CdL e CdD in Informatica — a.a. 2002/2003 e 2003/2004
Esercitazione scritta di **ALGEBRA** (Prof. Rao) venerdì 20 febbraio 2004

NOME E COGNOME	MATRICOLA

1 Si completino le seguenti definizioni:
Se A è un anello commutativo unitario e $f, g \in A[x]$, un polinomio $d \in A[x]$ si dice *massimo comun divisore* di f e g se e solo se ....

....

Un elemento x di un anello R si dice *nilpotente* se e solo se ....

---

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

- $\big(((\neg p) \Rightarrow r\big) \wedge \big((\neg r) \Rightarrow \big((\neg p) \vee (\neg q)\big)\big)\big) \Longrightarrow q$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- $\big(\big(((\neg p) \wedge (\neg q)) \Rightarrow r\big) \wedge \big((\neg p) \wedge (\neg r)\big)\big) \Rightarrow q$ è una tautologia. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- Scelta comunque un'applicazione iniettiva non vuota $f : A \rightarrowtail B$, esistono applicazioni suriettive $g : B \twoheadrightarrow A$ tali che $gf = \mathrm{id}_B$. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- La permutazione $\alpha = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 5 & 7 & 2 & 6 & 1 & 4 & 3 \end{pmatrix}$ è un elemento del gruppo $\mathbb{S}_7$ di periodo maggiore di cinque.
  vero ☐ *falso* ☐ *dati insufficienti* ☐
  Inoltre, la stessa permutazione α è di classe dispari. *vero* ☐ *falso* ☐ *dati insufficienti* ☐
- 5 divide il massimo comun divisore di 78865119827336320982473555631214670768787587528578728578 5720 e 1454523890198776765262666382758572857 8575. *vero* ☐ *falso* ☐ *dati insufficienti* ☐

---

3 Decomposto $m = 1025$ in prodotto di naturali primi, si calcoli $|\mathcal{U}(\mathbb{Z}_{1025})| = \ldots\ldots$ Sia $u := [32]_{1025}$. È vero che $u \in \mathcal{U}(\mathbb{Z}_{1025})$? ☐ no, non è vero, perché ....

☐ sì, è vero, perché ....

Nel secondo caso, si calcolino nel gruppo $\mathcal{U}(\mathbb{Z}_{1025})$ il periodo e l'inverso di u: $|u| = \ldots\ldots$, $u^{-1} = \ldots\ldots$ Si calcoli poi il resto di $n = 2^{1000} + 2^{1005} + 2^{1010} + 2^{1015} + 2^{1020} + 2^{1024}(41!)$ modulo m: $n \bmod m = \ldots\ldots$.

Infine, nell'anello $\mathbb{Z}_{1025}$, si calcolino:

- il numero degli elementi invertibili: .... • il numero degli elementi cancellabili: ....
- il numero degli elementi invertibili non cancellabili: ....
- il numero degli elementi cancellabili non invertibili: ....
- il numero degli elementi non cancellabili: .... • il numero dei divisori dello zero: ....
- il numero degli elementi nilpotenti: ....

e si dia almeno un esempio di:

- un elemento nilpotente non nullo: .... • un elemento idempotente diverso da $[0]_{1025}$ e da $[1]_{1025}$: ....

---

4 Disegnare due grafi connessi tra loro non isomorfi che abbiano esattamente cinque vertici, dei quali almeno due di grado 1 ed almeno uno di grado 3. Oppure: ciò non è possibile ☐.

5 Siano $S=\{1,2,3,4\}$, $T=T(S)$, il monoide delle trasformazioni di S, $X=\{f\in T \mid f(2)=2\}$ e $Y=\{f\in T \mid f(2)\neq 2\}$. Calcolare: $|X|=\dots\,$, $|Y|=\dots\,$, $|\mathcal{P}_2(X)|=\dots\,$, $|Y\smallsetminus X|=\dots\,$.

X è una parte stabile di T? *sì* □ *no* □ Ne è un sottomonoide? *sì* □ *no* □.

Y è una parte stabile di T? *sì* □ *no* □ Ne è un sottomonoide? *sì* □ *no* □.

Se almeno uno tra X e Y è un monoide (rinominiamolo M, dunque $M=\dots$), M è un gruppo? *sì* □ *no* □ M è commutativo? *sì* □ *no* □ $\mathcal{U}(M)$ è un gruppo? *sì* □ *no* □ $|\mathcal{U}(M)|=\dots\,$.

---

6 Sia $(D,|)$ l'insieme dei naturali divisori di 315, ordinato per divisibilità.
Disegnarne qui a fianco il diagramma di Hasse e stabilire quanto segue:
$(D,|)$ è un reticolo? *sì* □ *no* □, è una catena? *sì* □ *no* □,
è un reticolo distributivo? *sì* □ *no* □,
è un reticolo complementato? *sì* □ *no* □,
è un reticolo booleano? *sì* □ *no* □.

In $(D,|)$ l'elemento 3 ha:
- nessun complemento *no* □ *sì* □
- un unico complemento *no* □ *sì* □, *esso è* ....
- più di un complemento *no* □ *sì* □, *essi sono* ....

$\sup\{3,5,9\}$ non esiste □, oppure è .... ; $\inf\{9,15\}$ non esiste □, oppure è .....

Si determini una parte propria B di D, con $|B|>4$, tale che $(B,|)$ sia un reticolo di Boole:

$B=\{\dots\dots\dots\dots\}$.

---

7 Si consideri l'applicazione $f: a\in\mathbb{Z}\mapsto [a^2]_{29}\in\mathbb{Z}_{29}$. f è ben definita? *sì* □ *no* □. Nel caso, è iniettiva? *sì* □ *no* □, è suriettiva? *sì* □ *no* □, è un omomorfismo di gruppi? *sì* □ *no* □, è un omomorfismo di anelli? *sì* □ *no* □.

Sia ρ la relazione binaria in $\mathbb{Z}$ definita ponendo, per ogni $a,b\in\mathbb{Z}$,

$$a\,\rho\,b :\iff f(a)=f(b).$$

ρ è un'equivalenza? *sì* □ *no* □. Nel caso ρ sia un'equivalenza, calcolare $|\mathbb{Z}/\rho| = \dots\dots$ e descrivere le seguenti classi di equivalenza:
$[3]_\rho = \dots\dots\dots\dots$, $[28]_\rho = \dots\dots\dots\dots$.

---

8 Si determini $n\in\mathbb{N}$ in modo tale che i due polinomi $f=x^6+2nx^5+7x^4-8nx^3-40x^2+8nx+44$ e $g=x^4+(2n+1)x^3+(2n+9)x^2+(11-4n)x-22$ su $\mathbb{Z}$ abbiano esattamente due radici intere in comune (*suggerimento: si calcoli, in* $\mathbb{Q}[x]$, *un massimo comun divisore di* f *e* g). Per tale valore di n, si decompongano poi f e g in prodotto di polinomi monici irriducibili, prima in $\mathbb{Q}[x]$, poi in $\mathbb{R}[x]$. [Risposte: $n=\dots$

In $\mathbb{Q}[x]$: $f=\dots\dots\dots\dots$ $g=\dots\dots\dots\dots$

In $\mathbb{R}[x]$: $f=\dots\dots\dots\dots$ $g=\dots\dots\dots\dots$]

---

9 Esistono delle coppie $(u,v)\in\mathbb{Z}\times\mathbb{Z}$ tali che $225u+83v=1$? □ *no* □ *sì, una è data da* $u=\dots$, $v=\dots$.
Esistono delle coppie $(h,k)\in\mathbb{Z}\times\mathbb{Z}$ tali che $450h+166k=1$? □ *no* □ *sì, una è data da* $h=\dots$, $k=\dots$.

Di ciascuna delle seguenti equazioni congruenziali si trovi l'insieme (rispettivamente S_1, S_2, S_3, S_4) delle soluzioni intere:

$1660x\equiv_{4500} 30.$ $S_1=\dots\dots\dots\dots$

$1660x\equiv_{4500} 60.$ $S_2=\dots\dots\dots\dots$

$1660x\equiv_{4500} 90.$ $S_3=\dots\dots\dots\dots$

$1660x\equiv_{4500} 120.$ $S_4=\dots\dots\dots\dots$
