CdL in Informatica — a.a. 2005/2006

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao)   venerdì 13 ottobre 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?

- $\mathbb{N}$ è un sottogruppo di $(\mathbb{Z},+)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $(\mathcal{P}(\mathbb{Z}),\subseteq)$ è un reticolo booleano. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $283147470324 \cdot 741234162617$ è un numero primo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $283147470324 \cdot 741234162617 + 2$ è un numero primo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Se n è il numero di pagine dell'elenco telefonico di Bologna del prossimo anno, $\binom{4n^3+1}{2}$ è pari.
  vero ☐ *falso* ☐ *dati insufficienti* ☐
- La relazione binaria $\sim$ definita in $\mathbb{Z}$ ponendo, per ogni $a,b\in\mathbb{Z}$, $a\sim b :\iff ab$ è pari
  è un'equivalenza. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Si completi: scelti comunque due insiemi finiti A e B si ha $|A|+|B| = |A\cup B|$ . . . .

Per definizione, una relazione binaria $\sim$ su un insieme A è *antisimmetrica* se e solo se:

. . . .

---

3 Sia $X=\{1,2,3,4,5,6,7,8,9\}$. Si elenchino esplicitamente gli elementi dei seguenti insiemi:

$\{x\in X \mid x+4=11\} =$ . . . . $\{Y\in\mathcal{P}(X) \mid 3\in Y \wedge |Y|=1\} =$ . . . .

$\{x\in X \mid x+10=21\} =$ . . . . $\{Y\in\mathcal{P}(X) \mid 13\in Y \wedge |Y|=4\} =$ . . . .

$\{x\in X \mid (\exists y\in X)(x+y=4)\} =$ . . . .

$\{x\in X \mid (x\equiv_7 12 \vee x\equiv_5 44)\wedge x^2\equiv_{13} 3\} =$ . . . .

$\{Y\cap\{1,4,15\} \mid Y\in\mathcal{P}(X)\} =$ . . . .

---

4 Sia $V=\{n\in\mathbb{N} \mid 1<n<20\}$. Si considerino i seguenti insiemi:

$$A=\big\{\{a,b\}\subseteq V \mid \mathrm{MCD}(a,b)>1\big\} \qquad C=\big\{\{a,b\}\subseteq V \mid a+b=24\big\}$$
$$B=\big\{\{a,b\}\subseteq V \mid \mathrm{MCD}(a,b)=1\big\} \qquad D=\big\{\{a,b\}\subseteq V \mid ab=24\big\}$$

Alcuni tra questi sono l'insieme dei lati di un grafo (semplice) con insieme dei vertici V. Disegnare uno dei grafi così ottenuti (*specificando quale!*, se ne consiglia uno col minimo possibile numero di lati) e completare la tabella a destra.

	(V,A)		(V,B)		(V,C)		(V,D)	
	sì	*no*	*sì*	*no*	*sì*	*no*	*sì*	*no*
è un grafo?								
nel caso lo sia:								
è completo								
è connesso								
ha circuiti euleriani								
ha cammini euleriani								

---

5 Si consideri la forma proposizionale $\Phi : \big((p\wedge q)\Rightarrow(p\vee r)\big) \Longrightarrow (q\Rightarrow r)$. Quale valore di verità assume Φ in ciascuno dei seguenti casi:

p,q,r veri: Φ ☐ *vero* ☐ *falso* p vero, q,r falsi: Φ ☐ *vero* ☐ *falso*

Φ è ☐ *una tautologia*, ☐ *contingente*, ☐ *una contraddizione.*

---

6 Sia $S = \{(1,4),(4,1),(1,5),(1,100),(5,4),(3,2),(21,10)\}$, e sia $f\colon (n,m) \in S \mapsto [n]_m \in \mathcal{P}(\mathbb{Z})$.
f è iniettiva? *sì* □ *no* □, suriettiva? *sì* □ *no* □.
Siano definite in S le relazioni binarie $\sim$ e ρ ponendo, per ogni $(a,b),(c,d) \in S$,

$$(a,b) \sim (c,d) :\iff (a,b)^f = (c,d)^f \qquad \text{e} \qquad (a,b)\ \rho\ (c,d) :\iff (a,b)^f \subseteq (c,d)^f.$$

$\sim$ è una equivalenza? *sì* □ *no* □; ρ è un ordinamento? *sì* □ *no* □.
Si consideri $T := \operatorname{im} f$ ordinato per inclusione.
T ha minimo? □ *no* oppure □ *sì, esso è* . . . .
Ha massimo? □ *no* oppure □ *sì, esso è* . . . .
Ha elementi minimali? □ *no* oppure □ *sì, essi sono* . . . .
Ha elementi massimali? □ *no* oppure □ *sì, essi sono* . . . .
$(T, \subseteq)$ è un reticolo? *sì* □ *no* □. Nel caso lo sia, è
distributivo? *sì* □ *no* □, complementato? *sì* □ *no* □, booleano? *sì* □ *no* □.
Disegnarne a fianco il diagramma di Hasse.

---

7 Sia S un insieme tale che $|S| = 1876$. Indicare (*non calcolare!*) $|S \times S| =$ . . . . . . , $|\mathrm{Rel}(S)| =$ . . . . . . , $|\mathrm{Map}(S,S)| =$ . . . . . . , $|\mathrm{SurjMap}(S,S)| =$ . . . . Siano a e b due elementi distinti di S, sia n il numero delle partizioni di $S \setminus \{a\}$ e sia m il numero delle relazioni di equivalenza in $S \setminus \{b\}$. Allora si ha:
□ $n < m$, □ $n = m$, □ $n > m$, □ *nessuna delle precedenti*, □ *impossibile stabilirlo.*

---

8 Calcolare: $19^2 \bmod 127 =$ . . . . , $19^3 \bmod 127 =$ . . . . , $19^{-1} \bmod 127 =$ . . . . , $19^{98765321} \bmod 127 =$ . . . . . Si trovi l'insieme (rispettivamente S_1, S_2, S_3, S_4) di tutte le soluzioni intere di ciascuna delle seguenti equazioni congruenziali:

$19x \equiv_{127} 1.$ $S_1 =$ . . . . $127x \equiv_{19} 1.$ $S_2 =$ . . . .

$19x \equiv_{1270} 10.$ $S_3 =$ . . . . $1270x \equiv_{190} 130.$ $S_4 =$ . . . .

Nell'anello $\mathbb{Z}_{127}$ quanti sono gli elementi non invertibili? . . . . E quanti sono quelli non invertibili nell'anello $\mathbb{Z}_{1270}$? . . . .

---

9 Si considerino i polinomi $f_0 = 6x^7 + 12x^6 + 3x^5 - 8x^4 - 11x^3 - 3x^2 + 2x - 1$, $g_0 = 2x^6 + 2x^5 - x^4 - 2x^3 - 2x^2 + x$, $h = 2x^2 - 1$, $f = hf_0$, $g = hg_0$. Si calcoli il massimo comun divisore monico d di f e g in $\mathbb{Q}[x]$:

$d =$ . . . .

e si fattorizzino d, g, f in prodotto di eventuali invertibili e fattori irriducibili monici in $\mathbb{Q}[x]$:

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

$f =$ . . . .

Sia m un minimo comune multiplo di f e g in $\mathbb{Q}[x]$. Il grado di m è . . . , oppure: □ è *impossibile stabilirlo.*

Esistono $a, b \in \mathbb{Q}[x]$ tali che $k = af - bg$ se k è:

h *sì* □ *no* □, $h + 1$ *sì* □ *no* □, $h^2 g_0 + f - x^5 d$ *sì* □ *no* □, $f_0/d - g_0/d$ *sì* □ *no* □.

Si fattorizzi g in prodotto di eventuali invertibili e fattori irriducibili monici in $\mathbb{R}[x]$:

$g =$ . . . .
