CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II , RECUPERO)
19 MARZO 2013

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. Posto $S = \{2, 6, 10, 20\}$ e indicato con $\mathbb{P}$ l'insieme dei numeri naturali primi, si descrivano esplicitamente gli elementi di ciascuno degli insiemi:

$A = \{p \in \mathbb{P} \mid (\exists x \in S)(p|x)\}$ $\qquad$ $B = \{p \in \mathbb{P} \mid (\exists x \in S)(p \nmid x)\}$

$C = \{p \in \mathbb{P} \mid (\forall x, y \in S)(p|x \Rightarrow p|y)\}$ $\qquad$ $D = \{\mathrm{MCD}(a, b) \mid (a, b) \in S \times S\}$

$E = \{\mathrm{rest}(a, 5) \mid a \in S\}$ $\qquad$ $F = \{\mathrm{rest}(a, b) \mid a, b \in S\}$.

Esercizio 2. Per ogni $n \in \mathbb{N}^{\#}$ esiste una ed una sola coppia $(E(n), D(n)) \in \mathbb{N} \times \mathbb{N}^{\#}$ tale che $D(n)$ sia dispari e $n = 2^{E(n)}D(n)$. Dopo aver enunciato il Teorema Fondamentale dell'Aritmetica, giustificare questa affermazione.

Con le stesse notazioni, sia $*$ l'operazione binaria in $\mathbb{N}^{\#}$ definita ponendo, per ogni $a, b \in \mathbb{N}^{\#}$, $a * b = 2^{E(a)}D(b)$.

(*i*) $*$ è associativa?; $*$ è commutativa?; $*$ è iterativa (vale cioè $a * a = a$ per ogni $a \in \mathbb{N}^{\#}$)?

(*ii*) Esiste in $(\mathbb{N}^{\#}, *)$ un elemento neutro a destra, un elemento neutro a sinistra, un elemento neutro?

(*iii*) Tra le seguenti parti di $\mathbb{N}^{\#}$, dire quali sono chiuse e quali no: $2\mathbb{N}^{\#}$ (l'insieme degli interi positivi pari), $2\mathbb{N} + 1$ (l'insieme degli interi positivi dispari), $\{1, 2\}$, $\{2, 3\}$, $\{100\}$.

(*iv*) Esiste in $(2\mathbb{N} + 1, *)$ un elemento neutro a destra, un elemento neutro a sinistra, un elemento neutro?

Esercizio 3. Per ogni $n \in S := \mathbb{N}^{\#} \setminus \{1\}$, sia p_n il minimo primo positivo divisore di n. Si consideri l'applicazione $f : n \in S \mapsto n/p_n \in \mathbb{N}^{\#}$.

(*i*) f è iniettiva? f è suriettiva?

(*ii*) Sia $\sim$ il nucleo di equivalenza di f. Si elenchino gli elementi di $[6]_\sim$ e di $[12]_\sim$; si descrivano in modo esplicito gli elementi di $[17]_\sim$.

(*iii*) È vero che $[4n]_\sim = \{4n\}$ per ogni $n \in \mathbb{N}^{\#}$?

Sia Σ la relazione d'ordine definita in S ponendo, per ogni $n, m \in S$, $n \;\Sigma\; m$ se e solo se o $n = m$ oppure $f(n)$ è un divisore proprio di $f(m)$.

(*iv*) Descrivere gli (eventuali) elementi minimali e massimali in (S, Σ), nonché gli eventuali minimo e massimo di (S, Σ).

(*v*) Determinare, in (S, Σ), l' insieme dei minoranti e quello dei maggioranti di $\{4, 6\}$.

(*vi*) (S, Σ) è un insieme totalmente ordinato? È un reticolo? Nel caso, è distributivo? È complementato?

(*vii*) Disegnare il diagramma di Hasse di $T = \{4, 6, 8, 13, 27, 72\} \subset S$, ordinato da Σ.

(*viii*) (T, Σ) è un insieme totalmente ordinato? È un reticolo? Nel caso, è distributivo? È complementato?

Esercizio 4. Per ogni primo (positivo) p, sia $f_p = \overline{20}x^4 - x^2 + \bar{3} \in \mathbb{Z}_p[x]$.

(*i*) Si determinino i primi p tali che f_p sia monico;

(*ii*) Si determinino i primi p tali che f_p abbia $-\bar{1}$ come radice;

(*iii*) Si determinino i primi p tali che f_p sia divisibile, in $\mathbb{Z}_p[x]$, per $g = x^2 - x - \bar{2}$, tenendo presente che $g = (x + \bar{1})(x - \bar{2})$.

(*iv*) Si determinino i primi p tali che f_p sia divisibile, in $\mathbb{Z}_p[x]$, per $h = x^3 - x^2 - \bar{2}x$, tenendo presente che $h = xg = x(x + \bar{1})(x - \bar{2})$.