Seminar 14 - 10.01.2022

Lema Chineză a Resturilor - Aplicații

Rezolvați 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 $m_i \in \mathbb{N}$, $m_i \geq 2$
cu $(m_i, m_j) = 1$, $\forall i \neq j$.

Algoritm de rezolvare

Notăm $m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, $m_i' = \frac{m}{m_i}$

Calculăm t_i = inversul lui m_i' modulo m_i

Sistemul dat are o sol. unică modulo m și este dată de $x = a_1 \cdot t_1 \cdot m_1' + \ldots + a_k \cdot t_k \cdot m_k'$.

Ex. 1 : Rezolvați sistemul :

$$\begin{cases} x \equiv 4 \mod 8 \\ x \equiv 3 \mod 7 \\ x \equiv 1 \mod 5 \end{cases}$$

$m_1 = 8$ $\quad m_1' = 35$ $\quad a_1 = 4$

$m_2 = 7$ $\quad m_2' = 40$ $\quad a_2 = 3$

$m_3 = 5$ $\quad m_3' = 56$ $\quad a_3 = 1$

$m = 8 \cdot 7 \cdot 5 = 280$

Calculăm t_1, t_2, t_3

t_1 - inversul lui m_1' mod m_1.

În $\mathbb{Z}_8$: $\hat{m_1'} = \hat{35} = \hat{3}$

Aflăm t_1 cu alg. lui Euclid, $(8, 3) = 1$

$8 = 3 \cdot 2 + 2$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2$

$1 = 3 - 2 = 3 - (8 - 3 \cdot 2) = 3 \cdot 3 - 8$

$t_1 = 3$

Obs: t_1 nu este unic în $\mathbb{Z}$ (este unic în $\mathbb{Z}_8$)

t_2 inversul lui m_2' mod m_2, 40 (mod 7)

$40 \equiv 5 \mod 7$ $\quad$ (În $\mathbb{Z}_7$, $\hat{40} = \hat{5}$)

$7 = 5 \cdot 1 + 2$ $\quad 1 = 5 - 2 \cdot 2 = 5 - (7 - 5) \cdot 2 =$

$5 = 2 \cdot 2 + 1$ $\quad 1 = 5 \cdot 3 - 7 \cdot 2 \quad \Rightarrow t_2 = 3$

$2 = 1 \cdot 2$

În $\mathbb{Z}_7$: $\hat{1} = \hat{5} \cdot \hat{3} - \cancel{\hat{7} \cdot \hat{2}} \Rightarrow \hat{1} = \hat{5} \cdot \hat{3}$

t_3 = inversul lui $56 \bmod 5$

$56 \equiv 1 \bmod 5 \quad \Rightarrow t_3 = 1$

$a_1 = 4,\ a_2 = 3,\ a_3 = 1,\ m_1' = 35,\ m_2' = 40,\ m_3' = 56$

$t_1 = 3,\ t_2 = 3,\ t_3 = 1.$

$x = a_1 \cdot t_1 \cdot m_1' + a_2\, t_2 \cdot m_2' + a_3 \cdot t_3 \cdot m_3'$

$x = 4 \cdot 3 \cdot 35 + 3 \cdot 3 \cdot 40 + 1 \cdot 1 \cdot 56$

$x = 420 + 360 + 56 = 836$

$836 \equiv 276 \bmod 280$

Soluțiile sistemului $\{280k + 276 \mid k \in \mathbb{Z}\}$

Verificare: $280k + 276 \equiv 276 \equiv 4 \bmod 8$

$280k + 276 \equiv 276 \equiv 3 \bmod 7$

$280k + 276 \equiv 276 \equiv 1 \bmod 5$

Ex. 2 : $\begin{cases} x \equiv 3 \mod 14 \\ x \equiv 1 \mod 9 \\ x \equiv 2 \mod 5 \end{cases}$

$m_1 = 14$ $\quad m_1' = 45$ $\quad a_1 = 3$

$m_2 = 9$ $\quad m_2' = 70$ $\quad a_2 = 1$

$m_3 = 5$ $\quad m_3' = 126$ $\quad a_3 = 2$

$m = 14 \cdot 9 \cdot 5 = 630$

t_1 = inversul lui m_1' mod m_1.

$(45, 14) = 1$

$45 = \underline{\underline{14}} \cdot 3 + \underline{\underline{3}}$

$14 = \underline{\underline{3}} \cdot 4 + \underline{\underline{2}}$

$3 = 2 \cdot 1 + 1$

$2 = 1 \cdot 2$

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

$= 3 \cdot 5 - 14 = (45 - 14 \cdot 3) \cdot 5 - 14$

$= 45 \cdot 5 - 14 \cdot 16$

$45 \cdot 5 \equiv 1 \mod 14 \Rightarrow t_1 = 5$

Continuare - Ex.

Inele. Ideale.

Fie A un inel comutativ, I, J ideale în A. Atunci:

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

Ex. 3: Fie I, J două ideale în $(\mathbb{Z}, +, \cdot)$. Calculați $I+J$, $I \cap J$, $I \cdot J$.

Rez:

! Orice ideal al lui $\mathbb{Z}$ este principal, adică $I = a\mathbb{Z}$ cu $a \in \mathbb{Z}$.

$I = a\mathbb{Z}$, $J = b\mathbb{Z}$.

$I \cdot J = \{a \cdot k \cdot b \cdot l \mid k, l \in \mathbb{Z}\} = \{ab \cdot t \mid t \in \mathbb{Z}\} = ab\mathbb{Z}$

$a\mathbb{Z} + b\mathbb{Z} = d\mathbb{Z}$ $\qquad d = ?$

$a\mathbb{Z} + b\mathbb{Z} \subseteq d\mathbb{Z}$ $\qquad d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z}$.

$$\left.\begin{array}{l} a \in d\mathbb{Z} \Rightarrow d \mid a \\ b \in d\mathbb{Z} \Rightarrow d \mid b \end{array}\right\} \Rightarrow$$

$\Rightarrow d \mid (a, b)$.

Afirm că $d = (a, b)$

"$\subseteq$" OK.

"$\supseteq$" $d\mathbb{Z} \subseteq a\mathbb{Z} + b\mathbb{Z} \iff \boxed{d = a \cdot k + b \cdot l,}$ $k, l \in \mathbb{Z}$.

Scrierea este dată de Alg. lui Euclid.

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

• $a\mathbb{Z} \cap b\mathbb{Z} = m\mathbb{Z}$ $\qquad m = [a, b]$

"$\subseteq$" $$\left.\begin{array}{l} m \in a\mathbb{Z} \iff a \mid m \\ m \in b\mathbb{Z} \iff b \mid m \end{array}\right\} \Rightarrow [a, b] \mid m.$$

$m\mathbb{Z} \subseteq a\mathbb{Z} \cap b\mathbb{Z}$

$m = [a, b] \Rightarrow \left.\begin{array}{l} a \mid m \Rightarrow m \in a\mathbb{Z} \\ b \mid m \Rightarrow m \in b\mathbb{Z} \end{array}\right\} \Rightarrow m \in a\mathbb{Z} \cap b\mathbb{Z}$

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

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

Inele de polinoame. Rel. lui Viete.

Rel. lui Viete: $f \in K[X]$, K = corp $(= \mathbb{Q}, \mathbb{R}, \mathbb{C})$.

$f = a_m X^m + a_{m-1} X^{m-1} + \ldots + a_1 X + a_0$, $a_i \in K$.

$x_1, x_2, \ldots, x_m$ rădăcinile lui f. $(x_i \in \mathbb{C})$

$$\begin{cases} x_1 + x_2 + \ldots + x_m = -\dfrac{a_{m-1}}{a_m} \\ x_1 x_2 + x_1 x_3 + \ldots + x_1 x_m + x_2 x_3 + \ldots + x_2 x_m + \ldots + x_{m-1} x_m = \dfrac{a_{m-2}}{a_m} \\ \displaystyle\sum_{1 \le i < j < k \le m} x_i x_j x_k = -\dfrac{a_{m-3}}{a_m} \quad \ldots \quad x_1 x_2 \ldots x_m = (-1)^m \dfrac{a_0}{a_m} \end{cases}$$

Exemplu: $n=3$, $f = aX^3 + bX^2 + cX + d \in \mathbb{C}[X]$,

$x_1, x_2, x_3 \in \mathbb{C}$ rădăcinile sale. $a \neq 0$.

$$f = a(X-x_1)(X-x_2)(X-x_3)$$

$$f = a\left(X^2 - (x_1+x_2)X + x_1x_2\right)(X-x_3)$$

$$f = a\left[X^3 - (x_1+x_2+x_3)X^2 + (x_1x_2+x_1x_3+x_2x_3)\cdot X - x_1x_2x_3\right]$$

$$aX^3 + bX^2 + cX + d = a\left[X^3 - (x_1+x_2+x_3)X^2 + (x_1x_2+x_1x_3+x_2x_3)\cdot X - x_1x_2x_3\right]$$

$$b = -a(x_1+x_2+x_3) \Rightarrow x_1+x_2+x_3 = -\frac{b}{a}$$

Ex. 4: Fie $P(X) = X^3 - 5X^2 + 3X + 2$, cu rădăcinile complexe $\alpha_1; \alpha_2, \alpha_3$. Aflați polinomul MONIC (adică coef. termenului de grad maxim este 1) care are ca rădăcini pe $2\alpha_1 - 1$, $2\alpha_2 - 1$, $2\alpha_3 - 1$.

Rez: $Q(X) = (X - \beta_1)(X - \beta_2)(X - \beta_3)$, "$\beta_1$", "$\beta_2$", "$\beta_3$"

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

$\beta_1 + \beta_2 + \beta_3 = 2\alpha_1 - 1 + 2\alpha_2 - 1 + 2\alpha_3 - 1$

$= 2(\alpha_1 + \alpha_2 + \alpha_3) - 3$

$= 2 \cdot 5 - 3 = 7.$

$X^3 - 5X^2 + 3X + 2$

Rel. lui Viete:

$\alpha_1 + \alpha_2 + \alpha_3 = 5 \quad \left(-\frac{-5}{1}\right)$

$\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3 = 3$

$\alpha_1\alpha_2\alpha_3 = -2$

$\beta_1\beta_2 + \beta_1\beta_3 + \beta_2\beta_3 = (2\alpha_1 - 1)(2\alpha_2 - 1) + (2\alpha_1 - 1)(2\alpha_3 - 1) + (2\alpha_2 - 1)(2\alpha_3 - 1) =$

$= 4\alpha_1\alpha_2 - 2\alpha_1 - 2\alpha_2 + 1 + 4\alpha_1\alpha_3 - 2\alpha_1 - 2\alpha_3 + 1 + 4\alpha_2\alpha_3 - 2\alpha_2 - 2\alpha_3 + 1$

$= 4(\alpha_1\alpha_2 + \alpha_1\alpha_3 + \alpha_2\alpha_3) - 4(\alpha_1 + \alpha_2 + \alpha_3) + 3 = 4 \cdot 3 - 4 \cdot 5 + 3 = -5$

$$\beta_1\beta_2\beta_3 = (2\alpha_1 - 1)(2\alpha_2 - 1)(2\alpha_3 - 1) =$$

$$= (4\alpha_1\alpha_2 - 2\alpha_1 - 2\alpha_2 + 1)(2\alpha_3 - 1) =$$

$$= 8\alpha_1\alpha_2\alpha_3 - 4\alpha_1\alpha_2 - 4\alpha_1\alpha_3 - 4\alpha_2\alpha_3 + 2\alpha_1 + 2\alpha_2 + 2\alpha_3 - 1$$

$$= 8\cdot(-2) - 4\cdot 3 + 2\cdot 5 - 1$$

$$= -16 - 12 + 10 - 1 = -19$$

$$Q(x) = x^3 - 7x^2 + (-5)x - (-19)$$

$$= x^3 - 4x^2 - 5x + 19$$