CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (I E II GRUPPO)
19 OTTOBRE 2012

Svolgere i seguenti esercizi, *giustificando tutte le risposte*. Sui fogli consegnati vanno indicati: nome, cognome, matricola e gruppo di appartenenza. Non è necessario consegnare la traccia.

Esercizio 1. Assegnati numeri interi a, b, d, r, si dica cosa significano, per definizione, le frasi:
(i) a è divisore di b;
(ii) a è multiplo di b;
(iii) d è un massimo comun divisore tra a e b;
(iv) r è il resto della divisione di a per b. In quest'ultimo caso, è necessario premettere una condizione su b, quale?

Esercizio 2. Si studino iniettività e suriettività dell'applicazione

$$\varphi\colon (a,b) \in \mathbb{N} \times \mathbb{N} \longmapsto 2^a 3^b \in \mathbb{N}^{\#}.$$

Detto $\mathcal{R}_\varphi$ il nucleo di equivalenza di φ, per ogni $(a,b) \in \mathbb{N} \times \mathbb{N}$ si determini $[(a,b)]_{\mathcal{R}_\varphi}$.

Si verifichi che la relazione binaria Σ così definita in $\mathbb{N}^{\#} \times \mathbb{N}^{\#}$:

$$\big(\forall (a,b),(c,d) \in \mathbb{N}^{\#} \times \mathbb{N}^{\#}\big)\big((a,b)\ \Sigma\ (c,d) \iff 2^a 3^b \leq 2^c 3^d\big)$$

è una relazione d'ordine. Σ è totale? $(\mathbb{N}^{\#} \times \mathbb{N}^{\#}, \Sigma)$ è un reticolo? Nel caso lo sia, è distributivo?, è complementato?

Dire se le seguenti affermazioni sono vere o false (giustificando la risposta):
(1) $(\forall (a,b),(c,d) \in \mathbb{N}^{\#} \times \mathbb{N}^{\#})\ \big((a,b)\ \Sigma\ (c,d) \Rightarrow (a \leq c\ \wedge\ b \leq d)\big)$
(2) $(\forall (a,b),(c,d) \in \mathbb{N}^{\#} \times \mathbb{N}^{\#})\ \big((a \leq c\ \wedge\ b \leq d) \Rightarrow (a,b)\ \Sigma\ (c,d)\big)$

Esercizio 3. Si consideri il sottoinsieme $A = \{ax^3 + bx^2 + cx + d \mid a,b,c,d \in \mathbb{Z}_3\}$ di $\mathbb{Z}_3[x]$ e, per ogni $f = ax^3 + bx^2 + cx + d \in A$, si ponga $f' = \bar{3}ax^2 + \bar{2}bx + c$. Caratterizzare i polinomi che costituiscono

$$B = \{f \in A \mid f' = 0\}$$

in termini dei loro coefficienti (ciò che si chiede è dunque determinare condizioni necessarie e sufficienti su a, b, c e d affinché un polinomio $f = ax^3 + bx^2 + cx + d \in A$ appartenga a B).

Quanti sono gli elementi di B? Determinare la forma dei polinomi $f \in B$ che sono:
(i) divisibili per x;
(ii) divisibili per $x - \bar{1}$;
(iii) divisibili per $x + \bar{1}$.
Tra i polinomi in B, quanti sono quelli invertibili in $\mathbb{Z}_3[x]$? E quanti quelli irriducibili?

Esercizio 4. Si studi l'operazione binaria $*$ definita in $\mathbb{Z}_6 \times \mathbb{Z}_6$ ponendo, per ogni $a,b,c,d \in \mathbb{Z}_6$,

$$(a,b) * (c,d) = (ac, bc).$$

(i) Si stabilisca se $*$ è associativa, se è commutativa, se ammette elemento neutro.
(ii) Verificare se $T := \mathbb{Z}_6 \times \{\bar{0}, \bar{3}\}$ è chiusa rispetto a $*$.
(iii) Utilizzando opportune equazioni congruenziali, determinare, se esiste, un elemento $(u,v) \in T$ tale che $(\bar{5},\bar{3}) * (u,v) = (u,v) * (\bar{5},\bar{3}) = (\bar{1},\bar{3})$.