

Matematica del discreto

M2 - Gruppi, anelli e campi

11 gennaio 2014 - Laurea on line

1. Siano $p(x) = 4x^4 + 3x^3 + 2x^2 + x + 1$ e $q(x) = x^2 - 3$ due polinomi. Trovare quoziente e resto della divisione di $p(x)$ per $q(x)$ nel caso in cui i coefficienti sono presi in \mathbb{Z} , in \mathbb{Z}_2 e in \mathbb{Z}_7 .

(a) coefficienti in \mathbb{Z} :

$$\begin{array}{r|l}
 \begin{array}{r}
 4x^4 + 3x^3 + 2x^2 + x + 1 \\
 4x^4 \\
 \hline
 3x^3 + 14x^2 + x + 1 \\
 3x^3 \\
 \hline
 14x^2 + 10x + 1 \\
 14x^2 \\
 \hline
 10x + 43
 \end{array} & \begin{array}{l}
 x^2 - 3 \\
 \hline
 4x^2 + 3x + 14
 \end{array}
 \end{array}$$

il quoziente è $q(x) = 4x^2 + 3x + 14$, il resto $r(x) = 10x + 43$.

(b) coefficienti in \mathbb{Z}_2 : attenzione, riduco tutti i coefficienti modulo 2, quindi $p(x) = x^3 + x + 1$ e $q(x) = x^2 + 1$

$$\begin{array}{r|l}
 \begin{array}{r}
 x^3 + 2x^2 + x + 1 \\
 x^3 + x \\
 \hline
 1
 \end{array} & \begin{array}{l}
 x^2 + 1 \\
 \hline
 x
 \end{array}
 \end{array}$$

il quoziente è $q_2(x) = x$, il resto $r_2(x) = 1$.

(c) coefficienti in \mathbb{Z}_7 : attenzione, riduco tutti i coefficienti modulo 7, quindi $p(x) = 4x^4 + 3x^3 + 2x^2 + x + 1$ e $q(x) = x^2 + 4$

$$\begin{array}{r|l}
 \begin{array}{r}
 4x^4 + 3x^3 + 2x^2 + x + 1 \\
 4x^4 \\
 \hline
 3x^3 + x + 1 \\
 3x^3 \\
 \hline
 3x + 1
 \end{array} & \begin{array}{l}
 x^2 + 4 \\
 \hline
 4x^2 + 3x
 \end{array}
 \end{array}$$

il quoziente è $q_7(x) = 4x^2 + 3x$, il resto $r_7(x) = x + 1$.

In realtà era sufficiente svolgere solo la prima divisione, infatti $[4x^2 + 3x + 14]_2 = x = r_2(x)$ e $[10x + 43]_2 = 1 = q_2(x)$, mentre $[4x^2 + 3x + 14]_7 = 4x^2 + 3x = r_7(x)$ e $[10x + 43]_2 = 3x + 1 = q_7(x)$.

2. Scrivere come prodotto di cicli disgiunti la permutazione π di S_9

$$\pi = (1\ 2\ 3\ 4)(3\ 4\ 5\ 6)(5\ 6\ 7\ 8)(7\ 8\ 9)$$

e determinarne il periodo. Esiste una permutazione di S_9 di periodo 12?

eseguendo il prodotto da destra a sinistra delle quattro permutazioni si ottiene

1	2	3	4	5	6	7	8	9
							8	9
				6	7	5		8
		4	5	3		6		
2	3	1		4				
2	3	1	5	4	7	6	9	8

quindi $\pi = (1\ 2\ 3)(4\ 5)(6\ 7)(8\ 9)$. L'ordine di π è il massimo comune multiplo tra le lunghezze dei cicli disgiunti in cui si fattorizza, che è 6. In S_9 esistono permutazioni di ordine 12, basta che si fattorizzino come prodotto di cicli disgiunti il cui massimo comune multiplo sia a 12 e la somma delle lunghezze di tutti i cicli sia minore o uguale a 9, ad esempio la permutazione $\sigma = (1\ 2\ 3\ 4)(5\ 6\ 7)$ ha ordine 12.

3. Determinare gli elementi del gruppo $(\mathbb{Z}_{15}^*, \cdot)$ e calcolare il periodo di ciascuno.

Gli elementi del gruppo $(\mathbb{Z}_{15}^, \cdot)$ sono gli interi da 1 a 14 che sono primi con 15, ovvero 1, 2, 4, 7, 8, 11, 13, 14. Poiché sono 8, il loro periodo deve essere un divisore di 8, ovvero 1, 2, 4 o 8.*

o(1): $1^1 \equiv 1$, quindi $o(1) = 1$;

o(2): $2^1 \equiv 2$, $2^2 \equiv 4$, $2^3 \equiv 8$, $2^4 \equiv 1$, quindi $o(2) = 4$;

o(4): $4^1 \equiv 4$, $4^2 \equiv 1$, quindi $o(4) = 2$;

o(7): $7^1 \equiv 7$, $7^2 \equiv 4$, $7^3 \equiv -2$, $7^4 \equiv 1$, quindi $o(7) = 4$;

o(8): $8^1 \equiv 8$, $8^2 \equiv 4$, $8^3 \equiv 2$, $8^4 \equiv 1$, quindi $o(8) = 4$;

o(11): $11^1 \equiv 11$, $11^2 \equiv 1$, quindi $o(11) = 2$;

o(13): $13^1 \equiv -2$, $13^2 \equiv 4$, $13^3 \equiv 7$, $13^4 \equiv 1$, quindi $o(13) = 4$;

o(14): $14^1 \equiv -1$, $14^2 \equiv 1$, quindi $o(14) = 2$;

4. Calcolare l'inversa della matrice a coefficienti in \mathbb{R}

$$\begin{pmatrix} 1 & 2 & 3 \\ -2 & 1 & 4 \\ -1 & 3 & 2 \end{pmatrix}$$

utilizzando il metodo di Gauss-Jordan.

Si ha:

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ -2 & 1 & 4 & 0 & 1 & 0 \\ -1 & 3 & 2 & 0 & 0 & 1 \end{array} \right) \xrightarrow[\text{III}+I]{\text{II}+2I} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 5 & 10 & 2 & 1 & 0 \\ 0 & 5 & 5 & 1 & 0 & 1 \end{array} \right) \xrightarrow{\text{III}-\text{II}}$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 5 & 10 & 2 & 1 & 0 \\ 0 & 0 & -5 & -1 & -1 & 1 \end{array} \right) \xrightarrow[\text{-III}/5]{\text{II}/5} \left(\begin{array}{ccc|ccc} 1 & 2 & 3 & 1 & 0 & 0 \\ 0 & 1 & 2 & \frac{2}{5} & \frac{1}{5} & 0 \\ 0 & 0 & 1 & \frac{1}{5} & \frac{1}{5} & -\frac{1}{5} \end{array} \right) \xrightarrow[\text{I}-3\text{III}]{\text{II}-2\text{III}}$$

$$\left(\begin{array}{ccc|ccc} 1 & 2 & 0 & \frac{2}{5} & -\frac{3}{5} & \frac{3}{5} \\ 0 & 1 & 0 & 0 & -\frac{1}{5} & \frac{2}{5} \\ 0 & 0 & 1 & \frac{1}{5} & \frac{1}{5} & -\frac{1}{5} \end{array} \right) \xrightarrow{\text{I}-2\text{II}} \left(\begin{array}{ccc|ccc} 1 & 0 & 0 & \frac{2}{5} & -\frac{1}{5} & -\frac{1}{5} \\ 0 & 1 & 0 & 0 & -\frac{1}{5} & \frac{2}{5} \\ 0 & 0 & 1 & \frac{1}{5} & \frac{1}{5} & -\frac{1}{5} \end{array} \right)$$

L'inversa cercata è dunque

$$\begin{pmatrix} \frac{2}{5} & -\frac{1}{5} & -\frac{1}{5} \\ 0 & -\frac{1}{5} & \frac{2}{5} \\ \frac{1}{5} & \frac{1}{5} & -\frac{1}{5} \end{pmatrix}$$