GAZETA MATEMATICĂ

SERIA B

PUBLICAŢIE LUNARĂ PENTRU TINERET

Fondată în anul 1895

ANUL CXIV nr. 10 **octombrie 2009**

ARTICOLE ŞI NOTE MATEMATICE

LEMA CHINEZĂ A RESTURILOR: FORMULĂRI, DEMONSTRAŢII, APLICAŢII

Cornel Berceanu[1)]

Abstract. This article presents, at an elementary level, the Chinese Remainder Theorem, with applications obtained taking as examples various elementary rings.

Keywords: modulus, congruence, ring, Garner's algorithm

MSC : 11D04

1. Introducere

Lema chineză a resturilor (pe scurt, LCR) este o temă clasică a aritmeticii modulare, aşa cum se poate citi în lucrarea [1], p. 182-199. Generalizarea LCR în cadrul unui inel unitar şi nenul abstract este tratată în lucrarea [2], p. 365. Date istorice legate de LCR pot fi găsite în [3], p. 177-180. O bună construcţie a aritmeticii lui $\mathbb{Z}$ este realizată în [5], p. 9-21. Obiectivele lucrării de faţă sunt suficient de bine definite de titlul lucrării.

A. Noţiuni necesare

Numim *modul* orice număr întreg cel puţin egal cu 2. Fie m un modul fixat. *Mulţimea resturilor modulo* m se notează cu R_m şi se defineşte prin $R_m = \{0, 1, \ldots, m-1\}$. În baza teoremei de împărţire cu rest (pe scurt, TIR), fiecare număr întreg z se poate reprezenta în mod unic sub forma:

$$z = mq + r, \qquad 0 \leq r < m, \tag{1}$$

unde q şi r sunt numere întregi. Din (1) obţinem pentru câtul q şi restul r al împărţirii lui z la m: $q = [z/m] \in \mathbb{Z}$ şi $r = z - m\,[z/m] \in R_m$, unde simbolul $[\,]$ desemnează partea întreagă. Restul r din (1) se notează $z \bmod m$ (simbol care se citeşte z *modulo* m şi se mai numeşte *redusul lui* z *modulo* m).

[1)]Lector univ. dr., Catedra de Matematică-Informatică, Facultatea de Ştiinţe, Universitatea din Bacău.

Pentru fiecare $r \in R_m$, mulţimea:

$$\{z \in \mathbb{Z} \mid z \mod m = r\} = \{mq + r \mid q \in \mathbb{Z}\}$$

se numeşte *r-clasa de resturi modulo m. Mulţimea claselor de resturi modulo* m se notează cu $\mathbb{Z}_m$ şi se defineşte prin:

$$\mathbb{Z}_m = \{\{mq + 0 \mid q \in \mathbb{Z}\},\ \{mq + 1 \mid q \in \mathbb{Z}\}, \ldots, \{mq + (m-1) \mid q \in \mathbb{Z}\}\}.$$

Mulţimea $\mathbb{Z}_m$ fiind o partiţie a mulţimii $\mathbb{Z}$, fiecare număr întreg z aparţine unei unice clase de resturi modulo m, notată cu $\widehat{z}$.

Relaţia de congruenţă modulo m se defineşte prin: $z_1 \equiv z_2 (\mod m) \Leftrightarrow$ $\Leftrightarrow \widehat{z_1} = \widehat{z_2} \in \mathbb{Z}_m$, unde $z_1, z_2 \in \mathbb{Z}$. Relaţia de congruenţă modulo m este o relaţie de echivalenţă pe $\mathbb{Z}$.

Echivalenţa pentru $z_1, z_2 \in \mathbb{Z}$ a condiţiilor:
(i) $\widehat{z_1} = \widehat{z_2} \in \mathbb{Z}_m$,
(ii) $z_1 \bmod m = z_2 \bmod m$ şi
(iii) m divide diferenţa $z_1 - z_2$
fundamentează definirea pe $\mathbb{Z}_m$ a operaţiilor: $\widehat{a} + \widehat{b} = \widehat{a+b}$ şi $\widehat{a} \cdot \widehat{b} = \widehat{a \cdot b}$ $(a, b \in \mathbb{Z})$.

Atunci $(\mathbb{Z}_m, +, \cdot)$ este un inel unitar şi comutativ, numit *inelul claselor de resturi modulo m. Indicatorul* modulului m este numărul de elemente din mulţimea $\{r \in R_m \mid r \perp m\}$, unde scrierea $r \perp m$ este o presurtare a scrierii $(r, m) = 1$. Numărul de elemente inversabile din inelul $(\mathbb{Z}_m, +, \cdot)$ este egal cu indicatorul lui m deoarece $\widehat{a} \in \mathbb{Z}_m$ este inversabil în acest inel dacă şi numai dacă $a \perp m$, unde $a \in \mathbb{Z}$.

B. Formulări ale LCR

Se consideră fixată o mulţime de t module $(t \geq 2)$, $S = \{m_1, m_2, \ldots, m_t\}$. Notăm $T = \{1, 2, \ldots, t\}$.

Formularea LCR în limbajul aritmeticii modulare. *Modulele din mulţimea S satisfac condiţia* $m_i \perp m_j$ *oricare ar fi* $i \neq j$ *din T. Fie date numerele* $r_1, r_2, \ldots, r_t$ *cu* $r_i \in R_{m_i}$ $(i = 1, 2, \ldots, t)$. *Să se determine toate numerele întregi z care satisfac sistemul de relaţii:*

$$\begin{cases} z \mod m_1 = r_1 \\ z \mod m_2 = r_2 \\ \quad \ldots\ldots\ldots \\ z \mod m_t = r_t, \end{cases} \tag{2}$$

sistem ce se poate scrie sub forma $z \equiv r_i \pmod{m_i}$, $i \in T$.

Formularea LCR în limbajul funcţiilor. *Funcţia de S-reducere modulară se defineşte prin:* $f : \mathbb{Z} \to R_{m_1} \times R_{m_2} \times \ldots \times R_{m_t}$, $f(z) =$ $= (z \bmod m_1,\ z \bmod m_2, \ldots, z \bmod m_t)$. *Atunci* $m_i \perp m_j$ *pentru toţi* $i \neq j$ *din T este condiţia necesară şi suficientă pentru ca funcţia f să fie surjecţie.*

Formularea LCR în limbajul morfismelor de inele. *Fie funcţia* $\varphi : \mathbb{Z} \to \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \mathbb{Z}_{m_t}$ *definită prin*:

$$\varphi(z) = (z + m_1\mathbb{Z}, z + m_2\mathbb{Z}, \ldots, z + m_t\mathbb{Z}) .$$

Atunci:

1) φ *este un morfism de la inelul* $\mathbb{Z}$ *la inelul produs* $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times \ldots \times \times \mathbb{Z}_{m_t}$;

2) φ *este un epimorfism dacă şi numai dacă* $m_i \perp m_j$ *pentru toţi* $i \neq j$ *din* T.

2. Demonstraţii elementare

Scop. În această secţiune dăm demonstraţii elementare ale LCR, formulată în limbajul reducerii modulare, adică rezolvăm sistemul de relaţii (2) din paragraful 1.B (în condiţiile formulate în acel paragraf).

Cunoştinţe necesare. Reamintim următoarele rezultate (a se vedea [5]), în care a, b, c, $b_1, b_2, \ldots, b_t$ sunt numere întregi:

Dacă $a \perp b_i$ $(i = 1, 2, ..., t)$ *, atunci* $a \perp b_1 b_2 ... b_t$.

Dacă $a \mid bc$ *şi* $a \perp b$, *atunci* $a \mid c$ (*Gauss, Euler*).

Dacă $a \mid c$, $b \mid c$ *şi* $a \perp b$, *atunci* $ab \mid c$.

O caracterizare a condiţiei $a \perp b$ **în cazul a două module** a **şi** b **date.** Fie a şi b două module care satisfac condiţia $a \perp b$. Împărţim numerele $1 \cdot a$, $2 \cdot a, ..., (b-1) \cdot a$ la b şi obţinem, în baza TIR:

$$i \cdot a = bq_i + r_i,$$

unde $q_i \in \mathbb{Z}$ şi $r_i \in R_b$ ($i = 1, 2, ..., b-1$). Deoarece $a \perp b$ şi j nu e divizibil cu b pentru $j = 1, 2, ..., b-1$, are loc egalitatea de mulţimi:

$$\{r_1, r_2, ..., r_{b-1}\} = \{1, 2, ..., b-1\} .$$

Prin urmare, există un unic element $u \in \{1, 2, ..., b-1\}$ pentru care are loc relaţia $u \cdot a = bq_u + 1$. Elementul u se va numi *inversul lui* a *modulo* b.

Evident, dacă există un element $u \in \{1, 2, ..., b-1\}$ astfel încât $u \cdot a = = bq + 1$ pentru un număr întreg $q > 0$, atunci $a \perp b$. În concluzie, $a \perp b$ dacă şi numai dacă a este inversabil modulo b ($a, b \geq 2$ numere întregi).

Soluţia standard a sistemului de relaţii (2). Introducem notaţiile: $M = m_1 m_2 ... m_t$ şi $M_i = M/m_i$ $(i = 1, 2, ..., t)$. Deoarece $m_i \perp m_j$ oricare ar fi $i \neq j$ din T, are loc relaţia $m_i \perp M_i$ pentru fiecare $i \in T$. Date fiind numerele $r_1, r_2, ..., r_t$, cu $r_i \in R_{m_i}$ $(i = 1, 2, ..., t)$, definim întregul nenegativ z^* prin:

$$z^* = r_1 u_1 M_1 + ... + r_t u_t M_t.$$

Fie i un element fixat din T. Deoarece $r_i u_i M_i = m_i (r_i q_i) + r_i$ şi m_i divide M_j pentru orice $j \in T \setminus \{i\}$, deducem că $z^* = m_i \cdot Q_i + r_i$, unde:

$$Q_i = r_i q_i + \sum_{j \in T \setminus \{i\}} (r_j u_j M_j) / m_i$$

este un număr întreg nenegativ.

Numărul întreg nenegativ z_s definit prin:

$$z_s = ((r_1u_1) \bmod m_1) M_1 + ... + ((r_lu_l) \bmod m_l) M_l$$

îl numim *soluţia standard* a sistemului de relaţii (2). Denumirea se justifică în baza următoarelor fapte: $0 \leq z_s \leq z^*$ şi:

$$z_s = z^* - M \sum_{j=1}^{t} \left[\frac{r_j u_j}{m_j} \right] = m_i Q_i^* + r_i,$$

unde $Q_i^* = Q_i - M_i \sum_{j=1}^{t} \left[\frac{r_j u_j}{m_j} \right] \geq 0$ este un număr întreg (pentru $i = 1, 2, ..., t$).

Numărul întreg pozitiv z_p definit prin $z_p = z_s \bmod M$ îl numim *soluţia principală* a sistemului de relaţii (2). Au loc relaţiile: $z_p \in R_M$, $z_p \leq z_s$ şi $z_p = z_s - kM$, unde $k = [z_p/M]$. Aşadar, avem $z_p = m_i \widetilde{q}_i + r_i$, unde $\widetilde{q}_i = Q_i^* - kM_i \geq 0$ este număr întreg ($i = 1, 2, ..., t$).

Soluţia generală a sistemului de relaţii (2). Fie z un număr întreg care este soluţie a sistemului (2). Atunci diferenţa $z - z_p$ este un multiplu întreg al numărului m_i pentru orice $i \in T$, deci $z - z_p$ este un multiplu întreg al numărului $[m_1, m_2, ..., m_t] = M$. Există atunci un număr întreg k astfel încât $z = z_p + kM$. Reciproc, pentru fiecare număr întreg k, numărul întreg $z = z_p + kM$ este soluţie a sistemului (2), deoarece:

$$z = m_i \tilde{q}_i + r_i + kM = m_i (\tilde{q}_i + kM_i) + r_i,$$

pentru orice $i \in T$.

În concluzie, soluţia generală a sistemului (2) este dată de formula $z = z_p + kM$, $k \in \mathbb{Z}$.

Algoritmul lui Garner de determinare a soluţiei principale z_p (vezi [1]). Acest algoritm permite reprezentarea soluţiei principale z_p a sistemului (2) sub forma:

$$z_p = a_1 + a_2 m_1 + a_3 m_1 m_2 + ... + a_t m_1 m_2 ... m_{t-1},$$

unde $a_i \in R_{m_i}$ pentru toţi $i = 1, 2, ..., t$.

Fie u_{ij} inversul lui m_i modulo m_j, pentru toţi $i < j$ din T. Admitem provizoriu că are loc (2). Problema se reduce la determinarea valorilor întregi $a_i \in R_{m_i}$, pentru toţi $i = 1, 2, ..., t$.

Pas iniţial. Avem $a_1 = r_1$.

Pas curent. Presupunem determinate valorile numerelor întregi $a_1, a_2, \ldots, a_{k-1}$ ($3 \leq k - 1 \leq t - 2$). Putem scrie:

$$\prod_{i=1}^{k-1} u_{ik} z_p \equiv \prod_{i=1}^{k-1} u_{ik} (a_1 + a_2 m_1 + a_3 m_1 m_2 + ... + a_k m_1 m_2 ... m_{k-1}) (\bmod m_k) \equiv$$

$$\equiv \prod_{i=1}^{k-1} u_{ik}\,(a_1 + a_2m_1 + a_3m_1m_2 + ... + a_{k-1}m_1m_2...m_{k-2}) + a_k (\mod m_k),$$

de unde $\prod_{i=1}^{k-1} u_{ik}z_p \equiv r_k \ (\mod m_k)$.

Atunci:

$$a_k = \left(\prod_{i=1}^{k-1} u_{ik}\,(a_1 + a_2m_1 + a_3m_1m_2 + ... + a_{k-1}m_1m_2...m_{k-2}) - r_k\right) (\mod m_k).$$

Demonstraţia faptului că formula (2) este validă pentru valorile întregilor a_i furnizate de algoritmul de mai sus o omitem, pentru detalii putându-se consulta [1], p. 189-190.

Standardizare. Fie dată o *t-mulţime* ($t \geq 2$), $S = \{m_1, m_2, ..., m_t\}$. Spunem că S este un *t-sistem normal de module* dacă sunt îndeplinite condiţiile: (i) $m_1, m_2, ..., m_t \geq 2$ sunt numere întregi şi (ii) $m_i \perp m_j$ pentru orice $i \neq j$ din $T = \{1, 2, ..., t\}$.

Fie dat un t-sistem normal de module $S = \{m_1, m_2, ..., m_l\}$. Următoarea succesiune de paşi o numim *algoritm standard* (asociat lui S):

a) Se calculează produsul $m_1m_2...m_l = M$.

b) Pentru $i = 1, 2, ..., t$ se calculează raportul $\dfrac{M}{m_i} = M_i$.

c) Pentru $i = 1, 2, ..., t$ se determină numărul $u_i \in R_{m_i}$, cu $u_iM_i \equiv 1 \pmod{m_i}$.

Dacă se dau numerele $r_1, r_2, ..., r_t$, cu $r_i \in R_{m_i}$ $(i = 1, 2, ..., t)$, atunci *algoritmul standard extins* include paşii suplimentari:

d) Pentru $i = 1, 2, ..., t$ se calculează numărul $(r_iu_i) \bmod m_i = r_i^*$.

e) Se calculează suma $r_1^*M_1 + r_2^*M_2 + ... + r_t^*M_t = z_s$.

Observaţii:

- Numărul întreg z_s furnizat de algoritmul standard extins este soluţia standard a sistemului (2) de relaţii.
- Dacă z este o soluţie a sistemului (2) de relaţii, atunci există un întreg unic k pentru care $z = z_s + kM$ (**existenţa**: din $z = z_p + aM$ şi $z_s = z_p + bM$, deducem că $z = z_s + kM$, unde k este diferenţa de numere întregi $a - b$).

3. Aplicaţii

A1. Teorema de descompunere a unei fracţii ordinare în fracţii simple ([3], p. 179).

Numim *fracţie simplă*: (i) orice număr întreg şi (ii) fracţiile ordinare de forma $\dfrac{r}{p^k}$, unde $p > 0$ este număr întreg prim, $k \geq 1$ este număr întreg şi $r \in \{1, 2, .., p - 1\}$.

Teoremă (*Gauss*, 1801). *Fie* $\frac{n}{m}$ *o fracţie ordinară ireductibilă nesimplă, cu numitorul descompus în factori primi:* $m = a^{\alpha}b^{\beta}...l^{\lambda}$. *Atunci fracţia* $\frac{n}{m}$ *se descompune în mod unic sub forma*:

$$\frac{n}{m} = k + \frac{a_1}{a} + \frac{a_2}{a^2} + ... + \frac{a_\alpha}{a^\alpha} + \ldots + \frac{l_1}{l^1} + \frac{l_2}{l^2} + ... + \frac{l_\lambda}{l^\lambda}, \qquad (*)$$

unde $k \in \mathbb{Z}$, $a_i \in R_a$ $(i = 1, 2, ..., \alpha)$, ...,$l_j \in R_l$ $(j = 1, 2, ..., \lambda)$.

Demonstraţie.

Existenţa unei descompuneri de tip $(*)$: Notăm $m_1 = a^\alpha$, $m_2 = b^\beta$,.... ..., $m_t = l^\lambda$, unde $t \geq 2$, deoarece fracţia ordinară $\frac{n}{m}$ nu este simplă. Atunci mulţimea $S = \{m_1, m_2, ..., m_t\}$ este un t-sistem normal de module şi $M = m$,, $M_i = \frac{m}{m_i}$ $(i = 1, 2, ..., t)$.

Reducem întregul $n > 0$ în raport cu modulele $m_1, m_2, ..., m_t$: $r_i = n \bmod m_i$, pentru $i = 1, 2, ..., t$. Algoritmul standard extins ne furnizează întregul $z_s = r_1^* M_1 + r_2^* M_2 + ... + r_t^* M_t > 0$. Atunci putem scrie $n = z_s + kM = r_1^* \frac{m}{m_1} + ... + r_t^* \frac{m}{m_t} + km$, deci:

$$\frac{n}{m} = k + \frac{r_1^*}{m_1} + ... + \frac{r_t^*}{m_t}, \qquad (4)$$

unde $k \in \mathbb{Z}$ şi $0 < r_i^* < m_i$ ($r_i^* > 0$ este o consecinţă a teoremei fundamentale a aritmeticii), pentru toţi $i = 1, 2, ..., t$.

Pentru i fixat în $T = \{1, 2, ..., t\}$, fie $m_i = p^k$ ($p > 0$ prim). O consecinţă a TIR este faptul că r_i^* se scrie sub formă de polinom în p şi având coeficienţii în R_p : $r_i^* = c_0 p^0 + c_1 p^1 + ... + c_s p^s$, unde $0 \leq s < k$, $c_j \in R_p$, pentru $j = 1, 2, ..., s$ şi $c_s \neq 0$.

Rezultă că:

$$\frac{r_i^*}{p^k} = \frac{c_0}{p^k} + \frac{c_1}{p^{k-1}} + ... + \frac{c_s}{p^{k-s}}. \qquad (5)$$

Înlocuind în (4) fracţiile $\frac{r_i^*}{m_i}$ cu sumele din membrul drept al egalităţii (5), obţinem pentru fracţia $\frac{n}{m}$ o descompunere de tipul $(*)$ din enunţ.

Unicitatea: Fie:

$$\frac{n}{m} = k' + \frac{n_1}{m_1} + ... + \frac{n_t}{m_t} \qquad (6)$$

o descompunere oarecare de tip $(*)$, unde $\frac{n_1}{m_1} = \frac{a_1}{a^1} + \frac{a_2}{a^2} + ... + \frac{a_\alpha}{a^\alpha}$ etc. Din (6) rezultă $n = k'm + n_1 M_1 + ... + n_l M_l$.

Pentru fiecare $i = 1, 2, ..., t$ avem $r_i \equiv r_i^* M_i \equiv n_i M_i \pmod{m_i}$. Cum $M_i \perp m_i$, urmează că $r_i^* \equiv n_i \pmod{m_i}$, deci $r_i^* = n_i$ Acum $n = k'm + z_s = km + z_s$, deci $k' = k$. $\square$

Exemple. Descompunerea fracţiei $\frac{35}{72}$, unde $72 = 2^3 \cdot 3^2 = 8 \cdot 9$. Avem: $m_1 = 8$, $m_2 = 9$, $M_1 = 9$, $M_2 = 8$, $u_1 = 1$, $u_2 = 8$. Reduceri modulare: $r_1 = 35 \bmod 8 = 3$, $r_2 = 35 \bmod 9 = 8$, $r_1^* = (1 \cdot 3) \bmod 8 = 3$, $r_2^* = (8 \cdot 8) \bmod 9 = 1$. Acum putem scrie:

$$\frac{35}{72} = \frac{3 \cdot 9}{72} + \frac{1 \cdot 8}{72} = \frac{3}{8} + \frac{1}{9} = \frac{2+1}{8} + \frac{1}{9} = \frac{1}{4} + \frac{1}{8} + \frac{1}{9}.$$

Procedând analog obţinem descompunerile: pentru fracţia supraunitară $\frac{91}{72} = \frac{1}{4} + \frac{1}{8} + \frac{2}{3} + \frac{2}{9}$, iar pentru fracţia subunitară $\frac{5}{72} = (-1) + \frac{1}{2} + \frac{1}{8} + \frac{1}{3} + \frac{1}{9}$.

A2. Problema interpolării polinomiale ([4], p. 122-127).

Notăm cu $\mathbb{P}$ mulţimea polinoamelor într-o variabilă x cu coeficienţi reali. Fie $f(x)$ un polinom neconstant din $\mathbb{P}$ şi fie $x - a$ un polinom monic şi ireductibil (a număr real). Cum $f(x) \bmod (x-a) = f(a)$, avem: $(x-a) \perp f(x)$ dacă $f(a) \neq 0$ şi $(x-a) | f(x)$ dacă $f(a) = 0$. Dacă $f(a) \neq 0$, atunci $\frac{1}{f(a)} f(x) \equiv 1 (\bmod (x-a))$, deci polinomul constant $\frac{1}{f(a)}$ este inversul lui $f(x)$ modulo $x - a$.

Problema interpolării polinomiale. *Fiind date t ($t \geq 2$) numere reale diferite $x_1, x_2, ..., x_t$ şi alte t numere oarecare $y_1, y_2, ..., y_t$, să se găsească polinomul $f(x)$ de grad minim care satisface următoarele t condiţii:*

$$f(x_1) = y_1,\ f(x_2) = y_2, ..., f(x_t) = y_t.$$

Rezolvare. Definim modulele $m_i(x) = x - x_i$ ($i = 1, 2, ..., t$). Pentru orice $i \neq j$ din $T = \{1, 2, ..., t\}$ avem: $m_i(x_j) = x_j - x_i \neq 0$, deci $m_i(x) \perp m_j(x)$. Prin urmare, mulţimea $\{m_i(x) \mid i = 1, 2, ..., t\}$ este un t-sistem normal de module. Atunci: $M(x) = (x - x_1)(x - x_2)...(x - x_t) = m_1(x) m_2(x) ... m_t(x)$;

$$M_i(x) = \prod_{j \in T \setminus \{i\}} (x - x_j), \text{ pentru } i = 1, 2, ..., t;$$

$$u_i = \frac{1}{M_i(x_i)} = \frac{1}{\prod_{j \in T \setminus \{i\}} (x_i - x_j)}, \text{ pentru } i = 1, 2, ..., t.$$

Polinomul $L(x) = y_1 u_1 M_1(x) + ... + y_l u_l M_l(x)$ este soluţia standard a sistemului format din cele t condiţii din enunţul problemei. Cum *grad* $L(x) < t$, polinomul $L(x)$ este soluţia principală. Polinomul $L(x)$ se numeşte *polinomul de interpolare al lui Lagrange.* Deoarece $f(x) = L(x) + kM(x)$ (k număr real) este soluţia generală pentru polinoamele din $\mathbb{P}$ care satisfac cele t condiţii din enunţul problemei, soluţia problemei este $f(x) = L(x)$. □

Concluzie: Problema interpolării polinomiale este LCR în variantă polinomială.

A3. Varianta polinomială de descompunere a unei fracţii în sumă de fracţii simple. Un polinom din $\mathbb{P}$ se numeşte *monic* dacă coeficientul termenului său dominant este egal cu 1. Fie $f(x),\ g(x) \in \mathbb{P}$. Scriem

$f(x)\perp g(x)$ dacă şi numai dacă $f(x)$ şi $g(x)$ au un singur divizor comun monic, polinomul constant $d(x)=1$.

Numim $\mathbb{P}$-*fracţie ordinară* orice expresie de forma $\dfrac{f(x)}{g(x)}$, unde $f(x),g(x)\in\mathbb{P}$, $f(x)\perp g(x)$ şi $g(x)$ este polinom monic.

Fie $\mathbb{F}$ mulţimea tuturor $\mathbb{P}$-fracţiilor ordinare. Atunci $(\mathbb{F},+,\cdot)$ este corpul de fracţii al domeniului de integritate $(\mathbb{P},+,\cdot)$.

Polinoamele monice şi ireductibile din $\mathbb{P}$ au forma: (i) $x+a$ $(a\in\mathbb{R})$ sau (ii) x^2+bx+c $(b,c\in\mathbb{R}$ şi $b^2-4c<0)$. O consecinţă a TIR în $\mathbb{P}$ este următoarea: Dacă $B\in\mathbb{P}$, grad$B\in\{1,2\}$ şi $f(x)$ este un polinom de grad $n\geq 0$ din $\mathbb{P}$, atunci $f(x)=c_oB^0+c_1B^1+\ldots+c_sB^s$ $(B^0\equiv 1)$, unde: dacă grad$B=1$ avem $s=n$, c_i este polinom constant $(i=1,2,...,s)$ şi $c_s\neq 0$, iar dacă grad$B=2$ avem $s=\left[\dfrac{n}{2}\right]$, grad $c_i\leq 1$ $(i=1,2,...,s)$ şi $c_s\neq 0$.

O $\mathbb{P}$-fracţie ordinară se numeşte *simplă* dacă are una din formele: (i) este polinom nenul din $\mathbb{P}$ sau (ii) $\dfrac{a(x)}{(A(x))^\alpha}$, unde $A(x)$ este un polinom monic şi ireductibil, $\alpha\geq 1$ este un număr întreg, iar $a(x)\in\mathbb{P}$ cu grad$a(x)<$ grad$A(x)$.

Teoremă. *Fie* $\dfrac{n(x)}{m(x)}$ *o* $\mathbb{P}$*-fracţie ordinară nesimplă, cu numitorul descompus în factori monici şi ireductibili*: $m(x)=(A(x))^\alpha(B(x))^\beta....(L(x))^\lambda$. *Atunci fracţia* $\dfrac{n}{m}$ *se descompune în mod unic sub forma*:

$$\frac{n}{m}=k+\frac{a_i}{A^1}+\frac{a_2}{A^2}+...+\frac{a_\alpha}{A^\alpha}+...+\frac{l_1}{L^1}+\frac{l_2}{L^2}+...+\frac{l_\lambda}{L^\lambda},\qquad(**)$$

unde $k\in\mathbb{P}$, $a_i\in\mathbb{P}$ *şi* grad$a_i<$ grad$A$ $(i=1,2,...,\alpha)$,...., $l_j\in\mathbb{P}$ *şi* grad$l_j<$ grad$L$ $(j=1,2,...,\lambda)$.

Demonstraţia teoremei precedente se obţine din demonstraţia teoremei lui *Gauss*, înlocuind peste tot numerele întregi cu polinoame din $\mathbb{P}$. □

Concluzie. Teorema de mai sus (aplicată în clasa a XII-a la integrarea funcţiilor reale raţionale) este încă un aspect al LCR (în varianta polinomială).

A4. Problema interpolării polinomiale în varianta Garner. Considerăm problema interpolării în următorul caz special: să se determine un polinom $f(x)$ de grad minim, cu proprietatea că $f(k)=k^n$ pentru orice $k\in\{0,1,...,n\}$. Atunci $\{x,x-1,x-2,...,x-n\}$ este un $(n+1)$-sistem normal de module. Evident, $f(x)=x^n$. În baza algoritmului lui *Garner*:

$$f(x)=x^n=a_1+a_2x+a_3x(x-1)+...+a_{n+1}x(x-1)...(x-n+1),$$

unde $a_i\in\mathbb{R}$ $(i=1,2,...,n+1)$. Determinarea constantelor reale a_i $(i=1,2,...,n+1)$ se poate realiza prin rezolvarea sistemului de ecuaţii liniare $f(k)=k^n$ $(k=0,1,2,...,n)$. Coeficienţii a_i $(i=1,2,...,n+1)$ au următoarea

interpretare combinatorială: $a_{i+1} = \left\{ \begin{matrix} n \\ i \end{matrix} \right\}$ reprezintă numărul de partiţii cu i clase ale unei mulţimi cu n elemente, aceste numere fiind numite *numere Stirling de a doua speţă.*

Concluzie finală. $(\mathbb{P}, +, \cdot)$ este o $\mathbb{R}$-algebră în care şirurile de polinoame $\sigma = (1, x, x^2, x^3, ...)$ şi $\varphi = (1, x, x(x-1), x(x-1)(x-2), ...)$ sunt baze ale $\mathbb{R}$-spaţiului vectorial $\mathbb{P}$. Trecerea de la polinoame din σ la polinoame din φ este încă un aspect al LCR (în varianta Garner polinomială).

Bibliografie

[1] Ion D. Ion, C. Niţă, *Elemente de aritmetică cu aplicaţii în tehnici de calcul*, Ed. Tehnică, Bucureşti, 1978.
[2] Ion D. Ion, Nicolae Radu, *Algebră*, Ed. Didactică şi Pedagogică, Bucureşti, 1991.
[3] N. Mihăileanu, *Istoria matematicii*, vol. 2, Ed. Ştiinţifică şi Enciclopedică, Bucureşti, 1981.
[4] G. Polya, *Descoperirea în matematică*, Ed. Ştiinţifică, Bucureşti, 1971.
[5] I. M. Vinogradov, *Bazele teoriei numerelor*, Ed. Academiei, Bucureşti, 1954.