CdS in Informatica — a.a. 2008/2009

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) mercoledì 14 luglio 2009

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: giovedì 16 luglio, ore 9, aula E, DMA

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

- È assegnato un intero $n > 100$. Si ha $n! \equiv_{n-3} 3000$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Negli anelli booleani ogni elemento diverso dall'unità è un divisore dello zero. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- In un arbitrario anello, ogni elemento non invertibile è non cancellabile. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Nell'anello $\mathbb{Z}_{315}$ gli elementi $[197]_{315}$ e $[9]_{315}$ sono l'uno inverso dell'altro. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Il numero dei divisori di $2^{35}3^{21}5^{7}$ è minore del numero dei divisori di $7^{7}11^{35}13^{21}$. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- Nel gioco del lotto, il numero delle possibili sestine è maggiore di 2^{26}. *vero* ☐ *falso* ☐ *dati insuff.* ☐
- È data una proposizione p. La proposizione '$(p \Rightarrow p) \Rightarrow 11^4 < 5$' è vera. *vero* ☐ *falso* ☐ *dati insuff.* ☐

---

2 Per definizione, dato un insieme A, σ è una partizione di A, se e solo se:...............................

....

La biezione canonica dall'insieme delle relazioni di equivalenza di A a quello delle partizioni di A è:

$$\alpha \in \mathrm{Eq}(A) \mapsto \ldots\ldots\ldots \in \mathrm{Part}(A).$$

Si elenchino le partizioni di $S := \{1, 3, 7\}$: ....

---

3 Con $A = \{a \in \mathbb{N} \mid a < 9\}$, sia $\circ$ l'operazione binaria in A definita dalla tavola di Cayley a sinistra.

$\circ$	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	1	1	1	1	1	1	1	1
2	2	1	0	8	7	6	5	4	3
3	3	1	8	6	4	2	0	7	5
4	4	1	7	4	1	7	4	1	7
5	5	1	6	2	7	3	8	4	0
6	6	1	5	0	4	8	3	7	2
7	7	1	4	7	1	4	7	1	4
8	8	1	3	5	7	0	2	4	6

$\circ$ è commutativa? *sì* ☐ *no* ☐. Sapendo che $\circ$ è associativa, $(A, \circ)$ è un semigruppo? *sì* ☐ *no* ☐, è un monoide? *sì* ☐ *no* ☐, è un gruppo? *sì* ☐ *no* ☐.

In $(A, \circ)$, l'elemento neutro: ☐ *non esiste*, oppure: ☐ *esiste, è:* .... Se l'elemento neutro esiste, nella tabella che segue si indichi con una crocetta se l'elemento in testa alla colonna è o non è simmetrizzabile; e, nel primo caso, se ne determini periodo e simmetrico.

	0	1	2	3	4	5	6	7	8
non simmetrizzabile									
simmetrizzabile									
periodo									
simmetrico									

Si indichi con U l'insieme degli elementi simmetrizzabili di $(A, \circ)$. $(U, \circ)$ è un gruppo? *sì* ☐ *no* ☐. Esiste $v \in U$ tale che ogni $u \in U$ sia potenza di v? Un tale v: ☐ *non esiste*, oppure: ☐ *esiste, ad esempio:* $v =$ .... In questo caso si consideri la corrispondenza α da $\mathbb{Z}_6$ ad U di grafico $\{([n]_6, v^n) \mid n \in \mathbb{Z}\}$ (dove le potenze v^n sono calcolate rispetto all'operazione $\circ$). α è un'applicazione: $\mathbb{Z}_6 \to U$? *sì* ☐ *no* ☐; un omomorfismo da $(\mathbb{Z}_6, +)$ a $(U, \circ)$? *sì* ☐ *no* ☐; un isomorfismo da $(\mathbb{Z}_6, +)$ a $(U, \circ)$? *sì* ☐ *no* ☐.

---

4 Con A e $\circ$ come nell'esercizio nr. 3, si studi l'applicazione $f\colon (x, y) \in A \times A \mapsto x \circ y \in A$. f è iniettiva? *sì* ☐ *no* ☐, f è suriettiva? *sì* ☐ *no* ☐. Esistono applicazioni $g\colon A \to A \times A$ tali che $fg = \mathrm{id}_{A\times A}$? ☐ *no*, oppure: ☐ *sì, un esempio è*

$$g : \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) \end{pmatrix}$$

Esistono applicazioni $h\colon A \to A \times A$ tali che $hf = \mathrm{id}_A$? ☐ *no*, oppure: ☐ *sì, un esempio è*

$$h : \begin{pmatrix} 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) & (\ , \ ) \end{pmatrix}$$

Sia $\sim_f$ il nucleo di equivalenza di (ovvero: l'equivalenza associata a) f. Calcolare $|(A \times A)/\sim_f| =$ .... Descrivere, elencandone gli elementi, le classi:

$[(0,6)]_{\sim_f} = \{ \ldots\ldots\ldots\ldots\ldots\ldots \}$; $[(0,5)]_{\sim_f} = \{ \ldots\ldots\ldots\ldots\ldots\ldots \}$

---

5 Si descrivano esplicitamente gli insiemi, rispettivamente A, B, C, dei numeri naturali n tali che esista un grafo (semplice) G con esattamente 8 vertici di cui uno, v, di grado n e tale che ...

(a) ... G sia connesso, abbia esattamente 6 lati e, tra i vertici di G diversi da v, uno abbia grado 1 e tre abbiano grado 2; [$A =$ . . . .

(b) ... tra i vertici di G diversi da v, uno sia isolato, uno abbia grado 1 e ciascuno degli altri cinque abbia grado 2 o 4; [$B =$ . . . .

(c) ... tra i vertici di G diversi da v, uno abbia grado 2, due abbiano grado 3, uno abbia grado 8, e gli altri tre abbiano grado 1. [$C =$ . . . .

---

6 Si considerino le relazioni binarie α, β, γ definite in $\mathbb{N}$ ponendo, per ogni $n, m \in \mathbb{N}$,

$$n\ \alpha\ m :\iff \big((n \bmod 7 < m \bmod 7) \wedge (n \bmod 10 < m \bmod 10)\big)$$
$$n\ \beta\ m :\iff \big((n \bmod 7 \le m \bmod 7) \wedge (n \bmod 10 \le m \bmod 10)\big)$$
$$n\ \gamma\ m :\iff \big((n \bmod 7 < m \bmod 7) \vee (n \bmod 10 < m \bmod 10)\big)$$

Quali tra queste tre sono: . . . . e quali non sono: . . . . relazioni d'ordine? Se almeno una di esse lo è, detta questa ρ (quindi $\rho =$ . . . .), si risponda alle domande che seguono.
Rispetto a ρ, esiste $\max \mathbb{N}$? ☐ *no*, oppure: ☐ *sì*, $\max \mathbb{N} =$ . . . . $(\mathbb{N}, \rho)$ ha elementi minimali? ☐ *no*, oppure: ☐ *sì, ma meno tre; essi sono:* . . . . , oppure: ☐ *sì, più di due; tre di essi sono:* . . . . Sia $S = \{1, 23, 27, 71, 75, 96, 144, 210\}$. Si disegni in alto a destra il diagramma di Hasse di (S, ρ). (S, ρ) è un reticolo? *sì* ☐ *no* ☐, nel caso lo sia è complementato? *sì* ☐ *no* ☐, distributivo? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐. Rispetto a ρ, $\max S =$ . . . o: ☐ $\max S$ *non esiste*; $\inf\{27, 75, 96\} =$ . . . . , o: ☐ $\inf\{27, 75, 96\}$ *non esiste*.

---

7 Con $n = 2910(61^{22} + 22^{61}) + 22^{291} + 61^{293} - 100$, calcolare: $n \bmod 291 =$ . . . . ; $n^2 \bmod 291 =$ . . . . .
Determinare gli insiemi (risp. S_1, S_2, S_3) di tutte le soluzioni intere di ognuna delle equazioni conguenziali:

$$(22 \cdot 61)x \equiv_{291} 1 \qquad (172 \cdot 229)x \equiv_{291} 1 \qquad (22 \cdot 97)x \equiv_{291} 194$$

$S_1 =$ . . . . ; $S_2 =$ . . . . ; $S_3 =$ . . . .

---

8 Trovare in $\mathbb{Z}_6[x]$, se possibile, due polinomi f e g di gradi rispettivamente 4 e 2 tali che fg abbia grado 2. ☐ *Non esistono tali polinomi*, oppure: ☐ *ne esistono, ad esempio:* $f =$ . . . . *e* $g =$ . . . . Trovare in $\mathbb{Z}_{14}[x]$, se possibile, un polinomio h di grado 3 che abbia più di cinque radici in $\mathbb{Z}_{14}$. ☐ *Non esistono tali polinomi*, oppure: ☐ *ne esistono, ad esempio* $h =$ . . . .

---

9 Siano, in $\mathbb{Q}[x]$, $f = x^5 + 7x^4 + 26x^3 + 53x^2 + 63x + 30$ e $g = x^4 + 3x^3 + 4x^2 - 3x - 5$. Si determini il massimo comun divisore monico d tra f e g in $\mathbb{Q}[x]$:

$d =$ . . . .

f ha un divisore in $\mathbb{Q}[x]$ di grado tre? ☐ *no*, oppure: ☐ *sì, ad esempio:* . . . .

f ha un divisore irriducibile in $\mathbb{Q}[x]$ di grado tre? ☐ *no, perché* . . . .

. . . .

oppure: ☐ *sì, ad esempio:* . . . .
