Seminar 12

Lema chineză a Resturilor

$\mathbb{Z}_{mn} \simeq \mathbb{Z}_m \times \mathbb{Z}_n$, $(m,n)=1$.

Aplicație: Rezolvarea sistemelor de forma:

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

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

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

Alg. de rezolvare:

$m = m_1 \cdot m_2 \cdot \ldots \cdot m_k$, $m_i' = \frac{m}{m_i}$, $i = \overline{1,k}$

Obs.: $(m_i, m_i') = 1$.

Se calculează t_i = inversul lui m_i' mod m_i.

Sistemul de mai sus are o unică soluție mod m dată de: $a_1 t_1 m_1' + a_2 t_2 m_2' + \ldots + a_k t_k m_k'$.

Ex. 1: Rezolvați sistemul:

$$\begin{cases} x \equiv 1 \mod 4 \\ x \equiv 2 \mod 3 \\ x \equiv 1 \mod 5 \end{cases}$$

$m_1 = 4$ $m_1' = 15$ $a_1 = 1$

$m_2 = 3$ $m_2' = 20$ $a_2 = 2$

$m_3 = 5$ $m_3' = 12$ $a_3 = 1$.

$m = 60$

t_1 : inversul lui 15 mod 4. În $\mathbb{Z}_4$:

$\hat{15} = \hat{3}$, $\hat{3}^{-1} = \hat{3}$, $t_1 = 3$

Obs: $\hat{15} = \hat{-1}$, $t_1' = -1$.

t_2 : $\hat{20} = \hat{-1}$ $\Rightarrow t_2 = -1$. (sau $t_2' = 2$).

în $\mathbb{Z}_3$

t_3 : în $\mathbb{Z}_5$: $\hat{12} = \hat{2}$, $\hat{2}^{-1} = \hat{3}$, $t_3 = 3$.

$a_1 t_1 m_1' + a_2 t_2 m_2' + a_3 t_3 m_3' =$

$= 1 \cdot 3 \cdot 15 + 2 \cdot (-1) \cdot 20 + 1 \cdot 3 \cdot 12,$

$= 45 - 40 + 36 = 41.$

$41 \equiv 1 \mod 4$
$41 \equiv 2 \mod 3$
$41 \equiv 1 \mod 5$

Sol. sistemului:
$x \in \{60k + 41 \mid k \in \mathbb{Z}\}.$

$a_1 t_1' m_1' + a_2 t_2' m_2' + a_3 t_3 m_3' =$

$= -15 + 2 \cdot 2 \cdot 20 + 3 \cdot 12 = -15 + 80 + 36 = 101.$

$101 \equiv 41 \pmod{60}$

Ex. 2: Rez. sistemul:

$$\begin{cases} x \equiv 3 \mod 5 \\ x \equiv 5 \mod 7 \\ x \equiv 4 \mod 12 \end{cases}$$

$m_1 = 5$ $\quad m_1' = 84$ $\quad a_1 = 3$
$m_2 = 7$ $\quad m_2' = 60$ $\quad a_2 = 5$
$m_3 = 12$ $\quad m_3' = 35$ $\quad a_3 = 7.$
$m = 420$

Rez:

t_1: $\hat{1}$ în $\mathbb{Z}_5$: $\hat{84} = \hat{4}$; $\hat{4}^{-1} = \hat{4}$ $(\text{sau } \hat{-1})$ $\rightarrow t_1 = 4.$

t_2: $\hat{1}$ în $\mathbb{Z}_7$: $\hat{60} = \hat{4}$; $\hat{4}^{-1} = \hat{2}$ $\rightarrow t_2 = 2.\ (-5)$

t_3: Var. 1: $\hat{35} = \hat{11}$ $(= \hat{-1})$

Var. 2: Algoritmul lui Euclid → împărțiri cu rest

Reminder: $a, b \in \mathbb{Z}$, $(a,b) = d \Rightarrow \exists m, n \in \mathbb{Z}$ a.î. $d = am + b \cdot n$

Algoritmul lui Euclid [- calculăm d.
- găsim scrierea $d = am + bn.$

$(35, 12) = 1 \Rightarrow 1 = 35 \cdot m + 12n$

$t_3 = m.$

Alg. lui Euclid: $|a| > |b|$.

$a = b \cdot q_0 + r_0$ (b ↑, r_0 rest.)

$b = r_0 \cdot q_1 + r_1$ $\qquad d = r_{k+1}$

$r_0 = r_1 \cdot q_2 + r_2$

$\vdots$

$r_{k-1} = r_k \cdot q_{k+1} + r_{k+1}$

$r_k = r_{k+1} \cdot q_{k+2}$

$(35, 12) = 1$.

$35 = 12 \cdot 2 + 11$

$12 = 11 \cdot 1 + 1$

$11 = 1 \cdot 11$

$1 = 12 - 11 \cdot 1 = 12 - (35 - 12 \cdot 2)$

$= 3 \cdot 12 - 35$

$t_3 = -1$.

$a_1 t_1 m_1' + a_2 t_2 m_2' + a_3 t_3 m_3' =$

$= 3 \cdot 4 \cdot 84 + 5 \cdot 2 \cdot 60 + 7 \cdot (-1) \cdot 35 =$

$= 1008 + 600 - 245 = 1363$

$1363 \equiv 103 \pmod{420}$

$420 \cdot 3 = 1260$

$x \in \{ 420k + 103 \mid k \in \mathbb{Z} \}$.

Ex. 3: Aflați inversul lui 7 mod 40 cu Alg. lui Euclid.

Rez:

$40 = 7 \cdot 5 + 5$

$7 = 5 \cdot 1 + 2$

$5 = 2 \cdot 2 + 1$

$2 = 1 \cdot 2$

$(7, 40) = 1$

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

$= 3 \cdot 5 - 2 \cdot 7 = 3(40 - 7 \cdot 5) - 2 \cdot 7 =$

$= 3 \cdot 40 - 17 \cdot 7 \Rightarrow \hat{7}^{-1} = -\hat{17}$ în $\mathbb{Z}_{40}$.

$1 = 3 \cdot 40 - 17 \cdot 7 \rightarrow \hat{1} = -\hat{17} \cdot \hat{7}$

T: $\begin{cases} x \equiv 3 \mod 8 \\ x \equiv 6 \mod 9 \\ x \equiv 1 \mod 7 \end{cases}$

Inele de polinoame

Ex. 4: Calculați idealul generat de 2 și X în $\mathbb{Z}[X]$ și $\mathbb{Q}[X]$, $\mathbb{Z}[X]/(2,X)$.

Ref:

A inel, $I \subseteq A$. I ideal dacă:

- $(I,+) \leq (A,+)$
- $ax \in I$, $\forall a \in A, \forall x \in I$

În $\mathbb{Z}[X]$:

$(2,X) = \{2f + X \cdot g \mid f,g \in \mathbb{Z}[X]\}$

Obs: A inel, $x_1, \dots, x_k \in A$.

$(x_1, \dots, x_k) = \{a_1x_1 + \dots + a_kx_k \mid a_i \in A\}$.

$f = a_0 + a_1X + \dots + a_mX^m$, $m \in \mathbb{N}$, $a_i \in \mathbb{Z}$.

$g = b_0 + b_1X + \dots + b_mX^m$, $m \in \mathbb{N}$, $b_i \in \mathbb{Z}$.

$2f + Xg = 2(a_0 + a_1X + \dots + a_mX^m) + X(b_0 + b_1X + \dots + b_mX^m) =$

$= 2a_0 + 2a_1X + \dots + 2a_mX^m + b_0X + b_1X^2 + \dots + b_mX^{m+1} =$

$= \underbrace{2a_0}_{\in\mathbb{Z}} + \underbrace{(2a_1+b_0)}_{\in\mathbb{Z}}X + \underbrace{(2a_2+b_1)}_{\in\mathbb{Z}}X^2 + \dots$

$2f + Xg$ - are termenul liber un nr. par

$(2,X)$ = mulțimea polinoamelor cu termenul liber par

$(=) \{f \in \mathbb{Z}[X] \mid f(0) \text{ par}\}$.

↳ trebuie demonstrată prin dublă incluziune

$\mathbb{Z}[X]/(2,X)$

$f \in \mathbb{Z}[X]$ arbitrar

$f = a_0 + a_1X + \dots + a_mX^m = a_0 + X(a_1 + a_2X + \dots + a_mX^{m-1})$

$\Rightarrow f = a_0 + X \cdot g$.

$\in (2,X)$

$X \cdot g = 2 \cdot 0 + X \cdot g$

$\Rightarrow \hat{f} = \hat{a_0} < \begin{matrix} \hat{0} & \text{dacă } a_0 \text{ par} \\ \hat{1} & \text{dacă } a_0 \text{ impar} \end{matrix}$

$\mathbb{Z}[X]/(2,X) \cong \mathbb{Z}_2$.

$f = a_0 + X \cdot g$

Caz 1: $a_0 = 2k$: $f = 2 \cdot k + X \cdot g \in (2,X)$.
$\in \mathbb{Z}[X]$ $\in \mathbb{Z}[X]$

Caz 2: $a_0 = 2k+1$: $f = 1 + \underbrace{2 \cdot k + X \cdot g}_{\in \mathbb{Z}[X]} \in (2,X)$
$\in \mathbb{Z}[X]$

$f_m \mathbb{Z}[X]/(2,X)$: $\hat{f} = \hat{1} + \underbrace{(\widehat{2k + Xg})}_{\hat{0}} = \hat{1}$

Obs: $I = (f_1, \dots, f_k)$, $f_i \in K[X]$.

$\deg f_1 \leq \deg f_2 \leq \dots \leq \deg f_k$.

$f \in K[X]$, $f = f_1 \cdot g_1 + f_2 \cdot g_2 + \dots + f_k \cdot g_k + r$

$r \notin I$, $\deg r < \deg f_1$.

$f = f_k \cdot g_k + r_1$

Ex. 5: Calculați următoarele inele factor:

a. $\mathbb{Z}[X]/(X^3)$ c. $\mathbb{Z}[X]/(X^2+1)$

b. $\mathbb{Z}[X]/(X^2-2)$ d. $\mathbb{Z}[X]/(2)$.

Rez:

a. $(X^3) = \{X^3 f \mid f \in \mathbb{Z}[X]\}$

$= \{a_3X^3 + a_4X^4 + .. + a_mX^m \mid m \in \mathbb{N}, m \geq 3, a_i \in \mathbb{Z}\}$.

$f \in \mathbb{Z}[X]$, $f = a_0 + a_1X + .. + a_mX^m$

$f = a_0 + a_1X + a_2X^2 + X^3 \cdot g \in (X^3)$

$\hat{f} = \overline{a_0 + a_1X + a_2X^2}$

$\mathbb{Z}[X]/(X^3)$ = mulțimea claselor tuturor resturilor posibile la împărțirea cu X^3

SCR = mulțimea polinoamelor de grad cel mult 2.

$\mathbb{Z}[X]/(X^m)$, SCR = polinoame de grad cel mult $m-1$.

b. $\mathbb{Z}[X]/(X^2-2) \simeq \mathbb{Z}[\sqrt{2}] = \{a+b\sqrt{2} \mid a,b \in \mathbb{Z}\}$.

În general, $\mathbb{Z}[X]/(X^2-p) \simeq \mathbb{Z}[\sqrt{p}]$, $p \in \mathbb{N}$, p prim

$f = X^5 - 2X^4 + 7X + 4$.

$$\begin{array}{r|l} X^5 - 2X^4 + 7X + 4 & X^2 - 2 \\ \hline -X^5 + 2X^3 & X^3 - 2X^2 + 2X - 4 \\ \hline -2X^4 + 2X^3 + 7X + 4 & \\ 2X^4 - 4X^2 & \\ \hline 2X^3 - 4X^2 + 7X + 4 & \end{array}$$

$$\begin{array}{r} -2x^3 \quad +4x \\ \hline -4x^2+11x+4 \\ 4x^2 \quad -8 \\ \hline 11x-4. \end{array}$$

$f(\sqrt{2}) = (\sqrt{2})^5 - 2(\sqrt{2})^4 + 7\sqrt{2} + 4 =$

$= 4\sqrt{2} - 8 + 7\sqrt{2} + 4 = 11\sqrt{2} - 4.$

$\mathbb{Z}[X]/(X^2-2)$, $\hat{X}^2 = \hat{2}$

$\varphi : \mathbb{Z}[X] \longrightarrow \mathbb{Z}[\sqrt{2}]$

$\varphi(f) = f(\sqrt{2})$

φ morfism de inele surjectiv , $\ker\varphi = (X^2-2)$.

TFI : $\mathbb{Z}[X]/(X^2-2) \simeq \mathbb{Z}[\sqrt{2}]$.

c. $\mathbb{Z}[X]/(X^2+1) \simeq \mathbb{Z}[i] = \{a+bi \mid a,b \in \mathbb{Z}\}$.

d. $\mathbb{Z}[X]/(2) \simeq \mathbb{Z}_2[X]$

$\hat{f} = \hat{a}_0 + \hat{a}_1 X + \dots + \hat{a}_m X^m$.

$f = 2\cdot g + h$, h are coef. doar 0 și 1.

e. $\mathbb{Z}[X]/((X-1)(X+2)) = \mathbb{Z}[X]/(X^2+X-2)$

Obs (Ex.):

$\mathbb{Q}[X]/(X^2-1) \simeq \mathbb{Q}\times\mathbb{Q}$.

$\mathbb{Z}[X]/(X^2-1) \not\simeq \mathbb{Z}\times\mathbb{Z}$ $(\simeq \{(a,b) \mid a,b \in \mathbb{Z},\ a \equiv b \bmod 2\})$

LCR: A inel (com., unitar), $I, J \trianglelefteq A$ cu $I + J = A$

$$A/_{I \cap J} \simeq A/_{I \cdot J} \simeq A/_I \times A/_J.$$

$$\mathbb{Z}[X]/_{(X(X+1))} \simeq \mathbb{Z} \times \mathbb{Z}.$$

$1 \in (X) + (X+1) = \mathbb{Z}[X]$.