17.12.2024

Dănilă Tudor-Mihail
grupa 134

Test SAI 2

(2)

~~Fie~~ $f = x^4+5$

$f \cdot g \equiv 1 \pmod{(x^3+1)}$

$$f = x^4+5 = \widehat{x(x^3+1)-x+5} \equiv \widehat{-x+5} \pmod{(x^3+1)}$$

Fie $g = ax^2+bx+c$

$$f \cdot g = (-x+5)(ax^2+bx+c) =$$

$$= -ax^3 - bx^2 - cx + 5ax^2 + 5bx + 5c =$$

$$= -ax^3 + (5a-b)x^2 + (5b-c)x + 5c =$$

$$= \widehat{\underbrace{-a(x^3+1)}_{\overset{\shortparallel}{0} \pmod{(x^3+1)}} + (5a-b)x^2 + (5b-c)x + 5c + a} \Rightarrow$$

$$\Rightarrow f \cdot g \equiv \widehat{(5a-b)x^2 + (5b-c)x + (5c+a)} \pmod{(x^3+1)}$$

$$f \cdot g = \hat{1} \Rightarrow \begin{cases} 5a-b=0 \Leftrightarrow \cancel{b} = a = \frac{b}{5} \\ 5b-c=0 \Leftrightarrow c = 5b \\ 5c+a=1 \Leftrightarrow 25b + \frac{b}{5} = 1 \Rightarrow \frac{126b}{5} = 1 \Rightarrow \end{cases}$$

$$\Rightarrow \begin{cases} a = \frac{1}{126} \\ b = \frac{5}{126} \\ c = \frac{25}{126} \end{cases}$$ $\Rightarrow$ Cum sistemul are soluție $\Rightarrow f$ este inversabil în $\mathbb{Q}[x]/(x^3+1)$, iar inversul său este

$$g = \frac{1}{126}x^2 + \frac{5}{126}x + \frac{25}{126}$$

4. $N = 774^{148}$

$$\begin{array}{r|l} 774 & 2 \\ 387 & 3 \\ 129 & 3 \\ 43 & 43 \\ 1 & \end{array} \Rightarrow 774 = 2 \cdot 3^2 \cdot 43$$

$$774^{148} = (2 \cdot 3^2 \cdot 43)^{148} = 2^{148} \cdot (3^2)^{148} \cdot 43^{148} =$$

$$= 2^{148} \cdot 3^{296} \cdot 43^{148} = (2^6)^{24} \cdot 2^4 \cdot (3^3)^{98} \cdot 3^2 \cdot 43^{148} =$$

$$= 64^{24} \cdot 2^4 \cdot 27^{98} \cdot 3^2 \cdot 43^{148}$$

$$\left.\begin{array}{l} 64 \equiv 1 \pmod 7 \\ 27 \equiv -1 \pmod 7 \\ 43 \equiv 1 \pmod 7 \end{array}\right| \Rightarrow N = \underbrace{(\hat{1})^{24}}_{1} \cdot 2^4 \cdot (\widehat{-1})^{98} \cdot 3^2 \cdot (\hat{1})^{148} \equiv$$

$$= 2^4 \cdot 3^2 \equiv \widehat{16} \cdot 9 \equiv \widehat{144} \equiv \hat{4} \pmod 7$$

✓

3. $\begin{cases} 2x \equiv 8 \pmod{12} \\ x \equiv 3 \pmod{35} \end{cases} \overset{2 \mid 8 \checkmark,\ 2 \mid 12}{\Longleftrightarrow} \begin{cases} x \equiv 4 \pmod 6 \\ x \equiv 3 \pmod{35} \end{cases}$ ✓

$6 \cdot 35 = 210 \Rightarrow$ căutăm inversul în $\mathbb{Z}_{210}$, mai exact printre

$(3 + M_{35}) \subset \mathbb{Z}_{210}$

~~384~~ $38 \not\equiv 4 \pmod 6$

$73 \not\equiv 4 \pmod 6$

$108 \not\equiv 4 \pmod 6$

$143 \not\equiv 4 \pmod 6$

$178 \equiv 4 \pmod 6$ ✓

Verificare pentru sistemul inițial:

$2 \cdot 178 = 356$

$$\begin{array}{l} 356 : 12 = 29 \Rightarrow 356 \equiv 8 \pmod{12} \checkmark \\ \underline{24} \\ 116 \\ \underline{108} \\ = = 8 \end{array}$$

$$\begin{array}{l} 178 : 35 = 5 \Rightarrow 178 \equiv 3 \pmod{35} \checkmark \\ \underline{175} \\ = = 3 \end{array}$$

$\Rightarrow x = 178$

$S = \{ \dots \}$.

1. Fie $f = x^4 + 2x^3 + 5x^2 + 3x + 1$

$f \rightarrow$ ireductibil $\Leftrightarrow$ nu are rădăcini

Notăm $f = g \cdot h$

<u>cazul i</u>

$g \rightarrow$ grad 1, $h \rightarrow$ grad 3

Dacă $g \rightarrow$ grad $1 \Rightarrow \exists$ o soluție printre $\frac{u}{v}$ din a lui f

$\frac{u}{v} = 1 \Rightarrow$ posibile soluții: ± 1

$f(1) = 1 + 2 + 5 + 3 + 1 \neq 0$

$f(-1) = 1 - 2 + 5 - 3 + 1 = 2 \neq 0$

$\Rightarrow$ cazul i FALS

Cazul ii

$g \to$ grad 2, $h \to$ grad 2

Fie $g = a_0 + a_1 X + a_2 X^2$ și $h = b_0 + b_1 X + b_2 X^2$

$f = g \cdot h \Rightarrow$

$\Rightarrow f = (a_0 + a_1 X + a_2 X^2)(b_0 + b_1 X + b_2 X^2) =$

$= a_0 b_0 + a_0 b_1 X + a_0 b_2 X^2 + a_1 b_0 X + a_1 b_1 X^2 + a_1 b_2 X^3 +$

$+ a_2 b_0 X^2 + a_2 b_1 X^3 + a_2 b_2 X^4 =$

$= a_0 b_0 + (a_0 b_1 + a_1 b_0) X + (a_0 b_2 + a_1 b_1 + a_2 b_0) X^2 + (a_1 b_2 + a_2 b_1) X^3 +$

$+ a_2 b_2 X^4$

$f = X^4 + 2X^3 + 5X^2 + 3X + 1 \Rightarrow$

$$\Rightarrow \begin{cases} a_0 b_0 = 1 \Rightarrow a_0 = b_0 = \pm 1 \\ a_2 b_2 = 1 \Rightarrow a_2 = b_2 = \pm 1 \\ a_0 b_1 + a_1 b_0 = 3 \Rightarrow a_0(a_1 + b_1) = \pm 3 \\ a_1 b_2 + a_2 b_1 = 2 \Rightarrow a_2(a_1 + b_1) = \pm 2 \\ a_0 b_2 + a_1 b_1 + a_2 b_0 = 5 \end{cases} \Bigg| \Rightarrow \begin{cases} a_1 + b_1 = 3 \\ a_1 + b_1 = 2 \end{cases} \text{ FALS} \Rightarrow$$

$\Rightarrow f \to$ ireductibil în $\mathbb{Q}[X]$ ✓