AL110 - Algebra 1 - A.A. 2014/2015
Appello B (Febbraio 2015)

Matricola (O ALTRO IDENTIFICATIVO) → [ ]

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

---

esercizio	1.1	1.2.1	1.2.2	1.3	2.1	2.2	2.3	2.4.1	2.4.2	3.1	3.2	3.3	3.4
punti max	3	1	3	2	2	5	2	1	3	2	4	4	3
valutazione													

esercizio	4.1	4.2	4.3	4.4	4.5	4.6	5.1	5.2	6.1	6.2a	6.2b	6.3
punti max	1	2	2	2	3	4	4	5	6	1	4	2
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.*
– *La soluzione degli esercizi deve essere scritta negli appositi spazi bianchi di questo fascicoletto. Non debbono essere consegnati altri fogli.*

LEGGERE LE AVVERTENZE

NON SFOGLIARE IL TESTO

PRIMA CHE VENGA DATO UFFICIAMENTE
INIZIO ALLA PROVA DAL DOCENTE

ESERCIZIO 1.

(1) Sia X un insieme non vuoto e sia $\mathcal{P}(X)$ il suo insieme delle parti.
Se $\mathcal{S}$ è un sottoinsieme non vuoto di $\mathcal{P}(X)$ che gode della seguente proprietà:
se $A, B \in \mathcal{S}$ allora $A \setminus B \in \mathcal{S}$.
Dimostrare che se $A, B \in \mathcal{S}$ allora $A \cap B \in \mathcal{S}$.

(2) Si definisca la seguente relazione ρ nell'insieme dei numeri naturali $\mathbb{N}$:

$$a\rho b \quad :\Longleftrightarrow \quad a^2 \equiv b^2 \pmod{7}\,.$$

(2.1) Determinare se ρ è una relazione di equivalenza su $\mathbb{N}$.

(2.2) Nel caso di risposta affermativa, determinare il numero delle classi di equivalenza che costituiscono la partizione di $\mathbb{N}$, associata a ρ.

(3) Siano $a, b, c \in \mathbb{Z}$ e sia $c\mathbb{Z} := \{cx \mid x \in \mathbb{Z}\}$.
Se esistono, determinare esplicitamente due interi $n, m \in \mathbb{Z}$ (dipendenti da a e b) in modo tale che:

$$a\mathbb{Z} \cap b\mathbb{Z} = n\mathbb{Z} \quad \text{e} \quad a\mathbb{Z} \cup b\mathbb{Z} = m\mathbb{Z}\,,$$

altrimenti dare controesempi espliciti.

ESERCIZIO 2.

(1) Enunciare il cosìdetto "Piccolo" Teorema di Fermat.

(2) Dare una dimostrazione del "Piccolo" Teorema di Fermat.

(3) Determinare il più piccolo intero positivo x , $1 \leq x \leq 10$, tale che:

$$5^{38} \equiv x \pmod{11}.$$

(4.1) Determinare per quali valori del parametro λ, con $0 \leq \lambda \leq 7$, il seguente sistema di congruenze è risolubile:

$$\begin{cases} 3X \equiv 2 \pmod{5} \\ 4X \equiv 2\lambda \pmod{8} \\ 4X \equiv 11 \pmod{13} \end{cases}.$$

(4.2) Per il più piccolo valore positivo di λ, con $1 \leq \lambda \leq 7$, per il quale il sistema (4.1) è risolubile, determinare le sue soluzioni.

ESERCIZIO 3.

Nell'anello di polinomi $A := (\mathbb{Z}[T], +, \cdot)$ si consideri il sottoinsieme B dei polinomi di A che hanno termine noto multiplo di 3, cioè

$$B := \{3b_0 + b_1T + b_2T^2 + \cdots + b_nT^n \mid n \geq 0,\, b_k \in \mathbb{Z} \text{ per ogni } k,\, 0 \leq k \leq n\}\,.$$

(1) Stabilire se B è un ideale dell'anello commutativo A.

(2) Determinare due polinomi β_1 e β_2 in B in modo tale che:

$$B := \beta_1 A + \beta_2 A\,.$$

(3) Si può determinare un unico polinomio β in B in modo tale che $B := \beta A$?

(4) Determinare esplicitamente, se esiste, un omomorfismo di anelli $\varphi : \mathbb{Z}[T] \to \mathbb{Z}/3\mathbb{Z}$ in modo tale che $\mathrm{Ker}(\varphi) = B$.

Ripetere Matricola (o altro identificativo) $\rightarrow$ $\boxed{}$

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

ESERCIZIO 4. Sull'insieme $G := \{(x, y) \in \mathbb{R}\times\mathbb{R} \mid x \neq 0\}$ si definisca l'operazione binaria $\star : G \times G \longrightarrow G$ ponendo:

$$(x, y) \star (a, b) := (xa, xb + y) \qquad \text{presi comunque } (x, y), (a, b) \in G,$$

e si dia per buono che l'operazione $\star$ sia associativa.

(1) Si stabilisca se $\star$ è commutativa.
(2) Si dimostri che G ha l'elemento neutro, rispetto a $\star$.
(3) Si dimostri che $(G, \star)$ è un gruppo.
(4) Si determini l'ordine degli elementi $(-1, 0)$ e $(1, 1)$ di G.
(5) Si elenchino gli elementi del sottogruppo $H := \langle(-1, 0)\rangle$ di G, e si stabilisca se H è normale in G.
(6) Si consideri il sottoinsieme

$$K := \{(1, r) \mid r \in \mathbb{R}\}.$$

Si stabilisca se K è un sottogruppo di $(G, \star)$, precisando se K è normale in $(G, \star)$.

ESERCIZIO 5. Utilizzando una delle formulazioni del Principio di Induzione, il candidato affronti i seguenti quesiti.

(1) Sia $\{F_n \mid n \in \mathbb{N}\}$ la successione dei numeri del Fibonacci, i.e.,

$$F_0 := 0, F_1 := 1, F_n := F_{n-1} + F_{n-2}, \qquad \text{per ogni } n \geq 2.$$

Si dimostri che, per ogni intero positivo n, vale una, e una soltanto, fra le seguenti uguaglianze:

(1a) $F_0 + F_2 + \ldots + F_{2n} = F_{2(n+1)} - 1.$

(1b) $F_0 + F_2 + \ldots + F_{2n} = F_{2n+1} - 1.$

(1c) $F_0 + F_2 + \ldots + F_{2n} = F_{n+2} - 1.$

(1d) $F_0 + F_2 + \ldots + F_{2n} = F_{2n-1} - 1.$

(2) Si dimostri che, per ogni intero positivo $n \geq 1$, il numero

$$(3 + \sqrt{5})^n + (3 - \sqrt{5})^n$$

è un intero pari.

ESERCIZIO 6. Il candidato risolva le seguenti questioni, esibendo un argomento conciso ed esauriente.

(1) Si consideri il polinomio
$$f(T) := T^5 - 2T^4 + 5T^3 - 6T + 12 \in \mathbb{Z}[T]\,.$$
Dando per buono che $1+i$ è una radice complessa di $f(T)$, si determini la decomposizione di $f(T)$ come prodotto di fattori irriducibili in $\mathbb{Z}[T]$.

(2) Sia $\mathbb{N}^+$ l'insieme degli interi positivi. Si munisca l'insieme $P := \mathbb{N}^+ \times \mathbb{N}^+$ dell'ordine $\leq$ lessicografico associato alla divisibilità, i.e., si ponga
$$(a,b) \leq (c,d) :\Longleftrightarrow (a \text{ divide } c \quad \text{e} \quad a \neq c) \vee (a = c \quad \text{e} \quad b \text{ divide } d)$$
e si dia per buono che $\leq$ sia un ordine parziale su P.

(2a) Si dica se $(P, \leq)$ è totalmente ordinato.

(2b) Dati $p,\ q$ due numeri naturali primi distinti, si ponga
$$S := \{(p,p), (p,q), (p,q^2), (p^2,q), (p^2,p)\}.$$
Si disegni il grafico dell'ordine $\leq$ su S. Si determinino elementi massimali e minimali di S, eventuale massimo e/o minimo di S ed estremo superiore di S in $(P, \leq)$.

(3) Si consideri l'anello quoziente $A := \mathbb{Q}[T]/(T^3-1)$. Si dica se ciascuno degli elementi $[T^6-1] := T^6 - 1 + (T^3-1)$, $[T^2+T] := T^2 + T + (T^3-1) \in A$ è invertibile o non è invertibile; quando esiste, si determini esplicitamente l'inverso in A.

SOLUZIONE ESERCIZIO 1.

(1) Basta osservare che $A \setminus (A \setminus B) = A \cap B$.

(2.1) ρ è una relazione di equivalenza su $\mathbb{N}$, perché si verifica direttamente che è riflessiva, simmetrica e transitiva.

(2.2) Le classi di equivalenza sono 4: $[0]_\rho, [1]_\rho, [2]_\rho, [3]_\rho$.

(3) Si dimostra che n deve coincidere con $\mathrm{mcm}(a, b)$ (a meno del segno), mentre non può esistere in generale un intero m con la proprietà indicata (si prenda ad esempio $a = 2$ e $b = 3$).

SOLUZIONE ESERCIZIO 2.

(3) $x \equiv 5^{38} \equiv (5^{10})^3 5^8 \equiv 5^8 \equiv 4 \pmod{11}$.

(4.1) $2|\lambda$, cioè $\lambda = 0, 2, 4, 6$

(4.2) Per $\lambda = 2$, la soluzione del sistema è $x \equiv 19 \pmod{130}$.

SOLUZIONE ESERCIZIO 3.

(1) Osservare che $B - B \subseteq B$ e $B \cdot A \subseteq B$.

(2) Con un semplice ragionamento si trova che $\beta_1 = 3$ e $\beta_2 = T$.

(3) Se esistesse β tale che $B = \beta A$ allora β dovrebbe avere grado 0 (perché $3 \in \beta A$) e quindi dovrebbe essere $\beta = 3$. Però, $\beta \neq 3$, dal momento che $3A \subsetneq B$ (essendo $T \in B$ ma $T \notin 3A$).

(4) Basta definire $\varphi : \mathbb{Z}[T] \to \mathbb{Z}/3\mathbb{Z}$ ponendo $\varphi(f(T)) := [f(0)]_3$, per ogni $f(T) \in \mathbb{Z}[T]$.

SOLUZIONE ESERCIZIO 4.

(1) $(1, 1) \star (-1, 0) = (-1, 1)$ mentre $(-1, 0) \star (1, 1) = (-1, -1)$, dunque $\star$ non è commutativa.

(2) L'elemento neutro di G, rispetto a $\star$ è $(1, 0)$.

(3) Sappiamo già che $\star$ è associativa e, per (2), esiste l'elemento neutro di G, rispetto a $\star$. Inoltre, è facilmente visto che l'inverso del generico elemento $(a, b) \in G$ è $(a^{-1}, -ba^{-1})$ che appartiene a G. Dunque $(G, \star)$ è un gruppo (non abeliamo).

(4) $(-1, 0)$ ha ordine 2, mentre $(1, 1)$ ha ordine infinito.

(5) Per (4), $(-1, 0)$ ha ordine 2, quindi $H = \{(-1, 0), (1, 0)\}$. Si vede facilmente che H non è normale in G. Infatti, l'inverso di $(1, 1)$ è $(1, -1)$ e si ha

$$(1, 1) \star (-1, 0) \star (1, -1) = (-1, 2) \notin H.$$

(6) Si ha, per ogni $r, s \in \mathbb{R}$,

$$(1, r) \star (1, s)^{-1} = (1, r) \star (1, -s) = (1, r - s) \in K.$$

Ciò prova che K è un sottogruppo di G. Inoltre, per ogni elemento $(a, b) \in G$ e per ogni $(1, r) \in K$, si ha

$$(a, b) \star (1, r) \star (a, b)^{-1} = (a, b) \star (1, r) \star (a^{-1}, -ba^{-1}) = (a, ar+b) \star (a^{-1}, -ba^{-1}) = (1, ar) \in K,$$

e quindi K è normale in G.

SOLUZIONE ESERCIZIO 5.

(1) La prima e la quarta uguaglianza sono false per $n = 1$. La terza è falsa per $n = 2$. Bisogna provare che la seconda è vera. Per $n = 1$ si ha $F_0 + F_2 = 1 = F_3 - 1$. Sia adesso $n \geq 1$. Sia adesso $n \geq 1$ e assumiamo di aver dimostrato che $F_0 + F_2 + \ldots + F_{2n} = F_{2n+1} - 1$. Dobbiamo dimostrare che $F_0 + F_2 + \ldots + F_{2(n+1)} = F_{2(n+1)+1} - 1$. Si ha, per ipotesi induttiva,

$$F_0 + F_2 + \ldots + F_{2(n+1)} = F_{2n+1} - 1 + F_{2n+2} = F_{2n+3} - 1 = F_{2(n+1)+1} - 1.$$

L'asserto è così completamente provato.

(2) L'asserzione è triviale per $n = 1$. Adesso supponiamo $n \geq 1$ e assumiamo che $(3 + \sqrt{5})^h + (3 - \sqrt{5})^h$ sia un intero pari, per ogni $1 \leq h \leq n$. Dobbiamo provare che $(3 + \sqrt{5})^{n+1} + (3 - \sqrt{5})^{n+1}$ è un intero pari. Osserviamo adesso che $x := 3 + \sqrt{5}, y := 3 - \sqrt{5}$ sono soluzioni dell'equazione $T^2 - 6T + 4 = 0$. Si ha dunque $x^2 = 6x - 4, y^2 = 6y - 4$, e quindi

$$\begin{aligned} x^{n+1} + y^{n+1} = &\ x^2 x^{n-2} + y^2 y^{n-2} = x^{n-2}(6x - 4) + y^{n-2}(6y - 4) \\ = &\ 6(x^n + y^n) - 4(x^{n-1} + y^{n-1}) \end{aligned}$$

e, poiché, per ipotesi induttiva ampia, $x^n + y^n, x^{n-1} + y^{n-1}$ sono interi pari, si ha che $x^{n+1} + y^{n+1}$ è un intero pari. L'asserzione segue dunque dal Principio di Ampia Induzione.

SOLUZIONE ESERCIZIO 6.

(1) Poiché f ha coefficienti reali e $a := 1 + i$ è una radice di f, allora anche $\overline{a} := 1 - i$ è radice di f, e quindi il polinomio $(T - a)(T - \overline{a}) = T^2 - 2T + 2$ è un fattore irriducibile di f in $\mathbb{R}[T]$, a fortiori in $\mathbb{Z}[T]$. Si ha, svolgendo la divisione, $f(T) = (T^2 - 2T + 2)(T^3 + 3T + 6)$. Il secondo polinomio è irriducibile su $\mathbb{Z}[T]$, essendo un 3-Eisenstein.

(2) Gli elementi massimali di S sono $(p^2, p), (p^2, q)$, quelli minimali sono $(p, p), (p, q)$, dunque S non ha massimo, né minimo. L'estremo superiore di S in $(P, \leq)$ è (p^2, pq).

(3) $\mathrm{MCD}(T^2 + T, T^3 - 1) = 1$ (quindi $[T^2 + T]$ è invertibile); mentre $\mathrm{MCD}(T^6 - 1, T^3 - 1) = T^3 - 1$ (in particolare, $[T^6 - 1] = [0]$ e ovviamente non è invertibile). Dalla relazione di Bézout:

$$\frac{1}{2}(-T - 2)(T^3 - 1) + \frac{1}{2}(T^2 + T - 1)(T^2 + T) = 1$$

si ricava che $[T^2 + T]^{-1} = [\frac{1}{2}(T^2 + T - 1)]$.