AL1 - Algebra 1: fondamenti - A.A. 2003/2004

Valutazione "in itinere" - II Prova

Matricola (O ALTRO IDENTIFICATIVO) $\rightarrow$

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

esercizio	1	2			3	4			5		6			7				
punti max	5	2	10	4	6	5	4	2	4	6	4	5	6	4	4	2	2	4
punti assegnati																		
totale																		

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

ESERCIZIO 1. Determinare tutte le eventuali soluzioni della congruenza:

$$21X \equiv 14 \pmod{77}\,.$$

ESERCIZIO 2. **(1)** Enunciare il Teorema di Wilson.

(2) Dimostrare il Terorema di Wilson.

(3) Stabilire se, tramite il Teorema di Wilson, si possono caratterizzare i numeri interi primi ed, in caso affermativo, dimostrare tale risultato.

ESERCIZIO 3. Determinare tutte le eventuali soluzioni del sistema di congruenze:

$$\begin{cases} 3X \equiv 1 \pmod{5} \\ 4X \equiv 4 \pmod{11} \\ -3X \equiv 2 \pmod{7}\ . \end{cases}$$

ESERCIZIO 4. **(1)** Mostrare che l'insieme prodotto cartesiano $G := \mathbb{Z} \times \mathbb{Q}$ con l'operazione $\star$ definita nella maniera seguente:

$$(a,b) \star (x,y) := (a+x, 2^x b + y) \quad \forall\ (a,b)\,,\ (x,y) \in \mathbb{Z} \times \mathbb{Q}\,,$$

forma un gruppo.

(2) Stabilire se $(G, \star)$ è un gruppo abeliano.

(3) Sia $H := \mathbb{Z} \times \mathbb{Z}$. Stabilire se $(H, \star)$ è un sottogruppo di $(G, \star)$.

ESERCIZIO 5. Siano dati $f(X) := X^3 - X^2 - X - 2$ e $g(X) := X^3 - 2X^2 + X - 2$ due polinomi in $\mathbb{Z}[X] \subset \mathbb{Q}[X]$.

(1) Utilizzando il Teorema di Ruffini, determinare tutte le eventuali radici in $\mathbb{Z}$ di $f(X)$ e di $g(X)$.

(2) Utilizzando l'algoritmo euclideo delle divisioni successive, calcolare in $\mathbb{Q}[X]$ il polinomio $d(X) := \mathrm{MCD}(f(X), g(X))$ e determinare due polinomi $\alpha(X)$, $\beta(X) \in \mathbb{Q}[X]$ in modo tale che:

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

ESERCIZIO 6. Sia $t \in \mathbb{R}$. Sia $\boldsymbol{M}(t)$ l'insieme delle matrici del tipo seguente:

$$\begin{pmatrix} a+b & b \\ tb & a \end{pmatrix}, \qquad \text{con } a\,,\ b \in \mathbb{R}\,.$$

(1) Mostrare che, per ogni $t \in \mathbb{R}$, $(\boldsymbol{M}(t), +, \cdot\,)$ è un sottoanello dell'anello delle matrici $(\boldsymbol{M}_{2,2}(\mathbb{R}), +, \cdot\,)$.

(2) Stabilire se, per ogni $t \in \mathbb{R}$, $(\boldsymbol{M}(t), +, \cdot\,)$ è un anello commutativo e se, per ogni $t \in \mathbb{R}$, è un anello unitario.

(3) Si prenda $t = -1$. Stabilire se ogni elemento non nullo di $(\boldsymbol{M}(-1), +, \cdot\,)$ è invertibile (in $(\boldsymbol{M}(-1), +, \cdot\,)$).

ESERCIZIO 7. Siano date le seguenti permutazioni:

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

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

(2) Determinare l'ordine di σ e di τ.

(3) Calcolare $\tau^{-1}\sigma\tau (= \tau \circ \sigma \circ \tau^{-1})$ e determinarne l'ordine.

SOLUZIONI

ESERCIZIO 1. $x \equiv 8, 19, 30, 41, 52, 63, 74 \pmod{77}$.

ESERCIZIO 2. Vedere gli appunti del corso.

ESERCIZIO 3. $x \equiv 67 \pmod{9 \cdot 11 \cdot 7}$.

ESERCIZIO 4. (1, a) L'operazione $\star$ è associativa, infatti:

$$((a,b) \star (x,y)) \star (u,v) = (a+x\ , 2^x b + y) \star (u,v) = ((a+x)+u,\ 2^u(2^x b + y) + v)\,,$$

$$(a,b) \star ((x,y) \star (u,v)) = (a,b) \star (x+u,\ 2^u y + v) = (a + (x+u),\ 2^{(x+u)} b + 2^u y + v)\,.$$

(1, b) L'elemento neutro rispetto all'operazione $\star$ è $(0,0)$.

(1, c) L'inverso di un elemento $(a,b) \in G$ rispetto all'operazione $\star$ è l'elemento:

$$(-a,\ \frac{-b}{2^a}) \in G\,.$$

(2) $(G, \star)$ non è un gruppo abeliano. Infatti:

$$(a,b) \star (x,y) = (a+x\ , 2^x b + y) \qquad (x,y) \star (a,b) = (x+a\ , 2^a y + b)\,,$$

quindi, ad esempio,

$$(0,1) \star (1,1) = (1,3) \neq (1,1) \star (0,1) = (1,2)\,.$$

(3) Da (1, c) discende immediatamente che $(H, \star)$ non è un sottogruppo di $(G, \star)$ (ad esempio, l'inverso di $(1,1) \in H$ appartiene a $G \setminus H$, perché $-1/2 \in \mathbb{Q} \setminus \mathbb{Z}$).

ESERCIZIO 5. (1) L'unica radice intera di $f(X)$ è 2 ; l'unica radice intera di $g(X)$ è 2 .

(2) $d(X) = X - 2$. Inoltre $f(X) = (X-2)(X^2+X+1)$, $g(X) = (X-2)(X^2+1)$. Si vede facilmente (utilizzando l'algoritmo euclideo) che:

$$1 = (X+1)(X^2+1) - X(X^2+X+1)\,,$$

quindi:

$$(X-2) = (X+1)(X-2)(X^2+1) - X(X-2)(X^2+X+1) = (X+1)g(X) - Xf(X)\,,$$

dunque $\alpha(X) = -X$, $\beta(X) := X + 1$.

ESERCIZIO 6. (1):

$$\begin{pmatrix} a+b & b \\ tb & a \end{pmatrix} - \begin{pmatrix} c+d & d \\ td & c \end{pmatrix} = \begin{pmatrix} (a-c)+(b-d) & b-d \\ t(b-d) & a-c \end{pmatrix} \in \boldsymbol{M}(t)\,;$$

$$\begin{pmatrix} a+b & b \\ tb & a \end{pmatrix} \cdot \begin{pmatrix} c+d & d \\ td & c \end{pmatrix} = \begin{pmatrix} (a+b)(c+d) + tbd & (a+b)d + bc \\ (c+d)tb + tad & tdb + ac \end{pmatrix} = \begin{pmatrix} \alpha+\beta & \beta \\ t\beta & \alpha \end{pmatrix} \in \boldsymbol{M}(t)\,,$$

dove $\alpha := ac + tbd$, $\beta := (a+b)d + bc$.

(2) La matrice

$$I := \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} 1+0 & 0 \\ t \cdot 0 & 1 \end{pmatrix} \in \boldsymbol{M}(t)\,, \quad \forall\ t \in \mathbb{R}$$

è l'elemento neutro rispetto al prodotto (righe per colonne) di $\boldsymbol{M}(t)$.

L'anello $\boldsymbol{M}(t)$ è commutativo. Infatti:

$$\begin{pmatrix} c+d & d \\ td & c \end{pmatrix} \cdot \begin{pmatrix} a+b & b \\ tb & a \end{pmatrix} = \begin{pmatrix} \gamma+\delta & \delta \\ t\delta & \gamma \end{pmatrix}\,,$$

dove $\gamma := ca + tdb = \alpha$, $\delta := (c+d)b + da = bc + bd + ad = (a+b)d + bc = \beta$.

(3) Si noti che se $a \neq 0$ e $b \neq 0$, allora:

$$\begin{pmatrix} a+b & b \\ -b & a \end{pmatrix}^{-1} = \begin{pmatrix} a'+b' & b' \\ -b' & a' \end{pmatrix} \in \boldsymbol{M}(-1)\,,$$

dove $a' := (a+b)/\Delta$, $b' := -b/\Delta$ e $\Delta := a^2 + ab + b^2$.

ESERCIZIO 7.

(1) $\sigma = (135)(47)(26)\,, \quad \tau = (1246)(357)\,.$

(2) $\mathrm{Ord}(\sigma) = 6\,, \quad \mathrm{Ord}(\tau) = 12\,.$

(3)

$$\tau^{-1}\sigma\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 4 & 5 & 6 & 1 & 7 & 2 & 3 \end{pmatrix} = (14)(257)(36)\,.$$

$\mathrm{Ord}(\tau^{-1}\sigma\tau) = 6\,.$

AL1 - Algebra 1: fondamenti - A.A. 2003/2004

Valutazione "in itinere" - II Prova

Matricola (O ALTRO IDENTIFICATIVO) $\rightarrow$

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

esercizio	1	2			3	4			5		6			7		
punti max	5	2	10	4	6	5	4	2	4	6	2	3	4	4	5	6
punti assegnati																
totale																

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

ESERCIZIO 1. Determinare tutte le eventuali soluzioni della congruenza:

$$14X \equiv 21 \pmod{77}.$$

ESERCIZIO 2. **(1)** Enunciare il Teorema di Wilson.

(2) Dimostrare il Teorema di Wilson.

(3) Stabilire se, tramite il Teorema di Wilson, si possono caratterizzare i numeri interi primi ed, in caso affermativo, dimostrare tale risultato.

ESERCIZIO 3. Determinare tutte le eventuali soluzioni del sistema di congruenze:

$$\begin{cases} 3X \equiv 1 \pmod{5} \\ 4X \equiv 8 \pmod{11} \\ -3X \equiv 4 \pmod{7} \end{cases}.$$

ESERCIZIO 4. **(1)** Mostrare che l'insieme prodotto cartesiano $G := \mathbb{Q} \times \mathbb{Z}$ con l'operazione $*$ definita nella maniera seguente:

$$(a,b) * (x,y) := (3^y a + x, b + y) \quad \forall\ (a,b)\,,\ (x,y) \in \mathbb{Q} \times \mathbb{Z}\,,$$

forma un gruppo.

(2) Stabilire se $(G, *)$ è un gruppo abeliano.

(3) Sia $H := \mathbb{Z} \times \mathbb{Z}$. Stabilire se $(H, *)$ è un sottogruppo di $(G, *)$.

ESERCIZIO 5. Siano dati $f(X) := X^3 - 3X^2 + X - 3$ e $g(X) := X^3 - 2X^2 - 2X - 3$ due polinomi in $\mathbb{Z}[X] \subset \mathbb{Q}[X]$.

(1) Utilizzando il Teorema di Ruffini, determinare tutte le eventuali radici in $\mathbb{Z}$ di $f(X)$ e di $g(X)$.

(2) Utilizzando l'algoritmo euclideo delle divisioni successive, calcolare in $\mathbb{Q}[X]$ il polinomio $d(X) := \mathrm{MCD}(f(X), g(X))$ e determinare due polinomi $\alpha(X)$, $\beta(X) \in \mathbb{Q}[X]$ in modo tale che:

$$d(X) = \alpha(X)f(X) + \beta(X)g(X) \qquad \text{[Identità di Bézout]}.$$

ESERCIZIO 6. Siano date le seguenti permutazioni:

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

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

(2) Determinare l'ordine di σ e di τ.

(3) Calcolare $\tau^{-1}\sigma\tau (= \tau \circ \sigma \circ \tau^{-1})$ e determinarne l'ordine.

gruppo $(\boldsymbol{\Gamma}, \cdot\ )$.

ESERCIZIO 7. Sia $\lambda \in \mathbb{R}$. Sia $\boldsymbol{M}(\lambda)$ l'insieme delle matrici del tipo seguente:

$$\begin{pmatrix} x+y & y \\ \lambda y & x \end{pmatrix}, \qquad \text{con } x\,,\ y \in \mathbb{R}\,.$$

(1) Mostrare che, per ogni $\lambda \in \mathbb{R}$, $(\boldsymbol{M}(\lambda), +, \cdot\ )$ è un sottoanello dell'anello delle matrici $(\boldsymbol{M}_{2,2}(\mathbb{R}), +, \cdot\ )$.

(2) Stabilire se, per ogni $\lambda \in \mathbb{R}$, $(\boldsymbol{M}(\lambda), +, \cdot\ )$ è un anello commutativo e se, per ogni $\lambda \in \mathbb{R}$, è un anello unitario.

(3) Si prenda $\lambda = -1$. Stabilire se ogni elemento non nullo di $(\boldsymbol{M}(-1), +, \cdot\ )$ è invertibile (in $(\boldsymbol{M}(-1), +, \cdot\ )$).

SOLUZIONI

ESERCIZIO 1. $x \equiv 7, 18, 29, 40, 51, 62, 73 \pmod{77}$.

ESERCIZIO 3. $x \equiv 57 \pmod{5 \cdot 11 \cdot 7}$.

ESERCIZIO 5. (1) L'unica radice intera di $f(X)$ è 3 ; l'unica radice intera di $g(X)$ è 3 .

(2) $d(X) = X - 3$. Inoltre $f(X) = (X-3)(X^2+1)$, $g(X) = (X-3)(X^2+X+1)$. Si vede facilmente (utilizzando, ad esempio, l'algoritmo euclideo) che:

$$1 = (X+1)(X^2+1) - X(X^2+X+1)\,,$$

quindi:

$$(X-3) = (X+1)(X-3)(X^2+1) - X(X-3)(X^2+X+1) = (X+1)f(X) - Xg(X)\,,$$

dunque $\alpha(X) := X + 1$, $\beta(X) := -X$.

ESERCIZIO 6.

(1) $\sigma = (173)(526)$, $\tau = (2534)(176)$.

(2) $\mathrm{Ord}(\sigma) = 3$, $\mathrm{Ord}(\tau) = 12$.

(3)

$$\tau^{-1}\sigma\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 3 & 2 & 5 & 7 & 1 & 4 & 6 \end{pmatrix} = (135)(476).$$

$\mathrm{Ord}(\tau^{-1}\sigma\tau) = 3$.

PER GLI ALTRI ESERCIZI, VEDERE LE SOLUZIONI DATE IN PRECEDENZA.

AL1 - Algebra 1: fondamenti - A.A. 2003/2004

Valutazione "in itinere" - II Prova

Matricola (O ALTRO IDENTIFICATIVO) $\rightarrow$ [   ]

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

esercizio	1	2			3	4			5		6			7		
punti max	5	2	10	4	6	5	4	2	4	6	4	5	6	2	3	4
punti assegnati																
totale																

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

ESERCIZIO 1. Determinare tutte le eventuali soluzioni della congruenza:

$$28X \equiv 21 \pmod{77}.$$

ESERCIZIO 2. **(1)** Enunciare il Teorema di Wilson.

(2) Dimostrare il Teorema di Wilson.

(3) Stabilire se, tramite il Teorema di Wilson, si possono caratterizzare i numeri interi primi ed, in caso affermativo, dimostrare tale risultato.

ESERCIZIO 3. Determinare tutte le eventuali soluzioni del sistema di congruenze:

$$\begin{cases} 3X \equiv 3 \pmod{5} \\ 4X \equiv 9 \pmod{11} \\ -3X \equiv 4 \pmod{7} \end{cases}.$$

ESERCIZIO 4. **(1)** Mostrare che l'insieme prodotto cartesiano $G := \mathbb{Q} \times \mathbb{Z}$ con l'operazione $*$ definita nella maniera seguente:

$$(a, b) * (x, y) := (5^y a + x, b + y) \quad \forall\, (a, b)\,,\ (x, y) \in \mathbb{Q} \times \mathbb{Z}\,,$$

forma un gruppo.

(2) Stabilire se $(G, *)$ è un gruppo abeliano.

(3) Sia $H := \mathbb{Z} \times \mathbb{Z}$. Stabilire se $(H, *)$ è un sottogruppo di $(G, *)$.

ESERCIZIO 5. Siano dati $f(X) := X^3 + 2X^2 + X + 2$ e $g(X) := X^3 + 3X^2 + 3X + 2$ due polinomi in $\mathbb{Z}[X] \subset \mathbb{Q}[X]$.

(1) Utilizzando il Teorema di Ruffini, determinare tutte le eventuali radici in $\mathbb{Z}$ di $f(X)$ e di $g(X)$.

(2) Utilizzando l'algoritmo euclideo delle divisioni successive, calcolare in $\mathbb{Q}[X]$ il polinomio $d(X) := \mathrm{MCD}(f(X), g(X))$ e determinare due polinomi $\alpha(X)$, $\beta(X) \in \mathbb{Q}[X]$ in modo tale che:

$$d(X) = \alpha(X)f(X) + \beta(X)g(X) \qquad \text{[Identità di Bézout]}.$$

ESERCIZIO 6. Sia $\lambda \in \mathbb{R}$. Sia $\boldsymbol{M}(\lambda)$ l'insieme delle matrici del tipo seguente:

$$\begin{pmatrix} x + y & y \\ \lambda y & x \end{pmatrix}, \qquad \text{con } x\,,\ y \in \mathbb{R}\,.$$

(1) Mostrare che, per ogni $\lambda \in \mathbb{R}$, $(\boldsymbol{M}(\lambda), +, \cdot\,)$ è un sottoanello dell'anello delle matrici $(\boldsymbol{M}_{2,2}(\mathbb{R}), +, \cdot\,)$.

(2) Stabilire se, per ogni $\lambda \in \mathbb{R}$, $(\boldsymbol{M}(\lambda), +, \cdot\,)$ è un anello commutativo e se, per ogni $\lambda \in \mathbb{R}$, è un anello unitario.

(3) Si prenda $\lambda = -1$. Stabilire se ogni elemento non nullo di $(\boldsymbol{M}(-1), +, \cdot\,)$ è invertibile (in $(\boldsymbol{M}(-1), +, \cdot\,)$).

ESERCIZIO 7. Siano date le seguenti permutazioni:

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

(1) Scrivere σ e τ come prodotto di cicli disgiunti.
(2) Determinare l'ordine di σ e di τ.
(3) Calcolare $\tau^{-1}\sigma\tau (= \tau \circ \sigma \circ \tau^{-1})$ e determinarne l'ordine.

SOLUZIONI

ESERCIZIO 1. $x \equiv 9, 20, 31, 42, 53, 64, 75 \pmod{77}$.

ESERCIZIO 3. $x \equiv 71 \pmod{5 \cdot 11 \cdot 7}$.

ESERCIZIO 5. (1) L'unica radice intera di $f(X)$ è -2 ; l'unica radice intera di $g(X)$ è -2 .

(2) $d(X) = X + 2$. Inoltre $f(X) = (X+2)(X^2+1)$, $g(X) = (X+2)(X^2+X+1)$. Si vede facilmente (utilizzando, ad esempio, l'algoritmo euclideo) che:

$$1 = (X+1)(X^2+1) - X(X^2+X+1)\,,$$

quindi:

$$(X+2) = (X+1)(X+2)(X^2+1) - X(X+2)(X^2+X+1) = (X+1)f(X) - Xg(X)\,,$$

dunque $\alpha(X) := X + 1$, $\beta(X) := -X$.

ESERCIZIO 7.

(1) $\sigma = (1253)(46)$, $\tau = (143527)$.

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

(3)

$$\tau^{-1}\sigma\tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 & 7 \\ 1 & 5 & 6 & 7 & 4 & 3 & 2 \end{pmatrix} = (2547)(36).$$

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

PER GLI ALTRI ESERCIZI, VEDERE LE SOLUZIONI DATE IN PRECEDENZA.