AL1 - Algebra 1: fondamenti - A.A. 2004/2005

Valutazione "in itinere" - II Prova

Matricola (O ALTRO IDENTIFICATIVO) → ____

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

esercizio	1.1	1.2	2	3.1	3.2	3.3	3.4	3.5	4.1	4.2	5.1	5.2	5.3	5.4	6.1	6.2	6.3	7.1	7.2
punti max	3	3	4	2	8	5	6	2	4	6	2	3	6	3	2	4	6	5	5
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.

(1) Utilizzando il "metodo di sostituzione", determinare tutte le eventuali soluzioni del sistema:

$$\begin{cases} X \equiv 1 \pmod{13} \\ X \equiv 2 \pmod{17} \end{cases}.$$

(2) Determinare tutte le eventuali soluzioni della congruenza:

$$3X \equiv 94 \pmod{101}.$$

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

$$\begin{cases} X \equiv 16 \pmod{17} \\ X \equiv 2 \pmod{11} \\ X \equiv 10 \pmod{13} \end{cases}.$$

ESERCIZIO 3. (1) Enunciare il "Piccolo" Teorema di P. Fermat.

(2) Dimostrare il "Piccolo" Teorema di P. Fermat.

(3) Siano $x, y, a \in \mathbb{Z}$, dimostrare che

$$x|a \ \wedge \ y|a \ \wedge \ \mathrm{MCD}(x,y) = 1 \ \Rightarrow \ xy|a\,.$$

(4) Utilizzando il "Piccolo" Teorema di P. Fermat (ed il punto (3)), dimostrare che per ogni intero $a \in \mathbb{Z}$, si ha che:

$$10 \mid a^5 - a\,.$$

(5) Mostrare che ogni numero naturale (scritto in base 10) ha la stessa cifra delle unità della sua quinta potenza [ad esempio, se $a = 1\mathbf{3}$, $a^5 = 371293$].

ESERCIZIO 4. Siano dati $f(X) := 4X^4 - 12X^3 + 13X^2 - 8X + 2$ e $g(X) := 4X^3 - 12X^2 + 11X - 3$ due polinomi in $\mathbb{Z}[X] \subset \mathbb{Q}[X]$.

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

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

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

ESERCIZIO 5. Sia $A := \mathbb{Z}/\equiv_3 := \{[0]_3, [1]_3, [2]_3\}$. Si consideri l'insieme prodotto cartesiano $R := A \times A$ con le operazioni definite nella maniera seguente:

$$\begin{aligned} &(a,b) + (c,d) := (a+c, b+d)\,, \\ &(a,b) \cdot (c,d) := (ac - bd, ad + bc)\,, \qquad \forall\ (a,b)\,,\ (c,d) \in A \times A\,. \end{aligned}$$

(1) Sapendo che l'operazione di prodotto in R è associativa e che valgono le proprietà distributive della somma rispetto al prodotto, mostrare che $(R, +, \cdot)$ è un anello.

(2) Stabilire se $(R, +, \cdot)$ è un anello commutativo o/e unitario.

(3) Determinare esplicitamente il gruppo $(\boldsymbol{U}(R), \cdot)$ degli elementi invertibili dell'anello $(R, +, \cdot)$.

(4) Stabilire se $(R, +, \cdot)$ è un dominio o se è un campo.

ESERCIZIO 6. Siano date le seguenti permutazioni:

$$\sigma := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 3 & 4 & 5 & 2 & 1 & 6 \end{pmatrix}, \quad \tau := \begin{pmatrix} 1 & 2 & 3 & 4 & 5 & 6 \\ 4 & 3 & 2 & 5 & 6 & 1 \end{pmatrix} \in \boldsymbol{S}_6 .$$

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

(2) Determinare l'ordine di σ e di τ (dove *l'ordine di una permutazione* $\alpha \in \boldsymbol{S}_6$ è il più piccolo intero positivo n tale che α^n coincide con la permutazione identica).

(3) Calcolare $\sigma \circ \tau$, $\tau \circ \sigma$ e $(\sigma \circ \tau)^{-1}$.

ESERCIZIO 7. **(1)** Dare la definizione di omomorfismo da un gruppo $(G, \cdot)$ ad un gruppo $(G', \star)$.

(2) Dare esplicitamente un esempio di omomorfismo suriettivo (non banale) di gruppi.

SOLUZIONI

Soluzione Esercizio 1.
(1) $x \equiv 53 \pmod{13 \cdot 17}$.
(2) $x \equiv 65 \pmod{101}$.

Soluzione Esercizio 2. $x \equiv 101 \pmod{17 \cdot 11 \cdot 13}$.

Soluzione Esercizio 3.
(1) , **(2)** *e* **(3)** sono esercizi di carattere teorico e sono completamente svolti negli appunti del corso.
(4) $5 \mid a^5 - a$, per il "Piccolo" Teorema di Fermat.
$2 \mid a^2 - a$, per il "Piccolo" Teorema di Fermat, cioè $a^2 \equiv a \pmod 2$, dunque anche $a^3 = a^2 \cdot a \equiv a \cdot a \equiv a^2 \equiv a \pmod 2$. Pertanto, $a^5 \equiv a^4 \equiv a^3 \equiv a^2 \equiv a \pmod 2$, dunque $2 \mid a^5 - a$.
Si conclude applicando **(3)** (prendendo $x = 5$ e $y = 2$).
(5) Questa è un'altra formulazione di **(4)**, in quanto $10^k \equiv 0 \pmod{10}$, per ogni $k \geq 1$.

Soluzione Esercizio 4.
(1) L'unica radice razionale di $f(X)$ è $1/2$.
Le radici razionali di $g(X)$ sono $1/2$, 1, $3/2$.
(2) Il MCD monico è $d(X) = X - 1/2$.
$f = gq_1 + r_1$, $g = r_1q_2 + r_2$, $r_1 = r_2q_3 + 0$
dove:

$$q_2 = r_2 = 2X - 1, \quad q_3 = X - 2, \quad r_1 = 2X^2 - 5X + 2 \quad q_1 = X\,.$$

Quindi:

$$r_2 = -q_2 f + (1 + q_1q_2)g\,; \quad d = -(1/2)q_2 f + (1/2)(1 + q_1q_2)g\,.$$

Pertanto, per quanto riguarda l'identità di Bézout:
$\alpha(X) = -(1/2)q_2 = -X + 1/2, \qquad \beta(X) = (1/2)(1 + q_1q_2) = X^2 - (1/2)X + (1/2)$.
Soluzione Esercizio 5.
(1) , **(2)** R risulta essere un anello, commutativo, unitario (con unità $([1]_3, [0]_3)$), privo di divisori dello zero.
$\boldsymbol{U}(R) = R \setminus \{0\}$ (a questo si arriva calcolando esplicitamente l'inverso di ogni elemento non nullo di R, cioè risolvendo un semplice sistema lineare in 2 equazioni in due incognite nel campo $\mathbb{Z}/\equiv_3$), quindi R è un campo.

Soluzione Esercizio 6.
(1) $\sigma = (135)(24)(6)$, $\tau = (1456)(23)$.
(2) L'ordine di σ è 6, l'ordine di τ è 4.
(3) $\sigma \circ \tau = (125634)$, $\tau \circ \sigma = (125436)$, $(\sigma \circ \tau)^{-1} = (143652)$.

Soluzione Esercizio 7.
(1) è un esercizio di carattere teorico (definizione): consultare gli appunti del corso.
(2) Consultare gli appunti del corso per vari esempi del tipo richiesto.