18-11-2024

Seminar 7
Structuri algebrice în informatică

$n \geq 2$, $(\mathbb{Z}_n, +, \cdot)$ inel comutativ

$U(\mathbb{Z}_n) = \{\hat{x} \mid \gcd(x, n) = 1\}$

1) Aflați $\hat{17}^{-1}$ în $\mathbb{Z}_{31}$.

Caut $\hat{u} \in \mathbb{Z}_{31}$, a.î. $\hat{17} \cdot \hat{u} = \hat{u} \cdot \hat{17} = \hat{1}$

$\exists\, k \in \mathbb{Z}$ a.î. $17 \cdot u = 31k + 1$

$31k - 17u = 1$

$31 = 1 \cdot 17 + 14$

$17 = 1 \cdot 14 + 3$

$14 = 3 \cdot 4 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2 + 0$

$\gcd(31, 17) = 1$

$1 = 3 - 2 = 17 - 14 - (14 - 3 \cdot 4) =$

$= 17 - (31 - 17) - 14 + 3 \cdot 4 =$

$= 2 \cdot 17 - 31 - 31 + 17 + (17 - 14) \cdot 4 =$

$= 7 \cdot 17 - 2 \cdot 31 - 4 \cdot 14 =$

$= 7 \cdot 17 - 2 \cdot 31 - 4(31 - 17) =$

$= 11 \cdot 17 - 6 \cdot 31 \Rightarrow (k, u) = (-31, -11)$

$\hat{1} = \hat{11} \cdot \hat{17} + \hat{0} \Rightarrow \hat{17}^{-1} = \hat{11}$

În general $\gcd(x, n) = 1$, găsim $u, v \in \mathbb{Z}$ cu

$ux + vn = 1 \Rightarrow \hat{u} \cdot \hat{x} = \hat{1}$ în $\mathbb{Z}_n \Rightarrow \hat{x}^{-1} = \hat{u}$

2) Fie $f(X) = X^5 - 2X^4 + 3X - 1$ și $g(X) = X^3 + X + 2 \in \mathbb{R}[X]$.

Aflați $\gcd(f, g)$ și $u, v \in \mathbb{R}[X]$ cu $u \cdot f + g \cdot v = \gcd(f, g)$

//

$x^5 - 2x^4 + 3x - 1$ | $x^3 + x + 2$

$-x^5 - x^3 - 2x^2$ | $x^2 - 2x + 1$

$= -2x^4 - x^3 - 2x^2 + 3x - 1$

$+2x^4 + 2x^3 + 4x$

$= \cancel{-2x^4} + x^3 - 2x^2 + 7x - 1$

$\cancel{-x^3 - x - 2}$

$= -2x^2 + 6x - 3$

$= -x^3 + 7x - 1$

$x^3 + x + 2$

$= 8x + 1$

$f = \overbrace{(x^3 + x + 2)}^{g}(x^2 - 2x - 1) + 8x + 1$

$-2x^2 + 6x - 3$ | $x^2 - 2x + 1$

$-x^2 + 2x - 1$

$= -3x^2 + 8x - 4$

$x^2 - 2x - 1$ | $8x + 1$

$-x^2 - \frac{1}{8}x$ | $\frac{1}{8}x$

$=$

$x^3 + x + 2$ | $8x + 1$

$-x^3 - \frac{1}{8}x^2$ | $\frac{1}{8}x^2 - \frac{1}{64}x + \frac{65}{512}$

$= -\frac{1}{8}x^2 + x + 2$

$\frac{1}{8}x^2 + \frac{1}{64}x$

$= \frac{65}{64}x + 2$

$-\frac{65}{64}x - \frac{65}{512}$

$= \frac{959}{512}$

$g = \cancel{(x^3 + x \cdot} (8x + 1)\left(\frac{1}{8}x^2 - \frac{1}{64}x + \frac{65}{512}\right) + \frac{959}{512}$

$$\begin{array}{r|l} gX+1 & \frac{959}{512} \\ \hline & \end{array}$$

$$gX+1 = \frac{959}{512}\cdot \underline{\quad} + 0 \Rightarrow \gcd(f,g) = \frac{959}{512}$$

$$u\cdot f + g\cdot v = \gcd(f,g)$$

$$\frac{959}{512} = g - (gX+1)\underbrace{\left(\frac{1}{g}X^2 - \frac{1}{64}X + \frac{65}{512}\right)}_{h(X)} =$$

$$= g - [f - g(X^2-2X-1)]\cdot h(X) = \cancel{(X^2-2X)\cdot g - f\cdot}$$

$$= g - f\cdot h(X) + g(X^2-2X+1)h(X) = \underbrace{-f\cdot h}_{\in \mathbb{R}[X]} + g\underbrace{(1+(X^2-2X-1)h)}_{\in \mathbb{R}[X]}$$

$$\begin{cases} u_0 = -h \\ v_0 = 1+(X^2-2X-1)h \end{cases}$$

$$\begin{cases} uf + vg = \frac{959}{512} \\ u_0 f + v_0 g = \frac{959}{512} \end{cases}$$

$$f(u-u_0) = g(v_0-v)$$

$$uf(u-u_0) + g(v-v_0) = 0$$

f, g prime între ele și $f \mid g(v_0-v)$

$$\Rightarrow f \mid v_0 - v$$

$$v_0 - v = f - t(X),\ t \in \mathbb{R}[X]$$

$$v = v_0 - f\cdot t(X)$$

$$u - u_0 = \frac{g(v_0-v)}{f} = \frac{g\cdot f\cdot t(X)}{f} = g\cdot t(X) \Rightarrow$$

$$\Rightarrow u = g\cdot t(X) + u_0$$

$$S = \{ (g \cdot t(X) + MO,\ v_0 - f \cdot t(X)) \mid t \in \mathbb{R}[X] \}$$

3) Fie $f(X) = X^5 + \hat{2}X^3 + X + \hat{1}$

$g(X) = \hat{2}X^3 - X + \hat{5} \in \mathbb{Z}_7[X]$. Aflați $\gcd(f,g)$ și toate $u, v \in [X]$

$X^5 + \hat{2}X^3 + X + \hat{1} \quad | \quad \hat{2}X^3 - X + \hat{3}$

$-X^5 + \hat{4}X^3 - \hat{5}X^2 \quad | \quad \hat{4}X^2 + \hat{3}$

$= X^3 - \hat{5}X^2 + X + \hat{1}$

$- X^3 + \hat{3}X - \hat{9}$

$= -\hat{5}X^2 + \hat{5}X - \hat{1}$

$\| \cdot \hat{2}$

$\hat{2}X^2 + \hat{5}X - \hat{1}$

~~$\hat{2}X^2 + 4$~~

$\hat{2}X^3 - X + \hat{3} \quad | \quad \hat{2}X^2 + \hat{5}X - \hat{1}$

de continuat acasă

4) Aflați toate polinoamele $f \in \mathbb{R}[X]$ de grad ≤ 3. care la împărțirea la $X-2$ dau restul 3 și -11- $(X-1)^2$ dau restul $2X+5$.

~~$f = g_1 \cdot (X-2) + 3 \Rightarrow f(2) = 3$~~ $f(2) = 3$ (din prima condiție)

~~$f_2 = g_1 (X-1)^2 + 2X + 5$~~

$$\begin{cases} f(2) = 3 \\ f(X) = h(X) \cdot (X-1)^2 + 2X + 5 \end{cases} \Leftrightarrow \begin{cases} f(2) = 3 \\ f(X) = (aX - 2a - 6)(X-1)^2 + 2X + 5 \end{cases}$$

grad $f \leq 3 \Rightarrow$ grad $h \leq 1 \Rightarrow h(X) = aX + b$

$f(2) = h(2) + 9 \Leftrightarrow h(2) = -6 \Leftrightarrow 2a + b = -6 \Leftrightarrow b = -6 - 2a$

4/

$f(x) = (ax - 2a - 6)(x^2 - 2x + 1) + 2x + 5 = \ldots$ etc

$a \in \mathbb{R}$

5)

Prop: Fie $f(x) = a_n x^n + a_{n-1} x^{n-1} + \ldots + a_1 x + a_0$

$\in \mathbb{Z}[x]$ și $a_n \neq 0$

dacă $\frac{u}{v}$, $v, u \in \mathbb{Z}$, $v \neq 0$, $(u, v) = 1$ este rădăcină

a.î. $f \Rightarrow u / a_0$ și v / a_n

Dem: $f(\frac{u}{v}) = 0 \Leftrightarrow a_n \cdot \frac{u^n}{v^n} + \ldots + a_1 \frac{u}{v} + a_0 =$

$= a_n \cdot u^n + a_{n-1} u^{n-1} \cdot v + \ldots + a_1 u \cdot v^{n-1} + a_0 \cdot v^n \Rightarrow$

$u \mid$ $\quad$ $v \mid$

$\Rightarrow u / a_0 \cdot v^n \} \Rightarrow u / a_0$

$(u, v) = 1$

$v / a_n \cdot u^n \} \Rightarrow v / a_n$

$(v, u) = 1$

L> recomprunzi în factori ireductibili în $\mathbb{Z}[x]$ și $\mathbb{Q}[x]$

$f_1(x) = x^4 + 6x^3 - 22x + 15$

$f_2(x) = 6x^4 - x^3 - 40x^2 - 31x - 6$

$\frac{u}{v}$ cu $(u, v) = 1 \Rightarrow \begin{matrix} u / 15 \\ v / 1 \end{matrix}$ $u \in \{\pm 1\}$

Schema lui Horner

	x^4	x^3	x^2	x	x^0
	1	6	0	-22	15
1	1	7	7	-15	0
1	1	7	7	-15	0

$f(x) = (x-1)(x^3+7x^2+7x-15) = (x-1)^2(x^2+8x+15) =$

$= (x-1)^2(x+3)(x+5)$