CdL in Informatica — a.a. 2005/2006
Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) lunedì 17 luglio 2006

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *IV (Cutolo)*	PREFERENZA PER L'ESAME ☐ *urgenti* ☐ *non urgenti*

1 La forma proposizionale $\big((p \Rightarrow q) \Rightarrow p\big) \iff (q \Rightarrow p)$ è ☐ *una tautologia*, ☐ *una contraddizione*, ☐ *nessuna delle due*, ☐ *entrambe*.

---

2 Si consideri l'operazione binaria $*$ definita in $S = \mathbb{Z} \times \mathbb{Z}$ ponendo, per ogni $a, b, c, d \in \mathbb{Z}$,

$$(a, b) * (c, d) = (ac, b + d).$$

$*$ è commutativa? *sì* ☐ *no* ☐, è associativa? *sì* ☐ *no* ☐, esistono in $(S, *)$ elementi neutri? *sì* ☐ *no* ☐, nel caso, indicarne uno: . . . . e dire se ce ne sono altri: *sì* ☐ *no* ☐.

	cancellabile		simmetrizzabile		*se simmetrizzabile:*	
	sì	*no*	*sì*	*no*	simmetrico	periodo
$(0, 0)$						
$(-1, 0)$						
$(5, 1)$						
$(1, 1)$						

Con riferimento all'operazione $*$, completare la tabella a sinistra. Esistono in S elementi:
simmetrizzabili ma non cancellabili? *sì* ☐ *no* ☐
(nel caso, uno è . . . .);
cancellabili ma non simmetrizzabili? *sì* ☐ *no* ☐
(nel caso, uno è . . . .);
non cancellabili? *sì* ☐ *no* ☐
(nel caso, uno è . . . .).

Elencare tutti gli elementi idempotenti in $(S, *)$: . . . .

$(S, *)$ è un semigruppo? *sì* ☐ *no* ☐, un monoide? *sì* ☐ *no* ☐, un gruppo? *sì* ☐ *no* ☐; l'insieme $\mathbb{Z} \times 2\mathbb{Z}$ ne è una parte stabile? *sì* ☐ *no* ☐.

Dire quali delle seguenti applicazioni sono e quali non sono omomorfismi (rispetto alle operazioni indicate):

$\alpha\colon (a, b) \in (S, *) \mapsto a \in (\mathbb{Z}, +)$; $\gamma\colon a \in (\mathbb{Z}, \cdot) \mapsto (a, 0) \in (S, *)$; $\varepsilon\colon a \in (\mathbb{Z}, +) \mapsto (a, a) \in (S, *)$;
$\beta\colon (a, b) \in (S, *) \mapsto b \in (\mathbb{Z}, +)$; $\delta\colon a \in (\mathbb{Z}, \cdot) \mapsto (a, 1) \in (S, *)$; $\zeta\colon a \in (\mathbb{Z}, +) \mapsto (1, a) \in (S, *)$.

sono omomorfismi: . . . . ; non sono omomorfismi: . . . .

---

3 Sia t un numero intero positivo, e sia $n = 17653^t + 37^3\binom{25}{11}$. Stabilire se:
- almeno uno tra $n-2$, $n-1$, n, $n+1$, $n+2$ è multiplo di 5 *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- 40 divide $(n-2)(n-1)n(n+1)(n+2)$ *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- almeno uno tra n^7-3, n^7-1, n^7+1 è multiplo di 3 *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- almeno due tra n^7-3, n^7-1, n^7+1 sono multipli di 3 *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- almeno uno tra $n-2$, $n-1$, $n+1$, $n+2$ è multiplo di 5 *vero* ☐ *falso* ☐ *dati insufficienti* ☐

Si calcoli $n \bmod 5 =$ . . . . nel caso in cui $t = 892367$.

---

4 Sia D l'insieme dei divisori positivi di 36. Si consideri D ordinato dalla relazione d'ordine ρ definita ponendo, per ogni $a, b \in D$,

$$a \mathrel{\rho} b :\iff \big(a \mid b \wedge (a \bmod 10) \leq (b \bmod 10)\big).$$

Disegnare a fianco il diagramma di Hasse di D.
Esiste $\min D$? ☐ *no*, oppure: ☐ *sì, ed esso è* . . . .
Esiste $\max D$? ☐ *no*, oppure: ☐ *sì, ed esso è* . . . .
$\inf\{3, 12\} =$ . . . . , oppure: ☐ $\inf\{3, 12\}$ *non esiste*
$\sup\{3, 12\} =$ . . . . , oppure: ☐ $\sup\{3, 12\}$ *non esiste*
D è un reticolo? ☐ *no* ☐ *sì*.
Elencare tutti gli elementi minimali di D: . . . . , oppure: ☐ *non ne esistono*
Elencare tutti gli elementi massimali di D: . . . . , oppure: ☐ *non ne esistono*

Sia Y la parte di X della cardinalità massima possibile tale che Y, munito dell'ordinamento indotto da ρ, sia un reticolo (dunque $X \setminus Y = \{$. . . . .$\}$ e $|Y| =$ . . .). Questo reticolo è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.

5 *Completare:* il piccolo teorema di Fermat asserisce che, scelti comunque un intero a ed un primo positivo p, si ha $a^{\cdots} \equiv_p a$.

---

6 Sia $n = 1789$. Esiste un grafo semplice $G = (V, L)$ tale che $|V| = n$ e $|L| = \binom{n}{2} - 1$? *sì* □ *no* □ *impossibile stabilirlo* □. Ne esistono due tra loro non isomorfi? *sì* □ *no* □ *impossibile stabilirlo* □.
Se un tale grafo G esiste, esso è connesso? *sì* □ *no* □ *impossibile stabilirlo* □,
è una foresta? *sì* □ *no* □ *impossibile stabilirlo* □,
ha cammini euleriani? *sì* □ *no* □ *impossibile stabilirlo* □,
ha circuiti euleriani? *sì* □ *no* □ *impossibile stabilirlo* □.
Quante componenti connesse ha il suo grafo complementare? . . . . . .

7

la relazione è	ρ sì	ρ no	σ sì	σ no	τ sì	τ no	φ sì	φ no	ψ sì	ψ no
riflessiva										
antiriflessiva										
simmetrica										
antisimmetrica										
transitiva										
di ordine stretto										
di ordine largo										
di equivalenza										

Si completi la tabella, con riferimento alle relazioni binarie definite in $\mathbb{Z}$ come qui specificato.

Per ogni $a, b \in \mathbb{Z}$:

$a \;\rho\; b :\iff a^2 + 4 \equiv_7 b^2 - 3$

$a \;\sigma\; b :\iff a^2 + b = 1$

$a \;\tau\; b :\iff (a \le b \vee b \le a)$

$a \;\varphi\; b :\iff a + 1 = b + 1$

$a \;\psi\; b :\iff a - 1 \equiv_8 b + 3$

---

8 Il polinomio $p = x^8 - 5$ è irriducibile in $\mathbb{Q}[x]$? *sì* □ *no* □. Perché? . . . .
Si considerino i polinomi $h = 8x^4 - 16x^3 + 11x - 4$ e $k = 4x^3 - 12x^2 + 11x - 3$.

L'intero $h(3)$ è □ *pari*, □ *dispari*, □ *né pari né dispari*, □ *sia pari che dispari*. Siano

$$f = p^2 h \qquad \text{e} \qquad g = (x-3)^3 pk.$$

Si trovino il massimo comun divisore *monico* d di f e g e l'insieme $C = \{c \in \mathbb{Q} \mid f(c) = g(c) = 0\}$:

$d =$ . . . . , $C =$ . . . .

Si decompongano poi d e g in prodotto di un elemento invertibile e polinomi monici irriducibili:

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

Detti infine f_2 e g_2 i polinomi f e g riguardati come polinomi a coefficienti in $\mathbb{Z}_2$ si scrivano f_2 e g_2 come prodotti di polinomi irriducibili monici in $\mathbb{Z}_2[x]$:

$f_2 =$ . . . . $g_2 =$ . . . .

e se ne indichino il massimo comun divisore *monico* d^* ed il minimo comune multiplo *monico* m^*:

$d^* =$ . . . .

$m^* =$ . . . .

---

9 Tenendo presente che $1 = 21 \cdot 281 - 59 \cdot 100$, si determini $100^{-1} \bmod 21 =$ . . . . e si trovi l'insieme (rispettivamente S_1, S_2) di tutte le soluzioni intere di ciascuna delle seguenti equazioni congruenziali:

$200x \equiv_{42} 6$. $S_1 =$ . . . . $210x \equiv_{59} 10$. $S_2 =$ . . . .
