insieme $S \cup \{id\}$, munito dell'operazione di prodotto operativo, costituisce un gruppo? *sì* ☐ *no* ☐.

Nel caso in cui almeno una delle due risposte precedenti sia positiva, indicare i periodi di ciascuno degli elementi nel corrispondente gruppo:

f ha periodo . . . . g ha periodo . . . . fg ha periodo . . . . (id ha periodo . . . .)

Sia $h : \mathbb{Z} \times \mathbb{Z} \longrightarrow \mathbb{Z} \times \mathbb{Z}$ un'applicazione tale che $\operatorname{im} h$ sia finito. Allora:

fgh è: iniettiva *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐, suriettiva *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.

---

5 Siano $A = \{1, 2, 3, 4\}$ e $B = \{n \in \mathbb{Z} \mid 0 < n < 10\}$. Siano ρ e σ le relazioni binarie in B^A definite da:

$$\forall f, g \in B^A \qquad f \;\rho\; g \iff f(3) = g(3)$$
$$f \;\sigma\; g \iff \exists i \in B \quad \left|f^{-1}(\{i\})\right| = \left|g^{-1}(\{i\})\right|$$

ρ è una relazione di equivalenza? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐
σ è una relazione di equivalenza? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

Se almeno una delle due è una relazione di equivalenza, con riferimento a questa (specificare quale: . . . .), si indichi la cardinalità dell'insieme quoziente: $\left|B^A/_{\dots}\right| =$ . . . . . e quella della classe di equivalenza di $\iota : x \in A \mapsto x \in B$: $\left|[\iota]_{\dots}\right| =$ . . . . . .

---

6 [*Riportare i calcoli relativi a questo esercizio e le motivazioni alle risposte sul retro di questo foglio*]
Dati in $\mathbb{Q}[x]$ i polinomi $f = x^7+6x^6+13x^5+10x^4-5x^3-14x^2-9x-2$ e $g = x^5+4x^4+3x^3-5x^2-8x-3$, con l'algoritmo euclideo si trovino: il massimo comun divisore *monico* d di f e g; dei polinomi u, $v \in \mathbb{Q}[x]$ tali che $d = uf + vg$; l'insieme C delle radici razionali comuni a f e g. Calcolati poi i quozienti $g_1 = g/d$ e $f_1 = f/d$, si trovino: il massimo comun divisore *monico* d_1 di f_1 e g_1; dei polinomi u_1, $v_1 \in \mathbb{Q}[x]$ tali che $d_1 = u_1 f_1 + v_1 g_1$; l'insieme C_1 delle radici razionali comuni a f_1 e g_1.

[Risposte: $d =$ . . . . . .
$u =$ . . . . . $v =$ . . . . . .
$C = \{c \in \mathbb{Q} \mid f(c) = 0 = g(c)\} =$ . . . . . .
$g_1 =$ . . . . . $f_1 =$ . . . . . .
$d_1 =$ . . . . . .
$u_1 =$ . . . . . $v =$ . . . . . .
$C_1 = \{c \in \mathbb{Q} \mid f_1(c) = 0 = g_1(c)\} =$ . . . . .]

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 $(x+1)^4 = hf + kg$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐
Esistono in $\mathbb{Q}[x]$ dei polinomi s e t tali che $(x-1)^4 = sf + tg$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐

Qual è il massimo comun divisore *monico* dei polinomi ff_1 e gg_1? . . . . . [*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 $\mathbb{Z}_3$? $C_3 = \{c \in \mathbb{Z}_3 \mid f_3(c) = 0 = g_3(c)\} =$ . . . . . .
