AL1 - Algebra 1: fondamenti - A.A. 2002/2003

Appello C

MATRICOLA (O ALTRO IDENTIFICATIVO): .....

COGNOME: ..... **NOME:** .....

esercizio	1	2	3	4	5	6	7	8
punti max	2	5	10	(2, 2, 3)	(2, 3, 5)	8	(4,2)	8
punti assegnati								
totale								

AVVERTENZE : *Svolgere gli esercizi in modo conciso, ma esauriente, nello spazio assegnato. Fino a* **2** punti ulteriori *potranno essere assegnati agli elaborati scritti in modo molto chiaro.*

ESERCIZIO 1. Per ogni $n \geq 1$, si consideri l'espressione:

$$s_n := 1 + \frac{1}{2^1} + \frac{1}{2^2} + \ \ldots \ + \frac{1}{2^{n-1}} + \frac{1}{2^n} \, .$$

Provare per induzione su $n \geq 1$ che vale una delle seguenti formule:

(a) $s_n = 2 + \frac{1}{2^{n-1}}$;

(b) $s_n = 2 - \frac{1}{2^n}$;

(c) $s_n = 1 + \frac{2 \cdot n}{2^{n+1}}$;

ESERCIZIO 2. Determinare tutte le eventuali soluzioni del sistema di congruenze:

$$\begin{cases} 3X \equiv 5 \pmod 7 \\ 2X \equiv 1 \pmod 5 \\ X \equiv 6 \pmod 9 \end{cases} .$$

ESERCIZIO 3. Enunciare e dimostrare il Teorema di Euler(o)–Fermat relativo alle congruenze modulo un intero $n \geq 2$. Discutere, poi, il caso particolare in cui $n = p$ è un numero primo.

ESERCIZIO 4. Siano date le seguenti permutazioni:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 7 & 6 & 4 & 3 & 1 & 2 & 5 \end{pmatrix} , \quad \tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 2 & 4 & 3 & 5 & 1 & 7 & 6 \end{pmatrix} \in \boldsymbol{S}_7 \, .$$

(1) Scrivere σ e τ come prodotto di cicli disgiunti.

(2) Determinare l'ordine di σ e di τ.

(3) Calcolare $\tau^{-1}\sigma$ e $\sigma\tau^{-1}$ e determinare di entrambe le permutazioni l'ordine.

ESERCIZIO 5. Si consideri l'insieme R di tutte le matrici del tipo:

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} , \qquad \text{con } a \, , \ b \in \mathbb{Z} \, .$$

(1) Dimostrare che R è un sottoanello, ma non un ideale, dell'anello di tutte le matrici $(\boldsymbol{M}_{2,2}(\mathbb{Z}), +, \cdot)$.

(2) Stabilire se $(R, +, \cdot)$ è commutativo, se $(R, +, \cdot)$ è unitario, se $(R, +, \cdot)$ è un campo.

(3) Fissato $n \geq 2$, si consideri l'insieme $\boldsymbol{I}_n$ di tutte le matrici del tipo:

$$\begin{pmatrix} a & 0 \\ 0 & nb \end{pmatrix}, \qquad \text{con } a\,,\ b \in \mathbb{Z}\,.$$

Stabilire se $\boldsymbol{I}_n$ è un ideale di R. In caso di risposta affermativa, determinare sotto quali eventuali condizioni su n, $\boldsymbol{I}_n$ risulta essere un ideale massimale di R.

ESERCIZIO 6. Sia $(G,\ \cdot)$ un gruppo, sia $(H,\ \cdot)$ un sottogruppo di $(G,\ \cdot)$ e sia $g \in G$. Supponiamo che il sottogruppo $(\langle g \rangle,\ \cdot)$ di $(G,\ \cdot)$ generato da g abbia ordine n e supponiamo che $g^m \in H$, per qualche intero $m \geq 1$ tale che $\mathrm{MCD}(n, m) = 1$. Dimostare che $g \in H$.

ESERCIZIO 7. Dati due polinomi $f(T) := -3 + 6T - 6T^2 + 3T^3$, $g(T) := -2 + T + T^2$ in $\mathbb{Q}[T]$ utilizzando l'algoritmo euclideo delle divisioni successive:

(1) determinare *il* polinomio *monico* $d(T) := \mathrm{MCD}(f(T), g(T)) \in \mathbb{Q}[T]$,

(2) determinare un'espressione del tipo $d(T) = a(T)f(T) + b(T)g(T)$ (cioè determinare due polinomi $a(T), b(T) \in \mathbb{Q}[T]$) [identità di Bézout].

ESERCIZIO 8. Sia $(R, +, \cdot\ )$ un anello commutativo unitario. Dimostrare che $(R, +, \cdot\ )$ è un campo se e soltanto se ogni ideale non nullo di $(R, +, \cdot\ )$ coincide con $(R, +, \cdot\ )$ stesso.

SOLUZIONI

Soluzione Esercizio 1. (b) $\boldsymbol{s}_n = 2 - \frac{1}{2^n}$. Infatti, per $n = 1$, si ha $\boldsymbol{s}_1 = 1 + \frac{1}{2} = 2 - \frac{1}{2^1}$. Passo induttivo:

$$\boldsymbol{s}_n = \boldsymbol{s}_{n-1} + \frac{1}{2^n} = 2 - \frac{1}{2^{n-1}} + \frac{1}{2^n} = 2 - \frac{1}{2^n}\,;$$

Soluzione Esercizio 2. (Teorema Cinese dei Resti) Soluzione: $x \equiv 123 \pmod{7 \cdot 5 \cdot 9 = 315}$.

Soluzione Esercizio 3.

(1) $\sigma = (175)(26)(34)\,, \quad \tau = (1245)(3)(67)\,.$

(2) $\mathrm{Ord}(\sigma) = 6\,, \quad \mathrm{Ord}(\tau) = 4\,.$

(3)

$$\tau^{-1}\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 7 & 4 & 6 & 3 & 5 & 2 \end{pmatrix} = (1)(27)(3465)\,,$$

$$\sigma\tau^{-1} = \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 6 & 7 & 2 & 3 & 5 & 1 & 4 \end{pmatrix} = (16)(2743)(5)\,.$$

$\mathrm{Ord}(\tau^{-1}\sigma) = 4$, $\mathrm{Ord}(\sigma\tau^{-1}) = 4\,.$

Soluzione Esercizio 5.

(1) Siano date due matrici in R:

$$A := \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix}\,, \quad A' := \begin{pmatrix} a' & 0 \\ 0 & b' \end{pmatrix}\,.$$

Allora:

$$A - A' = \begin{pmatrix} a - a' & 0 \\ 0 & b - b' \end{pmatrix} \in R\,,$$
$$AA' = \begin{pmatrix} aa' & 0 \\ 0 & bb' \end{pmatrix} \in R\,.$$

Si noti che, in generale $R \cdot \boldsymbol{M}_{2,2}(\mathbb{Z}) \not\subseteq R$. Ad esempio:

$$\begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \cdot \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 0 & a \\ b & 0 \end{pmatrix} \notin R\,.$$

(2) R è un anello unitario con la stessa unità di $(\boldsymbol{M}_{2,2}(\mathbb{Z}), +, \cdot\,)$:

$$I = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}\,.$$

R è un anello commutativo, perché:

$$AA' = \begin{pmatrix} aa' & 0 \\ 0 & bb' \end{pmatrix} = \begin{pmatrix} a'a & 0 \\ 0 & b'b \end{pmatrix} = A'A\,.$$

R possiede divisori dello zero, quindi non è un campo. Infatti,

$$\begin{pmatrix} a & 0 \\ 0 & 0 \end{pmatrix} \begin{pmatrix} 0 & 0 \\ 0 & b' \end{pmatrix} = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}\,.$$

(3) E' subito visto che:

$$\boldsymbol{I}_n \cdot R \subseteq \boldsymbol{I}_n\,.$$

Ovviamente essendo R un anello commutativo, anche $R \cdot \boldsymbol{I}_n \subseteq \boldsymbol{I}_n$, dunque $\boldsymbol{I}_n$ è un ideale di R. L'applicazione

$$\varphi : R \to \frac{\mathbb{Z}}{n\mathbb{Z}}\,,\ \begin{pmatrix} a & 0 \\ 0 & b \end{pmatrix} \mapsto b + n\mathbb{Z}\,,$$

è un omomorfismo suriettivo di anelli, avente come nucleo proprio l'ideale $\boldsymbol{I}_n$. Pertanto si conclude facilmente, dal teorema fondamentale dell'omomorfismo per anelli, che $\boldsymbol{I}_n$ è un ideale massimale di R se e soltanto se $n\mathbb{Z}$ è un ideale massimale di $\mathbb{Z}$, cioè se e soltanto se n è un numero primo.

Soluzione Esercizio 6. Siano $a, b \in \mathbb{Z}$ tali che $an + bm = 1$. Allora:

$$g = g^1 = g^{an+bm} = g^{an} g^{bm} = (g^n)^a (g^m)^b = 1 \cdot (g^m)^b \in H\,.$$

Soluzione Esercizio 7. (1)

$$\begin{aligned} f(T) &= g(T)q_1(T) + r_1(T)\,, \quad \text{dove } q_1(T) := -9 + 3T\,,\ \ r_1(T) := 21(-1+T)\,, \\ g(T) &= r_1(T)q_2(T) + 0\,, \quad \text{dove } q_2(T) := \tfrac{2}{21} + \tfrac{1}{21}T \end{aligned}$$

Pertanto, il polinomio monico $-1 + T = \frac{1}{21} r_1(T)$ è il $\mathrm{MCD}(f(T), g(T))$.

(2) $\frac{1}{21} r_1(T) = \frac{1}{21} f(T) - \frac{1}{21} q_1(T) g(T)$, quindi:

$$a(T) := \frac{1}{21}\,, \quad b(T) := \frac{1}{7}(-3+T)\,.$$