CdL in Informatica — a.a. 2005/2006

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao)   giovedì 29 giugno 2006

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?

- La formula $\big(p \vee \neg p\big) \implies \big(p \wedge q \wedge \neg r \wedge (s \vee t)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $[205018345]_{3^{100}}$ è invertibile nell'anello $\mathbb{Z}_{3^{100}}$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Esiste un'algebra di Boole di cardinalità compresa tra 1500 e 1600. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Sia $\sigma \in \mathbb{S}_9$. Allora $(2\,1\,6\,8)\sigma^{11}(1\,2)(1\,4\,5)$ è di classe pari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\{a \in \mathbb{N} \mid a^2 \equiv_{19} 9 \ \wedge\ 10 \le a \le 25\} = \{b \in \mathbb{Z} \mid b \equiv_6 4 \ \wedge\ 14 \le b \le 24\}$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- L'applicazione $a \in \mathbb{N} \mapsto [2a]_8 \in \mathbb{Z}_8$ è suriettiva. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'operazione binaria $*$ definita in $\mathbb{Z}$ ponendo, per ogni $a, b \in \mathbb{Z}$, $a * b = 13$ è associativa.
  vero ☐ *falso* ☐ *dati insufficienti* ☐

---

2 *Si completi:* se l'anello (commutativo unitario) A è un . . . . , il numero delle radici di un polinomio non nullo $f \in A[x]$ non può superare il grado di f.

---

3 Indicare, se esiste:

– il minimo intero n maggiore di 1 che sia coprimo con 2, 3, 4, 5, 6 e 7. n= . . . . , oppure ☐ *tale n non esiste*

– il massimo intero n che sia coprimo con 2, 3, 4, 5, 6 e 7. n= . . . . , oppure ☐ *tale n non esiste*

---

4 Sia $S = \{1, 2, 3\}$, si calcoli $|\mathcal{P}(S)| =$ . . . . ; si consideri l'applicazione $f := X \in \mathcal{P}(S) \longmapsto |X| + 1 \in \mathbb{N}$. f è un omomorfismo da $\big(\mathcal{P}(S), \cap\big)$ a $(\mathbb{N}, \cdot)$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.

Sia $\sim$ l'unica relazione di equivalenza in $\mathcal{P}(S)$ tale che, per ogni $X, Y \in \mathcal{P}(S)$:

$$(X^f = Y^f \Rightarrow X \sim Y) \quad \wedge \quad (|X \smallsetminus Y| \ge 2 \Rightarrow X \not\sim Y) \quad \wedge \quad \varnothing \sim \{3\} \not\sim \{2,3\} \quad \wedge \quad S \not\sim \{1,2\}.$$

Si calcoli $|\mathcal{P}(S)/{\sim}| =$ . . . e si indichino le classi di equivalenza modulo $\sim$ elencandone esplicitamente gli elementi:

$$\mathcal{P}(S)/{\sim} = \Big\{ \ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots \Big\}$$

---

5 Siano $a = 337$, $b = 119$ e $p = 65537$. Tenendo presente che p è un numero primo, per ciascuna delle seguenti equazioni congruenziali si trovi l'insieme (rispettivamente $S_1, S_2, S_3, S_4, S_5, S_6$) di tutte le soluzioni intere:

$2ax \equiv_{2b} 4$. $S_1 =$ . . . . $3pax \equiv_{3b} 6p$. $S_2 =$ . . . .

$2ax \equiv_{2b} 3$. $S_3 =$ . . . . $2ax \equiv_{8b} 6a$. $S_4 =$ . . . .

$bx \equiv_a 1$. $S_5 =$ . . . . $3ab^2x \equiv_a 5$. $S_6 =$ . . . .

Si calcolino l'inverso di b modulo a e l'insieme S delle soluzioni dell'equazione diofantea $ax + by = 1$: $b^{-1} \bmod a =$ . . . . ,

$$S = \{(\alpha, \beta) \in \mathbb{Z} \times \mathbb{Z} \mid a\alpha + b\beta = 1\} = \ldots\ldots\ldots\ldots\ldots\ldots$$

Sia $(\alpha, \beta) \in S$ e sia $m = ab$. $[a\alpha]_m$ è idempotente in $\mathbb{Z}_m$? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐ (*Suggerimento:* si osservi che $a\alpha = a\alpha(a\alpha + b\beta)$). Si consideri l'applicazione

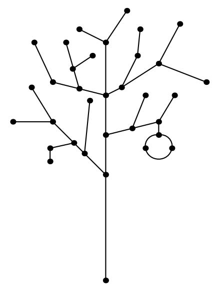
$$f \colon [n]_m \in \mathbb{Z}_m \longmapsto [a\alpha n]_m \in \mathbb{Z}_m.$$

f è un omomorfismo di anelli? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐, un isomorfismo? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐. f è un omomorfismo di anelli unitari? *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.

Posto $h = b^5 - 1$, si calcoli il periodo di $[b]_h$ in $\mathbb{Z}_h$: $\circ([b]_h) =$ . . . . , e poi il resto modulo h di $t := b^{458576780576} + b(b^2+1)(b^2-1)$: $t \bmod h =$ . . . .

---

6 Il grafo disegnato a destra è connesso? *sì* □ *no* □; è un albero? *sì* □ *no* □. Ha un cammino euleriano? *sì* □ *no* □. Ha un albero di supporto (cioè; un sottoalbero massimale)? *sì* □ *no* □.



Senza sforzare inutilmente la vista cercando di contare sul disegno vertici e lati, calcolare la differenza tra il numero v dei vertici ed il numero l dei lati: $v - l = \dots\dots$

Esiste un multigrafo con (esattamente) 163 vertici, tutti di grado 7? *sì* □ *no* □. Se almeno un tale grafo esiste, si risponda alle seguenti domande:

- esso è connesso? *sì* □ *no* □ *impossibile stabilirlo* □
- ne esistono almeno due non isomorfi? *sì* □ *no* □ *impossibile stabilirlo* □.

---

7 Sia S l'insieme dei numeri naturali divisori di 24, e sia $\delta = \{(a,b) \in S \times S \mid a \mid b\}$.

Allora $|S| = \dots\dots$. Siano:

$$\alpha = \delta \cup \{(3,2)\} \qquad \beta = \delta \cup \{(4,2)\} \qquad \gamma = \delta \cup \{(3,8),(6,8)\}.$$

Se almeno uno tra α, β e γ (*si specifichi quale:* $\dots\dots$) è il grafico di una relazione d'ordine in S, detta ρ questa relazione, si disegni a destra il diagramma di Hasse di (S,ρ) e si risponda alle domande che seguono (altrimenti: □ *nessuno dei tre insiemi è il grafico di una relazione d'ordine in* S).

(S,ρ) è totalmente ordinato? *sì* □ *no* □, è un reticolo *sì* □ *no* □, nel caso, è un reticolo complementato? *sì* □ *no* □, distributivo? *sì* □ *no* □, booleano? *sì* □ *no* □.

Sia indichino in (S,ρ):
$\inf\{6,8\} = \dots\dots\dots\dots$, oppure: □ $\inf\{6,8\}$ *non esiste*;
$\sup\{4,6\} = \dots\dots\dots\dots$, oppure: □ $\sup\{4,6\}$ *non esiste*.

---

8 Dati in $\mathbb{Q}[x]$ i polinomi $f = 2x^6 + 12x^5 - 48x^4 - 144x^3 - 96x^2 + 384x + 1024$ e $g = 2x^4 + 4x^3 - 96x^2 + 64x + 512$, si trovino il massimo comun divisore *monico* d di f e g e l'insieme $C = \{c \in \mathbb{Q} \mid f(c) = g(c) = 0\}$:

$d = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$, $C = \dots\dots\dots\dots$.

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

$d = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$,

$f = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$, $g = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$.

Siano infine f_3 e g_3 i polinomi f e g riguardati come polinomi a coefficienti in $\mathbb{Z}_3$. Si scrivano f_3 e g_3 come prodotti di un polinomio invertibile e di polinomi irriducibili monici in $\mathbb{Z}_3[x]$:

$f_3 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$ $g_3 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

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

$d^* = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

$m^* = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$
