Seminar 13 - 12.01.2022

Aplicație - Lema Chineză a Resturilor

Se consideră sistemul :

$$\begin{cases} x \equiv a_1 \pmod{m_1} \\ x \equiv a_2 \pmod{m_2} \\ \vdots \\ x \equiv a_k \pmod{m_k} \end{cases}$$

unde $m_i \in \mathbb{N}$, $m \geq 2$

$(m_i, m_j) = 1$, $\forall i \neq j$.

$(a_i \in \mathbb{Z})$

Algoritm de rezolvare a sistemului :

- $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, $m_i' = \frac{m}{m_i}$ (Obs.: $(m_i, m_i') = 1$)
- t_i = inversul mod m_i al lui m_i' ($m_i' t_i \equiv 1 \bmod m_i$)
- Sistemul are soluție unică mod m, dată de :

$$x = a_1 t_1 m_1' + a_2 t_2 m_2' + \ldots + a_k t_k m_k'.$$

$S = \{ m \cdot l + x \mid l \in \mathbb{Z} \}$

Ex. 1 : Rezolvați în $\mathbb{Z}$ sistemul :

$$\begin{cases} x \equiv 7 \pmod{11} \\ x \equiv 5 \pmod{6} \\ x \equiv 2 \pmod{5} \end{cases}$$

$m_1 = 11$ $\quad m_1' = 30$ $\quad a_1 = 7$

$m_2 = 6$ $\quad m_2' = 55$ $\quad a_2 = 5$

$m_3 = 5$ $\quad m_3' = 66$ $\quad a_3 = 2$.

$m = 11 \cdot 6 \cdot 5 = 330$

Calculăm t_1, t_2, t_3.

- t_1 = inversul lui 30 modulo 11. $\quad (30, 11) = 1$.

Aplicăm Alg. lui Euclid :

$$30 = 11 \cdot 2 + 8$$
$$11 = 8 \cdot 1 + 3$$
$$8 = 3 \cdot 2 + 2$$
$$3 = 2 \cdot 1 + 1$$
$$2 = 1 \cdot 2$$

$$1 = 3 - 2 \cdot 1 = 3 - (8 - 3 \cdot 2) =$$
$$= 3 \cdot 3 - 8 = (11 - 8) \cdot 3 - 8 =$$
$$= 11 \cdot 3 - 8 \cdot 4 = 11 \cdot 3 - (30 - 11 \cdot 2) \cdot 4$$
$$= 11 \cdot 11 - 30 \cdot 4$$

$$1 = 11 \cdot 11 - 30 \cdot 4$$

mod 11 : $\quad 1 \equiv -30 \cdot 4 \pmod{11}$

$\Rightarrow t_1 = -4$.

Obs: $\hat{t_1} = \hat{30}^{-1}$ în $\mathbb{Z}_{11}$

$\hat{t_1} = \hat{8}^{-1}$ în $\mathbb{Z}_{11}$

$\hat{t_1} = \hat{7} = \widehat{-4}$

$t_2 \cdot 55 \equiv 1 \mod 6$

$55 = 6 \cdot 9 + 1$

$1 = 55 \cdot 1 - 6 \cdot 9$

$\Rightarrow t_2 = 1$

$t_3 \cdot 66 \equiv 1 \mod 5$

$66 = 5 \cdot 13 + 1$

$1 = 66 \cdot 1 - 5 \cdot 13$

$\Rightarrow t_3 = 1.$

$m_1' = 30, \quad m_2' = 55, \quad m_3' = 66, \quad a_1 = 7, \quad a_2 = 5, \quad a_3 = 2,$

$t_1 = -4, \quad t_2 = 1, \quad t_3 = 1.$

$t_1' = 7$

$x = 7 \cdot (-4) \cdot 30 + 5 \cdot 1 \cdot 55 + 2 \cdot 1 \cdot 66 = -840 + 275 + 132 = -433$

$-433 \equiv -103 \equiv 227 \pmod{330}$

$x = 7 \cdot 7 \cdot 30 + 5 \cdot 1 \cdot 55 + 2 \cdot 1 \cdot 66 = 1470 + 275 + 132 = 1877$

$1877 \equiv 227 \pmod{330}$

Soluția sistemului: $\{330k + 227 \mid k \in \mathbb{Z}\}.$

Verificare

$330k + 227 \equiv 227 \equiv 7 \mod 11$

$330k + 227 \equiv 227 \equiv 5 \mod 6$

$300k + 227 \equiv 227 \equiv 2. \mod 5$

Inele. Ideale

Fie $(A,+,\cdot)$ un inel com., $I, J \trianglelefteq A$ (ideale).
Atunci:

- $I+J = \{a+b \mid a\in I, b\in J\}$
- $I\cap J = \{a \mid a\in I$ şi $a\in J\}$ sunt ideale în A.
- $I\cdot J = \{ab \mid a\in I, b\in J\}$

Idealele lui $(\mathbb{Z},+,\cdot)$ sunt de forma $n\mathbb{Z}$ cu $n\in\mathbb{Z}$.
Orice ideal al lui $\mathbb{Z}$ este principal.

Ex. 2: Fie $a\mathbb{Z}, b\mathbb{Z} \trianglelefteq \mathbb{Z}$.

a. $a\mathbb{Z}+b\mathbb{Z} = d\mathbb{Z}$, $d=(a,b)$

"$\subseteq$" $\underline{a\mathbb{Z}+b\mathbb{Z} \subseteq d\mathbb{Z}}$

Fie $x\in a\mathbb{Z}+b\mathbb{Z}$, $x = a\cdot k+b\cdot l$, $k,l\in\mathbb{Z}$.

$d=(a,b) \Rightarrow d\mid a$ şi $d\mid b \Rightarrow d\mid ak+bl = x \Rightarrow x\in d\mathbb{Z}$.

Alternativ: Este suficient să arătați că $a, b\in d\mathbb{Z}$.

Obs: $a\in d\mathbb{Z} \Leftrightarrow d\mid a$

" $\supseteq$ " $\quad d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$

Cum $d = (a, b)$, știm că $d = ak + bl$, $k, l \in \mathbb{Z}$ (vezi Alg. lui Euclid) $\Rightarrow d \in a\mathbb{Z} + b\mathbb{Z} \Rightarrow d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$.

b. $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$, $\quad m = [a, b]$.

" $\subseteq$ " $\quad x \in a\mathbb{Z} \cap b\mathbb{Z} \Rightarrow \begin{cases} x \in a\mathbb{Z} \\ x \in b\mathbb{Z} \end{cases} \Rightarrow \begin{cases} a \mid x \\ b \mid x \end{cases} \Rightarrow [a, b] = m \mid x.$

$\Rightarrow x \in m\mathbb{Z}$.

" $\supseteq$ " $\quad x \in m\mathbb{Z} \Rightarrow \left.\begin{matrix} m \mid x \\ m = [a, b] \end{matrix}\right\} \Rightarrow \begin{cases} a \mid m \mid x \\ b \mid m \mid x \end{cases} \Rightarrow \begin{cases} a \mid x \Rightarrow x \in a\mathbb{Z} \\ b \mid x \Rightarrow x \in b\mathbb{Z} \end{cases}$

$\Rightarrow x \in a\mathbb{Z} \cap b\mathbb{Z}$.

c. $(a\mathbb{Z}) \cdot (b\mathbb{Z}) = (ab)\mathbb{Z}$

Exemplu: $\quad (10\mathbb{Z} + 6\mathbb{Z}) \cap 4\mathbb{Z} = 2\mathbb{Z} \cap 4\mathbb{Z} = 4\mathbb{Z}$.

$10\mathbb{Z} + (6\mathbb{Z} \cap 4\mathbb{Z}) = 10\mathbb{Z} + 12\mathbb{Z} = 2\mathbb{Z}$.

Inele de polinoame. Rel. lui Viète

Rel. lui Viète: $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0 \in K[X]$

$(K = \mathbb{Q}, \mathbb{R}, \mathbb{C})$, $x_1, x_2, \ldots, x_n$ rădăcinile sale $(x_i \in \mathbb{C})$

$$x_1 + x_2 + \ldots + x_n = -\frac{a_{n-1}}{a_n}$$

$$x_1x_2 + x_1x_3 + \ldots + x_1x_n + x_2x_3 + \ldots + x_2x_n + \ldots + x_{n-1}x_n = \frac{a_{n-2}}{a_n}$$

$$\sum_{1 \le i < j < k \le n} x_i x_j x_k = -\frac{a_{n-3}}{a_n}$$

$\vdots$

$$x_1 x_2 \ldots x_n = (-1)^n \cdot \frac{a_0}{a_n}$$

Obs: $f = a_n X^n + a_{n-1} X^{n-1} + \ldots + a_1 X + a_0$, $x_1, x_2, \ldots, x_n$ rădăcinile sale. Atunci $f = a_n (X - x_1)(X - x_2) \ldots (X - x_n)$

Ex. 3: Fie $f(X) = X^3 + 7X^2 - 3X + 16 \in \mathbb{C}[X]$, $\alpha_1, \alpha_2, \alpha_3$ rădăcinile sale. Calculați polinomul MONIC $g(X) \in \mathbb{C}[X]$ care are ca rădăcini pe $\underset{\beta_1}{\underbrace{3\alpha_1 - 2}}$, $\underset{\beta_2}{\underbrace{3\alpha_2 - 2}}$, $\underset{\beta_3}{\underbrace{3\alpha_3 - 2}}$.

Rez: $f(X) = X^3 + 7X^2 - 3X + 16$

$f(\alpha_i) = 0, \ \forall i = \overline{1,3}$.

Rel. lui Viete pt. f (și $\alpha_1, \alpha_2, \alpha_3$):

$$\begin{cases} \alpha_1 + \alpha_2 + \alpha_3 = -7 \\ \alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = -3 \\ \alpha_1\alpha_2\alpha_3 = -16 \end{cases}$$

coef. termenului de grad maxim = 1

g este polinomul MONIC care are ca răd. pe $\beta_1, \beta_2, \beta_3$.

$g(X) = \underset{1}{a}(X - \beta_1)(X - \beta_2)(X - \beta_3)$

$g(X) = (X^2 - \beta_1 X - \beta_2 X + \beta_1\beta_2)(X - \beta_3) = X^3 - \beta_1 X^2 - \beta_2 X^2 - \beta_3 X^2 + \beta_1\beta_2 X + \beta_1\beta_3 X + \beta_2\beta_3 X - \beta_1\beta_2\beta_3$

$$g(X) = X^3 - (\beta_1+\beta_2+\beta_3)X^2 + (\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3)X - \beta_1\beta_2\beta_3.$$

$$\beta_1+\beta_2+\beta_3 = 3\alpha_1 - 2 + 3\alpha_2 - 2 + 3\alpha_3 - 2 = 3(\alpha_1+\alpha_2+\alpha_3) - 6 =$$
$$= 3\cdot(-7) - 6 = -21 - 6 = -27$$

$$\beta_1\beta_2+\beta_1\beta_3+\beta_2\beta_3 = (3\alpha_1-2)(3\alpha_2-2) + (3\alpha_1-2)(3\alpha_3-2) +$$
$$+(3\alpha_2-2)(3\alpha_3-2) = 9\alpha_1\alpha_2 - 6\alpha_1 - 6\alpha_2 + 4 + 9\alpha_1\alpha_3 - 6\alpha_1 - 6\alpha_3 + 4 +$$
$$+ 9\alpha_2\alpha_3 - 6\alpha_2 - 6\alpha_3 + 4 = 9(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) - 12(\alpha_1+\alpha_2+\alpha_3) + 12$$
$$= 9\cdot(-3) - 12\cdot(-7) + 12 = -27 + 96 = 69$$

$$\beta_1\beta_2\beta_3 = (3\alpha_1-2)(3\alpha_2-2)(3\alpha_3-2) = (9\alpha_1\alpha_2 - 6\alpha_1 - 6\alpha_2 + 4)(3\alpha_3-2)$$
$$= 27\alpha_1\alpha_2\alpha_3 - 18\alpha_1\alpha_2 - 18\alpha_1\alpha_3 - 18\alpha_2\alpha_3 + 12\alpha_1 + 12\alpha_2 + 12\alpha_3 - 8$$
$$= 27\alpha_1\alpha_2\alpha_3 - 18(\alpha_1\alpha_2+\alpha_1\alpha_3+\alpha_2\alpha_3) + 12(\alpha_1+\alpha_2+\alpha_3) - 8$$
$$= 27\cdot(-16) - 18\cdot(-3) + 12\cdot(-7) - 8 =$$
$$= -432 + 54 - 84 - 8 = 470$$

$$g(x) = X^3 + 27X^2 + 69X - 470.$$

Alternativă: $\beta_i = 3\alpha_i - 2 \Rightarrow \alpha_i = \frac{\beta_i+2}{3}$, $f\left(\frac{X+2}{3}\right) = ?$