Università degli Studi di Roma Tre
Corso di Laurea in Matematica – a.a. 2010/2011
AL110 – Algebra 1
Appello X

esercizio	1.1	1.2	2.1	2.2	3.1	3.2	3.3	4.1	4.2(a)	4.2(b)
punti max	3	4	3	4	3	2	4	4	3	4
punti assegnati										
totale										

esercizio	5.1	5.2	5.3	6.1	6.2	6.3	7.1	7.2(a)	7.2(b)
punti max	2	8	3	3	8	4	3	2	4
punti assegnati									
totale									

Esercizio 1. Si consideri il sistema di congruenze lineari

$$\begin{cases} 2T \equiv 5 \pmod{7} \\ hT \equiv h+1 \pmod{25} \end{cases} \qquad h \in \mathbb{Z}$$

nell'indeterminata T.

(1) Si determinino tutti e soli i valori di $h \in \mathbb{Z}$ per i quali il sistema assegnato ammette soluzioni.

(2) Dopo aver verificato che $\overline{h} := 2011^{2021}$ è uno dei valori trovati in **(1)**, si determinino esplicitamente le soluzioni del sistema, per $h = \overline{h}$.

Esercizio 2. Per ciascuno dei seguenti gruppi ciclici, se ne esibiscano tutti e soli i generatori.

(1) Il gruppo additivo $(\mathbb{Z}/19\mathbb{Z}, +)$ (cioè, si determinino tutti gli interi k con $0 \leq k \leq 18$ in modo tale che $\mathbb{Z}/19\mathbb{Z} = \{n \cdot [k]_{19} \mid 0 \leq n \leq 18\}$).

(2) Il gruppo moltiplicativo $((\mathbb{Z}/19\mathbb{Z})^{\star}, \cdot)$ (cioè, si determinino tutti gli interi h con $1 \leq h \leq 18$ in modo tale che $(\mathbb{Z}/19\mathbb{Z})^{\star} = \{([h]_{19})^m \mid 1 \leq m \leq 18\}$).

Esercizio 3. Sia A un anello, T un'indeterminata su A, e $f(T) := T^3 + 3 \in A[T]$.

(1) Si determinino tutti e soli i fattori irriducibili del polinomio $f(T)$, per ognuno dei seguenti casi dell'anello:

$$A \in \{(\mathbb{Z}, +, \cdot),\ (\mathbb{Q}, +, \cdot),\ (\mathbb{R}, +, \cdot),\ (\mathbb{C}, +, \cdot),\ \mathbb{F}_2 := (\mathbb{Z}/2\mathbb{Z}, +, \cdot)\}.$$

(2) Si determini, motivando adeguatamente la risposta, se l'anello quoziente $S := \mathbb{F}_2[T]/(f(T))$ è un dominio e/o un campo.

(3) Denotata con $\pi : \mathbb{F}_2[T] \longrightarrow S$ la proiezione canonica, si ponga $\alpha := \pi(T) \in S$. Si stabilisca se l'elemento $\alpha^4 + \alpha^2 + 1 \in S$ è un invertibile (nell'anello S) o se è un divisore dello zero (nell'anello S).

Esercizio 4. Sia T un'indeterminata su $\mathbb{Q}$. Nell'anello $\mathbb{Q}[T]$ si considerino i polinomi

$$f(T) := T^3 + T^2 + T + 1, \qquad g(T) := T^3 + 6T^2 + 11T + 6\,.$$

(1) Si determini in $\mathbb{Q}[T]$ il $\mathrm{MCD}(f(T), g(T))$.

(2) Si risolva, con un argomento chiaro e conciso, ciascuna delle seguenti questioni.

- **(a)** Esistono due polinomi $x(T), y(T) \in \mathbb{Q}[T]$ in modo tale che $x(T)f(T) + y(T)g(T) = 1$? In caso affermativo, determinarli esplicitamente.
- **(b)** Esistono due polinomi $u(T), v(T) \in \mathbb{Q}[T]$ in modo tale che $u(T)f(T) + v(T)g(T) = T^2 - 1$? In caso affermativo, determinarli esplicitamente.

Esercizio 5.

(1) Enunciare il Teorema Cinese dei Resti.

(2) Dimostrare il Teorema Cinese dei Resti.

(3) Determinare tutte le soluzioni del seguente sistema di congruenze:

$$\begin{cases} X \equiv 3 \pmod{7} \\ X \equiv 2 \pmod{5} \\ X \equiv 6 \pmod{11} \\ X \equiv 4 \pmod{13}\,. \end{cases}$$

Esercizio 6. Sia $f(T) \in \mathbb{Z}[T]$ un polinomio non nullo a coefficienti interi e sia p un intero primo.

(1) Enunciare il Teorema di Lagrange sul numero (massimo) delle soluzioni della congruenza $f(T) \equiv 0 \pmod{p}$.

(2) Dimostrare il Teorema di Lagrange (enunciato in (1)).

(3) Sia n un numero naturale non nullo e *non primo*. Mostrare con un esempio che la conclusione del Teorema di Lagrange non vale (in generale) per la congruenza $f(T) \equiv 0 \pmod{n}$.

Esercizio 7. Sia $f : \mathbb{N} \longrightarrow \mathbb{Z}/16\mathbb{Z}$ la funzione definita ponendo $f(n) := [n^4]_{16}$, per ogni $n \in \mathbb{N}$.

(1) Si determinino tutti e soli gli elementi di $f(\mathbb{N})$.

(2) Detta $\mathcal{R}_f$ la relazione di equivalenza su $\mathbb{N}$ indotta da f

$$(\text{cioè, } (n', n'') \in \mathcal{R}_f :\Leftrightarrow f(n') = f(n''), \text{ con } n', n'' \in \mathbb{N}),$$

si determinino

(a) la classe di equivalenza di $5 \in \mathbb{N}$ modulo $\mathcal{R}_f$;

(b) la cardinalità dell'insieme $\mathbb{N}/\mathcal{R}_f$ [ovvero si descrivano eplicitamente gli elementi (= classi di equivalenza) dell'insieme quoziente $\mathbb{N}/\mathcal{R}_f$].