CdL in Informatica — a.a. 2006/2007

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) mercoledì 20 giugno 2007

NOME E COGNOME	MATRICOLA

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

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

- Il polinomio $(x^3+2)(x+5)$ è irriducibile in $\mathbb{Q}[x]$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- È fissato un polinomio $f \in \mathbb{Z}_{19}[x]$ di grado 8 i cui fattori irriducibili monici hanno gradi 2, 3, 3. f ha radici in $\mathbb{Z}_{19}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- È data una tautologia Φ. La forma $(p \Rightarrow p) \iff \Phi$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esistono infiniti interi m tali che $19478236 = 19478236 \bmod m$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Ogni reticolo booleano è distributivo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\mathbb{N}, -)$ è un gruppo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\mathbb{N}, +)$ è un gruppo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- In $\mathbb{S}_5$ esiste una trasposizione τ tale che $(2\,5)(1\,5)\tau$ sia la permutazione identica. *vero* ☐ *falso* ☐ *dati insuff.* ☐

---

2 Per definizione, un elemento x di un semigruppo $(S, *)$ è cancellabile a destra se e solo se:

....

Si fornisca un esempio di elemento non cancellabile a destra in $(\mathbb{Z}, \cdot)$: . . . . ; oppure: ☐ *non ne esistono.*

---

3 Siano $S = \{1,2,3,4,5\}$, $A = \{(u,v) \in S \times S \mid u = v+1\}$, $B = \big\{X \in \mathcal{P}(S) \mid (\forall a,b,c \in S)(X \neq \{a,b,c\})\big\}$.

Si calcolino $|A| =$ . . . . , $|B| =$ . . . . , $|B \setminus A| =$ . . . . , $|\mathcal{P}_2(A)| =$ . . . . , $|\operatorname{Map}(A,S)| =$ . . . . , $|\operatorname{InjMap}(A,S)| =$ . . . . , $|\operatorname{InjMap}(B,A)| =$ . . . . .

---

4 Si consideri L'anello $(R, +, \cdot)$, dove $R = \{a,b,c,d,e,f,g,h\}$ è tale che $|R| = 8$ e $+$ e $\cdot$ sono definite dalle tavole di Cayley (si ricorda che queste indicano, ad esempio, che $c+f=e$ e $bg=g$):

$+$	a	b	c	d	e	f	g	h
a	a	b	c	d	e	f	g	h
b	b	e	d	f	g	h	a	c
c	c	d	a	b	f	e	h	g
d	d	f	b	e	h	g	c	a
e	e	g	f	h	a	c	b	d
f	f	h	e	g	c	a	d	b
g	g	a	h	c	b	d	e	f
h	h	c	g	a	d	b	f	e

$\cdot$	a	b	c	d	e	f	g	h
a	a	a	a	a	a	a	a	a
b	a	b	a	b	e	e	g	g
c	a	a	c	c	a	c	a	c
d	a	b	c	d	e	f	g	h
e	a	e	a	e	a	a	e	e
f	a	e	c	f	a	c	e	f
g	a	g	a	g	e	e	b	b
h	a	g	c	h	e	f	b	d

Lo zero di R è $0_R =$ . . . .
R è commutativo? *sì* ☐ *no* ☐
R è unitario? *sì* ☐ *no* ☐. Nel caso, la sua unità è $1_R =$ . . . .
Si elenchino in R gli elementi:
invertibili: ....
cancellabili: ....
divisori dello zero: ....
idempotenti: ....
R è un dominio di integrità? *sì* ☐ *no* ☐
R è un campo? *sì* ☐ *no* ☐

R è isomorfo all'anello $(\mathbb{Z}_8, +, \cdot)$? *sì* ☐ *no* ☐; R è isomorfo all'anello $(\mathcal{P}(\{1,2,3\}), \Delta, \cap)$? *sì* ☐ *no* ☐.

---

5 Determinare (se esiste) una coppia $(x,y) \in \mathbb{Z} \times \mathbb{Z}$ tale che $302x + 298y = 2$ e $200 < y < 300$:
$x =$ . . . . e $y =$ . . . . , oppure ☐ *tale coppia non esiste.*

Per ognuna delle seguenti equazioni congruenziali si trovi l'insieme (risp. S_1, S_2, S_3) di tutte le soluzioni intere:

$149x \equiv_{151} 2$. $\Big[S_1 =$ . . . . $\Big]$. $151x \equiv_{149} 2$. $\Big[S_2 =$ . . . . $\Big]$. $151x \equiv_{149} 149$. $\Big[S_3 =$ . . . . $\Big]$.

Calcolare $44^{9999} \bmod 149 =$ . . . . Qual è il periodo di $[44]_{149} \in \mathcal{U}(\mathbb{Z}_{149})$? . . . . .

E qual è il periodo di $[148]_{149} \in \mathcal{U}(\mathbb{Z}_{149})$? . . . . .

6 Un albero G ha (esattamente) 144 vertici, 142 dei quali hanno grado 2. Quali sono i gradi dei due rimanenti vertici? . . . e . . . , oppure: ☐ *impossibile stabilirlo.* Quanti lati ha G? . . . . . Esistono due tali alberi non isomorfi tra loro? *sì* ☐ *no* ☐.

In un multigrafo connesso M con (esattamente) 800 lati e 100 vertici quanti lati vanno cancellati per ottenere un sottoalbero massimale? . . . . , oppure: ☐ *è impossibile stabilirlo.* M ha circuiti euleriani? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.

---

7 Un generatore casuale fornisce un intero positivo n. Sia $m = 3(6n + 1)$.
$[9]_m \in \mathcal{U}(\mathbb{Z}_m)$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐. $[10]_m \in \mathcal{U}(\mathbb{Z}_m)$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.
$[1]_m \in \mathcal{U}(\mathbb{Z}_m)$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.
$|\mathcal{U}(\mathbb{Z}_m)|$ è ☐ *pari,* ☐ *dispari,* ☐ *né pari né dispari,* ☐ *sia pari che dispari,* ☐ *impossibile stabilirlo.*

---

8 Sia $S = \mathbb{N} \times \mathbb{N}$ ordinato dalla relazione d'ordine ρ definita da: $\forall (a, a'), (b, b') \in S$,

$$(a, a')\ \rho\ (b, b') :\iff (a \leq b \wedge (a' \bmod 2) < (b' \bmod 2)).$$

(S, ρ) è totalmente ordinato? *sì* ☐ *no* ☐, è un reticolo? *sì* ☐ *no* ☐. Posto $T = \{(34, 3), (34, 5), (108, 1), (2, 11)\}$, si determini (in S) $\inf T =$ . . . . , oppure: ☐ $\inf T$ *non esiste.*
$(\mathbb{N}, <)$ è isomorfo a $\{(n, 2n) \mid n \in \mathbb{N}\}$, ordinato dall'ordinamento indotto da ρ? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐. Si disegni a fianco il diagramma di Hasse di $X := \{(4, 9), (11, 12), (3, 7), (6, 0), (12, 5)\}$ ordinato dall'ordinamento indotto da ρ. Questo è un reticolo? *sì* ☐ *no* ☐. Nel caso, è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐. $\min X =$ . . . . , oppure: ☐ $\min X$ *non esiste.* $\max X =$ . . . . , oppure: ☐ $\max X$ *non esiste.*

---

9 Siano $A = \{n \in \mathbb{N} \mid n < 30\}$ e $B = \{n \in \mathbb{N}^{\#} \mid n \leq 8\}$. Sia $f\colon A \to B$. Si considerino le relazioni binarie α, β e γ in A definite da: per ogni $x, y \in A$,

$$x\ \alpha\ y :\iff x^f = y^f + 1; \qquad x\ \beta\ y :\iff x^f + 1 = y^f + 1; \qquad x\ \gamma\ y :\iff x^f = y^f.$$

Quali tra α, β e γ sono: . . . . e quali non sono: . . . . equivalenze? Se possibile, si scelga una relazione di equivalenza ρ tra α, β e γ (dunque $\rho =$ . . .). Si ha $|A/\rho| =$ . . . . , oppure: ☐ *è impossibile calcolare* $|A/\rho|$. Nell'ulteriore ipotesi che f sia suriettiva, si ha $|A/\rho| =$ . . . . , oppure: ☐ *anche in questo caso è impossibile calcolare* $|A/\rho|$. Esiste $f \in \mathrm{Map}(A, B)$ tale che $|A/\rho| = |A|$, se ρ è definita come sopra? *sì* ☐ *no* ☐. Infine, se $f\colon x \in A \mapsto 2 + (x \bmod 4) \in B$, si ha $|A/\rho| =$ . . . . e $[14]_\rho = \{$ . . . . $\}$ (dunque $\left|[14]_\rho\right| =$ . . . .).

---

10 Si consideri l'operazione binaria $\perp$ definita in $T := \mathbb{Q}[x] \setminus \{0\}$ ponendo, per ogni $f, g \in T$, $f \perp g$ uguale al massimo comun divisore tra f e g che abbia coefficiente direttore 4. L'operazione $\perp$ è commutativa? *sì* ☐ *no* ☐, associativa? *sì* ☐ *no* ☐. Esiste in T elemento neutro rispetto a $\perp$? ☐ *no*, oppure: ☐ *sì, esso è* . . . . Posto $f = x^5 + x^3 + 5x^2 + 5$ e $g = x^4 - 2x^3 - 2x^2 - 2x - 3$, si calcoli $d := f \perp g$:

$$d = \ldots\ldots\ldots\ldots\ldots\ldots$$

e si scrivano f e g come prodotti di polinomi monici irriducibili $\mathbb{Q}[x]$:

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

$g + 9$ è irriducibile in $\mathbb{Q}[x]$? ☐ *no, perché* . . . . , oppure:
☐ *sì, perché* . . . .
