CORSO DI LAUREA IN INFORMATICA
PROVA SCRITTA DI ALGEBRA (GRUPPI I, II, RECUPERO)
11 LUGLIO 2016

Svolgere i seguenti esercizi,

***giustificando pienamente tutte le risposte*.**

Sui fogli consegnati vanno indicati: *nome, cognome, matricola e gruppo di appartenenza (I, II o recupero)*. Non è necessario consegnare la traccia.

Esercizio 1.

(i) Dare la definizione di *divisore* e di *multiplo* in $\mathbb{Z}$ di un numero intero.
(ii) Per un intero m, definire la relazione di *congruenza modulo* m in $\mathbb{Z}$, ...
(iii) ... e descrivere, per un arbitrario $a \in \mathbb{Z}$, $[a]_m$.
(iv) Determinare gli $m \in \mathbb{N}$ per i quali:
(α): $[3]_m = [21]_m$; (β): $[3]_m = [-3]_m$; (γ): $[3]_m = [3]_m^{-1}$;

Esercizio 2. Per ogni intero positivo m si definisca l'operazione binaria $*_m$ in $\mathbb{Z}_m$ ponendo, per ogni $a, b \in \mathbb{Z}_m$,

$$a *_m b = \overline{10}a + \bar{6}b.$$

(i) Dopo aver calcolato $\bar{1} *_m \bar{0}$, $\bar{0} *_m \bar{1}$, $(\bar{0} *_m \bar{0}) *_m \bar{1}$, $\bar{0} *_m (\bar{0} *_m \bar{1})$, caratterizzare gli $m \in \mathbb{N}^*$ tali che:
(α) $*_m$ sia commutativa;
(β) $*_m$ sia associativa;
(γ) $*_m$ sia associativa e commutativa.
(ii) Determinare tutti e soli gli $a \in \mathbb{Z}_{34}$ tali che $a *_{34} \bar{1} = \bar{0}$. Stabilire se $\bar{1}$ è cancellabile in $(\mathbb{Z}_{34}, *_{34})$.

Sia ora m il massimo intero positivo tale che $*_m$ sia associativa e poniamo $* = *_m$.

(iii) Decidere se $(\mathbb{Z}_m, *)$ ha elementi neutri a destra e/o a sinistra e, nel caso, descriverli *[Suggerimento: si trovino gli $a \in \mathbb{Z}_m$ tali che $a * \bar{0} = \bar{0}$]*.
(iv) Sia $X = \{\bar{6}n \mid n \in \mathbb{Z}_m\}$. X è una parte chiusa in $(\mathbb{Z}_m, *)$? Se lo è, decidere se $(X, *)$ ha elementi neutri a destra e/o a sinistra e, nel caso, descriverli.

Esercizio 3. Consideriamo la funzione resto, $f\colon (a, b) \in \mathbb{N} \times \mathbb{N}^* \longmapsto \mathrm{rest}(a, b) \in \mathbb{N}$. Sia $\mathcal{R}$ il suo nucleo di equivalenza.

(i) f è suriettiva?
(ii) La restrizione di f a $\mathbb{N} \times \{1000\}$ è iniettiva?
(iii) La restrizione di f a $\{1000\} \times \mathbb{N}^*$ è iniettiva?
(iv) Descrivere $[(4, 2)]_{\mathcal{R}}$.

Sia ora Σ la relazione d'ordine definita in $S := \mathbb{N} \times \mathbb{N}^*$ ponendo, per ogni $a, c \in \mathbb{N}$ e $b, d \in \mathbb{N}^*$:

$$(a, b)\ \Sigma\ (c, d) \iff \big((a, b) = (c, d) \vee f((a, b)) \text{ è un divisore proprio di } f((c, d))\big).$$

(v) Si determinino in (S, Σ) gli eventuali elementi minimali, massimali, minimo, massimo. (S, Σ) è un reticolo?
(vi) Si determini l'insieme dei minoranti in (S, Σ) dell'insieme $X := \{8, 15\} \times \{4, 5\}$. Decidere se esiste (e, nel caso, individuare) $\inf_{(S,\Sigma)} X$.
(vii) Esibire se esiste, o provare che non esiste, un sottoinsieme Y di S tale che (Y, Σ) sia un reticolo pentagonale.

Esercizio 4. Per ogni intero primo p, sia $f_p = x^3 - x + \bar{1} \in \mathbb{Z}_p[x]$.

(i) Determinare il minimo primo positivo $\bar{p}$ tale che $f_{\bar{p}}$ *non* sia irriducibile in $\mathbb{Z}_{\bar{p}}[x]$;
(ii) scrivere $f_{\bar{p}}$ come prodotto di polinomi monici irriducibili in $\mathbb{Z}_{\bar{p}}[x]$;
(iii) determinare $X = \{g \in \mathbb{Z}_{\bar{p}}[x] \mid (\forall a \in \mathbb{Z}_{\bar{p}})(f_{\bar{p}}(a) = \bar{0} \Rightarrow g(a) = \bar{0})\}$;
(iv) $h := \bar{2}x^3 + \bar{3}x + \bar{2}$ è associato a $f_{\bar{p}}$ in $\mathbb{Z}_{\bar{p}}[x]$?
(v) $t := \bar{3}x^3 - x + \bar{3}$ è associato a $f_{\bar{p}}$ in $\mathbb{Z}_{\bar{p}}[x]$?