CdS in Informatica — a.a. 2008/2009

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 20 marzo 2009

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: martedì 24 marzo, ore 9, aula C, DMA

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

- Ogni monoide finito è un gruppo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Ogni dominio di integrità finito è un campo. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'insieme dei cicli di lunghezza dispari costituisce un sottogruppo in $\mathbb{S}_7$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- L'insieme dei cicli di lunghezza pari costituisce un sottogruppo in $\mathbb{S}_7$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Sono assegnati $n, k \in \mathbb{N}$, e $k < n$. Si ha $\binom{n}{k} < 2^n$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- p, q, r, s, t sono assegnate proposizioni, e p è vera. La formula $\big(r \Rightarrow (s \vee t)\big) \Rightarrow \big((q \wedge t) \Rightarrow (p \vee r)\big)$ è vera. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Sia x un elemento di un semigruppo $(S, *)$. Per definizione, x è *cancellabile* in $(S, *)$ se e solo se ....

....

Dare un esempio di elemento non cancellabile nel semigruppo $(\mathbb{Z}, \cdot)$: . . . . , oppure: ☐ *non ne esistono.*

---

3 Sia $F = \{2, 3, 5, 7\}$. Si considerino le applicazioni

$$f \colon X \in \mathcal{P}(F) \longmapsto \begin{cases} \prod_{n\in X} n, & \text{se } X \neq \varnothing \\ 1, & \text{se } X = \varnothing \end{cases} \in \mathbb{N} \qquad g \colon n \in \mathbb{N} \longmapsto \begin{cases} 5n+3, & \text{se } n \text{ è pari} \\ 4n-15, & \text{se } n \text{ è dispari} \end{cases} \in \mathbb{Z}$$

f è iniettiva? ☐ *sì*, oppure: ☐ *no, perché* . . . . ,

f è suriettiva? ☐ *sì*, oppure: ☐ *no, perché* . . . .

f ha sezioni? *sì* ☐ *no* ☐. f ha retrazioni? *sì* ☐ *no* ☐. f ha una sezione che manda 24 in $\{2, 5\}$? *sì* ☐ *no* ☐.
f ha una retrazione che manda 24 in $\{2, 5\}$? *sì* ☐ *no* ☐. f ha una retrazione che manda 15 in $\{7\}$? *sì* ☐ *no* ☐.

g è iniettiva? ☐ *sì*, oppure: ☐ *no, perché* . . . . ,

g è suriettiva? ☐ *sì*, oppure: ☐ *no, perché* . . . .
g ha sezioni? *sì* ☐ *no* ☐. g ha retrazioni? *sì* ☐ *no* ☐.

fg è iniettiva? ☐ *sì*, oppure: ☐ *no, perché* . . . . ,

fg è suriettiva? ☐ *sì*, oppure: ☐ *no, perché* . . . .

Sia σ la relazione binaria definita in $\mathcal{P}(F)$ da $(\forall X, Y \in \mathcal{P}(F))\,(X \;\sigma\; Y :\Longleftrightarrow\; X^f \equiv_7 Y^f)$. σ è una relazione di equivalenza? ☐ *no, perché* . . . . , oppure: ☐ *sì, e si ha* $|\mathcal{P}(F)/\sigma| =$ . . . . e $\big|[\{2, 7\}]_\sigma\big| =$ . . . . .

Sia $S = \{2, 3, 5\}$ e siano ρ e τ le relazioni binarie definite in $\mathcal{P}(S)$ ponendo, per ogni $X, Y \in \mathcal{P}(S)$,

$$X \,\rho\, Y :\Longleftrightarrow X^f \bmod 3 \leq Y^f \bmod 3 \qquad \text{e} \qquad X \,\tau\, Y :\Longleftrightarrow X^f \bmod 5 < Y^f \bmod 5$$

ρ è una relazione di ordine stretto? *sì* ☐ *no* ☐, di ordine largo? *sì* ☐ *no* ☐,
τ è una relazione di ordine stretto? *sì* ☐ *no* ☐, di ordine largo? *sì* ☐ *no* ☐.

Se almeno una delle due è una relazione d'ordine, detta questa α, (dunque $\alpha =$ . . .), disegnare a fianco il diagramma di Hasse di $(\mathcal{P}(S), \alpha)$ e rispondere alle seguenti domande:
$(\mathcal{P}(S), \alpha)$ è un reticolo? *sì* ☐ *no* ☐, nel caso, è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.

Rispetto ad α,
$\max(\mathcal{P}(S)) =$ . . . . , oppure: ☐ $\max(\mathcal{P}(S))$ *non esiste*;
$\min(\mathcal{P}(S)) =$ . . . . , oppure: ☐ $\min(\mathcal{P}(S))$ *non esiste*;
$\inf\big(\{\varnothing, \{2, 3\}\}\big) =$ . . . . , oppure: ☐ $\inf\big(\{\varnothing, \{2, 3\}\}\big)$ *non esiste.*

---

4 Esiste un grafo connesso con (esattemente) 100 vertici e 93 lati? □ *sì*, oppure: □ *no, perché* . . . .

. . . .

Esiste un grafo connesso con (esattemente) 93 vertici e 100 lati? □ *sì*, oppure: □ *no, perché* . . . .

. . . .

---

5 Si calcoli $\varphi(7840) =$ . . . . (come di consueto, φ indica la funzione di Eulero; si tenga presente che $7840 = 2^5 \cdot 5 \cdot 49$). Nell'anello $\mathbb{Z}_{7840}$ il numero dei divisori dello zero è . . . . , il numero degli elementi invertibili è . . . . . $\mathbb{Z}_{7840}$ è un dominio di integrità? *sì* □ *no* □, è un campo? *sì* □ *no* □. Sia $X = \{[n]_{7840} \mid n \equiv_{70} 1\} \subseteq \mathbb{Z}_{7840}$. Nel gruppo additivo di $\mathbb{Z}_{7840}$, X è una parte stabile? *sì* □ *no* □, è un sottogruppo? *sì* □ *no* □. X è contenuto nel gruppo degli invertibili di $\mathbb{Z}_{7840}$? *sì* □ *no* □. Nel caso, ne è una parte stabile? *sì* □ *no* □, un sottogruppo? *sì* □ *no* □. X è un sottoanello di $\mathbb{Z}_{7840}$? *sì* □ *no* □.

---

6 Siano A e B due insiemi tali che $|A| = 7$, $|B| = 15$ e, posto $C := A \cap B$, si abbia $|C| = 4$. Allora:
$|A \cup B| =$ . . . . , $|A \triangle B| =$ . . . . , $|A \triangle C| =$ . . . . , $|A \cup B \cup C| =$ . . . . , $|A \cap C| =$ . . . . . Siano poi $U = \{X \in \mathcal{P}(B) \mid (C \subseteq X) \wedge (|X| = 7)\}$ e $V = \{X \in \mathcal{P}(B) \mid (C \subseteq X) \Rightarrow (|X| = 7)\}$. Si ha $U \subseteq V$? *sì* □ *no* □. Si ha $V \subseteq U$? *sì* □ *no* □. Si ha $A \in U$? *sì* □ *no* □. Si ha $A \in V$? *sì* □ *no* □. Indicare:
$|\mathrm{InjMap}(C, A)| =$ . . . . , $|\mathcal{P}_{|A|}(B)| =$ . . . . , $|U| =$ . . . . , $|V| =$ . . . .

---

7 Calcolare $7^6 \bmod 181 =$ . . . . e $(7^{156156} + 7^{150150})^7(7^{77} + 1) \bmod 181 =$ . . . . .

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

$2x + 49 \equiv_{181} 50x + 50$; $\quad 4x + 97 \equiv_{362} 100x + 100$; $\quad 6x + 146 \equiv_{543} 150x + 150$;

$S_1 =$ . . . . ; $\quad S_2 =$ . . . . ; $\quad S_3 =$ . . . . ;

---

8 In $\mathbb{Z}[x]$ si calcoli un massimo comun divisore d_1 tra i polinomi $f := 3x^5 + 13x^4 + 23x^3 + 19x^2 + 10x + 2$ e $g := (x + 1)^4$. $d_1 =$ . . . . Quanti massimi comuni divisori tra f e g esistono in $\mathbb{Z}[x]$? . . . . $3d_1$ è uno di essi? *sì* □ *no* □. Esiste in $\mathbb{Z}[x]$ un polinomio multiplo di f e di grado 6 di cui -1 sia radice? □ *no*, oppure: □ *sì, ad esempio:* . . . .

Si calcoli ora il massimo comun divisore monico d in $\mathbb{Q}[x]$ tra $f + 2$ e g:

$d =$ . . . . ;

esistono $a, b \in \mathbb{Q}[x]$ tali che $a(f + 2) + 3bg = d + 1$? *sì* □ *no* □

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

$f_2 =$ . . . .

Il massimo comun divisore in $\mathbb{Z}_2[x]$ tra f_2 e g_2 è: . . . .
