TEOREMA CHINEZĂ A RESTURILOR

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. □

Rezultatul de mai sus se numeşte *Teorema Chineză a Resturilor*. Acesta poate fi interpretat astfel: funcţia $f : \mathbb{Z}/(n_1 n_2)\mathbb{Z} \to \mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}$ definită prin $f(\widehat{x}) = (\overline{x}, \overline{\overline{x}})$ este un izomorfism de inele. Este uşor de văzut că f este morfism de inele, iar teorema chineză a resturilor este echivalentă cu faptul că f este surjectivă. Dar cum $|\mathbb{Z}/(n_1 n_2)\mathbb{Z}| = |\mathbb{Z}/n_1\mathbb{Z} \times \mathbb{Z}/n_2\mathbb{Z}| = n_1 n_2$ rezultă că f este şi injectivă. Această interpretare a teoremei chineze a resturilor ne sugerează următoarea generalizare:

Fie R un inel comutativ unitar şi I_1, I_2 ideale ale lui R cu proprietatea că $I_1 + I_2 = R$. 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. Mai mult, $I_1 \cap I_2 = I_1 I_2$.

Demonstraţia este similară celei de mai sus în care $R = \mathbb{Z}$. Se arată mai întâi că $(\overline{1}, \overline{\overline{0}})$ şi $(\overline{0}, \overline{\overline{1}})$ sunt în imaginea lui f. Deoarece $I_1 + I_2 = R$ există $x_1 \in I_1$ şi $x_2 \in I_2$ astfel încât $x_1 + x_2 = 1$. Atunci $f(\widehat{x}_2) = (\overline{1}, \overline{\overline{0}})$ şi $f(\widehat{x}_1) = (\overline{0}, \overline{\overline{1}})$ şi de aici se obţine $f(a_1 \widehat{x_2 + a_2} x_1) = (\overline{a}_1, \overline{\overline{a}}_2)$, deci f este surjectivă. □

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.

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

Temă.

1. Să se afle cea mai mică soluţie pozitivă a sistemului de congruenţe
$$\begin{cases} x \equiv 5 \bmod 18 \\ x \equiv 27 \bmod 35 \end{cases}$$
2. Rezolvaţi sistemul de congruenţe
$$\begin{cases} 6x \equiv 2 \bmod 8 \\ 5x \equiv 5 \bmod 6 \end{cases}$$
3. Arătaţi că $\mathbb{Q}[X]/(X^2-1) \simeq \mathbb{Q} \times \mathbb{Q}$, dar $\mathbb{Z}[X]/(X^2-1) \not\simeq \mathbb{Z} \times \mathbb{Z}$.