AL110 - Algebra 1 - A.A. 2014/2015
Valutazione "in itinere" - Seconda Prova (Gennaio 2015)

Matricola (O ALTRO IDENTIFICATIVO) → ☐

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

---

esercizio	1.1	1.2	2.1	2.2	2.3	2.4a	2.4b	3.1	3.2	3.3
punti max	2	3	2	2	3	2	4	3	3	1
valutazione										

esercizio	4.1	4.2a	4.2b	4.2c	5.1	5.2	5.3	6.1	6.2	6.3	6.4
punti max	5	4	4	5	2	5	8	4	2	4	8
valutazione											
TOTALE →								*"bonus"* →			

AVVERTENZE: *Svolgere gli esercizi in modo conciso, ma esauriente, nello spazio assegnato.*
– *Fino a* **due punti ulteriori (bonus)** *potranno essere assegnati agli elaborati scritti in modo molto chiaro.*
– *Fino a* **due punti ulteriori (bonus)** *potranno essere assegnati a coloro che consegneranno l'elaborato entro la prima scadenza fissata dai docenti ed otterranno una valutazione complessiva positiva.*

LEGGERE LE AVVERTENZE

NON SFOGLIARE IL TESTO

PRIMA CHE VENGA DATO UFFICIAMENTE INIZIO ALLA PROVA DAL DOCENTE

ESERCIZIO 1. Sia $f : \mathbb{N}^+ \to \mathbb{Z}$ l'applicazione definita nella maniera seguente:

$$f(x) := \begin{cases} \frac{x}{2} - 1 & \text{se } x \text{ è pari}\,, \\ -\left(\frac{x+1}{2}\right) & \text{se } x \text{ è dispari}\,. \end{cases}$$

(1) Stabilire se f è iniettiva o/e suriettiva o/e biiettiva.
(2) Nel caso in cui f sia biiettiva definire esplicitamente $f^{-1} : \mathbb{Z} \to \mathbb{N}^+$.

ESERCIZIO 2.

(1) Determinare la più piccola soluzione positiva della congruenza:

$$30X \equiv 35 \pmod{55}.$$

(2) Determinare per quali valori del parametro λ, con $0 \leq \lambda \leq 5$ il seguente sistema di congruenze è risolubile:

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

(3) Per ciascun valore *intero positivo* di λ (con $1 \leq \lambda \leq 5$) per il quale il sistema precedente è risolubile, determinare esplicitamente tutte le sue soluzioni.

(4) Sia $f : \mathbb{Z} \to (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$ l'applicazione definita ponendo

$$f(x) := ([x]_6, [x]_{13}, [x]_{11}), \text{ al variare di } x \in \mathbb{Z}.$$

(a) Stabilire se $f : \mathbb{Z} \to (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$ è un omomorfismo dall'anello $(\mathbb{Z}, +, \cdot)$ all'anello $((\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z}), +, \cdot)$ (quest'ultimo con le operazioni di somma e prodotto definite "componente per componente").

(b) Determinare $\mathrm{Im}(f)$ e, se f è un omomorfismo, $\mathrm{Ker}(f)$.

ESERCIZIO 3. Sia $\mathrm{GL}_2(\mathbb{Q})$ il gruppo moltiplicativo delle matrici 2×2 ad entrate in $\mathbb{Q}$ con determinante non nullo (dove il prodotto è l'usuale prodotto righe$\times$colonne di matrici). Si considerino i seguenti sottoinsiemi di $\mathrm{GL}_2(\mathbb{Q})$:

$$A := \left\{ \begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \mid a, b, c \in \mathbb{Q},\ ac \neq 0 \right\}, \quad B := \left\{ \begin{pmatrix} 1 & 0 \\ \beta & 1 \end{pmatrix} \mid \beta \in \mathbb{Q} \right\}.$$

(1) Dimostrare che A e B sono sottogruppi (moltiplicativi) di $\mathrm{GL}_2(\mathbb{Q})$.

(2) Sia $\varphi : A \to \mathrm{GL}_2(\mathbb{Q})$ l'applicazione definita nella maniera seguente:

$$\varphi\left(\begin{pmatrix} a & 0 \\ b & c \end{pmatrix} \right) := \begin{pmatrix} a & 0 \\ 0 & c \end{pmatrix}.$$

Mostrare che φ è un omomorfismo di gruppi e determinare $\mathrm{Ker}(\varphi)$.

(3) Stabilire se B è un sottogruppo normale di A.

ESERCIZIO 4. Sia $(\mathbf{S}_7, \circ)$ il gruppo delle permutazioni sull'insieme $\{1,2,3,4,5,6,7\}$ (cioè, il gruppo delle applicazioni biunivoche dell'insieme $\{1,2,3,4,5,6,7\}$ in sé stesso). Si risolvano le seguenti questioni.

(1) Al variare di $n \in \{2,3,4,5,6,7,8,11,12\}$ si determini, quando esiste, un elemento $\tau_n \in \mathbf{S}_7$ avente ordine esattamente uguale ad n.

(2) Si considerino adesso le seguenti permutazioni:

$$\lambda := (1\ 2\ 3\ 4)\,, \quad \mu := (4\ 6\ 2\ 7\ 5) \in \mathbf{S}_7\,.$$

(a) Si determini struttura ciclica, ordine e segno della seguente permutazione:

$$\lambda \circ \mu^{102}\,.$$

(b) Posto $\gamma := \lambda \circ \mu^{102}$ e considerato il sottogruppo ciclico $G := \langle \gamma \rangle$ di $\mathbf{S}_7$ generato da γ, si determinino tutti i sottogruppi di G, indicando per ciascuno di essi un generatore.

(c) Si stabilisca, se esiste, un omomorfismo di gruppi $\varphi : \mathbf{S}_3 \to G$ tale che $\mathrm{Im}(\varphi) = \langle \gamma^2 \rangle$.

ESERCIZIO 5.

(1) Enunciare il Teorema di Lagrange sui gruppi finiti e da esso dedurre il Teorema di Euler-Fermat.

(2) Si trovino le cifre delle decine e delle unità del numero intero 3^{100}.

(3) Si dimostri che, per ogni intero λ, il numero $\lambda^{15} - \lambda^3$ è divisibile per $5 \cdot 7 \cdot 8 \cdot 9 \cdot 13$.

ESERCIZIO 6. Sia T un'indeterminata su $\mathbb{Q}$ e sia

$$f(T) := -6 + 4T - 2T^2 + 3T^3 + T^4 \in \mathbb{Q}[T]\,.$$

(1) Si determini l'espansione di $f(T)$ come prodotto di polinomi (monici) irriducibili in $\mathbb{Q}[T]$.

(2) Si stabilisca se l'anello-quoziente $A := \mathbb{Q}[T]/(f(T))$ è un campo e/o un dominio di integrità. Se esistono, si esibiscano gli eventuali divisori dello zero dell'anello A.

(3) Se esiste, si calcoli esplicitamente l'inverso in A della classe $[T]_f := T + (f(T))$.

(4) Al variare del parametro $\lambda \in \mathbb{Q}$, si discuta l'invertibilità della classe $\alpha_\lambda := [T^2 + \lambda]_f := T^2 + \lambda + (f(T)) \in A$.

SOLUZIONE ESERCIZIO 1. L'applicazione f è biiettiva (notare che –tramite f– i numeri pari positivi vanno sopra $\mathbb{N}$, mentre i numeri dispari positivi vanno sopra gli interi relativi negativi) ed $f^{-1} : \mathbb{Z} \to \mathbb{N}^+$ è definita nella maniera seguente:

$$f^{-1}(y) := \begin{cases} 2(y+1) & \text{se } y \in \mathbb{N} \ , \\ -2y-1 & \text{se } y \in \mathbb{Z} \setminus \mathbb{N} \, . \end{cases}$$

SOLUZIONE ESERCIZIO 2.

- **(1)** $x = 3$. Notare che le soluzioni della congruenza sono date da $x \equiv 3 \bmod 11$ (ovvero, $x \equiv 3, 14, 25, 36, 47 \bmod 55$).
- **(2)** $\lambda = 0, 3$.
- **(3)** Per $\lambda = 3$, la soluzione è data da $x \equiv 17 \bmod 2 \cdot 13 \cdot 11 = 286$ (ovvero, $x \equiv 17, 303, 589 \bmod 6 \cdot 13 \cdot 11 = 858$) .
  (Si può anche notare, ma non era richiesto, che per $\lambda = 0$, le soluzioni sono date da $x \equiv 160, 446, 732 \bmod 6 \cdot 13 \cdot 11 = 858$.)
- **(4)** L'applicazione f è un omomorfismo di anelli. Per il Teorema Cinese dei Resti, $\mathrm{Im}(f) = (\mathbb{Z}/6\mathbb{Z}) \times (\mathbb{Z}/13\mathbb{Z}) \times (\mathbb{Z}/11\mathbb{Z})$; $\mathrm{Ker}(f) = (6 \cdot 13 \cdot 11)\mathbb{Z}$.

SOLUZIONE ESERCIZIO 3.

- **(1)** Svolgendo i calcoli è facile verificare che, prese comunque due matrici $X, Y \in A$ (rispettivamente, $X, Y \in B$), allora $XY^{-1} \in A$ (rispettivamente, $XY^{-1} \in B$). Quindi, A e B sono sottogruppi di $\mathrm{GL}_2(\mathbb{Q})$.
- **(2)** Una verifica diretta mostra che φ è un omomorfismo di gruppi. Inoltre, $\mathrm{Ker}(\varphi) = B$.
- **(3)** Da (2) segue che B è un sottogruppo normale.

SOLUZIONE ESERCIZIO 4.

- **(1)** Basta prendere $\tau_2 := (1\ 2)$, $\tau_3 := (1\ 2\ 3)$, $\tau_4 := (1\ 2\ 3\ 4)$, $\tau_5 := (1\ 2\ 3\ 4\ 5)$, $\tau_6 := (1\ 2\ 3\ 4\ 5\ 6)$, $\tau_7 := (1\ 2\ 3\ 4\ 5\ 6\ 7)$, $\tau_{12} := \tau_3 \circ (4\ 5\ 6\ 7)$ (infatti tali permutazioni sono disgiunte e hanno ordini coprimi, quindi $\mathrm{ord}(\tau_{12}) = 3 \cdot 4 = 12$). Poiché 11 non divide $\mathrm{Card}(\mathbf{S}_7) = 7!$, dal Teorema di Lagrange segue che in $\mathbf{S}_7$ non esistono elementi di ordine 11. Calcolando le possibili strutture cicliche di un elemento di $\mathbf{S}_7$ si evince che non possono esistere elementi di ordine 8.
- **(2)** **(a)** Essendo un 5-ciclo, μ ha ordine 5, e quindi $\mu^{102} = \mu^2 = (4\ 2\ 5\ 6\ 7)$. Quindi

  $$\lambda \circ \mu^{102} = (1\ 2\ 3\ 4) \circ (4\ 2\ 5\ 6\ 7) = (1\ 2\ 5\ 6\ 7) \circ (3\ 4)$$

  Dunque, $\gamma := \lambda \circ \mu^{102}$ è dispari essendo prodotto di una permutazione pari (un 5-ciclo) e una dispari (una trasposizione). Inoltre γ ha ordine 10, essendo prodotto di due permutazioni $(1\ 2\ 5\ 6\ 7)$, $(3\ 4)$ disgiunte aventi ordini coprimi (5 e 2, rispettivamente).

  (b) Da (a) segue che G è un gruppo ciclico di cardinalità 10. Dunque ha un unico sottogruppo H di ordine 5 e un unico sottogruppo H' di ordine 2. Per quanto visto in classe, un generatore di H è γ^2 e un generatore di H' è γ^5.

(c) Gli elementi non banali di $\mathbf{S}_3$ hanno ordine 3 o ordine 2. Poiché $\gamma^2 \in \mathrm{Im}(\varphi)$, esiste una permutazione $\eta \in \mathbf{S}_3$ tale che $\varphi(\eta) = \gamma^2$ e, per quanto visto in classe, l'ordine di $\varphi(\eta)$ deve dividere l'ordine di η, e tale ordine può essere 2 o 3, contraddizione, perché l'ordine di γ^2 è 5.

SOLUZIONE ESERCIZIO 5.

(1) Visto in classe (vedere appunti).

(2) Occorre calcolare la classe di resto di 3^{100} modulo 100. Sia φ l'indicatore di Eulero. Per il Teorema di Eulero-Fermat, $3^{\varphi(100)} \equiv_{100} 1$, i.e., $3^{40} \equiv_{100} 1$. Allora

$$3^{100} = (3^{40})^2 \cdot 3^{20} \equiv_{100} 3^{20}$$

Dunque è sufficiente calcolare 3^{20} modulo 100. Si ha

$$3^{20} \equiv_{100} (3^4)^5 \equiv_{100} (81)^5 \equiv_{100} (-19)^5 \equiv_{100} -99 \equiv_{100} 1$$

Dunque le ultime due cifre di 3^{100} sono 01.

(3) Si ha $x := \lambda^{15} - \lambda^3 = \lambda^3(\lambda^{12} - 1)$. Ovviamente basterà far vedere che x è divisibile per 5, 7, 8, 9, 13. Si ha $\varphi(5) = 4$, $\varphi(7) = 6$, $\varphi(8) = 4$, $\varphi(9) = 6$, $\varphi(13) = 12$. Dunque $\varphi(i)$ divide 12, per ogni $i \in I := \{5, 7, 8, 9, 13\}$.

Fissiamo $i \in I$. Se i divide λ, allora, a fortiori, i divide x.

Se invece i non divide λ, calcoliamo $\mathrm{MCD}(i, \lambda)$.

Se $i \neq 8, 9$, $\mathrm{MCD}(i, \lambda) = 1$ e per il Teorema di Eulero-Fermat si ha $\lambda^{\varphi(i)} \equiv_i 1$ e, poiché $\varphi(i)$ divide 12, $\lambda^{12} \equiv_i 1$, i.e., i divide $\lambda^{12} - 1$.

Se invece $i \in \{8, 9\}$ e i non divide λ, possiamo comunque supporre, senza perdita di generalità, che $\mathrm{MCD}(i, \lambda) = 1$ e concludere come prima, usando il Teorema di Eulero-Fermat. Infatti, se $i \in \{8, 9\}$ e p è un primo comune a i e λ, p è 2 o 3. Se $p = 2$, allora 8 divide λ^3 e quindi divide 8 divide x. Se $p = 3$, allora 27 divide λ^3 e, a fortiori, 9 divide x.

SOLUZIONE ESERCIZIO 6.

(1) Essendo 1 una radice di f, per il Teorema di Ruffini $T-1$ divide f in $\mathbb{Q}[T]$, e si ha

$$f(T) = (T-1)(T^3 + 4T^2 + 2T + 6)$$

il polinomio $T^3 + 4T^2 + 2T + 6$ è irriducibile in $\mathbb{Z}[T]$ e $\mathbb{Q}[T]$, essendo un polinomio di tipo "2-Eisenstein".

(2) L'anello A non è un dominio di integrità (a fortiori, non è un campo), perché f è riducibile in $\mathbb{Q}[T]$. La classe $[T-1]_f$ è un divisore dello zero di A, essendo $[T-1]_f[T^3 + 4T^2 + 2T + 6]_f = [0]_f$.

(3) Essendo $\mathrm{MCD}(f, T) = 1$, $[T]_f$ è invertibile in A. Poiché $[f]_f = [0]_f$, si ha

$$[6]_f = [4T - 2T^2 + 3T^3 + T^4]_f = [T]_f[4 - 2T + 3T^2 + T^3]_f$$

e quindi $[1]_f = [T]_f[\frac{1}{6}(4 - 2T + 3T^2 + T^3)]_f$. Pertanto

$$[T]_f^{-1} = [\frac{1}{6}(4 - 2T + 3T^2 + T^3)]_f.$$

(4) Poniamo $g_\lambda(T) := T^2 + \lambda$. Allora $[g_\lambda]_f$ NON è invertibile in A se e soltanto se $\mathrm{MCD}(g_\lambda, f) \neq 1$, i.e., se e soltanto se $T-1$ è un fattore di g_λ (ovviamente, per ragioni di grado, $T^3 + 4T^2 + 2T + 6$ non può essere fattore (irriducibile)

di g_λ). Per il Teorema di Ruffini, l'ultima asserzione equivale a $g_\lambda(1) = 0$, i.e., $\lambda = -1$. Dunque, $[g_\lambda]_f$ è invertibile in A se e soltanto se $\lambda \in \mathbb{Q} \setminus \{-1\}$.