AL110 - Algebra 1 - A.A. 2011/2012
Valutazione "in itinere" - II Prova

Cognome: ..... **Nome:** .....

Matricola (O ALTRO IDENTIFICATIVO) → ☐☐☐☐☐☐
UTILIZZARE LO STESSO IDENTIFICATIVO DELLA PRIMA PROVA

esercizio	1.1	1.2	1.3.1	1.3.2	2.1	2.2	2.3.1	2.3.2	2.3.3	3.1	3.2	3.3	3.4	3.5.1	3.5.2
punti max	2	6	1	4	3	2	2	2	4	3	2	3	3	4	6
valutazione															

esercizio	4.1	4.2	4.3	5.1	5.2	5.3	5.4	5.5.1	5.5.2	5.5.3	5.5.4	6.1.1	6.1.2	6.2.1	6.2.2
punti max	2	2	2	4	3	3	5	1	2	3	6	3	3	6	3
valutazione															

TOTALE →		*"bonus"* →	*"malus"* →

AVVERTENZE : *Svolgere gli esercizi in modo conciso, ma esauriente, nello spazio assegnato in questo fascicolo.* **Non consegnare altri fogli.**
Lo svolgimento preliminare ed i calcoli possono essere effettuati nei fogli bianchi che vengono consegnati agli studenti assieme a questo fascicolo. Tali fogli non devono essere riconsegnati.
– *Fino a* **due punti ulteriori (bonus)** *potranno essere assegnati agli elaborati scritti in modo molto chiaro.*
– *Fino a* **due punti (malus)** *potranno essere* **detratti** *dagli elaborati scritti in modo molto confuso o difficilmente leggibile.*

LEGGERE LE AVVERTENZE

NON SFOGLIARE IL TESTO
PRIMA CHE VENGA DATO UFFICIAMENTE INIZIO ALLA PROVA DAL DOCENTE

ESERCIZIO 1.

(1) Enunciare il Teorema Cinese dei Resti.

(2) Dimostrare, con poche frasi formulate in modo chiaro e conciso, il Teorema Cinese dei Resti, descrivendo esplicitamente una soluzione del sistema di congruenze.

(3) Si consideri il seguente sistema di congruenze per α intero con $1 \leq \alpha \leq 5$:

$$\begin{cases} 2X \equiv \alpha \pmod{6} \\ X \equiv 6 \pmod{7} \\ 2X \equiv 5 \pmod{11} \end{cases}.$$

(3.1) Determinare per quali valori di α (con $1 \leq \alpha \leq 5$) il sistema di congruenze è risolubile.

(3.2) Per ciascuno dei valori di α per il quale il sistema è risolubile, determinare esplicitamente tutte le soluzioni del sistema (mod 462).

ESERCIZIO 2. Sia $A := \mathbb{R} \times \mathbb{Z}$ l'anello prodotto diretto degli anelli $(\mathbb{R}, +, \cdot\ )$ e $(\mathbb{Z}, +, \cdot\ )$ (dove ricordiamo che per *prodotto diretto* si intende l'insieme prodotto cartesiano $\mathbb{R} \times \mathbb{Z}$ munito delle operazioni di somma e prodotto definite "componente per componente").

(1) Stabilire se $(A, +, \cdot\ )$ è un anello unitario, se è commutativo, se possiede divisori dello zero, se è un campo (nel caso non verifichi una delle proprietà elencate, si dia un appropriato controesempio).

(2) Sia $B := \{(x, 3y) \mid x, y \in \mathbb{Z}\} := \mathbb{Z} \times 3\mathbb{Z}$ $(\subseteq A)$. Stabilire se B è un sottoanello di $(A, +, \cdot\ )$, o/e se B è un ideale di $(A, +, \cdot\ )$.

(3) Su A si consideri la reguente relazione ρ_B, definita come segue, presi $\alpha_1,\ \alpha_2 \in A$:

$$\alpha_1\ \rho_B\ \alpha_2 :\Leftrightarrow \alpha_1 - \alpha_2 \in B\,.$$

(3.1) Verificare che ρ_B è una relazione di equivalenza su A.

(3.2) Sull'insieme-quoziente A/ρ_B si ponga

$$[\alpha_1]_{\rho_B} + [\alpha_2]_{\rho_B} := [\alpha_1 + \alpha_2]_{\rho_B} \quad \text{presi comunque } \alpha_1,\ \alpha_2 \in A\,.$$

Stabilire se $(A/\rho_B, +)$ è un gruppo.

(3.3) Sull'insieme-quoziente A/ρ_B si ponga

$$[\alpha_1]_{\rho_B} \cdot [\alpha_2]_{\rho_B} := [\alpha_1 \cdot \alpha_2]_{\rho_B} \quad \text{presi comunque } \alpha_1,\ \alpha_2 \in A\,.$$

Stabilire se $(A/\rho_B,\ +,\ \cdot)$ è un anello.

ESERCIZIO 3. Si affronti ciascuna delle seguenti questioni, fornendo un argomento conciso ed esauriente.

(1) Dato un intero positivo *dispari* n, si calcoli esplicitamente $[(n-1)(n+1)]_8$, cioè, si determini k con $0 \leq k \leq 7$ in modo tale che $[k]_8 = [(n-1)(n+1)]_8$. Stabilire se k dipende oppure non dipende dalla scelta di n.

(2) Si enunci il Teorema di Eulero–Fermat e si deduca da esso l'enunciato del "Piccolo" Teorema di Fermat.

(3) Si calcoli la classe resto modulo 7 di $\displaystyle\sum_{n=1}^{2012}(n!)^{2012}$, cioè, si determini r con $0 \leq r \leq 6$ in modo tale che

$$[r]_7 = \left[\sum_{n=1}^{2012}(n!)^{2012}\right]_7 .$$

(4) Siano p un numero primo e a un intero positivo minore di p. Determinare il resto di a^{p^2-p+1} nella divisione per p^2.

(5*) Sia $n := 2723^{2723}$.

(5.1) Dopo aver calcolato $\mathrm{MCD}(n, 10)$, si determini l'ultima cifra (i.e., la cifra delle unità) di n^{16}.

(5.2) Si dimostri che $n^4 - 1$ è divisibile per 80. [*Suggerimento: si provi a fattorizzare* $n^4 - 1$*, e si usi* (1) *per provare che* $n^4 - 1$ *è divisibile per 16.*]

(*) *Questo esercizio è opzionale (può contribuire all'ottenimento della lode).*

ESERCIZIO 4. Sia ℓ un intero fissato, $\ell \neq 0$. In $\mathbb{Z}$ si consideri la seguente operazione $\star$ (dipendente da ℓ) così definita:

$$a \star b := a + b - \ell \quad \text{presi comunque } a, b \in \mathbb{Z}\,.$$

(1) Verificare se $(\mathbb{Z}, \star)$ è oppure non è un gruppo abeliano.

(2) Stabilire se l'applicazione $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, \star)$, definita da

$$\varphi(a) := a(1 + \ell) + (1 - a)\ell, \quad \text{per ogni } a \in \mathbb{Z},$$

è oppure non è un omomorfismo di gruppi.

(3) Stabilire se $\varphi : (\mathbb{Z}, +) \to (\mathbb{Z}, \star)$ è oppure non è un isomorfismo di gruppi.

ESERCIZIO. 5 Si consideri la permutazione

$$\sigma := (3\ \ 5) \circ (5\ \ 7) \circ (1\ \ 2) \circ (2\ \ 4\ \ 6)^{1000} \in \boldsymbol{S}_7.$$

(1) Si determini decomposizione in cicli disgiunti, ordine e segno di σ.

(2) Si calcoli esplicitamente σ^{2012}.

(3) Si dica se possono esistere due 5–cicli $\lambda, \mu \in \boldsymbol{S}_7$ in modo tale che

$$\lambda \circ \sigma = \mu.$$

(4) Si dica se può esistere una trasposizione $\tau := (i\ \ j) \in \boldsymbol{S}_7$ tale che

$$\sigma \circ \tau = \tau \circ \sigma\,.$$

[Suggerimento: innanzitutto, si stabilisca se $\{\sigma(i), \sigma(j)\} \subseteq \{i, j\}$.]

(5) Sia adesso $G :=< \sigma >$ il sottogruppo di $(\boldsymbol{S}_7, \circ)$ generato da σ.

(5.1) Si trovino tutti i generatori di G.

(5.2) Determinare tutti i sottogruppi di G e, per ciascuno di tali sottogruppi, si esibisca un generatore.

(5.3) Si determini se può esistere un omomorfismo di gruppi $\varphi : G \longrightarrow \boldsymbol{S}_3$ tale che

$$\varphi(\sigma) := (1\ \ 2\ \ 3)\ (\in \boldsymbol{S}_3)\,.$$

(5.4) Si determini se può esistere un omomorfismo di gruppi $\psi : G \longrightarrow \boldsymbol{S}_3$ tale che

$$\psi(\sigma) := (1\ \ 2)\ (\in \boldsymbol{S}_3)\,.$$

Se ψ esiste, si determini la sua immagine $\mathrm{Im}(\psi) := \psi(G)$ ed il suo nucleo $\mathrm{Ker}(\psi) := \psi^{-1}(\mathbf{1})$ (dove $\mathbf{1}$ è la permutazione identica di $\boldsymbol{S}_3$). In tale caso, si applichi il Teorema Fondamentale di Omomorfismo di gruppi descrivendone le conseguenze.

ESERCIZIO 6.

(1) Siano dati $f(T) := T^3 + 6T^2 + 3T - 10$ e $g(T) := T^2 + 2T - 3$ due polinomi in $\mathbb{Z}[T] \subset \mathbb{Q}[T]$.

(1.1) Utilizzando l'algoritmo euclideo delle divisioni successive, calcolare in $\mathbb{Q}[T]$ il polinomio *monico* $d(T) := \mathrm{MCD}(f(T), g(T))$ e determinare due polinomi $\alpha(T),\ \beta(T) \in \mathbb{Q}[T]$ in modo tale che:

$$d(T) = \alpha(T)f(T) + \beta(T)g(T) \qquad \text{[Identità di Bézout in } \mathbb{Q}[T]\text{]}\,.$$

(1.2) Utilizzando il Teorema di Ruffini, determinare tutte le eventuali radici in $\mathbb{Q}$ di $f(T)$ e di $g(T)$.

(2) Sia p un numero primo e sia $f_p(T) := T^{2p} + pT^3 + pT + 2p$.

(2.1) Si discuta l'irriducibilità di $f_p(T)$ in $\mathbb{Z}[T],\ \mathbb{Q}[T],\ \mathbb{R}[T],\ \mathbb{C}[T]$, al variare del numero primo p.

(2.2) Per $p = 2$, si determinino i fattori irriducibili di $f_2(T)$ in $\mathbb{Z}[T],\ \mathbb{Q}[T],\ \mathbb{R}[T]$, $\mathbb{C}[T]$.