CdL in Informatica — a.a. 2005/2006

Esercitazione scritta di **ALGEBRA** (Proff. Cutolo e Rao) venerdì 17 febbraio 2006

NOME E COGNOME	MATRICOLA

GRUPPO □ *I (Rao)* □ *IV (Cutolo)* PREFERENZA PER L'ESAME □ *urgenti* □ *non urgenti*

1 Per definizione, un *dominio di integrità* è: ....

....

Si fornisca, se esiste, un esempio di:

– dominio di integrità: .... □ *non esiste*

– anello commutativo che non sia un dominio di integrità: .... □ *non esiste*

– campo che non sia un dominio di integrità: .... □ *non esiste*

---

2 Siano dati due interi n ed m tali che $15000n + 7^{18}m = -1$. Calcolare:

– $nm =$ . . . . ; oppure: □ *impossibile stabilirlo*;

– il minimo comune multiplo non negativo tra n ed m: . . . . ; oppure: □ *impossibile stabilirlo*;

– il massimo comun divisore non negativo tra n ed m: . . . . ; oppure: □ *impossibile stabilirlo*;

– vero o falso: m è pari. *sì* □ *no* □ *impossibile stabilirlo* □

– vero o falso: n è dispari. *sì* □ *no* □ *impossibile stabilirlo* □

– vero o falso: n e 7 sono coprimi. *sì* □ *no* □ *impossibile stabilirlo* □

– vero o falso: almeno uno tra n e m non è né pari né dispari. *sì* □ *no* □ *impossibile stabilirlo* □

---

3 Si consideri l'operazione binaria $*$ definita in $\mathbb{Z}$ ponendo, per ogni $a, b \in \mathbb{Z}$, $a * b = ab - a - b + 2$.
$*$ è commutativa? *sì* □ *no* □, associativa? *sì* □ *no* □; $(\mathbb{Z}, *)$ ha elemento neutro? *sì* □ *no* □, nel caso esso è? . . . . .
L'elemento 35 è cancellabile in $(\mathbb{Z}, *)$? *sì* □ *no* □; è simmetrizzabile? *sì* □ *no* □, nel caso il suo simmetrico è . . . . . L'elemento 0 è cancellabile in $(\mathbb{Z}, *)$? *sì* □ *no* □, è simmetrizzabile? *sì* □ *no* □, nel caso il suo simmetrico è . . . . .

Esiste in $(\mathbb{Z}, *)$ qualche elemento non cancellabile? *sì* □ *no* □; nel caso, un esempio è . . . . .

$(\mathbb{Z}, *)$ è un semigruppo *sì* □ *no* □, un monoide *sì* □ *no* □, un gruppo *sì* □ *no* □, un anello *sì* □ *no* □

---

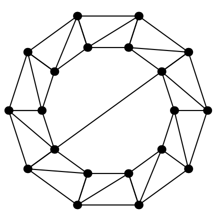
4 Scrivere la negazione della formula $\big((\neg p) \Rightarrow q\big) \vee \big((\neg r) \Rightarrow p\big)$ senza far comparire il condizionale ("$\Rightarrow$").

. . . .

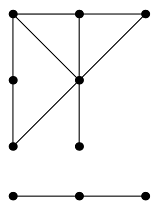
La formula ottenuta è □ *una tautologia*, □ *contingente*, □ *una contraddizione*.

---

5 Si considerino i grafi A e B disegnati in basso.
A ammette un circuito euleriano? *sì* □ *no* □ A ammette un cammino euleriano? *sì* □ *no* □
B ammette un circuito euleriano? *sì* □ *no* □ B ammette un cammino euleriano? *sì* □ *no* □
Se possibile, aggiungere un vertice e uno o due lati a ciascuno dei due grafi in modo che il grafo (semplice) risultante ammetta un circuito euleriano. La costruzione è
per A: □ *possibile* □ *impossibile*; per B: □ *possibile* □ *impossibile*.



A



B

6 Si determini un polinomio $f \in \mathbb{Q}[x]$ che abbia grado 5, coefficiente direttore 14 ed almeno otto radici intere: $f = \dots\dots\dots\dots\dots\dots\dots\dots\dots$, oppure $\square$ *un tale polinomio non esiste.*

---

7 Si considerino le quattro relazioni binarie α, β, γ, δ definite in $X := \{n \in \mathbb{N} \mid 0 < n \leq 10\}$ ponendo, per ogni $n \in \mathbb{Z}$, $\bar{n} := n \bmod 6$ e, per ogni $n, m \in X$,

$$n \;\alpha\; m :\iff \bar{n} \leq \bar{m}; \qquad n \;\gamma\; m :\iff 2\bar{n} = 2\bar{m};$$

$$n \;\beta\; m :\iff n-1 \mid m-1; \qquad n \;\delta\; m :\iff n+m = 11.$$

α è una equivalenza? *sì* $\square$ *no* $\square$, un ordine largo? *sì* $\square$ *no* $\square$, un ordine stretto? *sì* $\square$ *no* $\square$
β è una equivalenza? *sì* $\square$ *no* $\square$, un ordine largo? *sì* $\square$ *no* $\square$, un ordine stretto? *sì* $\square$ *no* $\square$
γ è una equivalenza? *sì* $\square$ *no* $\square$, un ordine largo? *sì* $\square$ *no* $\square$, un ordine stretto? *sì* $\square$ *no* $\square$
δ è una equivalenza? *sì* $\square$ *no* $\square$, un ordine largo? *sì* $\square$ *no* $\square$, un ordine stretto? *sì* $\square$ *no* $\square$

Se una delle quattro relazioni è una equivalenza, detta essa $\sim$ (dunque $\sim = \dots$), si indichi $|X/\!\sim\!| = \dots$ e si elenchino gli elementi di $[3]_\sim$:
$[3]_\sim = \{\dots\dots\dots\dots\dots\}$.
Se una delle quattro relazioni è un ordinamento, detto esso ρ (dunque $\rho = \dots$), si disegni a lato il diagramma di Hasse di (X, ρ). (X, ρ) è un reticolo? *sì* $\square$ *no* $\square$, un reticolo distributivo? *sì* $\square$ *no* $\square$, complementato? *sì* $\square$ *no* $\square$, booleano? *sì* $\square$ *no* $\square$. Si elenchino i maggioranti in (X, ρ) di $\{4, 5, 6\}$: $\dots\dots\dots\dots\dots$

---

8 Siano $p = 101$, $q = 31$ (dunque $pq = 3131$), $a = 3000$, $b = 3$, $c = 5$. Calcolare: $a^{-1} \bmod (pq) = \dots$, $a^{-1} \bmod p = \dots$, $a^{-1} \bmod q = \dots$, $c^{-1} \bmod q = \dots$, $(ac)^{-1} \bmod q = \dots$.

Per ciascuna delle seguenti equazioni congruenziali si trovi l'insieme (rispettivamente S_1, S_2, S_3, S_4, S_5) di tutte le soluzioni intere:

$ax \equiv_{pq} b.$ $\qquad S_1 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

$ax \equiv_{p} b.$ $\qquad S_2 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

$ax \equiv_{q} b.$ $\qquad S_3 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

$cax \equiv_{cp} cb.$ $\qquad S_4 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

$cax \equiv_{q} cb.$ $\qquad S_5 = \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots$

---

9 Si considerino i seguenti polinomi in $\mathbb{Q}[x]$: $\qquad a = 12x^6 - 14x^5 + 26x^4 - 50x^3 + 32x^2 - 4,$

$$b = 6x^5 - 4x^4 + 10x^3 - 20x^2 + 4x + 4, \qquad c = x^2 - 5$$

e siano poi $f = a^2c$ e $g = b^2c$. Si indichi il massimo comun divisore *monico* d di f e g:

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

e si scrivano d e g come prodotti di un polinomio invertibile e di polinomi irriducibili monici in $\mathbb{Q}[x]$:

$d = \dots\dots\dots\dots\dots\dots\dots$ $\qquad g = \dots\dots\dots\dots\dots\dots\dots$

Quante e quali sono le radici comuni a f e g?

$S = \{q \in \mathbb{Q} \mid f(q) = g(q) = 0\} = \dots\dots\dots\dots\dots$ $\qquad |S| = \dots$.

Siano infine f_5 e g_5 i polinomi f e g riguardati come polinomi a coefficienti in $\mathbb{Z}_5$. Si scrivano f_5 e g_5 come prodotti di un polinomio invertibile e di polinomi irriducibili monici in $\mathbb{Z}_5[x]$:

$f_5 = \dots\dots\dots\dots\dots\dots\dots$ $\qquad g_5 = \dots\dots\dots\dots\dots\dots\dots$

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

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

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