CdS in Informatica — a.a. 2009/2010
Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 25 marzo 2011

NOME E COGNOME	MATRICOLA

GRUPPO ☐ *I (Rao)* ☐ *rec. (Cutolo)*	ESAME: mercoledì 30 marzo, ore 9, aula D, DMA

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

- La formula $(p \Rightarrow q) \Longrightarrow \big((p \Rightarrow (\neg r)) \wedge (q \vee r)\big)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La formula $\big((p \Rightarrow (\neg r)) \wedge (q \vee r)\big) \Longrightarrow (p \Rightarrow q)$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Per ogni terna A, B, C di parti di un insieme S si ha:
  $A \cup (S \smallsetminus B) \subseteq (A \cup C) \cap \big((S \smallsetminus B) \cap C\big)$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Per qualche terna A, B, C di parti di un insieme S si ha:
  $A \cup (S \smallsetminus B) \subseteq (A \cup C) \cap \big((S \smallsetminus B) \cap C\big)$ *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La permutazione $(2\,3)(2\,4\,5)(2\,6\,7\,8)$
  - è un ciclo, *vero* ☐ *falso* ☐ *dati insufficienti* ☐
  - ha classe pari, *vero* ☐ *falso* ☐ *dati insufficienti* ☐
  - ha periodo 12. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

2 Un anello $(R, +, \cdot\,)$ è, per definizione, *booleano*, se e solo se ....

....

Si forniscano, ove possibile, esempi di:

un anello booleano non commutativo: ...., oppure: ☐ *non ne esistono;*

un anello booleano di cardinalità 512: ...., oppure: ☐ *non ne esistono;*

un anello booleano di cardinalità 1000: ...., oppure: ☐ *non ne esistono;*

un anello booleano infinito: ...., oppure: ☐ *non ne esistono.*

---

3 Sia $V = \{n \in \mathbb{N} \mid 1 \leq n \leq 4000\}$. Siano $A = \big\{\{x, y\} \,\big|\, x, y \in V, \quad x - y \text{ è pari e } (x-y)/2 \text{ è dispari}\big\}$,
$B = \big\{\{x, y\} \mid (x, y \in V) \wedge (x \equiv_4 -y)\big\}$ e $C = \big\{\{x, y\} \mid (x, y \in V) \wedge (x \equiv_2 y) \wedge (x \not\equiv_4 y)\big\}$.

(V, A) è un grafo *sì* ☐ *no* ☐; (V, B) è un grafo *sì* ☐ *no* ☐; (V, C) è un grafo *sì* ☐ *no* ☐.

Si scelga L come uno tra A, B e C in modo che $G := (V, L)$ sia un grafo: $L =$ .... Allora:
G è una foresta *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐, G è un albero *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐, G è connesso *sì* ☐ *no* ☐ *impossibile stabilirlo* ☐.
Quante componenti connesse ha G? ... qual è il grado di 32 in G? .....

---

4 Si consideri l'applicazione $f : t \in \mathbb{Z} \longmapsto 1 - 2t \in \mathbb{Z}$. f è iniettiva? *sì* ☐ *no* ☐, suriettiva? *sì* ☐ *no* ☐. f è un omomorfismo del gruppo $(\mathbb{Z}, +)$ in sé? *sì* ☐ *no* ☐, f è un omomorfismo del semigruppo $(\mathbb{Z}, \cdot)$ in sé? *sì* ☐ *no* ☐. La relazione binaria σ definita in $\mathbb{Z}$ ponendo: $(\forall\, x, y \in \mathbb{Z})$ $(x \,\sigma\, y \iff x^f \mid y^f)$ non è un ordinamento, perché...

Si consideri invece la relazione d'ordine stretto ρ definita in $\mathbb{Z}$ ponendo, (per ogni $x, y \in \mathbb{Z}$), $x \,\rho\, y$ se e solo se x^f è un divisore proprio di y^f. In $(\mathbb{Z}, \rho)$, 1 è minimale? *sì* ☐ *no* ☐. $(\mathbb{Z}, \rho)$ ha minimo? ☐ *no* ☐ *sì, esso è:* ... ; ha massimo? ☐ *no* ☐ *sì, esso è:* ... ; ha elementi minimali ☐ *no* ☐ *sì, essi sono:* .... ; ha elementi massimali ☐ *no* ☐ *sì, essi sono:* .... $(\mathbb{Z}, \rho)$ è un reticolo? *sì* ☐ *no* ☐. Se no, perché? ....

Siano $S = \{1, 2, -2, -3, -52\}$ e $T = S \cup \{0, 3, -5\}$, e si considerino questi insiemi ordinati rispetto all'ordinamento indotto da ρ. Si disegni a fianco il diagramma di Hasse di T.
T è un reticolo? *sì* ☐ *no* ☐ S è un reticolo? *sì* ☐ *no* ☐
Nel caso, S è distributivo? *sì* ☐ *no* ☐, complementato? *sì* ☐ *no* ☐, booleano? *sì* ☐ *no* ☐.

---

5 Il resto di $\binom{128}{3} + 2^{149}$ modulo 127 è . . . .

---

6 L'insieme $A := \{[3n]_{30} \mid n \in \mathbb{Z}\}$ è un sottoanello di $\mathbb{Z}_{30}$? *sì* □ *no* □. A, munito dell'operazione indotta dalla moltiplicazione in $\mathbb{Z}_{30}$, è un monoide. La sua unità è: . . . . . In *questo* monoide, l'inverso di $[-3]_{30}$ è . . . . .

---

7 Siano ρ e τ le relazioni binarie definite in $\mathbb{N}$ ponendo, $\forall\, x, y \in \mathbb{N}$

$x \,\rho\, y \iff x \geq y$; $\qquad x \,\tau\, y \iff x$ e y, scritti in base 10, hanno lo stesso numero di cifre.

Allora: ρ non è un'equivalenza perché: . . . .
Invece τ è una equivalenza. Calcolare $\left|[651]_\tau\right| =$ . . . . . $\left|\mathbb{N}/\tau\right|$ è □ *finito* o □ *infinito*? Nel primo caso, $\left|\mathbb{N}/\tau\right| =$ . . . . .

Sia $A = [651]_\tau$. Esprimere $|\mathcal{P}_2(A)| =$ . . . . Esistono applicazioni iniettive da A a $[156]_\tau$? □ *sì* □ *no*. Nel caso, indicare (non *calcolare!*) quante sono: . . . .

---

8 L'equazione diofantea $674x + 966y = 50$ □ *non ha soluzioni, perché* . . . . ,
oppure: □ *ha soluzioni* $(u, v) \in \mathbb{Z} \times \mathbb{Z}$, *e una è data da* $u =$ . . . . $e\ v =$ . . . . .

L'equazione diofantea $674x + 966y = 25$ □ *non ha soluzioni, perché* . . . . ,
oppure: □ *ha soluzioni* $(h, k) \in \mathbb{Z} \times \mathbb{Z}$, *e una è data da* $h =$ . . . . $e\ k =$ . . . . .

In particolare, per ciascuna delle seguenti equazioni congruenziali, si può trovare l'insieme (rispettivamente S_1, S_2, S_3, S_4) delle soluzioni intere:

$337x \equiv_{483} 1.$ $\quad S_1 =$ . . . .

$483x \equiv_{337} 1.$ $\quad S_2 =$ . . . .

$337x \equiv_{483} 25.$ $\quad S_3 =$ . . . .

$483x \equiv_{337} 25.$ $\quad S_4 =$ . . . .

---

9 Dati in $\mathbb{Q}[x]$ i polinomi $\quad f = x^6 + 17x^5 + 109x^4 + 312x^3 + 305x^2 - 249x - 495 \quad$ e
$g = x^4 + 9x^3 + 22x^2 - 32,$
si trovino il massimo comun divisore *monico* d di f e g ed i quozienti $f_1 = f/d$ e $g_1 = g/d$:

$d =$ . . . .

$f_1 =$ . . . . , $\quad g_1 =$ . . . .

Sapendo poi che $f_1(-3) = f_1(-5) = g_1(-4) = 0$, si decompongano d, f e g in prodotto di polinomi monici irriducibili nell'anello $\mathbb{Q}[x]$:

$d =$ . . . .

$f =$ . . . . , $\quad g =$ . . . .

Infine, riguardati i polinomi f e g a coefficienti in $\mathbb{Z}_5$, si trovino nell'anello $\mathbb{Z}_5[x]$ le fattorizzazioni in prodotto di polinomi monici irriducibili del massimo comun divisore monico d_5 e del minimo comune multiplo monico m_5 di f e di g:

$d_5 =$ . . . . , $\quad m_5 =$ . . . .
