TEOREMA CHINEZĂ A RESTURILOR

1. Teorema Chineză a Resturilor pentru numere întregi

Fie $n_1, n_2 \geq 2$ două numere întregi prime între ele. Fie a_1, a_2 numere întregi fixate. Considerăm sistemul de congruenţe

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ x \equiv a_2 \bmod n_2 \end{cases}$$

Vom arăta că sistemul dat are soluţii şi vom determina cea mai mică soluţie pozitivă a acestuia.

Deoarece $(n_1, n_2) = 1$ avem că $\widehat{n}_1$ este inversabil în $\mathbb{Z}/n_2\mathbb{Z}$, respectiv $\widehat{n}_2$ este inversabil în $\mathbb{Z}/n_1\mathbb{Z}$. Aşadar există $y_1, y_2 \in \mathbb{Z}$ cu proprietatea că $n_1 y_1 \equiv 1 \bmod n_2$, respectiv $n_2 y_2 \equiv 1 \bmod n_1$. Fie acum $x = a_1 n_2 y_2 + a_2 n_1 y_1$. Este evident că x este o soluţie a sistemului de congruenţe dat. Mai mult, sistemul are o infinitate de soluţii, deoarece $x + k n_1 n_2$ este de asemenea soluţie, oricare ar fi $k \in \mathbb{Z}$.

Ne propunem acum să determinăm cea mai mică soluţie pozitivă a sistemului. Scriem $x = n_1 n_2 q + r$ cu $0 \leq r < n_1 n_2$. Dacă $r = 0$, atunci cea mai mică soluţie pozitivă este $n_1 n_2$. În caz contrar, r este cea mai mică soluţie pozitivă. Este evident că r este o soluţie a sistemului. Să arătăm că este cea mai mică. Fie $0 < r' < r$ o altă soluţie. Atunci $r \equiv r' \bmod n_1$ şi $r \equiv r' \bmod n_2$, deci $n_1 \mid r - r'$ şi $n_2 \mid r - r'$. Cum $(n_1, n_2) = 1$ deducem că $n_1 n_2 \mid r - r'$. Pe de altă parte, $0 < r - r' < n_1 n_2$, contradicţie. □

Să remarcăm că $(n_1, n_2) = 1$ este, în general, o condiţie necesară: de exemplu, sistemul de congruenţe

$$\begin{cases} x \equiv 1 \bmod 4 \\ x \equiv 2 \bmod 6 \end{cases}$$

nu are soluţii.

Exerciţiul 1.1. Să se afle cea mai mică soluţie pozitivă a sistemului de congruenţe

$$\begin{cases} x \equiv 5 \bmod 18 \\ x \equiv 27 \bmod 35 \end{cases}$$

Exerciţiul 1.2. Rezolvaţi sistemul de congruenţe

$$\begin{cases} 6x \equiv 2 \bmod 8 \\ 5x \equiv 5 \bmod 6 \end{cases}$$

Rezultatele de mai sus se pot generaliza la mai mult de două numere.

Teorema 1.3. (Teorema chineză a resturilor) *Fie $s \geq 2$ şi fie $n_1, \ldots, n_s \geq 2$ numere întregi oricare două prime între ele. Fie $a_1, \ldots, a_s$ numere întregi fixate. Considerăm sistemul de congruenţe*

$$\begin{cases} x \equiv a_1 \bmod n_1 \\ \cdots\cdots\cdots \\ x \equiv a_s \bmod n_s \end{cases}$$

Acesta are o unică soluţie $0 < x \leq n_1 \cdots n_s$.

Proof. Vom arăta că sistemul dat are soluţii şi vom determina cea mai mică soluţie pozitivă a acestuia. Fie $m_i = \prod_{j \neq i} n_j$, $1 \leq i \leq s$. Deoarece $(n_i, m_i) = 1$ avem că $\widehat{m}_i$ este inversabil în $\mathbb{Z}/n_i\mathbb{Z}$, pentru orice $i = 1, \ldots, s$. Aşadar există $y_i \in \mathbb{Z}$ cu proprietatea că $m_i y_i \equiv 1 \bmod n_i$. Fie acum $x = \sum_{i=1}^{s} a_i y_i m_i$. Este evident că x este o soluţie a sistemului de congruenţe dat. Mai mult, sistemul are o infinitate de soluţii, deoarece $x + kn_1 \cdots n_s$ este de asemenea soluţie, oricare ar fi $k \in \mathbb{Z}$.

Ne propunem acum să determinăm cea mai mică soluţie pozitivă a sistemului. Scriem $x = n_1 \cdots n_s q + r$ cu $0 \leq r < n_1 \cdots n_s$. Dacă $r = 0$, atunci cea mai mică soluţie pozitivă este $n_1 \cdots n_s$. În caz contrar, r este cea mai mică soluţie pozitivă. Este evident că r este o soluţie a sistemului. Să arătăm că este cea mai mică. Fie $0 < r' < r$ o altă soluţie. Atunci $r \equiv r' \bmod n_i$, deci $n_i \mid r - r'$. Cum $n_1, \ldots, n_s$ sunt numere întregi oricare două prime între ele deducem că $n_1 \cdots n_s \mid r - r'$. Pe de altă parte, $0 < r - r' < n_1 \cdots n_s$, contradicţie. □

2. Teorema Chineză a Resturilor pentru polinoame

Vom considera acum inelul de polinoame $K[X]$ în locul lui $\mathbb{Z}$.

Teorema 2.1. (Teorema de interpolare a lui Lagrange) *Fie K un corp comutativ, $s \geq 2$ un număr întreg, $a_1, \ldots, a_s \in K$ oricare două distincte şi $b_1, \ldots, b_s \in K$. Considerăm sistemul de congruenţe*

$$\begin{cases} f(X) \equiv b_1 \bmod (X - a_1) \\ \cdots\cdots\cdots \\ f(X) \equiv b_s \bmod (X - a_s) \end{cases}$$

Acesta are o unică soluţie $f \in K[X]$ cu $\deg f \leq s - 1$.

Proof. Fie $m_i = \prod_{j \neq i} (X - a_j)$, $1 \leq i \leq s$. Deoarece $(X - a_i, m_i) = 1$ avem că $\widehat{m}_i$ este inversabil în $K[X]/(X - a_i)$, pentru orice $i = 1, \ldots, s$. Dar $K[X]/(X - a_i) \simeq K$ şi prin acest izomorfism $\widehat{m}_i$ corespunde lui $\prod_{j \neq i}(a_i - a_j)$, inversul său fiind $y_i = \prod_{j \neq i}(a_i - a_j)^{-1}$. Aşadar există $y_i \in K^\times$ cu proprietatea că $m_i y_i \equiv 1 \bmod (X - a_i)$. Fie acum $f = \sum_{i=1}^{s} b_i y_i m_i$. Este evident că f este o soluţie a sistemului de congruenţe dat şi $\deg f \leq s - 1$.

Să arătăm că f este unica soluţie cu această proprietate. Fie $g \in K[X]$ o altă soluţie cu $\deg g \leq s - 1$. Atunci $f \equiv g \bmod (X - a_i)$, deci $X - a_i \mid f - g$. Cum $X - a_1, \ldots, X - a_s$ sunt oricare două prime între ele deducem că $(X - a_1) \cdots (X - a_s) \mid f - g$. Pe de altă parte, $\deg(f - g) < s$, contradicţie. □

Remarca 2.2. Polinomul f construit mai sus se scrie sub forma

$$f(X) = \sum_{i=1}^{s} b_i \frac{\prod_{j\neq i}(X - a_j)}{\prod_{j\neq i}(a_i - a_j)}.$$

Acesta se numeşte *polinomul de interpolare Lagrange* asociat elementelor distincte $a_1, \ldots, a_s \in K$ şi elementelor $b_1, \ldots, b_s \in K$. Să remarcăm că $f(a_i) = b_i$ pentru orice $i = 1, \ldots, s$.

Exerciţiul 2.3. Fie $f \in \mathbb{Q}[X]$ un polinom de grad $n \geq 1$ care satisface condiţiile $f(i) = 2^i$ pentru orice $i = 0, 1, \ldots, n$. Aflaţi $f(n + 1)$.

3. Teorema Chineză a Resturilor pentru ideale

Fie $n_1, n_2 \geq 2$ două numere întregi prime între ele. Am demonstrat anterior că funcţia $f : \mathbb{Z}/(n_1n_2)\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ definită prin $f(\widehat{x}) = (\overline{x}, \overline{\overline{x}})$ este un izomorfism de inele. Se observă că dacă notăm $I_1 = n_1\mathbb{Z}$ şi $I_2 = n_2\mathbb{Z}$, atunci $I_1 + I_2 = \mathbb{Z}$ şi $I_1I_2 = I_1 \cap I_2$. Aceasta ne sugerează următoarea generalizare:

Definiţia 3.1. *Fie R un inel şi I_1, I_2 ideale bilaterale ale lui R cu proprietatea că $I_1 + I_2 = R$. Atunci idealele I_1 şi I_2 se numesc* comaximale.

Remarca 3.2. Dacă R este inel comutativ şi unitar, iar I_1, I_2 sunt ideale comaximale, atunci $I_1I_2 = I_1 \cap I_2$.

Exerciţiul 3.3. (i) Daţi un exemplu de inel comutativ (neunitar) R şi de două ideale comaximale $I_1, I_2 \subseteq R$ pentru care $I_1I_2 \neq I_1 \cap I_2$.
(ii) Fie R un inel unitar şi I_1, I_2 ideale comaximale. Atunci $I_1I_2 + I_2I_1 = I_1 \cap I_2$.
*(iii) Daţi un exemplu de inel necomutativ şi unitar R şi de două ideale comaximale $I_1, I_2 \subseteq R$ pentru care $I_1I_2 \neq I_1 \cap I_2$.

Teorema 3.4. *Fie R un inel şi I_1, I_2 ideale comaximale ale lui R. Atunci morfismul*

$$f : R/I_1 \cap I_2 \to R/I_1 \times R/I_2$$

definit prin $f(\widehat{x}) = (\overline{x}, \overline{\overline{x}})$ este un izomorfism de inele.

Proof. Se arată mai întâi că f este bine definit, iar apoi se arată că $(\overline{r}, \overline{\overline{0}})$ şi $(\overline{0}, \overline{\overline{s}})$ sunt în imaginea lui f pentru orice $r, s \in R$: deoarece $I_1 + I_2 = R$ există $x_1 \in I_1$ şi $x_2 \in I_2$ astfel încât $x_1 + x_2 = r$, respectiv există $y_1 \in I_1$ şi $y_2 \in I_2$ astfel încât $y_1 + y_2 = s$. Atunci $f(\widehat{x_2}) = (\overline{r}, \overline{\overline{0}})$ şi $f(\widehat{y_1}) = (\overline{0}, \overline{\overline{s}})$. De aici se obţine $f(\widehat{x_2 + y_1}) = (\overline{r}, \overline{\overline{s}})$, deci f este surjectiv. □

Teorema 3.4 admite următoarea generalizare:

Teorema 3.5. (Teorema chineză a resturilor) *Fie R un inel, $I_1, \ldots, I_n$, $n \geq 2$ ideale bilaterale ale lui R. Definim*

$$f : R \to R/I_1 \times \cdots \times R/I_n$$

prin $f(x) = (x + I_1, \ldots, x + I_n)$.
(i) f este morfism de inele şi $\operatorname{Ker} f = \bigcap_{i=1}^{n} I_i$*;*

(ii) f este surjectiv dacă şi numai dacă I_i şi $\bigcap_{j\neq i} I_j$ sunt comaximale pentru orice $i \neq j$. În acest caz există un izomorfism

$$\overline{f} : R/I \to R/I_1 \times \cdots \times R/I_n.$$

Proof. (i) Evident.
(ii) Dacă f este surjectiv, atunci pentru $r \in R$ există $a \in R$ cu proprietatea că $f(a) = (0 \bmod I_1, \ldots, 0 \bmod I_{i-1}, r \bmod I_i, 0 \bmod I_{i+1}, \ldots, 0 \bmod I_n)$, deci $a \in \bigcap_{j\neq i} I_j$ şi $r - a \in I_i$. Cum $r = (r-a) + a$ deducem că $I_i + \bigcap_{j\neq i} I_j = R$.
Reciproc este suficient să arătăm că orice element de forma $(0 \bmod I_1, \ldots, 0 \bmod I_{i-1}, r \bmod I_i, 0 \bmod I_{i+1}, \ldots, 0 \bmod I_n)$, $1 \leq i \leq n$ se găseşte în imaginea lui f. Cum $I_i + \bigcap_{j\neq i} I_j = R$ vor exista $u \in I_i$ şi $v \in \bigcap_{j\neq i} I_j$ astfel încât $r = u+v$. Se observă acum că $f(v) = (0 \bmod I_1, \ldots, 0 \bmod I_{i-1}, r \bmod I_i, 0 \bmod I_{i+1}, \ldots, 0 \bmod I_n)$.
Izomorfismul $\overline{f}$ se obţine din teorema fundamentală de izomorfism pentru inele. □

Definiţia 3.6. *Dacă R este un inel şi $I_1, \ldots, I_n$, $n \geq 2$ sunt ideale bilaterale ale lui R cu proprietatea că $I_i + I_j = R$ pentru orice $i \neq j$, atunci acestea se numesc* comaximale în perechi.

Exerciţiul 3.7. (i) Fie R un inel unitar şi $I_1, \ldots, I_n$, $n \geq 2$ ideale bilaterale ale lui R. Dacă $I_1, \ldots, I_n$ sunt comaximale în perechi, atunci I_i şi $\bigcap_{j\neq i} I_j$ sunt comaximale, pentru orice $i = 1, \ldots, n$.
(ii) Daţi un exemplu de inel comutativ (neunitar) R şi de trei ideale $I_1, I_2, I_3 \subseteq R$ comaximale în perechi pentru care I_1 şi $I_2 \cap I_3$ nu sunt comaximale.

Remarca 3.8. (i) Teorema Chineză a Resturilor are loc şi pentru ideale comaximale în perechi dacă R este inel unitar.
(ii) Dacă R este inel comutativ şi unitar, iar $I_1, \ldots, I_n$ sunt ideale comaximale în perechi, atunci $\bigcap_{i=1}^n I_i = \prod_{i=1}^n I_i$.

Exerciţiul 3.9. Arătaţi că $\mathbb{Q}[X]/(X^2-1) \simeq \mathbb{Q} \times \mathbb{Q}$, $\mathbb{Z}[X]/(X^2 - X) \simeq \mathbb{Z} \times \mathbb{Z}$, dar $\mathbb{Z}[X]/(X^2-1) \not\simeq \mathbb{Z} \times \mathbb{Z}$.