CORSO DI LAUREA TRIENNALE IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I E II)
17 GENNAIO 2018

Svolgere i seguenti esercizi,

giustificando pienamente tutte le risposte.

Sui fogli consegnati vanno indicati: **nome**, **cognome**, **matricola** e **gruppo di appartenenza**.

Non è necessario consegnare la traccia.

Esercizio 1.

(*i*) Si diano le definizioni di *divisore* e di *multiplo* in $\mathbb{Z}$ di un numero intero a.
(*ii*) Enunciare le proprietà che definiscono la divisione in $\mathbb{Z}$.
(*iii*) Per quali interi m è vero che:
(a) $\mathrm{rest}(15, m) = \mathrm{rest}(15, -m)$; (b) $\mathrm{rest}(15, m) = 3$; (c) $3[5]_m = ([5]_m)^3$.

Esercizio 2. Si consideri l'applicazione $f\colon n \in \mathbb{N}^* \mapsto |D(n)| \in \mathbb{N}^*$, dove $D(n)$ indica l'insieme dei divisori di n in $\mathbb{N}$.

(*i*) f è iniettiva? È suriettiva?
(*ii*) Determinare tutti e soli gli $n \in \mathbb{N}^*$ tali che $|D(n)| = 2$ e quelli tali che $|D(n)| = 4$.
(*iii*) Detto $\mathfrak{R}$ il nucleo di equivalenza di f, determinare tutti e soli gli $n \in \mathbb{N}^*$ tali che $[n]_{\mathfrak{R}}$ sia un insieme finito.
(*iv*) Calcolare $|D(2^{999}3^{599})|$.

Sia poi σ la relazione d'ordine in $\mathbb{N}^*$ definita da: per ogni $n, m \in \mathbb{N}^*$

$$n \,\sigma\, m \iff (n = m \vee f(n) < f(m)).$$

In $(\mathbb{N}^*, \sigma)$:

(*v*) determinare gli eventuali minimo, massimo, elementi minimali, elementi massimali;
(*vi*) determinare un $Y \subseteq \mathbb{N}^*$ tale che (Y, σ) sia totalmente ordinato e non esista alcun $K \subseteq \mathbb{N}^*$ tale che $Y \subset K$ e (K, σ) sia totalmente ordinato;
(*vii*) per ogni $m \in \mathbb{N}^*$, spiegare quali sono gli $n \in \mathbb{N}^*$ tali che n e m non siano confrontabili;
(*viii*) è vero o falso che, scelti comunque in $\mathbb{N}^*$ tre elementi x, y, z a due a due non confrontabili, $\{x, y\}$ e $\{y, z\}$ hanno gli stessi minoranti?
(*ix*) descrivere tutte le parti di $\mathbb{N}^*$ della forma $\{x, y\}$ tali che esista $\inf\{x, y\}$. $(\mathbb{N}^*, \sigma)$ è un reticolo?
(*x*) Fornire, se possibile, un esempio di una parte L di $\mathbb{N}^*$ tale che $|L| = 4$ e:
(a) (L, σ) sia un reticolo booleano; (b) (L, σ) sia un reticolo non booleano;
(c) (L, σ) non sia un reticolo.

Esercizio 3. Sia $*$ l'operazione binaria definita in $S = \mathbb{Z}_{163} \times \mathbb{Z}_{163}^*$ ponendo, per ogni $(a, b), (c, d) \in S$, $(a, b) * (c, d) = (a + bc, bd)$.

(*i*) Si provi che $(S, *)$ è un gruppo e che non è abeliano.
(*ii*) Facendo uso di una opportuna equazione congruenziale, si determini l'inverso di $(\overline{3}, \overline{52})$ in $(S, *)$.
(*iii*) Si decida se le seguenti parti di S: $T = \mathbb{Z}_{163}^* \times \mathbb{Z}_{163}^*$ e $K = \{(a, b) \in S \mid b = \overline{1} \vee b = -\overline{1}\}$ sono parti chiuse in $(S, *)$.
(*iv*) Determinare tutti e soli gli elementi $(a, b) \in S$ tali che $(a, b) * (a, b) = (\overline{0}, \overline{1})$.
(*v*) Vero o falso, e perché: scelto comunque $(a, b) \in S$ tale che $(a, b) * (a, b) = (\overline{0}, \overline{1})$, $H := \{(\overline{0}, \overline{1}), (a, b)\}$ è un sottogruppo di $(S, *)$.

Esercizio 4.

(*i*) In $\mathbb{Z}_5[x]$, il polinomio $x^3 - x + \overline{3}$ è irriducibile? Ha radici in $\mathbb{Z}_5$?
(*ii*) In $\mathbb{Z}_5[x]$, il polinomio $(x^3 - x + \overline{3})^2$ è irriducibile? Ha radici in $\mathbb{Z}_5$?
(*iii*) Sia K un campo finito. Supponiamo che $K[x]$ abbia esattamente n polinomi irriducibili monici di grado 2. Quanti sono in $K[x]$ i polinomi monici di grado 4 privi di radici ma non irriducibili?