Prova scritta di Algebra

9 settembre 2016

1. Si risolva il seguente sistema di congruenze lineari

$$\begin{cases} x \equiv 5 \mod 7 \\ 11x \equiv 1 \mod 13 \\ x \equiv 3 \mod 9 \end{cases}$$

Si determini la sua minima soluzione positiva.

2. In S_9 sia $\alpha = (4,9)(9,5,6)(5,9)(3,2,7)(2,4,3,7,5,1)$

a) Si scriva α come prodotto di cicli disgiunti e come prodotto di trasposizioni. Si dica se α è pari o dispari motivando la risposta.

b) Si determinino i sottogruppi di $\langle\alpha\rangle$ e si dica se $\langle\alpha^4\rangle = \langle\alpha^7\rangle$.

c) Si scriva la tabella motiplicativa del gruppo quoziente $\langle\alpha\rangle/\langle\alpha^3\rangle$

3. Sia $\varphi : \mathbb{Z}/16\mathbb{Z} \to \mathbb{Z}/2\mathbb{Z}$ la mappa definita da $[a]_{16} \mapsto [a^2]_2$.

a) Si verifichi che φ è ben definita.

b) Si verifichi che φ è un omomorfismo di anelli.

c) Si determini il nucleo di φ e si dica se φ è suriettiva.

4. Sia I l'ideale di $\mathbb{Q}[x]$ generato dal polinomio $f(x) = x^4 - x^3 + 2x^2 - x + 1$.

a) Si dica se I è un ideale massimale di $\mathbb{Q}[x]$ motivando la risposta.

b) Si determinino gli ideali massimali di $\mathbb{Q}[x]$ che contengono I.

c) Si dica se l'elemento $(x^2 + 1) + I$ è un elemento invertibile nell'anello $A := \mathbb{Q}[x]/I$.

5. Nell'anello $\mathbb{Z}_p[x]$, con p numero primo, si considerino i polinomi

$$f(x) = x^4 + 3, \qquad g(x) = x^2 - 6.$$

a) Determinare per quali primi p il polinomio $f(x)$ è divisibile per $g(x)$ in $\mathbb{Z}_p[x]$. $f(x)$ è irriducibile in $\mathbb{Q}[x]$?

b) Posto $p = 7$, scomporre $f(x)$ in irriducibili in $\mathbb{Z}_7[x]$.

c) Posto $p = 5$, trovare il massimo comun divisore monico di $f(x)$ e $g(x)$ ed esprimerlo nella forma

$$a(x)f(x) + b(x)g(x)$$

con $a(x), b(x) \in \mathbb{Z}_5[x]$.

Soluzioni

Esercizio 1.

Poichè $MCD(7, 13, 9) = 1$, il sistema ha soluzione.
La prima equazione del sistema ha soluzione

$$x = 5 + 7k \quad k \in \mathbb{Z}.$$

Sostituendo nella seconda si ottiene

$$11(5 + 7k) \equiv 1 \bmod 13$$

da cui moltiplicando e riducendo tutti i numeri modulo 13,

$$\begin{aligned} 3 + 12k &\equiv 1 \bmod 13 \\ -k &\equiv -2 \bmod 13 \\ k &\equiv 2 \bmod 13. \end{aligned}$$

Si ottiene quindi come soluzione

$$k = 2 + 13h \quad h \in \mathbb{Z},$$

da cui otteniamo le soluzioni comuni delle prime due conguenze

$$x = 5 + 7(2 + 13h) = 19 + 91h \quad h \in \mathbb{Z}. \tag{1}$$

Sostituiamo queste soluzioni nella terza equazione

$$\begin{aligned} 19 + 91h &\equiv 3 \bmod 9 \\ 1 + h &\equiv 3 \bmod 9 \\ h &\equiv 2 \bmod 9 \end{aligned}$$

da cui otteniamo la soluzione

$$h = 2 + 9l \quad l \in \mathbb{Z}.$$

Sostituendo infine il valore di h nell'espressione (1) otteniamo le soluzioni del sistema

$$x = 19 + 91(2 + 9l) = 201 + 819l.$$

La minima soluzione positiva è quindi 201.

Esercizio 2.

a) $\alpha = (1, 7, 5)(2, 9, 6, 4)$ è prodotto di cicli disgiunti.
$\alpha = (1, 7)(7, 5)(2, 9)(9, 6)(6, 4)$ è prodotto di trasposizioni
α è dispari, perché esprimibile come prodotto di un numero dispari di trasposizioni.

b) Scrivendo α come prodotto di cicli disgiunti, le lunghezze dei suoi cicli sono 3 e 4, perció il periodo di α è $m.c.m.(3, 4) = 12$. Quindi $\langle\alpha\rangle$ è un gruppo ciclico di ordine 12 e per il teorema sui sottogruppi dei gruppi ciclici, i sottogruppi di $\langle\alpha\rangle$ sono tutti ciclici e in corrinspondenza biunivoca con i divisori di 12, ovvero: $1, 2, 3, 4, 6, 12$. La corrispondenza è quella che fa corrispondere ad ogni sottogruppo il suo ordine. Abbiamo quindi il sottogruppo corrispondente a 1 che è $\{id\}$ e quello corrispondente a 12 che è $\langle\alpha\rangle$. Al divisore 3 corrisponde il sottogruppo $\langle\gamma\rangle$ dove γ deve essere una potenza di α di periodo 3. Quindi si può prendere $\gamma = \alpha^4$ ottenendo cosi il sottogruppo $\langle\alpha^4\rangle$. In modo analogo si vede che il sottogruppo di ordine 2

è $\langle\alpha^6\rangle$, il sottogruppo di ordine 4 è $\langle\alpha^3\rangle$, il sottogruppo di ordine 6 è $\langle\alpha^2\rangle$. Scriviamo per esteso questi sottogruppi come insiemi di elementi di *alpha* (non richiesto dall'esercizio, ma sembra che più studenti non abbiano ancora chiara la diferrenza tra ementi di un gruppo e sottogruppi!):

$$\langle\alpha\rangle = \{id, \alpha, \alpha^2, \alpha^3, \alpha^4, \alpha^5, \alpha^6, \alpha^7, \alpha^8, \alpha^9, \alpha^{10}, \alpha^{11}\},$$
$$\langle\alpha^2\rangle = \{id, \alpha^2, \alpha^4, \alpha^6, \alpha^8, \alpha^{10}\},$$
$$\langle\alpha^3\rangle = \{id, \alpha^3, \alpha^6, \alpha^9\},$$
$$\langle\alpha^4\rangle = \{id, \alpha^4, \alpha^8\},$$
$$\langle\alpha^6\rangle = \{id, \alpha^6\},$$
$$id = \{id\}.$$

Si ha che $\langle\alpha^4\rangle \neq \langle\alpha^7\rangle$, infatti α^4 ha periodo $12/MCD(12,4) = 3$ e quindi $\langle\alpha^4\rangle$ è l'unico sottogruppo di $\langle\alpha\rangle$ di ordine 3, mentre α^7 ha periodo $12/MCD(12,7) = 12$ e quindi $\langle\alpha^7\rangle = \langle\alpha\rangle$.

c)

$\cdot$	$\langle\alpha^3\rangle$	$\langle\alpha^3\rangle\alpha$	$\langle\alpha^3\rangle\alpha^2$
$\langle\alpha^3\rangle$	$\langle\alpha^3\rangle$	$\langle\alpha^3\rangle\alpha$	$\langle\alpha^3\rangle\alpha^2$
$\langle\alpha^3\rangle\alpha$	$\langle\alpha^3\rangle\alpha$	$\langle\alpha^3\rangle\alpha^2$	$\langle\alpha^3\rangle$
$\langle\alpha^3\rangle\alpha^2$	$\langle\alpha^3\rangle\alpha^2$	$\langle\alpha^3\rangle$	$\langle\alpha^3\rangle\alpha$

Esercizio 3.

a) Vediamo che φ è ben definita. Dobbiamo verificare se se $x, y \in \mathbb{Z}/16\mathbb{Z}$ e $x = y$, allora $\varphi(x) = \varphi(y)$. Abbiamo che $x = [a]_{16}$ e $y = [b]_{16}$ per qualche $a, b \in \mathbb{Z}$ e poichè $x = y$ deve essere $a \equiv b \bmod 16$. Ciò significa che $b = a + 16k$ per qualche $k \in \mathbb{Z}$. Allora abbiamo che

$$\varphi(y) = \varphi([b]_{16}) = \varphi([a + 16k]) = [(a + 16k)^2]_2 =$$
$$= [a^2 + 32ak + 256k^2]_2 = [a^2]_2 + [32ak]_2 + [256k^2]_2 = [a^2]_2 = \varphi([a]_{16}) = \varphi(x).$$

b) Dobbiamo verificare che per ogni $[a]_{16}, [b]_{16} \in \mathbb{Z}/16\mathbb{Z}$ si ha

$$\varphi([a]_{16} + [b]_{16}) = \varphi([a]_{16}) + \varphi([b]_{16}),$$
$$\varphi([a]_{16} \cdot [b]_{16}) = \varphi([a]_{16}) \cdot \varphi([b]_{16})$$
$$\varphi([1]_{16}) = [1]_2.$$

Si ha

$$\varphi([a]_{16} + [b]_{16}) = \varphi([a + b]_{16}) = [(a + b)^2]_2 = [a^2 + b^2 + 2ab]_2 =$$
$$= [a^2]_2 + [b^2]_2 + [2ab]_2 = [a^2]_2 + [b^2]_2 = \varphi([a]_{16}) + \varphi([b]_{16}),$$
$$\varphi([a]_{16} \cdot [b]_{16}) = \varphi([ab]_{16}) = [(ab)^2]_2 = [a^2b^2]_2 = [a^2]_2 \cdot [b^2]_2 = \varphi([a]_{16}) \cdot \varphi([b]_{16}),$$
$$\varphi([1]_{16}) = [1^2]_2 = [1]_2.$$

c) Abbiamo che

$$\begin{aligned} Ker\varphi &= \{[a]_{16} \in \mathbb{Z}/16\mathbb{Z} \mid \varphi([a]_{16}) = [0]_2\} \\ &= \{[a]_{16} \in \mathbb{Z}/16\mathbb{Z} \mid [a^2]_2 = [0]_2\} \\ &= \{[a]_{16} \in \mathbb{Z}/16\mathbb{Z} \mid a^2 \text{ è pari }\} \\ &= \{[a]_{16} \in \mathbb{Z}/16\mathbb{Z} \mid a \text{ è pari }\} \\ &= 2\mathbb{Z}/16\mathbb{Z}. \end{aligned}$$

Infine φ è suriettiva perchè gli elemnti del codominio sono $[0]_2$ e $[1]_2$ e abbiamo per esempio che

$$\varphi([0]_{16}) = [0]_2 \text{ e } \varphi([1]_{16}) = [1]_2.$$

Esercizio 4.

a) I è un ideale massimale di $\mathbb{Q}[x]$ se e solo se $f(x)$ è un polinomio irriducibile in $\mathbb{Q}[x]$. Fattorizziamo $f(x)$ in prodotto di irriducibili in $\mathbb{Q}[x]$. Osserviamo che $f(x)$ è un polinomio primitivo a coefficienti interi. Quindi per il lemma di Gauss è sufficiante cercare una fattorizzazione in $\mathbb{Z}[x]$. Usando il metodo di Ruffini si vede facilmente che $f(x)$ non ha radici in $\mathbb{Z}$. Quindi non è prodotto di un polinomio di primo grado e di uno di terzo in $\mathbb{Z}[x]$. Cerchiamo se f è il prodotto di due polinomi di secondo grado. Possiamo supporli monici.

$$f(x) = (x^2 + ax + b)(x^2 + cx + d) = x^4 + (a + c)x^3 + (b + ac + d)x^2 + (ad + bc)x + bd$$

da cui, eguagliando i coefficienti otteniamo il sistema

$$\begin{cases} a + c = -1 \\ b + ac + d = 2 \\ ad + bc = -1 \\ bd = 1 \end{cases}$$

Poichè cerchiamo solo soluzioni intere, dall'ultima equazione otteniamo subito che $b = d = \pm 1$. Così

$$\begin{cases} c = -1 - a \\ b + d + a(-1 - a) = 2 \\ b(a + c) = -1 \\ b = d = \pm 1 \end{cases} \quad \begin{cases} c = -1 - a \\ 2 + a(-1 - a) = 2 \\ b = 1 \\ b = d = \pm 1 \end{cases} \quad \begin{cases} c = -1 - a \\ a(-1 - a) = 0 \\ b = 1 \\ b = d \end{cases}$$

Dalla seconda equazione otteniamo che $a = 0, -1$ e quindi i possibili valori per la coppia (a, c) sono $(0, -1)$ e $(-1, c)$. Pertanto $f(x) = (x^2 + 1)(x^2 - x + 1)$ e I non è un ideale massimale di $\mathbb{Q}[x]$.

b) Gli ideali massimali di $\mathbb{Q}[x]$ che contengono I sono tutti e soli del tipo $(g(x))$ con $g(x)$ polinomio irriducibile che divide $f(x)$. Pertanto gli ideali massimali di $\mathbb{Q}[x]$ che contengono $(f(x))$ sono $(x^2 + 1)$ e $(x^2 - x + 1)$.

c) L'elemento $x^2 + 1 + I$ non è invertibile in $\mathbb{Q}[x]/I$ perchè come si è visto nel punto a) $x^2 + 1$ divide $f(x)$ e quindi il massimo comun divisore tra $f(x)$ e x^2+1 è x^2+1 e non è una costante.

Esercizio 5.

a) Osserviamo che $g(x)$ divide $f(x)$ in $\mathbb{Z}_p[x]$ se e solo se il resto della divisione di $f(x)$ per $g(x)$ in $\mathbb{Z}_p[x]$ è 0.

$$\begin{array}{rl|l} x^4 & +3 & x^2-6 \\ \cline{3-3} -x^4+6x^2 & & x^2+6 \\ \cline{1-2} 6x^2+3 & & \\ -6x^2+36 & & \\ \cline{1-2} 39 & & \end{array}$$

Quindi il resto della divisione il $\mathbb{Z}_p[x]$ è $[39]_p$ e $[39]_p = [0]_p$ se e solo se $39 \equiv 0 \bmod p$, cioè p è un divisore PRIMO di 39. Pertanto $p = 3, 13$.

In $\mathbb{Q}[x]$ il polinomio $f(x) = x^4 + 3$ è irriducibile per il criterio di Eisenstein applicato con $p = 3$.

b) Supponiamo ora $p = 7$. Allora $f(x) = x^4 + 3 = x^4 - 4 = (x^2 - 2)(x^2 + 2)$. Dobbiamo vedere se i polinomi $x^2 - 2$ e $x^2 + 2$ sono ulteriormente scomponibili. Questo accade se e solo se essi hanno radici in $\mathbb{Z}_7$. Una facile verifica mostra che $x^2 + 2$ non ha radici in $\mathbb{Z}_7$, mentre $x^2 - 2$ ha radici $3, 4$. Quindi la scomposizione in irriducibili di $f(x)$ in $\mathbb{Z}_7[x]$ è

$$f(x) = (x^2 + 2)(x - 3)(x - 4).$$

c) usiamo la divisione di f per g fatta sopra e riduciamo tutti i numeri modulo 5. Otteniamo che

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

da cui

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

e quindi

$$a(x) = -1 \quad \text{e} \quad b(x) = x^2 + 1.$$