LEMA CHINEZĂ A RESTURILOR

Prof. Ion Munteanu

Editura Casei Corpului Didactic Bacău
2026
ISBN: 978-606-619-433-4

CUPRINS

INTRODUCERE

Lucrarea *Lema chineză a resturilor* reprezintă o abordare într-o manieră simplă şi metodică a unor fapte ţinând de aritmetica în inele.

O primă formă a teoremei a fost conținută într-o carte a matematicianului chinez Sun Tzu: *Matematici clasice* (sec. III î.e.n.) și republicată mai târziu în 1247 de Qin Jiushao în *Tratat de matematică în nouă sectiuni.* Metode similare de rezolvare a sistemelor de congruențe simultane au fost descrise de Arybhata (sec.VI), Brahmagupta (sec. VII) și apar și în cartea lui Fibonacci: *Liber Abaci* (1202).

Lema chineză a resturilor (pe scurt LCR) are două variante: una numerică și una polinomială. Ea poate fi formulată folosind elemente de teoria divizibilității, folosind conceptul de funcție sau cu ajutorul structurilor algebrice.

Deși este un rezultat matematic foarte vechi, el este de mare actualitate prin domeniile diverse de aplicabilitate. Lema chineză a resturilor este folosită în criptografie, la cifrarea cu chei asimetrice. Utilizarea LCR în algoritmul de criptare RSA conduce la o diminuare semnificativă a amplorii calculelor dar totuși împiedică la fel de bine atacurile asupra lui. LCR poate fi utilizată la partajarea secretelor care constă în împărțirea unor date unui grup de oameni care pot reconstitui informația totală doar împreună.

Există o legătură profundă între lema chinezească a resturilor şi teorema de descompunere a fracţiilor raţionale în fracţii simple, după cum se va observa și în lucrare.

Capitolul 1 conţine o prezentare a teoriei divizibilităţii în $\mathbb{Z}$, algoritmul lui Euclid, cel mai mare divizor comun, cel mai mic multiplu comun, numere prime, descompunea în factori primi. În capitolul 2 sunt prezentate noţiunile de congruenţă şi lema chinezească a resturilor. Capitolul 3 abordează metodic mai întâi lema chinezească a resturilor apoi descompunerea fracţiilor raţionale în fracţii simple – aceste noţiuni fiind urmate de exerciţii relevante pentru formarea unei imagini complete despre tema respectivă.

CAPITOLUL 1

ALGORITMUL LUI EUCLID ŞI TEORIA DIVIZIBILITĂŢII ÎN $\mathbb{Z}$

În aceste capitol vom prezenta câteva elemente teoretice necesare abordării LCR în variantă aritmetică: elemente de divizibilitate în $\mathbb{Z}$, algoritmul lui Euclid, cel mai mare divizor comun, cel mai mic multiplu comun, numere prime, descompunea în factori primi.

§ 1.1. Noţiuni şi teoreme fundamentale.

a. *Teoria numerelor* se ocupă cu studiul proprietăţilor numerelor întregi.

Ce este un număr întreg? Vom numi întregi nu numai numerele şirului natural 1,2,3, ... (întregii pozitivi), ci şi zero şi întregii negativi $-1, -2, -3, \ldots$

Notaţii. Vom nota, de regulă, prin litere, numai numerele întregi. Cazurile, în care prin litere s-au notat şi numere care nu sunt întregi, dacă nu vor fi evidente vor fi menţionate în mod special.

Operaţii. Suma, diferenţa şi produsul a doi întregi a şi b sunt de asemenea întregi, dar câtul împărţirii lui a prin b (dacă b nu este egal cu zero) poate fi atât întreg, cât şi fracţionar.

b. În cazul în care câtul împărţirii lui a prin b este un întreg, notându-l cu litera q, avem $a = b \cdot q$, adică a este egal cu produsul lui b cu un întreg. Spunem atunci că a se divide prin b sau că b divide pe a. Totodată se zice că a este un multiplu al numărului b şi b un divizor al numărului a. Faptul că b divide pe a se scrie astfel : b/a.

   Avem următoarele două teoreme:

   1. Dacă a este un multiplu al lui m şi m un multiplu al lui b, atunci a este un multiplu al lui b. (*tranzitivitate*)

În adevăr, din $a = a_1 m, m = m_1 b$ rezultă $a = a_1 m_1 b$, unde $a_1 m_1$ este un număr întreg. Şi aceasta demonstrează teorema.

   2. Dacă într-o egalitate de forma $k + l + \cdots + n = p + q + \cdots + s$ se ştie despre toţi termenii, cu excepţia unui singur, că sunt multiplii lui b, atunci şi termenul rămas este un multiplu al lui b.

În adevăr, fie *k* acest termen. Avem

$l = l_1 b, \ldots, n = n_1 b,\ p = p_1 b, q = q_1 b, \ldots,\ s = s_1 b,\ k = p + q + \ldots + s - l - \ldots - n = (p_1 + q_1 + \cdots + s_1 - l_1 - \cdots - n_1)\ b.$ Şi aceasta demonstrează teorema.

c. În cazul general, care include drept caz particular pe acela când *a* se divide prin *b,* avem teorema :

Orice întreg a se reprezintă într-un mod unic printr-un întreg pozitiv b sub forma

$$a = bq + r\,; 0 \leq r < b.$$

Într-adevăr, o reprezentare a lui a în această formă se obţine luând bq egal cu cel mai mare multiplu al numărului b care nu-l întrece pe *a.* Presupunând că avem şi $a = bq_1 + r_1\ 0 \leq r < b$, obţinem $0 = b\,(q - q_1) + r - r_1$ de unde rezultă că $r - r_1$ este un multiplu al lui b. Cum însă $|r - r_1| < b$, ultima relaţie este posibilă numai dacă $r - r_1 = 0$, adică pentru $r = r_1$, de unde rezultă că şi $q = q_1$

Numărul q se numeşte *câtul necomplet,* iar numărul r - *restul* împărţirii lui a prin b.

E x e m plu. Fie $b = 14$. Avem

$$177 = 14 \cdot 12 + 9;\quad 0 < 9 < 14,$$

$$-64 = 14 \cdot (-5) + 6;\quad 0 < 6 < 14,$$

$$154 = 14 \cdot 11 + 0;\quad 0 = 0 < 14.$$

§ 1.2. Cel mai mare divizor comun a două numere.

În cele ce urmează, nu vom considera decât divizorii pozitivi ai numerelor. Orice întreg care divide simultan întregii $a, b \ldots, l$ se numeşte *divizor comun* al lor. Cel mai mare dintre divizorii comuni se numeşte *cel mai mare divizor comun* şi se notează cu simbolul $(a, b, \ldots, l)$. Existenţa celui mai mare divizor comun este evidentă, din cauză că numărul divizorilor comuni este finit. Dacă $(a, b, \ldots, l) = 1$, atunci $a, b, \ldots, l$ se numesc *prime între ele. D*acă fiecare dintre numerele $a, b, \ldots, l$ este prim cu oricare altul dintre aceste numere, atunci $a, b, \ldots, l$ se numesc *prime două câte două.* Numerele prime două cîte două sunt evident prime şi între ele. În cazul a două numere, noţiunile de «prime două câte două» şi de «prime între ele» coincid.

Exemple. Numerele $6,\ 10,\ 15$ sunt prime între ele, deoarece $(6, 10, 15) = 1$. Numerele $8, 13, 21$ sunt prime două câte două, deoarece $(8,13) = (8, 21) = (13, 21) = 1$.

Să ne ocupăm mai întâi de divizorii comuni a două numere.

1. *Dacă a este un multiplu al lui b, atunci mulţimea divizorilor comuni ai numerelor a si b coincide cu mulţimea divizorilor numărului b; în particular, (a, b) = b. (dacă b >0)*

Într-adevăr, orice divizor comun al numerelor *a* şi *b* este un divizor şi al numărului *b.* Reciproc, dacă *a* este un multiplu al lui *b,* atunci (1, b, § 1) orice divizor al numărului *b* este şi un divizor al numărului *a,* adică el va fi un divizor comun al numerelor *b* şi *a.* Aşadar, mulţimea divizorilor comuni ai numerelor *a* şi *b* coincide cu mulţimea divizorilor numărului *b*. Şi întrucât cel mai mare divizor al numărului *b* este însuşi *b,* rezultă că *(a, b) = b.*

2. *Dacă* $a = bq + c$, *atunci mulţimea divizorilor comuni ai numerelor a şi b coincide cu mulţimea divizorilor comuni ai numerelor b şi c; în particular (a, b) = (b, c).*

Într-adevăr, egalitatea de mai sus ne arată, că orice divizor comun al numerelor *a* şi *b* divide şi pe *c* şi deci *a* este un divizor comun al numerelor *b* şi c. Reciproc, aceeaşi egalitate ne arată că orice divizor comun al numerelor *b* şi *c* divide pe *a* şi deci este un divizor comun al numerelor *a* şi *b.* Aşadar, divizorii comuni ai numerelor *a* şi *b* sunt aceiaşi cu divizorii comuni ai numerelor *b* şi c; în particular, trebuie să coincidă, şi cei mai mari dintre aceşti divizori, adică (*a, b*)=(*b, c*).

Algoritmul lui Euclid. Pentru găsirea celui mai mare divizor comun, precum şi pentru deducerea proprietăţilor sale cele mai importante, se foloseşte *algoritmul lui Euclid.* Acesta din urmă constă în următoarele:

Fie *a* şi *b* întregi pozitivi. Conform cu *c*, §1.1, formăm şirul de egalităţi

$$a = bq_1 + r_2, 0 < r_2 < b\,,$$

$$b = r_2q_2 + r_3, 0 < r_3 < r_2\,,$$

$$r_2 = r_3q_3 + r_4, 0 < r_4 < r_3\,, \qquad (1)$$

.....

$$r_{n-2} = r_{n-1}q_{n-1} + r_n, 0 < r_n < r_{n-1},$$

$$r_{n-1} = r_nq_n\,,$$

care se termină, când obţinem un r_{n+1} =0. Acest lucru este inevitabil, deoarece şirul *b,* r_2, r_3.... fiind un şir de întregi descrescători, nu poate conţine mai mult decât *b* numere pozitive.

d. Considerând egalităţile (1) de sus în jos, ne convingem că divizorii comuni ai numerelor *a* şi *b* sunt aceiaşi cu divizorii comuni ai numerelor *b* şi r_2, apoi aceiaşi cu divizorii comuni ai numerelor r_2 şi r_3, ai numerelor r_3 şi r_4,..., ai numerelor r_{n-1} şi r_n şi în sfârşit că sunt aceiaşi cu divizorii numărului r_n. Totodată avem

$$(a, b) = (b, r_2) = (r_2, r_3) = \ldots = (r_{n-1}, r_n) = r_n.$$

Ajungem la următoarele rezultate:

1. *Mulţimea divizorilor comuni ai numerelor a şi b coincide cu mulţimea divizorilor celui mai mare divizor comun al lor.*

2. *Acest cel mai mare divizor comun este egal cu* r_n *, adică egal cu ultimul rest diferit de zero al algoritmului lui Euclid.*

Exemplu. Să aplicăm algoritmul lui Euclid la găsirea lui (525, 231). Găsim (calculele auxiliare sunt date în stânga):

525:231=2 525=231·2+63
462

231: 63=3 231=63·3+42

189

63:42=1 63=42·1+21

42

42:21=2 42=21·2.

42

==

Aici ultimul rest pozitiv este r_4= 21. Prin urmare, (525, 231) =21.

e. 1. *Notând cu litera m un întreg pozitiv oarecare, avem* $(am, bm) = (a, b)\, m.$

2. *Notând cu litera* δ *un divizor comun oarecare al numerelor a şi b avem* $\left(\frac{a}{\delta}, \frac{b}{\delta}\right) = \frac{(a,b)}{\delta}$. *În particular avem* $\left(\frac{a}{(a,b)}, \frac{b}{(a,b)}\right) = 1$, *adică câturile împărţirii a două numere prin cel mai mare divizor comun al lor sunt numere prime între ele.*

Să înmulţim egalităţile (1) membru cu membru cu *m.* Obţinem egalităţi noi, unde în locul lui *a, b,* r_2,.. ., r_n vom avea *am, bm,* r_2m,. . ., r_n *m.* De aceea (*am, bm*) = r_n *m* şi deci afirmaţia (1) este adevărată.

Aplicând afirmaţia (1), găsim $(a, b) = \left(\frac{a}{\delta}\delta, \frac{b}{\delta}\delta\right) = \left(\frac{a}{\delta}, \frac{b}{\delta}\right)\delta$ de unde rezultă afirmaţia 2.

f. 1. Dacă $(a, b) = 1$, *atunci* $(ac, b) = (c, b)$ (regula de simplificare)

În adevăr, (ac, b) divide ac şi bc, deci conform 1. d), el divide şi (ac, bc) care în virtutea lui 1.e) este egal cu *c ;* dar (ac, b) divide şi b, de aceea divide şi (c, b).

Reciproc, (c, b) divide ac şi b, de aceea divide şi (ac, b). Aşadar, (ac, b) şi (c, b) se divid unul pe altul şi prin urmare sunt egali între ei.

2. *Dacă (a, b)* = 1 *şi ac se divide prin b, atunci c se divide prin b.*

Într-adevăr, din cauză că $(a, b) = 1$, avem $(ac, b) = (c, b)$. Însă, odată ce *a c* este un multiplu al lui *b,* atunci (1, b) avem *(ac, b)* = *b,* adică şi (c, *b)* = *b,* adică *c* este un multiplu al lui *b.*

2'. *Dacă (a, b)* = 1 şi *(a, c)* = 1 atunci *(a, bc)* = 1

3. *Dacă fiecare dintre* a_1, a_2 ,. .., a_m *este prim cu fiecare dintre* b_1, b_2,. . ., b_n , *atunci şi produsul* $a_1\, a_2$ . .. a_m *este prim cu produsul* $b_1 b_2$. . . b_n. În adevăr (teorema 1), avem

$(a_1\, a_2$ . .. $a_m, b_k) = (a_2\, a_3$ . .. $a_m, b_k) = (a_3$. .. $a_m, b_k) = \ldots = (a_m, b_k) = b_k$

şi apoi, punând pentru prescurtare $a_1 a_2$ ... $a_m = A$, găsim pe aceeaşi cale

$$(b_1 b_2 . . . b_n, A) = (b_2 b_3 . . . b_n, A) = (b_3 . . . b_n, A) = (b_n, A) = 1.$$

§1.3.Cel mai mare divizor comun pentru mai mult de două numere.

Problema găsirii celui mai mare divizor comun a mai mult decât două numere se reduce la aceeaşi problemă pentru două numere. Anume, pentru a găsi cel mai mare divizor comun al numerelor $a_1, a_2, .., a_n$, formăm şirul de numere

$$(a_1, a_2) = d_2, \quad (d_2, a_3) = d_3, \quad (d_3, a_4) = d_4, \ldots, (d_{n-1}, a_n) = d_n$$

Numărul d_n va fi cel mai mare divizor comun al tuturor numerelor date. În adevăr divizorii comuni ai numerelor a_1, a_2 coincid cu divizorii lui d_2; de aceea, divizorii comuni ai numerelor a_1, a_2şi a_3 coincid cu divizorii comuni ai numerelor d_2 şi a_3, adică coincid cu divizorii lui d_3. Ne convingem apoi, că divizorii comuni ai numerelor a_1, a_2, a_3 şi a_4 coincid cu divizorii lui d_4 ş.a.m.d. şi, în sfârşit, că divizorii comuni ai numerelor $a_1, a_2, \ldots, a_n$ coincid cu divizorii lui d_n. Deoarece, însă, cel mai mare divizor al lui d_n este însuşi d_n, rezultă că el va fi cel mai mare divizor comun al numerelor $a_1, a_2, .., a_n$.

§ 1.4. Numere prime

Numărul 1 are un singur divizor pozitiv, anume pe 1. Din acest punct de vedere, numărul 1 ocupă un loc special în şirul numerelor naturale.

Orice întreg mai mare decât 1 are cel puţin doi divizori, anume pe 1 şi pe el însuşi. Dacă prin aceşti divizori se epuizează toţi divizorii pozitivi ai numărului întreg considerat, atunci acest număr se numeşte *prim*. Un număr mai mare ca 1 care admite în afară de 1 şi de el însuşi şi alţi divizori pozitivi se numeşte *compus.*

a. *Cel mai mic divizor diferit de unitate al unui număr întreg mai mare decât unu este un număr prim*.

În adevăr, fie q cel mai mic divizor diferit de unitate al unui întreg $a > 1$. Dacă q ar fi fost compus, atunci el ar avea un divizor q_1,cu condiţia $1 < q_1 < q$, dar numărul a fiind divizibil prin q, ar trebui să se dividă şi prin q_1 iar aceasta contrazice ipoteza noastră asupra numărului q.

b. *Cel mai mic divizor diferit de 1 al unui număr compus a (acesta va fi prim) nu întrece* $\sqrt{a}$.

În adevăr fie q acest divizor; atunci $a = qa_1, a_1 \geq q$, de unde înmulţind şi simplificând cu a_1, obţinem $a \geq q^2$ adică $q \leq \sqrt{a}$.

c. *Mulţimea numerelor prime este infinită*

Această teoremă rezultă din faptul că, oricare ar fi numerele prime $p_1, p_2, \dots, p_k$, diferite între ele, se poate obţine un nou număr prim, ce nu este cuprins între ele. Un astfel de număr va fi un divizor prim al sumei $p_1\, p_2 \dots p_k + 1$, care odată ce divide toată suma nu poate coincide cu niciunul dintre numerele prime $p_1, p_2, \dots, p_k$.

d. Pentru formarea tabelului numerelor prime ce nu întrec un număr dat *N*, există o metodă simplă numită *Ciurul lui Eratostene*. Ea constă în următoarele:

Se scriu numerele: $1, 2, \dots, N$. (1)

Primul număr al acestui şir mai mare decât unitatea este 2. El se divide numai prin 1 şi prin el însuşi, deci este prim. Să ştergem din şirul (1) (ca fiind compuşi) toţi multiplii lui 2 cu excepţia lui 2 însuşi. Primul număr neşters care-l urmează pe 2 va fi 3; el nu se divide prin 2 (altfel ar fi fost şters), prin urmare, 3 se divide numai prin 1 şi prin el însuşi, şi deci va fi de asemenea prim. Să ştergem din şirul (1) multiplii lui 3, cu excepţia lui 3 însuşi. Primul număr neşters care urmează după 3 va fi 5; el nu se divide nici prin 2 şi nici prin 3 (altfel ar fi fost şters). Aşadar, 5 nu se divide decât prin 1 şi prin el însuşi şi deci este de asemenea prim. ş.a.m.d.

Observaţie. După ce, prin metoda indicată, au fost şterse toate numerele multiple numerelor *prime* mai mici decât numărul *prim p,* atunci toate numerele neşterse mai mici decât p^2 vor fi prime. În adevăr, orice număr compus *a,* mai mic decât p^2, a fost deja şters, fiind un multiplu al celui mai mic divizor prim al său, care este $\leq\sqrt{a} < p$. De aici rezultă :

1. *Procedând la ştergerea multiplilor unui număr prim p, trebuie să începem această operaţie cu* p^2.
2. *Formarea tabelului numerelor prime mai mici sau egale cu N este terminată, când s-au tăiat toate numerele compuse, multiplii ai numerelor prime ce nu-l întrec pe* $\sqrt{N}$.

§ 1.5. Unicitatea descompunerii în factori primi

a. Orice număr întreg a este sau prim cu un număr dat prim p sau se divide prin p.

Într-adevăr, (a, p) fiind un divizor al lui p, poate fi egal sau cu 1 sau cu p. În primul caz a este prim cu p, în al doilea caz a se divide prin p.

b. Dacă un produs de mai mulţi factori se divide prin p *atunci cel puţin unul din factori se divide prin* p.

Într-adevăr (*a.*)fiecare factor este sau prim cu *p* sau se divide prin *p.* Dacă toţi factorii ar fi fost primi cu *p*, atunci şi produsul lor ar fi fost prim cu *p*, de aceea, cel puţin unul dintre factori se divide prin *p*.

c. *Orice număr întreg, mai mare decât unitatea, se descompune într-un produs de factori primi şi această descompunere este unică, dacă facem abstracţie de ordinea factorilor.*

Într-adevăr, fie *a* un număr întreg mai mare decât unitatea. Notând cu litera *p*, cel mai mic divizor prim al său, avem $a = p_1 a_1$. Dacă $a_1 > 1$, atunci, notând cu litera p_2 cel mai mic divizor prim al său, avem $a_1 = p_2 a_2$. Dacă $a_2 > 1$, atunci, în mod analog, se găseşte $a_2 = p_3 a_3$ ş.a.m.d., atâta timp cât nu se ajunge la un a_n egal cu unitatea. Atunci $a_{n-1} = p_n$. Înmulţind toate egalităţile găsite şi efectuând simplificarea, căpătăm următoarea descompunere a lui *a* în factori primi:

$$a = p_1 p_2 \dots p_n.$$

Să admitem că pentru acelaşi *a* mai există şi o a doua descompunere în factori primi $a = q_1 q_2 \dots q_s$. Atunci $p_1 p_2 \dots p_n = q_1 q_2 \dots q_s$. Membrul al doilea al acestei egalităţi se divide prin q_1. Prin urmare (*b.*), cel puţin unul dintre factorii din primul membru trebuie să se dividă prin q_1. Să presupunem, de exemplu, că p_1 se divide prin q_1 (ordinea factorilor poate fi schimbată după voie); atunci $p_1 = q_1$ (în afară de 1, p_1 se mai divide numai prin p_1). Simplificând ambii membri ai egalităţii cu $p_1 = q_1$ avem $p_2 \dots p_n = q_2 \dots q_s$.

Repetând raţionamentul precedent aplicat la această egalitate, obţinem $p_3 \dots p_n = q_3 \dots q_s$

ş.a.m.d., până ce, în sfârşit, în unul dintre membrii egalităţii, de exemplu, în primul membru, se vor fi simplificat toţi factorii. Dar simultan trebuie să se simplifice şi toţi factorii din membrul al doilea, deoarece egalitatea $1 = q_{n+1} \dots q_s$ este imposibilă pentru $q_{n+1}, \dots, q_s$

care-l întrec pe 1.

Aşadar, cea de a doua descompunere în factori primi este identică cu prima descompunere.

d. În descompunerea numărului *a* în factori primi, unii factori se pot repeta. Notând cu literele $p_1, p_2, \dots, p_k$ factorii diferiţi între ei şi cu literele $\alpha_1, \alpha_2, \dots, \alpha_k$ multiplicităţile, cu care aceşti factori intră în *a*, obţinem aşa-zisa descompunere canonică a numărului *a* în factori $a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}$

Exemplu. Descompunerea canonică a numărului 588.000 este dată prin $588.000 = 2^5 \cdot 3 \cdot 5^3 \cdot 7^2$.

e. Fie $a = {p_1}^{\alpha_1} {p_2}^{\alpha_2} \dots {p_k}^{\alpha_k}$ - descompunerea canonică a numărului *a.* Atunci toţi divizorii lui *a* sunt toate numerele de forma $d = {p_1}^{\beta_1} {p_2}^{\beta_2} \dots {p_k}^{\beta_k}$,

$$0 \le \beta_1 \le \alpha_1, 0 \le \beta_2 \le \alpha_2, \dots, 0 \le \beta_k \le \alpha_k \qquad (1)$$

Într-adevăr, să presupunem că d divide pe a. Atunci $a = dq$ şi, prin urmare, toţi divizorii primi ai lui d intră în descompunerea canonică a lui a cu exponenţii ce nu sunt mai mici decât aceia cu care ei intră în descompunerea canonică a lui d. Din această cauză, d are forma (1). Reciproc, orice d de forma (1) îl divide pe a.

Exemplu. Toţi divizorii numărului 720 = 2^4 3^2 5 se obţin dacă vom face ca în expresia $2^{\beta_1}3^{\beta_2}5^{\beta_k}$ exponenţii $\beta_1, \beta_2, \beta_3$ să parcurgă independent unul de altul valorile β_1= 0, 1, 2, 3, 4; β_2= 0, 1, 2; β_3= 0, 1. De aceea, aceşti divizori sunt 1, 2, 4, 8, 16, 3, 6, 12, 24, 48, 9, 18, 36, 72, 144, 5, 10, 20, 40, 80, 75, 30, 60, 120, 240, 45, 90, 180, 360, 720.

§ 1.6.Divizibilitatea în monoizi comutativi cu simplificare şi în domenii de integritate

Studiul divizibilităţii într-un monoid comutativ cu simplificare sau într-un domeniu de integritate constituie o generalizare a studiului divizibilităţii în $\mathbb{N}$ sau în $\mathbb{Z}$.

Divizibilitatea şi relaţia de asociere în divizibilitate într-un monoid comutativ cu simplificare

În cele ce urmează vom considera un monoid comutativ $(A,\cdot)$ cu simplificare, adică $ax = ay \Leftrightarrow x = y$ unde $x, y, a \in A$. Reamintim că notăm cu $U(A,\cdot)$ grupul elementelor inversabile ale monoidului $(A,\cdot)$. Relaţia "/" definită în A astfel

$$a/b \Leftrightarrow \exists x \in A, b = ax$$

se numeşte relaţia de divizibilitate în A, iar dacă a/b se spune că a divide pe b sau că b se divide prin a sau că a este un divizor al lui b sau că b este un multiplu al lui a. Relaţia "$\sim$" definită pe A astfel

$$a \sim b \Leftrightarrow a/b \text{ şi } b/a$$

se numeşte relaţia de asociere în divizibilitate, iar dacă $a \sim b$ se spune că a şi b sunt asociate în divizibilitate.

Din definiţiile relaţiilor "/" şi "$\sim$" se deduce:

$$a_1/b_1 \text{ şi } a_2/b_2 \rightarrow a_1a_2 \,/\, b_1b_2 \qquad (1)$$

$$a_1 \sim a_2 \text{şi } b_1 \sim b_2 \rightarrow a_1a_2 \sim b_1b_2 \qquad (2)$$

$$a \,/\, 1 \Leftrightarrow a \in U(A,\cdot) \Leftrightarrow a \sim 1$$

1. Teoremă.

1) Relaţia de divizibilitate este o relaţie de preordine, adică este reflexivă şi tranzitivă.

2) Relaţia de asociere în divizibilitate este o relaţie de echivalenţă.

Demonstaţie.

1) Pentru $\forall\, a \in A$ avem $a = 1a$, adică a/a. Deci relaţia de divizibilitate este reflexivă. Dacă a/b şi b/c atunci $\exists\, x, y \in A$ astfel încât $b = ax$ şi $c = by$ ceea ce implică $c = a(xy)$, adică a/c. Deci relaţia "/ " este tranzitivă.

2) Din definiţia relaţiei "$\sim$" rezultă că aceasta coincide cu intersecţia dintre relaţia "$/$ " şi inversa ei.

2.Teoremă. *Dacă* $a \in A$ *şi* $\hat{a}$ *este clasa de echivalenţă a lui* a *în raport cu "*$\sim$*" atunci*

$$\hat{a} = aU(A,\cdot) = \{ax \,/\, x \in U(A,\cdot)\}, \qquad (3)$$

adică două elemente sunt asociate în divizibilitate dacă şi numai dacă ele diferă printr-un factor inversabil.

Demonstaţie. Avem a/ax, iar dacă x este inversabil, atunci $a = (ax)x^{-1}$, adică ax/a. *Deci* $a \sim ax$, adică $ax \in \hat{a}$, pentru $\forall x \in U(A,\cdot)$. Prin urmare $aU(A) \subseteq \hat{a}$.

Invers, dacă $b \in \hat{a}$, atunci $a \sim b$, adică a/b *şi* b/a ceea ce implică $\exists\, x, y \in A$ astfel încât $b = ax$ şi $a = by$. Rezultă $b = bxy$, de unde urmează $xy = 1$, deci b este de forma $b = ax$ cu x inversabil. Prin urmare $\hat{a} \subseteq aU(A,\cdot)$. Astfel (3) este demonstrată.

3. Corolare

a) Clasa de elemente asociate cu 1 *este* $\hat{1} = U(A,\cdot)$. *Deci monoidul* $(A,\cdot)$ *este grup abelian dacă şi numai dacă orice două elemente din A sunt asociate în divizibilitate, adică relaţia de asociere în divizibilitate coincide cu relaţia universală pe A.*

b) Relaţia de divizibilitate este relaţie de ordine dacă şi numai dacă singurul element inversabil în $(A,\cdot)$ *este* 1, *ceea ce are loc dacă şi numai dacă relaţia de asociere în divizibilitate coincide cu relaţia de egalitate pe A.*

Observaţie. Pentru $\forall\, a \in A$ elementele inversabile şi elementele asociate cu a sunt divizori ai lui a. Un divizor al lui a diferit de aceştia se numeşte divizor propriu.

§ 1.7. Cel mai mare divizor comun şi cel mai mic multiplu comun în monoizi.

Considerăm $(A,\cdot)$ un monoid comutativ cu simplificare.

4. Definiţie. *Fie* $a_1, \ldots, a_n \in A$ *şi* $d \in A$. *Vom spune că* d *este un cel mai mare divizor comun* $(c.m.m.d.c.)$ *al elementelor* $a_1, \ldots, a_n \in A$ *dacă în mulţimea ordonată* $(A/\sim, \leq)$ *există* $inf(\hat{a}_1, \ldots, \hat{a}_n)$ *şi* $\hat{d} = inf(\hat{a}_1, \ldots, \hat{a}_n)$ *(1)*

Dacă $inf(\hat{a}_1, \ldots, \hat{a}_n) = \hat{1}$ adică 1 este un $c.m.m.d.c.$ al elementelor $a_1, \ldots, a_n$ atunci $a_1, \ldots, a_n$ se numesc relativ prime.

Dacă identificăm fiecare clasă din $A/\sim$ cu câte un reprezentant al ei, atunci faptul că d este un $c.m.m.d.c.$ al elementelor $a_1, \ldots, a_n$ se notează cu $d = (a_1, \ldots, a_n)$.

Observaţii.

a) Dacă $d = (a_1, \ldots, a_n)$, atunci $d' = (a_1, \ldots, a_n)$ dacă şi numai dacă $d' \sim d$. Prin urmare $c.m.m.d.c.$ dacă există, este determinat numai până la o asociere în divizibilitate.

b) Caracterizând pe (1) cu ajutorul relaţiei de divizibilitate avem: $d = (a_1, \ldots, a_n) \Leftrightarrow$

i) d / a_k pentru $\forall k \in \{1,2, \ldots, n\}$ şi *ii)* d' / a_k pentru $\forall k \in \{1,2, \ldots, n\} \Rightarrow d' / d$

c) $a_1 / a_2 \Leftrightarrow (a_1, a_2) = a_1$.

d) Dacă orice două elemente din A au un $c.m.m.d.c$, atunci pentru orice $a_1, a_2, a_3 \in A$ există (a_1, a_2, a_3) şi $((a_1, a_2), a_3) = (a_1, a_2)a_3) = (a_1, (a_2, a_3))$.

e) Dacă orice două elementele din A au un $c.m.m.d.c$, atunci pentru orice $n \in \mathbb{N}^*$ şi orice $a_1, \ldots, a_n \in A$ există $(a_1, \ldots, a_n)$.

5. Teoremă. *Dacă orice două elemente din A au un* $c.m.m.d.c$, *atunci pentru orice* $a, b, c \in A$ *avem:*

$$(a, b)c = (ac, bc); \qquad (2)$$

$$(a, b) = 1 \text{ şi } (a, c) = 1 \Rightarrow (a, bc) = 1; \qquad (3)$$

$$a/bc \text{ şi } (a, b) = 1 \Rightarrow a/c. \qquad (4)$$

Demonstraţie. Din $(a, b)/a$ şi $(a, b)/b$ rezultă $(a, b)c/ac$ şi $(a, b)c/bc$. Deci $(a, b)c/(ac, bc)$, adică $\exists\, x \in A$ astfel încât $(ac, bc) = (a, b)cx$ *(5)*

de unde urmează $(a, b)cx/ac$ şi $(a, b)cx/bc$ ceea ce implică $(a, b)x/a$ şi $(a, b)x/b$, de unde rezultă $(a, b)x/(a, b)$. Prin urmare x este inversabil ceea ce împreună cu (5) ne demonstrează pe (2). Folosind egalitatea $a = (a, ac)$, relaţia (2) şi ipoteza lui (3) avem $(a, bc) = ((a, ab), bc) = (a, (ac, bc)) = (a(a, b)c) = (a, c) = 1$ ceea ce demonstrează pe (3).

Acum demonstrăm pe (4). Folosind ipoteza lui (4) şi relaţia (2) avem

$$(a, c) = (a, (a, b)c) = (a, (ac, bc)) = ((a, ac), bc) = (a, bc) = a$$

adică $(a, c) = a$ ceea ce implică a/c.

6. Corolar. *Dacă* $d = (a, b)$ *şi* $a = da', b = db'$, *atunci* $(a', b') = 1$.

7. Definiţie. *Fie* $a_1, \ldots, a_n \in A$ *şi* $m \in A$. *Vom spune că* m *este un cel mai mic multiplu comun (*$c.m.m.m.c.$*) al elementelor* $a_1, \ldots, a_n$ *dacă în mulţimea ordonată* $(A/\sim, <)$ *există* $sup(\hat{a}_1, \ldots, \hat{a}_n)$ *şi* $\hat{m} = sup(\hat{a}_1, \ldots, \hat{a}_n)$ *(6)*

Dacă identificăm fiecare clasă din $A/\sim$ cu câte un reprezentant al ei, atunci faptul că m este un $c.m.m.m.c$ al elementelor $a_1, \ldots, a_n$ se notează cu $m = [a_1, \ldots, a_n]$.

Observaţii.

a) Dacă $m = [a_1, \ldots, a_n]$, atunci $m' = [a_1, \ldots, a_n]$ dacă şi numai dacă $m' \sim m$. Prin urmare $c.m.m.m.c$, dacă există, este determinat numai până la o asociere în divizibilitate.

b) Caracterizând pe (6) cu ajutorul relaţiei de divizibilitate avem:

$m = [a_1, \ldots, a_n] \Leftrightarrow$ *i)* $a_k \mid m$ pentru $\forall k \epsilon \{1,2, \ldots, n\}$ şi

ii) $a_k \mid m'$ pentru $\forall k \epsilon \{1,2, \ldots, n\} \Rightarrow m \mid m'$

c) $a_1 \mid a_2 \Leftrightarrow [a_1, a_2] = a_2$

d) Dacă orice două elemente din A au *un* $c.m.m.m.c$, atunci pentru orice $a_1, a_2, a_3 \in A$ există $[a_1, a_2, a_3]$ şi $[[a_1, a_2], a_3] = [a_1, a_2]a_3] = [a_1, [a_2, a_3]]$.

e) Dacă orice două elemente din A au un $c.m.m.m.c$, atunci pentru orice $n \in \mathbb{N}^*$ şi orice $a_1, \ldots, a_n \in A$ există $[a_1, \ldots, a_n]$

8. **Teoremă**. *Dacă pentru orice* $a_1, a_2 \in A$ *există* (a_1, a_2) *atunci există*

$$[a_1, a_2] \text{ şi } (a_1, a_2)\,[a_1, a_2] = a_1 a_2 \qquad (7)$$

§ 1. 8. Elemente ireductibile şi elemente prime

Noţiunea de număr prim se poate defini prin oricare dintre proprietăţile:

Fie $p \in \mathbb{Z}^*, p^* \neq \pm 1$.

i) p *nu are divizori diferiţi de* ± 1 *şi* $\pm p$.

ii) $a, b \in \mathbb{Z}; p \mid ab \Rightarrow p \mid a$ *sau* $p \mid b$.

Proprietăţile i) şi ii) nu sunt echivalente în orice monoid comutativ cu simplificare. Deci într-un monoid comutativ cu simplificare $(A, \cdot)$ oarecare proprietăţile i) şi ii) ne vor conduce la două noţiuni diferite.

9. **Definiţie**. *Un element* $p \in A$ *se numeşte element ireductibil dacă verifică condiţiile:*

1) p *nu este inversabil.*

2) p *nu are divizori proprii, adică* $x \in A, x \mid p \Rightarrow x$ *inversabil sau* $x \sim p$. *Un element neinversabil din A care nu este ireductibil se numeşte reductibil.*

Observaţii.

a) Un element $p \in A$ este ireductibil dacă şi numai dacă verifică condiţia 1) din definiţia de mai sus şi oricare dintre condiţiile:

2') $p = xy \Rightarrow x$ *inversabil sau* y *inversabil*

2") $p = xy \Rightarrow x \sim p$ *sau* $y \sim p$.

2"') $\hat{p}$ *este element minimal în* $(A/\sim \setminus \{\hat{1}\}, \leq)$.

b) Dacă $p \in A$ este ireductibil, atunci orice element din A asociat cu p este ireductibil.

10. **Definiţie**. *Un element $p \in A$ se numeşte element prim dacă verifică condiţiile:*

a) p este neinversabil.

b) $x, y \in A;\ p/xy \Rightarrow p/x$ sau p/y.

Observaţii.

a) Dacă $p \in A$ este prim, atunci orice element din A asociat cu p este prim.

b) Dacă $p \in A$ este prim şi p divide produsul $x_1 \cdot \ldots \cdot x_n$ de elemente din A, atunci p divide unul dintre factorii $x_1, \ldots, x_n$.

11. **Teoremă.**

1) Orice element prim din A este ireductibil.

2) Dacă orice două elemente din A au un $c.m.m.d.c$, atunci orice element ireductibil din A este prim.

§ 1.9. Monoizi factoriali.

Considerăm $(A,\cdot)$ un monoid comutativ cu simplificare.

12. **Definiţie**. *Fie $a \in A; x_i \in A, (i = 1, \ldots, k),\ y_j \in A\ \ (j = 1, \ldots, n)$ şi*

$$a = x_1 \cdot \ldots \cdot x_k \qquad (1)$$
$$a = y_1 \cdot \ldots \cdot y_n \qquad (2)$$

două descomuneri ale lui a în factori. Descompunerile (1) şi (2) se numesc asociate dacă $k = n$ şi dacă după o eventuală renumerotare a factorilor din (2) avem $x_i \sim y_i$ pentru $i = 1, \ldots, n$.

De exemplu, dacă $1 = u_1 \ldots u_k$, atunci descompunerea *(1)* este asociată cu descompunerea $a = (u_1 x_1) \ldots (u_k x_k)$.

13. **Definiţie**. *Un monoid comutativ cu simplificare $(A,\cdot)$ se numeşte monoid (semigrup) factorial sau cu descompunere unică în factori ireductibili dacă orice $a \in A$ neinversabil se descompune în produs de elemente ireductibile şi orice două descompuneri ale lui a în produse de elemente ireductibile sunt asociate, adică a are o descompunere unică (abstracţie făcând de o asociere) în produs de elemente ireductibile.*

Exemplu:

Din teorema fundamentală a aritmeticii rezultă că $(\mathbb{N}^*,\cdot)$ şi $(\mathbb{Z}^*,\cdot)$ sunt monoizi factoriali.

14. **Teoremă**. *Dacă A este un monoid factorial, atunci:*

1) Mulţimea ordonată $(A/\sim, \leq)$ *verifică condiţia minimalităţii, adică orice submulţime nevidă a lui* $A/\sim$ *are un element minimal.*

2) Orice pereche de elemente din A are un $c.m.m.d.c.$

15. **Teoremă**. *Un monoid comutativ cu simplificare A este monoid factorial dacă şi numai dacă verifică condiţiile:*

1) Mulţimea ordonată $(A/\sim, \leq)$ *verifică condiţia minimalităţii.*

2) Orice element ireductibil din A este prim.

Observaţie. Un monoid comutativ cu simplificare A este factorial dacă şi numai dacă orice $a \in A$ neinversabil are o descompunere în produs de elemente prime.

§ 1.10. Domenii factoriale şi domenii cu ideale principale.

Vom nota cu R un domeniu de integritate. Din faptul că R este domeniu de integritate rezultă că $(R^*,\cdot)$ este un monoid comutativ cu simplificare. Noţiunile şi rezultatele anterioare, relative la divizibilitate în monoizi comutativi cu simplificare, sunt aplicabile monoidului $(R^*,\cdot)$. Relaţia de divizibilitate "/" şi relaţia de asociere în divizibilitate "$\sim$" se extind de la R^* la R. Dacă $a, b \in R$ atunci

$$a/b \iff \exists\, x \epsilon\, R,\ b = ax \qquad (1)$$

şi

$$a \sim b \iff a/b \text{ şi } b/a. \qquad (2)$$

Relaţia de divizibilitate $''/''$ este o relaţie de preordine în R, iar relaţia de asociere în divizibilitate $''\sim''$ este o relaţie de echivalenţă pe R. Elementul zero se comportă faţă de aceste relaţii astfel*:* $a/0$ pentru orice $a \in R$*;* nici un element din R^*nu divide pe *0,* deci *0* este asociat numai cu *0.* Am notat cu $\hat{a}$ clasa de elemente asociate cu a. Deci $\hat{a} = aU(R,+,\bullet)$ unde $U(R,+,\bullet)$ este grupul elementelor inversabile ale lui R.

Prin urmare R este corp dacă şi numai dacă $R/\sim\ = \{\hat{0}, R^*\}$, adică mulţimea cât $R/\sim$ este formată numai din două clase. Relaţia $''\leq''$ definită pe $R/\sim$ astfel

$$\hat{a} \leq \hat{b} \iff a/b \qquad (3)$$

este o relaţie de ordine. Din *(1)* şi *(2)* urmează că pentru orice $a, b, c \epsilon\, R$ avem

$a/b, a/c \Rightarrow a/b + c$; $a/b + c$ *şi* $a/b \Rightarrow a/c$*;*

$$a/b \iff bR \subseteq aR; \qquad (4)$$

$$a \sim b \iff aR = bR. \qquad (5)$$

Echivalenţele *(4)* şi *(5)* caracterizează relaţiile de divizibilitate şi de asociere în divizibilitate cu ajutorul idealelor principale ale lui *R*. Din *(3), (4) şi (5)* rezultă*:*

$$\hat{a} \leq \hat{b} \Leftrightarrow bR \subseteq aR; \qquad (6)$$

$$\hat{a} = \hat{b} \Leftrightarrow aR = bR. \qquad (7)$$

16. **Definiţie**. *Un domeniu de integritate* $(R, +, \bullet)$ *se numeşte domeniu (inel) factorial sau cu descompunere unică în factori ireductibili dacă monoidul* $(R^*, \cdot)$ *este factorial.*

Prin urmare, un domeniu de integritate R se numeşte factorial dacă orice element din R nenul şi neinversabil are o descompunere unică, până la o asociere, în factori ireductibili.

17. **Teoremă.** *Dacă R este un domeniu cu ideale principale, atunci:*

1) *Pentru orice* $a, b \in R$ *există* $c.m.m.d.c.$ *şi* $c.m.m.m.c.$

2) $d = (a, b) \Leftrightarrow dR = aR + bR.$

3) $m = [a, b] \Leftrightarrow mR = aR \cap bR.$

18.**Corolare**

a) Dacă R este un domeniu cu ideale principale şi $a, b, d \in R$*, atunci* $d = (a, b) \Rightarrow \exists\, u, v \in R; d = au + bv$ *şi* $(a, b) = 1 \Leftrightarrow \exists u, v \in R;\ au + bv = 1.$

b) Într-un domeniu cu ideale principale un element este ireductibil dacă şi numai dacă este prim.

19. **Teoremă**. *Orice domeniu cu ideale principale este factorial.*

20. **Teoremă**. *Dacă R este un domeniu cu ideale principale şi* $a, b \in R$ *sunt două elemente relativ prime, adică* $(a, b) = 1$*, atunci inelele*

$R/(ab)$ *şi* $[R/(a)] \times [R/(b)]$ *sunt izomorfe.*

21. **Corolare**

a) (*Teorema chineză a resturilor*)*. Dacă* $a, b \in \mathbb{Z}$ *şi* $(a, b) = 1$*, atunci pentru orice* $c, d \in \mathbb{Z}$ *sistemul de congruenţe*

$$x \equiv c\ (mod a)$$

$$x \equiv d\ (mod b) \qquad (10)$$

are o soluţie întreagă x_0*, care este unică* $\mathrm{modulo}\ ab$*, adică pentru orice soluţie* x'_0 *a lui (10) avem* $x_0 = x'_0$ *(mod ab).*

b) Dacă $m, n \in \mathbb{N}^*$ *şi* $(m, n) = 1$*, iar* φ *este funcţia lui Euler, atunci*

$$\varphi\,(mn) = \varphi\,(m)\,\varphi\,(n)\,. \qquad (11)$$

c)Dacă $m \in N, m \leq 2$ *şi* $m = p_1^{k_1} \ldots p_n^{k_n};\ k_1 \geq 1, \ldots, k_n \geq 1 \qquad (12)$

este descompunerea lui m în factori primi diferiţi, atunci

$$\varphi(m)=\prod_{i=1}^{n} p_i^{k_i}(p_i-1). \qquad (13)$$

§ 1.11. Domenii euclidiene.

22. **Definiţie.** *Se numeşte domeniu (inel) euclidian o pereche formată dintr-un domeniu de integritate R şi o funcţie $\delta: R^* \to N$ care verifică condiţia: pentru $\forall\, a\in R$ şi $\forall\, b\in R^*$ există $q,r\in R$ astfel încât $a = bq + r$, unde $r = 0$ sau $\delta(r) < \delta(b)$.*

Exemple:

a) Din teorema împărţirii cu rest în $\mathbb{Z}$ rezultă că $\mathbb{Z}$ împreună cu funcţia

$\delta: \mathbb{Z} \to \mathbb{N}$, $\delta(n) = |n|$ este un domeniu euclidian.

b) Fie K un corp comutativ. Domeniul de integritate $K[X]$ împreună cu funcţia

$\delta: K[X]^* \to \mathbb{N}$, $\delta(f) = grad\, f$ este un domeniu euclidian.

23. **Teoremă**. *Dacă (R,δ) este un domeniu euclidian, atunci R este un domeniu cu ideale principale.*

Demonstraţie. Fie U un ideal al lui R. Dacă $U = \{0\}$, atunci $U = (0)$, adică U este principal. Dacă $U \neq \{0\}$, atunci fie $a \neq 0$ unul din elementele lui U care verifică condiţia $\delta(a) \leq \delta(x)$, pentru orice $x \in U^*$ *(1)*

Pentru orice $x \in U$ există $q,r \in R$ astfel încât $x = aq + r$, cu $r = 0$ sau $\delta(r) < \delta(a)$. *(2)*

De aici şi din $a,x \in U$, folosind ipoteza că U este ideal, rezultă $r = x - aq \in U$, ceea ce (conform lui (1) şi (2)) implică $r = 0$. Acum din (2) deducem $x = aq \in aR = (a)$. Deci $U \subseteq (a)$, iar din $a \in U$ urmează $(a) \subseteq U$. Astfel am arătat că $U = (a)$, adică U este un ideal principal.

24. **Corolare.**

a) Dacă (R, δ) este un domeniu euclidian, atunci R este un domeniu factorial.

b) Domeniile de integritate $\mathbb{Z}$ şi $K[X]$, unde K este un corp comutativ, sunt cu ideale principale, deci sunt factoriale.

Dacă (R,δ) este un domeniu euclidian, atunci pentru $\forall\, a,b\in R$ există $c.m.m.d.c.$ Acum vom prezenta un procedeu, numit *algoritmul lui Euclid,* de determinare a $c.m.m.d.c.$ a două elemente într-un inel euclidian. Dacă unul dintre elementele $a,b\in R$ este nul, atunci celălalt este $c.m.m.d.c.$ al lor. Dacă $a \neq 0$ şi $b \neq 0$, atunci există q_1 , $r_1\in R$ astfel încât $a = bq_1 + r_1$, unde $r_1 = 0$ sau $\delta(r_1) < \delta(b)$. Dacă $r_1 \neq 0$, atunci există q_2 , $r_2\in R$ astfel încât $b = r_1 q_2 + r_2$ unde $r_2 = 0$ sau $\delta(r_1) < \delta(r_2)$. Continuând acest procedeu dacă restul $r_2 \neq 0$

se obţine şirul descrescător de numere naturale $\delta(r_1) < \delta(r_2) > \ldots$. Rezultă că după un număr finit de paşi se obţine un rest nul, adică avem un şir de relaţii de forma:

$$a = bq_1 + r_1$$

$$b = r_1 q_2 + r_2$$

$$r_1 = r_2 q_3 + r_3 \qquad (3)$$

$$\vdots$$

$$r_{n-2} = r_{n-1} q_n + r_n$$

$$r_{n-1} = r_n q_{n-1}$$

unde $r_i \neq 0; i = 1, \ldots, n.$

25. Teoremă. *Dacă* (R, δ) *este un domeniu euclidian şi* $a, b \in R^*$, *atunci elementul* r_n *din relaţiile (3) este* $c.m.m.d.c.$ *al elementelor* a *şi* b.

Observaţie. Dacă (R, S) este un domeniu euclidian şi d este $c.m.m.d.c.$ al lui a şi b, atunci cu algoritmul lui Euclid se pot determina elementele $u, v \in R$ pentru care are loc relaţia din corolarul anterior adică $d = au + bv$.

§ 1 . 12. Divizibilitatea în $R[X]$.

Vom studia divizibilitaţea în $R[X]$, unde R este un domeniu de integritate. $R[X]$ este domeniu de integritate, iar elementele inversabile din $R[X]$ coincid cu elementele din R inversabile în R. Prin urmare două polinoame $f, g \in R[X]$ sunt asociate în divizibilitate dacă şi numai dacă există un element $a \in R^*$, inversabil în R astfel încât $f = ag$.

Observaţii.

a) Dacă $b \in R$ şi $f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n \in R[X]$, atunci $b/f \Leftrightarrow b/a_i$ pentru $i = 0, \ldots, n.$

b) Dacă $a \in R^*$ este ireductibil în R, atunci a este ireductibil şi în $R[X]$.

26. **Teoremă**. *Dacă* R *este un domeniu de integritate şi* $p \in R^*$ *este prim în* R, *atunci* p *este prim şi în* $R[X]$.

Demonstraţie. Dacă $f = a_0 + a_1X + a_2X^2 + \ldots + a_nX^n$,

$g = b_0 + b_1X + b_2X^2 + \ldots + b_mX^m \in R[X]$ şi p nu divide nici pe f nici pe g, atunci există coeficienţi ai lui f şi coeficienţi ai lui g care nu se divid cu p. Fie a_k şi b_l, coeficienţii, cu cei mai mici indici, care nu se divid cu p. Coeficientul $c_{k+l} = a_0b_{k+l} + a_1b_{k+l-1} + \cdots + a_kb_l + \cdots + a_{k+l}b_0$ al produsului fg nu se divide cu p deoarece termenul a_kb_l , din suma de mai sus

nu se divide cu p (întrucât p este prim) şi ceilalţi termeni se divid cu p. *Deci* fg nu se divide cu p.

27. **Definiţie**. *Fie R un domeniu factorial. Un polinom* $\varphi \epsilon\ R[X]$ *se numeşte primitiv dacă cel mai mare divizor comun al coeficienţilor săi este* 1.

Un polinom asociat cu un polinom primitiv este primitiv. Un polinom de gradul zero este primitiv dacă şi numai dacă este inversabil. Dacă K este un corp comutativ, atunci orice polinom nenul din $K[X]$ este primitiv. Dacă R este un domeniu factorial, $f \epsilon$ R[X], $f \neq 0$ şi a este cel mai mare divizor comun al coeficienţilor lui f, atunci

$$f = a\varphi \qquad (1)$$

unde (p este un polinom primitiv). O reprezentare de forma (1) a lui f se numeşte *canonică.*

Observaţie. Polinomul primitiv φ şi elementul $a \epsilon R$ din (1) sunt unic determinate până la o asociere.

28. **Lema lui Gauss**. *Dacă R este un domeniu factorial, atunci produsul a două polinoame primitive din* $R[X]$ *este un polinom primitiv.*

*Demonstraţie.*Fie φ_1, $\varphi_2 \epsilon R[X]$ polinoame primitive şi $\varphi = \varphi_1\ \varphi_2$. Dacă φ nu ar fi primitiv, atunci ar exista un divizor d neinversabil al coeficienţilor lui φ. Domeniul R fiind factorial d se descompune în factori ireductibili, iar dacă p este unul dintre aceşti factori, atunci p este prim şi $p/\varphi_1\ \varphi_2$. Rezultă că p/φ_1 sau p/φ_2 ceea ce constituie o contradicţie.

29. **Corolare**.

a) Dacă $f_1, f_2 \epsilon\ R[X]$ *şi* $f_1 = a_1\varphi_1$, $f_2 = a_2\varphi_2$ *sunt reprezentări canonice ale lui* f_1 *şi* f_2 *, iar* $a = a_1a_2$, $\varphi = \varphi_1\ \varphi_2$ *atunci* $f_1\ f_2 = a\ \varphi$ *este o reprezentare canonică a lui* $f_1\ f_2$ *.*

b) Dacă $a_1, a_2 \epsilon\ R^*$, *iar* $\varphi_1\ , \varphi_2 \epsilon R[X]$ *sunt polinoame primitive, atunci* $a_1\varphi_1 / a_2\varphi_2 \Leftrightarrow a_1/a_2$ *şi* φ_1/φ_2*Dacă* $f \epsilon R[X]$, *atunci notăm cu* $c(f)$*cel mai mare divizor comun al coeficienţilor lui* f *. Deci* $c(f_1\ f_2) == c(f_1)c(f_2)$.

30. **Teoremă.** *Fie R un domeniu factorial şi K corpul fracţiilor lui R. Dacă* $f \epsilon R[X]$, $gradf \leq 1$ *şi* f *este ireductibil în* $R[X]$, *atunci* f *este ireductibil în* $K[X]$.

Demonstraţie. Din ipoteza că f este ireductibil în $R[X]$ rezultă că f este primitiv în $R[X]$. Dacă $f = q_1\ q_2$ *(2)*

unde $q_1\ , q_2 \epsilon C[X]$ şi $b_i \epsilon R, (i = 1{,}2)$ este un multiplu comun al numitorilor coeficienţilor lui q_i , atunci putem scrie

$$\begin{aligned} q_1 &= a_1/b_1\ \cdot \varphi_1 \\ q_2 &= a_2/b_2\ \cdot \varphi_2\ , \end{aligned} \qquad (3)$$

unde $a_1, a_2 \epsilon\ R$ şi y_1, y_2 sunt polinoame primitive din $R[X]$. Din *(2) şi (3)* rezultă că în $R[X]$ avem: $b_1b_2f = a_1a_2\varphi_1\ \varphi_2$.

Întrucât f şi $\varphi_1\ \varphi_2$ sunt polinoame primitive, urmează că f este asociat în $R[X]$ cu $\varphi_1\ \varphi_2$. Acum, din ipoteza că f este ireductibil în $R[X]$ rezultă că φ_1, sau φ_2 este inversabil în $R[X]$, adică $\varphi_1 \epsilon\ U(R,+,\bullet)$ sau $\varphi_2\ \epsilon\ U(R,+,\bullet)$.*Deci* $q_1 \epsilon K^*$sau $q_2 \epsilon K^*$. Astfel am arătat că f este ireductibil în $K[X]$.

31. **Corolare**.

a) Un polinom $f \epsilon R[X]$ este ireductibil în $R[X]$ dacă şi numai dacă f este primitiv în $R[X]$ şi f este ireductibil în $K[X]$.

b) Un polinom $f \epsilon \mathbb{Z}[X]$ este ireductibil în $\mathbb{Z}[X]$ dacă şi numai dacă f este primitiv în $\mathbb{Z}[X]$ şi f este ireductibil în $\mathbb{Q}[X]$.

Într-adevăr, $\mathbb{Q}$ fiind corpul fracţiilor lui $\mathbb{Z}$, această afirmaţie rezultă din *a)*.

32. **Teoremă**. *Dacă R este un domeniu factorial, atunci $R[X]$ este un domeniu factorial.*

Acum vom arăta că există domenii factoriale care nu sunt cu ideale principale, adică clasa domeniilor cu ideale principale este strict inclusă în clasa domeniilor factoriale.

33. **Teoremă**. *Dacă R este domeniu de integritate şi R nu este corp, atunci $R[X]$ are ideale care nu sunt principale.*

Demonstraţie. Întâi arătăm că dacă $b \epsilon\ R^*$şi (b,x) este idealul generat de $\{b,X\}$, atunci $(b,X) = R[X] \Rightarrow \exists\, b^{-1} \epsilon\, R, bb^{-1} = 1.$ *(7)*

Într-adevăr, din ipoteza lui *(7)* rezultă că $bg + Xh = 1$ cu $g,h \epsilon\, R[X]$ ceea ce implică $bb_0 = 1$ unde $b_0$este termenul liber al lui g. Astfel implicaţia *(7)* este demonstrată.

Întrucât domeniul de integritate R nu este corp rezultă că există $a \epsilon\ R^*$ neinversabil. Presupunem că idealul (a,X) este principal, adică $(a,X) = (f)$ cu $f \epsilon\, R[X]$ de unde urmează f/a şi f/X . Din f/a rezultă $f \epsilon\, R$ ceea ce împreună cu f/X implică f inversabil (deoarece X este ireductibil). Deci $(a,X) = R[X]$ ceea ce conform lui *(7)* este o contradicţie. Prin urmare idealul (a,X) nu este principal.

CAPITOLUL 2

LEMA CHINEZĂ A RESTURILOR

În acest capitol prezentăm noțiuni de aritmetică modulară, lema chineză a resturilor precum și aplicații ale ei cum ar fi proprietatea de multiplicitate a funcţiei φ a lui Euler,algoritmul lui Garner, o metodă de înmulțire a numerelor mari, algoritmul de criptare RSA.

§2.1. Congruenţe. Noţiuni fundamentale.

a. Vom studia acum numerele întregi legându-ne de resturile împărţirii lor printr-un număr întreg pozitiv *m,* pe care-l vom numi *modul.*

Fiecărui număr întreg îi corespunde un rest determinat rezultat din împărţirea lui prin *m*. Dacă la două numere întregi *a* şi *b* corespund unul şi acelaşi rest *r*, atunci ele se zic *de acelaşi rest* faţă de modulul *m* sau congruenţe *modulo m*.

b. Congruenţa numerelor *a* şi *b*, modulo *m*, se scrie astfel:

$$a \equiv b(mod\ m),$$

şi se citeşte *a* congruent cu *b* modulo *m.*

c. Congruenţa numerelor a şi b modulo m este echivalentă cu:

1. *Posibilitatea reprezentării lui a sub forma* $a = b + mt$*, unde t este un număr întreg*

2. *Divizibilitatea lui* $a - b$ *prin m.*

În adevăr, din $a \equiv b(mod\ m)$, rezultă

$$a = mq + r, b = mq1\ + r, 0 \leq r < m,$$

de unde

$$a - b = m(q - \ q_1), a = b + mt, t = q\ - \ q_1$$

Reciproc, din $a = b + mt$, reprezentând *b* sub forma

$$b = \ mq_1 + r, 0 \leq r < m,$$

deducem

$$a = mq + r;\ q = q_1\ + t,$$

adică

$$a \equiv b(mod\ m).$$

Deci afirmaţia 1. este adevărată.

Din 1 rezultă nemijlocit afirmaţia 2.

§2.2. Proprietăţile congruenţelor, asemănătoare cu proprietăţile egalităţilor

a. Două numere congruente cu un al treilea număr, sunt congruente între ele

Rezultă din a,§ 2.1.

b. Congruenţele se pot aduna membru cu membru.

În adevăr, fie

$$a_1 \equiv b_1(mod\ m), a_2 \equiv b_2\ (mod\ m), \ldots, a_k \equiv b_k\ (mod\ m), \qquad (1)$$

Atunci (1,e,§1.1).

$$a_1 = b_1 + mt_1, a_2 = b_2 + mt_2, \ldots, a_k = b_k + mt_k\ , \qquad (2)$$

de unde

$$a_1 + a_2 + \ldots + a_k = b_1 + b_2 + \ldots + b_k + m(t_1 + t_2 + \ldots + t_k),$$

sau

$$a_1 + a_2 + \ldots + a_k = b_1 + b_2 + \ldots + b_k(mod\ m)$$

Un termen aflat într-un membru oarecare al unei congruenţe se poate trece în celălalt membru, schimbându-se semnul.

În adevăr, adunând congruenţa $a + b = c(mod\ m)$ cu congruenţa evidentă $-b \equiv -b(mod\ m)$, obţinem $a \equiv c - b(mod\ m)$.

Se poate aduna (sau scădea) la fiecare membru al unei congruenţe orice multiplu al modulului.

În adevăr, adunând congruenţa $a \equiv b(mod\ m)$ cu congruenţa evidentă $mk \equiv 0(mod\ m)$, se obţine $a + mk \equiv b(mod\ m)$.

c. Congruenţele se pot înmulţi membru cu membru.

În adevăr, să considerăm din nou congruenţele (1) şi egalităţile (2) care rezultă din ele. Înmulţind membru cu membru egalităţile (2), obţinem

$$a_1\ a_2 \ldots\ a_k = b_1\ b_2 \ldots\ b_k + mN,$$

unde *N*- este un număr întreg. Prin urmare

$$a_1\, a_2 \ldots\ a_k = b_1\, b_2 \ldots\ b_k\ (mod\ m).$$

Putem ridica ambii membrii ai unei congruenţe la o aceeaşi putere.

Aceasta rezultă din afirmaţia precedentă.

Se pot înmulţi ambii membri ai unei congruenţe cu un acelaţi număr întreg.

În adevăr, înmulţind congruenţa $a \equiv b(mod\ m)$ cu congruenţa evidentă $k \equiv k(mod\ m)$, obţinem $ak \equiv bk(mod\ m)$.

d. Proprietăţile b. şi c. (adunarea şi înmulţirea congruenţelor) se generalizează prin următoarea teoremă.

Dacă în expresia unei funcţii raţionale întregi cu coeficienţi întregi

$S = \sum A_{\alpha_1 \ldots \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k}$ *înlocuim* $A_{\alpha_1 \ldots \alpha_k}$ *,*$x_1, \ldots, x_k$ *prin numerele* $B_{\alpha_1 \ldots \alpha_k}$ *,*$y, \ldots, y_k$ *, congruente cu cele precedente modulo* m*, atunci noua expresie a lui* S *va fi congruentă modulo* m *cu cea precedentă.*

În adevăr, din

$$A_{\alpha_1 \ldots \alpha_k} \equiv B_{\alpha_1 \ldots \alpha_k}\ (mod\ m),$$

$$x_1\ \equiv\ y_1\ (mod\ m), \ldots\ x_k\ \equiv\ y_k\ (mod\ m)$$

găsim (c)

$$x_1^{\alpha_1} \equiv y_1^{\alpha_1}\ (mod\ m), \ldots\ , x_k^{\alpha_k} \equiv y_k^{\alpha_k} (mod\ m),$$

$$A_{\alpha_1 \ldots \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv\ B_{\alpha_1 \ldots \alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k}\ (mod\ m).$$

de unde sumând , obţinem

$$\sum A_{\alpha_1 \ldots \alpha_k} x_1^{\alpha_1} \ldots x_k^{\alpha_k} \equiv \sum B_{\alpha_1 \ldots \alpha_k} y_1^{\alpha_1} \ldots y_k^{\alpha_k}\ (mod\ m).$$

Dacă avem:

$$a \equiv b(mod\ m),\ a_1 \equiv b_1(mod\ m),\ \ldots .\ ,\ a_n \equiv b_n(mod\ m),\ x \equiv x_1(mod\ m),$$

atunci

$$ax^{\mathrm{n}} + a_1 x^{n-1}\ + \ldots + a_n \equiv\ bx^{\mathrm{n}} + b_1 x^{n-1}\ + \ldots + b_n(mod\ m)$$

Această afirmaţie este un caz particular al celei precedente.

e. Ambii membri ai unei congruenţe se pot împărţi prin divizorul lor comun, dacă acesta din urmă este prim cu modulul.

În adevăr, din $a \equiv b(mod\ m), a = a_1 d\ , b = b_1 d\ , (d\ , m) = 1$ rezultă că diferenţa $a - b$, egală cu $(a_1 - b_1)d$ se divide prin m. De aceea $(a_1 - b_1)$ se divide prin m, adică $a_1 \equiv b_1(mod\ m)$.

§2.3.Alte proprietăţi ale congruenţelor.

a. A*mbii membrii ai unei congruenţe şi modulul se pot înmulţi cu un acelaşi număr întreg.*

Într-adevăr, din $a \equiv b(mod\ m)$ rezultă $a = b + mt,\ ak = bk + mkt$ şi prin urmare $ak \equiv bk(mod\ mk)$

b. Ambii membri ai unei congruenţe şi modulul se pot împărţi prin oricare dintre divizorii lor comuni.

Într-adevăr, fie $a \equiv b(mod\ m),\quad a = a_1 d,\quad b = b_1 d,\quad m = m_1 d.$

Avem: $a = b + mt,\ a_1 d = b_1 d + m_1 dt,\ a_1 = b_1 m_1 t$ şi prin urmare, $a_1 = b_1(mod\ m_1)$.

c. Dacă congruenţa $a \equiv b$ are loc în raport cu mai mulţi moduli, atunci ea are loc şi în raport cu modulul egal cu cel mai mic multiplu comun al acestor moduli.

Într-adevăr, din $a \equiv b\ (mod\ m_1),\ a \equiv b\ (mod\ m_2), \dots ,\ a \equiv b\ (mod\ m_k),$ rezultă că diferenţa $a - b$ se divide prin toţi modulii $m_1, m_2, \dots, m_k$. De aceea ea trebuie să se dividă şi prin cel mai mic multiplu comun al acestor moduli, adică $a \equiv b\ (mod\ m)$.

d. Dacă congruenţa are loc în raport cu modulul m, atunci ea are loc şi în raport cu modulul d, egal cu un divizor oarecare al numărului m.

Într-adevăr, din $a \equiv b\ (mod\ m)$ rezultă că diferenţa $a - b$ trebuie să se dividă prin m; de aceea ea trebuie să se dividă şi prin orice divizor d al numărului m, adică $a \equiv b(mod\ d)$.

e. Dacă un membru al unei congruenţe şi modulul se divid printr-un număr oarecare, atunci şi celălalt membru al congruenţei trebuie să se dividă prin acelaşi număr.

Într-adevăr, din $a \equiv b\ (mod\ m)$ rezultă $a = b + mt$; dacă a şi m sunt multiplii lui d, atunci şi b trebuie să fie un multiplu al lui d, ceea ce s-a şi afirmat.

f. Dacă avem $a \equiv b\ (mod\ m)$, *atunci* $(a, m) = (b, m)$.

Într-adevăr, această egalitate rezultă nemijlocit din $a = b + mt$.

§2.4. Sistem complet de reziduuri.

a. Numerele de acelaşi rest sau, ceea ce este acelaşi lucru, congruenţe $modulo\ m$, formează *clasa de resturi* $modulo\ m$.

Din această definiţie rezultă că tuturor numerelor clasei le corespunde un acelaşi rest r şi că vom obţine toate numerele clasei dacă vom face ca numărul q să parcurgă, în expresia $mq + r$, toate numerele întregi. Corespunzător celor m valori diferite ale lui r, avem m clase de numere modulo m.

b. Orice număr al clasei se numeşte reziduu $modulo\ m$ în raport cu toate numerele din aceiaşi clasă. Reziduul obţinut pentru $q = 0$, egal cu însuşi restul r , se numeşte *cel mai mic reziduu care nu este negativ.*

Reziduul q, cel mai mic în valoare absolută, se numeşte *reziduu absolut minim*.

Este evident că pentru $r < \frac{m}{2}$, avem $q = r$; pentru $r > \frac{m}{2}$, avem $q = r - m$; în sfârşit dacă m este par şi $r = \frac{m}{2}$ atunci drept q se poate lua oricare dintre următoarele două numere $\frac{m}{2}$ şi $\frac{m}{2} - m = -\frac{m}{2}$.

Luând din fiecare clasă câte un reziduu, se obţine *sistemul complet de reziduuri* $modulo\ m$

De cele mai multe ori drept sistem complet de reziduuri se folosesc reziduuri minime ce nu sunt negative $0,1,\dots,m-1$ sau, de asemenea, reziduuri absolut minime. După cum rezultă din cele de mai sus, acestea din urmă se reprezintă, în cazul lui m impar, prin şirul

$$-\frac{m-1}{2}, \dots, -1, 0, 1, \dots, \frac{m-1}{2}$$

iar în cazul lui m par, prin oricare dintre şirurile

$$-\frac{m}{2}+1, \dots, -1, 0\ , 1, \dots, \frac{m}{2}$$

$$-\frac{m}{2}, \dots, -1, 0\ , 1, \dots, \frac{m}{2}-1$$

c. m *numere arbitrare, necongruente două câte două modulo* m*, formează un sistem complet de reziduuri în raport cu acel modul.*

Într-adevăr, nefiind congruente, aceste numere aparţin la clase diferite, şi deoarece numărul lor este m, adică egal cu numărul claselor, rezultă că în fiecare clasă se va găsi cu siguranţă un număr.

d. *Dacă* $(a, m) = 1$ *şi dacă* x *parcurge sistemul complet de reziduuri* $modulo\ m$*, atunci* $ax + b$ *unde* b *este un număr întreg arbitrar, parcurge de asemenea sistemul complet de reziduuri* $modulo\ m$.

Într-adevăr, vom avea tot atâtea numere $ax + b$ ca şi numere x, adică m în conformitate cu c., nu ne mai rămâne decât să arătăm că oricare două numere $ax_1 + b$ şi $ax_2 + b$ care corespund la x_1 şi x_2 necongruente, sunt ele însele necongruente $modulo\ m$.

Admiţând însă că $ax_1 + b \equiv ax_2 + b\ (mod\ m)$ ajungem la congruenţa $ax_1 \equiv ax_2\ (mod\ m)$, de unde, deoarece $(a, m) = 1$, obţinem $x_1 \equiv x_2$ (mod m) ceea ce cotrazice ipoteza că numerele x_1 şi x_2 nu sunt congruente.

§ 2.5. Sistem redus de reziduuri.

a. Numerele din aceeaşi clasă *modulo m* au cu acest modul acelaşi divizor comun.

Sunt în special importante clasele, pentru care acest divizor este egal cu unitatea, adică clasele care conţin numere prime cu modulul.

Luând din fiecare clasă de acest fel câte un reziduu, se obţine sistemul redus de reziduuri *modulo m*. Sistemul redus de reziduuri se poate deci forma din numerele sistemului complet, prime cu modulul. De obicei, sistemul redus de reziduuri se separă din sistemul de reziduuri minime ce nu sunt negative: $0, 1 \ldots, m - 1$. Deoarece printre aceste numere, numărul numerelor prime cu m este egal cu $\varphi(m)$, rezultă că numărul numerelor sistemului redus, ca şi numărul claselor care conţin numerele prime cu modulul este $\varphi(m)$.

Exemplu: Sistemul redus de reziduuri modulo 42 este:

1, 5, 11, 13, 17, 19, 23, 25, 29, 31, 37, 41.

b. Orice $\varphi(m)$ a numerelor necongruente $modulo\ m$ două câte două şi prime cu modulul, formează un sistem redus de reziduuri $modulo\ m$.

În adevăr, fiind necongruente şi prime cu modulul, aceste numere aparţin unor clase diferite care conţin numere prime cu modulul, şi cum acestea sunt în număr de $\varphi(m)$ adică tot atâtea ca şi clasele de tipul indicat, rezultă că în fiecare clasă se va găsi cu siguranţă câte un număr.

c. Dacă $(a, m) = 1$ şi x parcurge sistemul redus de reziduuri $modulo\ m$, atunci $a \cdot x$ parcurge de asemenea sistemul redus de reziduuri $modulo\ m$.

Într-adevăr, numărul numerelor $a \cdot x$ va fi egal cu numărul numerelor x, adică egal cu $\varphi(m)$. În conformitate cu b, ne mai rămâne deci să arătăm că numerele ax sunt necongruente $modulo\ m$ şi prime cu modulul. Prima afirmaţie este însă demonstrată în *d, §3.* 4 pentru numere de forma mai generală $ax + b$, iar cea de-a doua rezultă din

$$(a, m) = 1, (x, m) = 1.$$

§ 2.6. Teoremele lui Euler şi Fermat.

a. Pentru $m > 1$ *şi* $(a, m) = 1$ *avem (***teorema lui Euler***):*

$$a^{\varphi(m)} \equiv 1 \ (mod \ \text{m}).$$

Într-adevăr, dacă x parcurge sistemul redus de reziduuri $x = r_1, r_2, \dots, r_c$; $c = \varphi(m)$,

format din reziduuri minime ce nu sunt negative, atunci reziduurile minime nenegative $\rho_1, \rho_2, \dots, \rho_c$; ale numerelor $a \cdot x$ vor parcurge acelaşi sistem, dispus însă, în general, într-o altă ordine (c, § 2.5).

Înmulţind membru cu membru congruenţele

$$ar_1 = \rho_1 \ (mod \ m), ar_2 = \rho_2 \ (mod \ m), \dots, ar_c = \rho_c \ (mod \ m),$$

obţinem

$$a^c r_1 r_2 \dots r_c \equiv \rho_1 \rho_2 \dots \rho_c (mod \ m)$$

de unde, împărţind ambii membri prin produsul $r_1 r_2 \dots r_c = \rho_1 \rho_2 \dots \rho_c$ obţinem

$$a^c = 1 \ (\text{mod } m).$$

b. Pentru p *prim şi* a *nedivizibil cu* p*, avem (***teorema lui Fermat***):*

$$a^{p-1} \equiv 1 \ (mod \ p). \qquad (1)$$

Această teoremă este o consecinţă a teoremei *a*. pentru $m = p$. Ultimei teoreme i se poate da o formă mai convenabilă. Anume, înmulţind ambii membri ai congruenţei (1) prin a, obţinem congruenţa

$$a^p \equiv a \ (mod \ p)$$

adevărată pentru toţi a întregi, ea fiind adevărată şi pentru a multiplu de p.

§ 2.7. Lema chineză a resturilor

Ideea fundamentală a aritmeticii modulare este studiul unor probleme referitoare la numere întregi cu ajutorul resturilor acestora în raport cu unul sau mai multe numere naturale, $m_1, m_2, \dots, m_r > 1$ numite module.

Un rezultat central în aritmetica modulară este *lema chinezească a resturilor* care raportează numerele întregi la un sistem finit de numere naturale $m_1, m_2, \dots, m_r > 1$ astfel încât

$$(m_i, m_j) = 1 \text{ pentru } i \neq j$$

Lema 1. Fie $m_1, m_2, ..., m_r \in \mathbb{Z}$ astfel încât $(m_i, m_j) = 1$ pentru $i \neq j$. Pentru $a \in \mathbb{Z}$ avem :

1) $(m_i, a) = 1, 1 \leq i \leq r \Longrightarrow (m_1, m_2, \ldots, m_r, a) = 1$;

2) $m_i \mid a, 1 \leq i \leq r \Longrightarrow m_1, m_2, \ldots, m_r \mid a$.

Demonstraţie. 1) Fie $d = (m_1 m_2 \ldots m_r, a)$. Dacă $d \neq 1$ atunci există $p \in \mathbb{Z}$ prim astfel încât $p \mid d$. Din $p \mid d$ şi $d \mid m_1 m_2 \ldots m_r$, rezultă că $p \mid m_1 m_2 \ldots m_r$. Cum p este prim, există i astfel încît $p \mid m_i$. Dar avem şi $p \mid a$, deci p divide pe $(m_i, a) = 1$ (contradicţie !).

2) Afirmaţia este adevărată pentru $r = 1$. Fie $r > 1$ şi facem ipoteza că 2) este adevărată pentru $r - 1$. Cum $(m_i, m_r) = 1$, $1 \leq i \leq r - 1$, din 1) rezultă că

$$(m_1 m_2 \ldots m_{r-1}, m_r) = 1.$$

Fie $h, k \in \mathbb{Z}$ astfel încât $m_1 m_2 \ldots m_{r-1} \; h + m_r \, k = 1$. Conform ipotezei inducţiei, $m_1 m_2 \ldots m_{r-1} \mid a$. Dar $a = m_1 m_2 \ldots m_{r-1} \, ha + m_r \, ka$.

Şi cum avem încă $m_r \mid a$, rezultă că $m_1 m_2 \ldots m_r$ divide fiecare termen din membrul al doilea al ultimei egalităţi şi atunci $m_1 m_2 \ldots m_r$ divide şi membrul întâi, deci pe a.

2. Lema chinezească a resturilor. *Fie* $m_1, m_2, ..., m_r \in \mathbb{N}$ *mai mari decât* 1 *astfel încât* $(m_i, m_j) = 1$ pentru $i \neq j$. *Atunci, oricare ar fi* $u, a_1, a_2, \ldots, a_n \in \mathbb{Z}$ *există* $a \in \mathbb{Z}$ *unic determinat astfel încât* $a \equiv a_i (\mathrm{mod}\, m_i)$, $u \leq a < u + m$, unde $m = m_1 m_2 \ldots m_r$.

Demonstraţie. Fie $a, a' \in \mathbb{Z}$ astfel încât $u \leq a < u + m$, $u \leq a' < u + m$, $a \equiv a_i (\mathrm{mod}\, m_i), a' \equiv a_i (\mathrm{mod}\, m_i)$. Atunci $|a - a'| < m$ şi $a \equiv a' \, (\mathrm{mod}\, m_i)$, $1 \leq i \leq r$. Deci $m_i \mid a - a'$ pentru $i = 1, 2, \ldots, r$ şi din lema 1 rezultă că $m \mid a - a'$. Dar atunci $|a - a'| < m$ şi $m \mid a - a'$ implică $a = a'$. Am demonstrat astfel partea de unicitate din enunţul lemei.

Să notăm cu F mulţimea tuturor sistemelor ordonate de r numere naturale

$$(d_1, d_2, \ldots, d_r), \quad 0 \leq d_i < m_i, 1 \leq i \leq r.$$

Este clar că F are m elemente. Tot din m constă şi mulţimea E a numerelor naturale a astfel încât $u \leq a < u + m$. Reamintim că am convenit să notăm cu $a \bmod m_i$ restul împărţirii prin m_i a numărului întreg a, deci $0 \leq a \bmod m_i < m_i, 1 \leq i \leq r$.

Fie funcţia: $p : E \to F, \; p(a) = (a \bmod m_1, a \bmod m_2, \ldots, a \bmod m_r)$,

Oricare ar fi $a \in E$. Conform primei părţi a demonstraţiei, funcţia p este injectivă. Din

$\mathrm{card}\, E = \mathrm{card}\, F = m$ rezultă că p este surjectivă, deci p este bijecţie.

Fie $d_i = a_i \bmod m_i$, $1 \leq i \leq r$. Cum p este aplicaţie surjectivă, există $a \in E$ astfel încât

$a \bmod m_i = d_i, 1 \leq i \leq r$.

Aşadar, $a \bmod m_i = a_i \bmod m_i, 1 \leq i \leq r$.

Deci a şi a_i au acelaşi rest la împărţirea prin m_i , $1 \leq i \leq r$, de unde $a = a_i \, mod \, m_i$.

3. Corolar

Dacă $m_1, m_2, \ldots, m_r \in \mathbb{N}$ *mai mari decât* 1 *astfel încât* $(m_i, m_j) = 1$ *pentru* $i \neq j$, *atunci sistemul de congruenţe*

$$X - a_1 \equiv 0 \ (\mathrm{mod}\, m_1),$$

$$X - a_2 \equiv 0 \ (\mathrm{mod}\, m_2),$$

$$\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots$$

$$X - a_r \equiv 0 \ (\mathrm{mod}\, m_r),$$

admite o soluţie $a \in \mathbb{Z}$ *şi numai una, astfel încât* $u \leq a < u + m$, *oricare ar fi* $u \in \mathbb{Z}$, *unde* $m = m_1 m_2 \ldots m_r$.

Observaţie. Demonstraţia părţii de existenţă din lema chinezească a resturilor este neconstructivistă. Iată o demonstraţie care oferă o metodă de calcul al numărului $a \in \mathbb{Z}$ astfel încât $a = a_i \, mod \, m_i$, $1 \leq i \leq r$.

Fie $q_i = \frac{m}{m_1} = m_1 \ldots m_{i-1} m_{i+1} \ldots m_r, \quad 1 \leq i \leq r,$

Deoarece $(m_i, m_j) = 1$ pentru $i \neq j$, rezultă că $(m_i, q_i) = 1, \quad 1 \leq i \leq r.$ Aplicând teorema lui Euler, obţinem $q_i^{\varphi(m_i)} = 1 (mod \, m_i), \quad 1 \leq i \leq r.$ Cum $q_i \equiv 0 (mod \, m_j)$ pentru $i \neq j$, avem încă

$q_i^{\varphi(m_i)} = 0 (mod \, m_i), \ i \neq j.$ Aşadar, $e_i \equiv 1 (mod \, m_i)$, $1 \leq i \leq r$ şi $e_i \equiv 0 (mod \, m_i)$, pentru $i \neq j$.

Fie $b = a_1 e_1 + a_2 e_2 + \cdots + a_r e_r$.

Avem $b - a_i = a_i (e_i - 1) + \sum_{i \neq j} a_i e_j \equiv 0 (mod \, m_i), 1 \leq i \leq r,$

de unde

$$b \equiv a_i (mod \, m_i), 1 \leq i \leq r.$$

Luând $a = u + (b - u) mod \, m$, este clar că $u \leq a < u + m$ şi $a = a_i \, mod \, m_i$,

De exemplu, fie $m_1 = 2$, $m_2 = 3$, $m_3 = 5$, $a_1 = -4$, $a_2 = 8$, $a_3 = -1$ *şi* $u = 0$. Să determinăm prin metoda prezentată la observaţia de mai sus numărul întreg a, astfel încât $a = a_i \, mod \, m_i$, $1 \leq i \leq 3$. Avem

$$m = m_1 m_2 m_3 = 30$$

$$q_1 = 3 \times 5 = 15, \qquad q_2 = 2 \times 5 = 10, \quad q_3 = 2 \times 3 = 6$$

$e_1 = q_1^{\varphi(m_1)} = 15^{\varphi(2)} = 15,$

$e_2 = q_2^{\varphi(m_2)} = 10^{\varphi(3)} = 10^2 = 100$,

$e_3 = q_3^{\varphi(m_3)} = 10^{\varphi(5)} = 6^4 = 1296$,

şi deci

$$b = a_1e_1 + a_2e_2 + a_3e_3 = (-4) \cdot 15 + 8 \cdot 100 + (-1) \cdot 1296 = -556,$$

De unde $a = u + (b - u) mod\ m = (-556) mod\ 30 = 14$ pentru că $-556 = 30 \cdot (-19) + 14$.

Avem

$14 \equiv -4(mod\ 2)$, $14 \equiv 8(mod\ 3)$ şi $14 \equiv -1(mod\ 5)$. Dacă luăm $u = 18$, atunci $b - u = -556 - 18 = -574$ şi cum $-556 = 30 \cdot (-20) + 26$ avem

$$a = 18 + 26 = 44.$$

Deci $44 \equiv -4(mod\ 2), 44 \equiv 8(mod\ 3), 44 \equiv -1(mod\ 5)$.

Utilizarea lemei chinezeşti pentru determinarea lui *a* în accepţiunea de la observaţia precedentă presupune că avem o metodă de calcul a lui $\boldsymbol{\varphi}$(m), unde m este un număr natural.

4. **Propoziţie**. *Fie m un număr natural astfel încât $m = m_1\ m_2\ \dots\ m_r$, $(m_i, m_j) = 1$ pentru $i \neq j$. Atunci* $\boldsymbol{\varphi}(m) = \prod_{i=1}^{r} \varphi(m_i)$.

În particular, dacă m =$p_1^{e_1} p_2^{e_2} \dots p_r^{e_r}$, $e_i \geq 1$, este descompunerea în factori primi distincţi ($p_i \neq p_j$ pentru $i \neq j$) a lui m, atunci

$$\boldsymbol{\varphi}(m) = \prod_{i=1}^{r} p_i^{e_i} \left(1 - \frac{1}{p_i}\right) = m \prod_{i=1}^{r} \left(1 - \frac{1}{p_i}\right).$$

Demonstraţie. Pentru $u = 0$, lema chinezească a resturilor arată că aplicaţia $p : E \to F$, $p\ (a) = (a\ mod\ m_1, a\ mod\ m_2, \dots, a\ mod\ m_r)$, stabileşte o corespondenţă bijectivă între mulţimea E a numerelor întregi din intervalul $[0, m)$ şi mulţimea F a sistemelor de numere întregi $(d_1\ , d_2, \dots, d_r)$, $0 \leq d_i < m_i\ , 1 \leq i \leq r$.

Din lema 1. rezultă că $(a, m) = 1 \Leftrightarrow (a, m_1\ ) = 1\ , 1 \leq i \leq r$.

Pentru orice $i = 1,2, \dots, r$ există $b_i \epsilon \mathbb{Z}$ astfel încât $a = m_i\ b_i + a\ mod\ m_i$, de unde $(a, m_i) = 1 \Leftrightarrow (a\ mod\ m_i, m_i) = 1$.

Este clar că p stabileşte o corespondenţă bijectivă între numerele $a \epsilon E$ cu proprietatea $(a, m) = 1$ şi sistemele de numere $(d_1\ , d_2, \dots, d_r) \epsilon\ F$ cu proprietatea $(d_i\ , m_i\ ) = 1,\ 1 \leq i \leq r$. Cum numărul unor asemenea sisteme este evident $\varphi_{(m_1)} \varphi_{(m_2)} \dots \varphi_{(m_r)}$, deducem că $\varphi_{(m)} = \varphi_{(m_1)} \varphi_{(m_2)} \cdots \varphi_{(m_r)}$.

Deoarece pentru $p_i \neq p_j$ pentru $i \neq j$, avem $\left(p_i, p_j\ \right) = 1$ şi aplicând Lema 1 obţinem $(p_i^{e_i}, p_j^{e_j}) = 1$ pentru $i \neq j$. Întrucât $\varphi_{\left(p_i^{e_i}\right)} = p_i^{e_i} - p_i^{e_i - 1}$ ultima afirmaţie din enunţul propoziţiei este evidentă.

§ 2.8. Aplicaţii ale lemei chineze a resturilor (LCR)

A1. Proprietatea de multiplicitate a funcţiei φ a lui Euler.

Fie daţi modulii: $m_1, m_2, ..., m_t \geq 2$ $(t \geq 2)$ cu $m_i \perp m_j$ pentru $i \neq j$. Notăm:

$$M = m_1 m_2 ... m_t .$$

Cum inelele $\left(\mathbb{Z}_{m_i}, +, \cdot\right)$ sunt unitare ($i = 1, 2, ..., t$), atunci şi inelul produs $P := \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2} \times ... \times \mathbb{Z}_{m_t}$ este unitar şi $U(P) = U\left(\mathbb{Z}_{m_1}\right) \times U\left(\mathbb{Z}_{m_2}\right) \times ... \times U\left(\mathbb{Z}_{m_t}\right)$ (rezultat valabil pentru orice produs finit de inele unitare), deci $\left|U(P)\right| = \varphi(m_1)\varphi(m_2)...\varphi(m_t)$.

Deoarece $\mathbb{Z}_M \cong P$, avem $\left|U(P)\right| = \left|U\left(\mathbb{Z}_M\right)\right| = \varphi(M) = \varphi(m_1, m_2, ..., m_t)$. În concluzie, are loc următorul rezultat: *Dacă* $m_1, m_2, ..., m_t \geq 2$ *sunt numere întregi* $(t \geq 2)$ *şi dacă* $m_i \perp m_j$ *pentru* $i \neq j$, *atunci* $\varphi(m_1 m_2 ... m_t) = \varphi(m_1)\varphi(m_2)...\varphi(m_t)$.

Rezultatul de mai sus se numeşte *proprietatea de multiplicitate* a funcţiei φ.

- Dacă p=prim şi $n \in \mathbb{N}^*$,atunci din definiţia lui P rezultă că $\varphi\left(p^n\right) = p^n - p^{n-1} = p^n\left(1 - \frac{1}{p}\right)$.
- Dacă $n \in \mathbb{N} - \{0,1\}$ este număr compus şi dacă $n = p_1^{n_1} p_2^{n_2} ... p_t^{n_t}$ $\left(t \geq 2;\ p_1 < ... < p_t \text{ numere prime; } n_1, n_2, ..., n_t \in \mathbb{N}^*\right)$, atunci rezultă din multiplicitatea lui φ:

$$\varphi(n) = \varphi\left(p_1^{n_1}\right)\varphi\left(p_2^{n_2}\right)...\varphi\left(p_t^{n_t}\right) = p_1^{n_1} p_2^{n_2} ... p_t^{n_t}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_t}\right) =$$

$$= n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)...\left(1 - \frac{1}{p_t}\right).$$

De exemplu $\varphi(72) = \varphi\left(2^3 \cdot 3^2\right) = 72\left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 24$ = numărul de clase inversabile din inelul $\mathbb{Z}_{72}$.

A2. Algoritmul lui Garner

Fie daţi modulii: $m_1, m_2, ..., m_t \geq 2$ $(t \geq 2)$, cu $m_i \perp m_j$ *pentru* $i \neq j$. Pentru $j = 2,3,...,t$ şi $i = 1,2,..., j-1$, fie $c_{ij} \in \mathbb{R}_{m_j}$ inversul lui m_i modulo m_j:

$c_{ij} m_i \equiv 1 \left(\mathrm{mod}\, m_j\right)$ pentru $i = 1,2,..., j-1$.

INPUT: Se dau numerele $b_i \in \mathbb{R}_{m_i}$ $(i = 1,2,...,t)$

OUTPUT: Se determină numărul întreg *a* cu proprietăţile:

i) $0 \leq a < m_1 m_2 ... m_t =: M$;

ii) $a \bmod m_i = b_i$ $(i = 1,2,...,t)$.

Algoritmul lui Garner:

- Pas iniţial: $r_1 := b_1$
- Pas curent: pentru $i = 1,2, \dots, t-1$ luăm $r_{i+1} := \left(b_{i+1} \prod_{k=1}^{i} c_{k,i+1} - \sum_{l=1}^{i} r_l \prod_{k=l}^{i} c_{k,i+1}\right) \mathrm{mod} m_{i+1}$.
- Pas final: $a = r_1 + r_2 m_1 + r_3 m_1 m_2 + ... + r_t m_1 m_2 ... m_{t-1}$

Afirmaţia 1: *Avem* $0 \leq a < M$ *şi a=întreg.*

Demonstraţie: Ţinem cont de faptul că $r_i + 1 \leq m_i$ $(i = 1,2,...,t)$. Atunci

$$\begin{aligned} M &\geq m_1 m_2 ... m_{t-1} r_t + m_1 m_2 ... m_{t-1} \\ &\geq m_1 m_2 ... m_{t-1} r_t + m_1 m_2 ... m_{t-2} r_{t-1} + m_1 m_2 ... m_{t-2} \\ &\quad \dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots\dots \\ &\geq m_1 m_2 ... m_{t-1} r_t + m_1 m_2 ... m_{t-2} r_{t-1} + ... + m_1 r_2 ... m_1 \\ &> a \geq 0, \text{ deci } a = \text{întreg şi } 0 \leq a < M \end{aligned}$$

Afirmaţia 2: *Au loc relaţiile:* $a \bmod m_i = b_i$ *(*$i = 1,2,...,t$*).*

Demonstraţie: Avem: $a \equiv r_1 \equiv b_1 \left(\mathrm{mod}\, m_1\right)$, deci $a \bmod m_i = b_i$ (deoarece $b_1 \in \mathbb{R}_{m_1}$). Pentru fiecare $i = 2,3,...,t$ avem:

$$
\begin{aligned}
a &\equiv r_1 + r_2 m_1 + r_3 m_1 m_2 + \ldots + r_i m_1 m_2 \ldots m_{i-1} \\
&\equiv r_1 + r_2 m_1 + r_3 m_1 m_2 + \ldots + r_{i-1} m_1 m_2 \ldots m_{i-2} \\
&+ \left(b_i \prod_{k=1}^{i-1} c_{ki} - \sum_{l=1}^{i-1} r_l \prod_{k=l}^{i-1} c_{ki} \right) m_1 m_2 \ldots m_{i-1} \\
&\equiv r_1 + r_2 m_1 + r_3 m_1 m_2 + \ldots + r_{i-1} m_1 m_2 \ldots m_{i-2} \\
&+ b_i - r_1 - r_2 m_1 - r_3 m_1 m_2 - \ldots - r_{i-1} m_1 m_2 \ldots m_{i-2} \\
&\equiv b_i \left(\operatorname{mod} m_i \right)
\end{aligned}
,
$$

deci $a \bmod m_i = b_i$ (deoarece $b_i \in \mathbb{R}_{m_i}$).

Fie acum daţi întregii $a_1, a_2, \ldots, a_t$. Punem $b_i := a_i \bmod m_i$ ($i = 1, 2, \ldots, t$). Pentru $b_i \in \mathbb{R}_{m_i}$ ($i = 1, 2, \ldots, t$), algoritmul lui Garner furnizează întregul $a = r_1 + r_2 m_1 + \ldots + r_t m_1 m_2 \ldots m_{t-1}$, cu proprietăţile: $0 \le a < M$ şi $a \bmod m_i = b_i$ ($i = 1, 2, \ldots, t$). Acum

$$a \bmod m_i = b_i = a_i \bmod m_i, \text{ deci}$$

$$a \equiv a_i \left(\operatorname{mod} m_i \right)$$

pentru orice $i = 1, 2, \ldots, t$. Prin urmare, *a* este soluţie a sistemului de congruenţe

$$
\begin{cases}
x \equiv a_1 \left(\operatorname{mod} m_1 \right), \\
x \equiv a_2 \left(\operatorname{mod} m_2 \right), \\
\ldots\ldots\ldots\ldots\ldots\ldots \\
x \equiv a_t \left(\operatorname{mod} m_t \right)
\end{cases}
$$

şi $0 \le a < M$. Întregul *a* este un unic cu aceste proprietăţi (adică, (i) de a fi soluţie a sistemului de congruenţe şi (ii) de a aparţine mulţimii $[0, M) \cap \mathbb{Z}$). Evident, *a* este soluţie a LCR.

A3. O metodă de înmulţire a numerelor naturale mari.

Fie daţi modulii: $m_1, m_2, \ldots, m_t \ge 2$ $(t \ge 2)$, cu $m_i \perp m_j$ *pentru* $i \ne j$.

Pentru un număr întreg pozitiv *a*, numim *reprezentare modulară* relativă la modulii daţi t-uplul:

$$\rho(a) := (a \bmod m_1, \ldots, a \bmod m_t).$$

Fie acum *a* şi *b* două numere naturale mari. Dacă $\rho(a)=(a_1,a_2,...,a_t)$ şi $\rho(b)=(b_1,b_2,...,b_t)$ atunci din LCR obţinem:

$$\begin{aligned}\rho(a\cdot b)&=((a_1\cdot b_1)\bmod m_1,...,(a_t\cdot b_t)\bmod m_t)\\&=(c_1\bmod m_1,...,c_t\bmod m_t)\end{aligned}$$

unde $c=ab$ şi $c_1=c\bmod m_i$ $(i=1,2,...,t)$.

Ipoteză de lucru: Presupunem că $a,b\in[0,M)$ şi $c=ab\in[0,M)$, unde $M:=m_1m_2...m_t$.

Urmăm acum următorul algoritm:

Pas 1: calculăm $a_i:=a\bmod m_i$ şi $b_i:=b\bmod m_i$ pentru $i=1,2,...,t$.

Pas 2: calculăm $p_i:=a_i\cdot b_i$ pentru $i=1,2,...,t$.

Pas 3: calculăm $c_i:=p_i\bmod m_i$ pentru $i=1,2,...,t$.

Pas 4: aplicăm algoritmul lui Garner pentru $c_1,c_2,...,c_t$ cu $c_i\in\mathbb{R}_{m_i}$ $(i=1,2,...,t)$ şi obţinem întregul *c* cu proprietăţile $0\le c<M$ şi $c\bmod m_i=c_i$ $(i=1,2,...,t)$. Atunci, $a\cdot b=c$.

Observaţie. În cazul special $a<\sqrt{M}$ şi $b<\sqrt{M}$, atunci $ab<M$, deci ipoteza de lucru devine un fapt.

Exemplu. Fie modulii m_1=7, m_2=9 şi m_3=10. Atunci M=$m_1m_2m_3$=630 şi $\sqrt{M}=25$, … .

Fie *a*=16 şi *b*=24. Atunci $ab<M$. Găsim: $\rho(a)=(2,7,6)$şi $\rho(b)=(3,6,4)$;

$$\begin{aligned}p_1&=2\cdot3=6\\p_2&=7\cdot6=42,\\p_1&=6\cdot4=24\end{aligned}$$

c_1=6, c_2=6, c_3=4, unde $c_i=p_i\bmod m_i$ $(i=1,2,3)$

Aplicăm algoritmul lui Garner pentru $\rho(c)=(6,6,4)$:

- c_{12}=4, c_{13}=3, c_{23}=9;
- r_1=6

$$r_2 = \left(6 \prod_{k=1}^{1} c_{k2} - \sum_{l=1}^{1} rl \prod_{k=l}^{1} c_{k2} \right) \bmod m_2 .$$
$$= (6 \cdot 4 - 6 \cdot 4) \bmod 9 = 0$$

$$r_3 = \left(4 \prod_{k=1}^{2} c_{k3} - \sum_{l=1}^{2} rl \prod_{k=l}^{2} c_{k3} \right) \bmod m_3$$
$$= (4 \cdot 3 \cdot 9 - 6 \cdot 3 \cdot 9 - 0 \cdot 9) \bmod 10 = 6$$

deci $c = 6 + 0 \cdot 7 + 6 \cdot 7 \cdot 9 = 6 + 6 \cdot 63 = 384$.

A4. Criptografia cu chei publice (asimetrică)

La criptografia cu chei simetrice, pentru un criptanalist care cunoaşte metoda de criptare nu există mari dificultăţi în procesul de decriptare deoarece cheile de criptare şi decriptare coincid. Există criptosisteme în care metoda de criptare poate fi făcută publică. Aceasta înseamnă că şi criptanalistul cunoaşte metoda de criptare şi, totuşi, el nu este în măsură să decripteze criptotextul. Aceasta este cunoscută sub numele de criptografie cu chei publice (metoda de criptare poate fi făcută publică).

O astfel de idee simplă a fost luată în considerare târziu - la mijlocul anilor '70 deoarece teoria complexităţii calculului s-a dezvoltat abia în acea perioadă de timp. Această teoria dă informaţii privind complexitatea diferitelor calcule, de pildă privind timpul de calcul necesar pentru o anumită operaţie atunci când se folosesc cele mai bune calculatoare. O astfel de informaţie este foarte importantă în criptografie.

Deşi metoda de criptare este făcută publică, criptarea se poate face în siguranţă, deoarece unui criptanalist îi vor fi necesari zeci, poate sute de ani pentru a decripta mesajul cifrat.

Cifrarea se poate face într-o singură direcţie ("sens unic"). Deşi este uşor de mers în această direcţie, totuşi este imposibil de urmat direcţia opusă: decriptarea. Pentru exemplificare să considerăm cartea de telefon dintr-un mare oraş. Este foarte uşor să stabilim numărul de telefon al unei persoane precizate. Pe de altă parte, este foarte greu (chiar imposibil) de stabilit persoana care are un număr de telefon specificat.

Criptarea Rivest-Shamir-Adleman (RSA)

Cel mai larg utilizat şi verificat criptosistem cu chei publice a fost cel introdus de R. Rivest, A. Shamir şi L. Adleman, care este acum cunoscut ca RSA.

Acest cifru reprezintă standardul în domeniul semnăturilor digitale şi al confidenţialităţii cu chei publice. RSA este astăzi recunoscută ca cea mai sigură metodă de cifrare şi autentificare disponibilă comercial.

Acestă metodă de criptare se bazează pe o idee foarte simplă din teoria numerelor şi a rezistat la toate atacurile criptanaliştilor de până acum. Ideea se bazează pe faptul că, deşi este

uşor să înmulţeşti două numere prime mari, este însă extrem de greu să se reconstituie numerele din produsul lor. Astfel, produsul poate fi făcut public şi poate fi utilizat ca o cheie de criptare.

Iată în ce constă sistemul de criptare RSA.

Fie p şi q două numere prime mari distincte şi aleatoare (având aproximativ 100 cifre fiecare). Se notează :

$n = p \times q$ şi $\Phi(n) = (p-1)(q-1)$, unde Φ este funcţia Euler. Se alege un număr aleator mare $E > 1$ astfel încât $\big(E, \Phi(n)\big) = 1, 1 < E < \Phi(n)$ şi se calculează numărul D, care să satisfacă congruenţa:

$$ED = 1(mod\Phi(n)).$$

Numărul n este modulul, E este exponentul de criptare şi D exponentul de decriptare. Numerele n şi E formează cheia publică de criptare, iar $p, q, \Phi(n)$ şi D sunt secrete.

Metoda de criptare implică calcul exponenţial într-un câmp finit - *modulo n*. Mesajul cifrat se obţine din mesajul în clar printr-o transformare. Mesajul în clar este împărţit în blocuri care care sunt de fapt numere întregi între 0 şi numărul natural *n*. O mărime obişnuită pentru *n* este de 309 cifre zecimale ($n < 2^{1024}$). Fie unul din aceste blocuri din mesaj *M*, bloc ce are proprietatea $M \in (0, n-1)$; proprietate care se obţine din modul de împărţire a mesajului. Blocul cifrat, *C*, corespunzător blocului în clar, se obţine calculând:

$C = M^E (mod\ n)$, *E* reprezentând astfel cheia de criptare.

Decriptarea se face prin operaţia :

$M = C^D (mod\ n)$, unde *D* este cheia secretă de decriptare.

Cele două chei *E* şi *D* trebuie să satisfacă relaţia:

$M = C^D (mod\ n) = M^{ED} (mod\ n)$, pentru ca algoritmul să poată fi într-adevăr folosit.

Fundamentarea algorimului RSA este realizată de următoarea teoremă:

Teoremă. Fie *p* și *q* numere prime impare și *n*=*pq*. Se consideră $c \in \mathbb{N}$ cu $1 < c < \varphi(n)$ astfel încât c este relativ prim cu $\varphi(n)$. Fie d inversul multiplicativ al lui c modulo m. Atunci pentru orice $x \in \{0,1,...,n\}$ avem

$$x^{cd} \equiv x(modn).$$

Demonstrație. E suficient să tratăm cazul $x \geq 1$.

Deoarece c este relativ prim cu $\varphi(n)$, există conform Lemei lui Bézout inversul multiplicativ d al lui c modulo m. Fie $k \in \mathsf{N}$ astfel încât

$$cd = k\varphi(n)+1.$$

Tratăm două cazuri : întâi cazul în care x și n sunt relativ prime, apoi cazul contrar.

Cazul I. $(x,n)=1$

Conform Teoremei lui Euler,

$$x^{\varphi(n)} \equiv 1(mod n).$$

Atunci $x^{k\varphi(n)} \equiv 1(mod n)$, de unde $x^{cd} \equiv x \ (mod n)$.

Cazul II. $(x,n)>1$

Din $n=pq$, unde p și q sunt prime și $(x,n)>1$ rezultă $p|x$ sau $q|x$. Vom analiza primul caz, celălalt fiind analog.

Presupunem $p|x$. Nu avem $q|x$, altfel ar rezulta $n|x$, fals. Atunci $(x,q)=1$ și conform Teoremei lui Euler,

$$x^{\varphi(q)} \equiv 1(mod q).$$

Avem $\varphi(n)=\varphi(p)\varphi(q)$, unde $\varphi(p)=(p-1)$ si $\varphi(q)=(q-1)$.

Din congruența precedentă deducem $x^{\varphi(p)\varphi(q)} \equiv 1(mod q)$, de unde

$$x^{k\varphi(n)} \equiv 1(mod q).$$

Fie $j \in \mathbb{N}$ astfel încât $x^{k\varphi(n)} = 1 + jq$. Atunci $x^{cd} = x^{k\varphi(n)+1} = x + xjq$. Cum $p|x$, există $h \in \mathbb{N}$ astfel încât $x = ph$. Rezultă $xjq = pqjh = njh$, deci $n|xjq$. Din $x^{cd} = x + xjq$ și relația precedentă obținem $x^{cd} \equiv x \ (mod n)$, q.e.d.

Corolar. *Fie p, q, n, c și d ca în enunțul teoremei precedente și fie T un număr natural. Dacă $T \equiv M^c \ (mod n)$, atunci $T^d \equiv M \ (mod n)$.*

Securitatea algoritmului se bazează pe ideea de dificultate a factorizării unui număr mare. Pornind de la această idee numărul *n* se poate obţine prin produsul a două numere prime mari *p* şi *q*: *n=pq,* dar aflarea lui *p* şi *q* şi astfel a indicatorului lui Euler $\Phi(n) = (p-1)(q-1)$, devine mult mai greu de determinat având la dispoziţie *n*.

Folosind această metodă se poate obţine un sistem performant de cifrare cu cheie publică.

Algoritmul RSA

Generarea cheilor

1. Selectăm *p,q* (ambele prime, $p \neq q$)
2. Calculăm $n = p \times q$

3. Calculăm $\Phi(n) = (p-1)(q-1)$
4. Selectăm un întreg *E* astfel încât $(E, \Phi(n)) = 1, 1 < E < \Phi(n)$
5. Calculăm *D*, $D \equiv E^{-1}(mod\Phi(n))$
   Cheia publică PU= $\{E, n\}$
   Cheia privată PR= $\{D, n\}$

Criptarea

1. Textul clar $M < n$
2. Textul cifrat $C = M^E(mod\ n)$

Decriptarea

1. Textul cifrat *C*
2. Textul clar $M = C^D(mod\ n)$

Exemplu

Vom utiliza un cifru cu *p=47* şi *q=79.* Calculăm *n=pq=47×79=3713*. Indicatorul lui Euler pentru 3713 este $\Phi(3713) = 46 \times 78 = 3588$. Alegem *D=47. E* este inversul lui *D* modulo $\Phi(n)$.

E va fi *37* pentru a satisface relaţia: $ED\ mod(\Phi(n)) = 1, E = [(p-1)(q-1)+1]/D$. Astfel, pentru a coda mesajul *A sosit timpul* vom coda mai întâi fiecare literă a alfabetului. De exemplu: $A = 00, B = 01, \ldots, Y = 25, blanc = 26$.

Mesajul va deveni: $M = 0018\ 1418\ 0819\ 1908\ 1215\ 2011$. În continuare vom coda fiecare bloc de 4 cifre:

$$0018^E\ mod(n) = 00\ 1\ 837\ mod\ (3713) = 3091$$

$$1418^E mod(n) = 141837\ mod\ (3713) = 0943$$

$$0819^E\ mod(n) = 08\ 1\ 937\ mod\ (3713) = 3366$$

$$1908^E\ mod(n) = 190837\ mod\ (3713) = 2545$$

$$1215^E\ mod(n) = 121537\ mod\ (3713) = 0107$$

$$2011^E\ mod(n) = 201137\ mod\ (3713) = 2965.$$

Astfel mesajul cifrat devine: 3091 0943 3366 2545 0107 2965.

La decriptare se vor calcula pe rând:

$$3091^E\ mod(n) = 3\ 091^{37}\ mod(3713) = 0018$$

$$0943^E\ mod(n) = 08\ 1\ 9^{37} mod(3713) = 1418\ , \ldots\ ,$$

obţinând mesajul iniţial.

Algoritmul RSA utilizând LCR

Complexitatea decriptării RSA: $M = C^D(mod\ n)$ depinde direct de mărimea lui *D* şi a lui *N.* Exponentul *D* specifică numărul înmulţirilor modulare necesare pentru a ridica la putere

pe *C* şi modulul *n* determină mărimea rezultatelor intermediare. O modalitate de a reduce amploarea calculelor (mărimea lui *D* şi a lui *n*) este să ţinem seama de LCR de Mica teoremă a lui Fermat şi de o consecinţă directă a lor.

Teoremă. Dacă numărul întreg *a* nu este divizibil cu numărul întreg *p*-prim şi dacă

$$m \equiv n(\mathrm{mod}(p-1)) \Rightarrow a^n \equiv a^m(\mathrm{mod}p).$$

Această proprietate prevede că atunci când se lucrează modulo *p*-prim exponenţii pot fi reduşi $\mathrm{mod}(p-1)$. Acest lucru permite aplicarea algoritmului RSA folosind exponenţi semnificativ mai mici.

Decriptarea RSA utilizând LCR

Cum *p* şi *q* sunt prime, orice mesaj $M < n = p \times q$ este unic reprezentat de o pereche $[M_p, M_q]$, unde $M_p = M\ modp$ şi $M_q = M\ modq$. Mergând înapoi este mai uşor să obţinem *M* plecând de la numerele M_p, M_q, recombinându-le conform LCR, decât să folosim calculul $M = C^D(mod\ n)$. Prin utilizarea teoremei anterioare mărimea exponentului poate fi micşorată:

$M_p = M\ modp = (C^D mod\ n) modp = C^D modp$, deoarece $n = p \times q$. Mai mult $M_p = C^D mod(p-1) modp = C^{D_p} modp$, unde $D_p = Dmod(p-1)$. Analog $M_q = C^{D_q} modq$, unde $D_q = Dmod(q-1)$. În plus este uşor să observăm că mesajul cifrat *C* poate fi redus *modulo p*

înainte să calculăm M_p astfel lungimea operanzilor este redusă la jumătate. Cu cantităţile $C_p = C\ modp$ şi $C_q = C\ modq$ precum şi $D_p = Dmod(p-1)$ şi $D_q = Dmod(q-1)$ obţinem următoarele ecuaţii pentru M_p şi M_q: $M_p = C_p^{D_p}$ şi $M_q = C_q^{D_q}$.

Recombinarea lui M_p şi M_q pentru a obţine *M* se poate face conform LCR (pentru cazul $r = 2, m_1 = p, m_2 = q, m_1 m_2 = n = pq$). Mai mult decât atât calculele pot fi simplificate folosind Mica teoremă a lui Fermat:

$$\begin{aligned} M &= \left(M_p q(q^{-1} modp) + M_q p(p^{-1} modq)\right) modn \\ &= \left(M_p q(q^{p-2} modp) + M_q p(p^{q-2} modq)\right) modn \\ &= \left(M_p q(q^{p-1} modn) + M_q p(p^{q-1} modn)\right) modn \end{aligned}$$

Ultima egalitate provine din faptul că $a(bmodc) = (ab) mod(ac)$ pentru orice întregi nenegativi *a, b, c.* Ţinând cont că numerele $q^{p-1} modn$ şi $p^{q-1} modn$ sunt constante care pot fi precalculate, efortul de a recombina pe M_p şi M_q se reduce la două înmulţiri, o adunare şi o reducere *modulo n.* Calculăm $D_p = Dmod(p-1)$ şi $D_q = Dmod(q-1)$ care sunt necesari pentru recombinare şi $R_p = q^{p-1} modn$ şi $R_q = p^{q-1} modn$. Descrierea algoritmului RSA bazat pe LCR urmează următorii paşi:

1. Calculăm $C_p = C\ modp$ şi $C_q = C\ modq$.

2. Calculăm ridicările la putere $M_p = C_p^{D_p}$ şi $M_q = C_q^{D_q}$.
3. Calculăm coeficienţii $S_p = M_p R_p mod n$ şi $S_q = M_q R_q mod n$.
4. Calculăm $M = S_p + S_q$. Dacă $M \geq N$ calculăm $M := M - n$.

Algoritmul RSA utilizând LCR

1. Se dă mesajul *M.*
2. Se generează două numere prime între ele *p* şi *q*.
3. Se generează altă pereche de numere prime între ele *r* şi *s*.
4. Calculăm $n_1 = p \times q$.
5. Calculăm $n_2 = r \times s$.
6. Calculăm $\Phi_1 = (p-1)(q-1)$.
7. Calculăm $\Phi_2 = (r-1)(s-1)$.
8. Alegem e_1 astfel încât $1 < e_1 < \Phi_1$.
9. Alegem e_2 astfel încât $1 < e_2 < \Phi_2$.
10. Calculăm $d_1 = e_1^{-1} mod n_1$.
11. Calculăm $d_2 = e_2^{-1} mod n_2$.
12. Calculăm $t_1 = M mod n_1$.
13. Calculăm $t_2 = M mod n_2$.
14. Calculăm $y_1 = t_1^{e_1} mod n_1$.
15. Calculăm $y_2 = t_2^{e_2} mod n_2$.
16. Calculăm $a_1 = e_1^{-1} mod \Phi_1$.
17. Calculăm $a_2 = e_2^{-1} mod \Phi_2$.
18. Calculăm $b_1 = y_1^{a_1} mod n_1$.
19. Calculăm $b_2 = y_2^{a_2} mod n_2$.
20. Calculăm $f_1 = n_2^{-1} mod n_1$.
21. Calculăm $f_2 = n_1^{-1} mod n_2$.
22. Calculăm textul decodat $:= (b_1 \times n_2 \times f_1 + b_2 \times n_1 \times f_2) mod (n_1 \times n_2)$

Exemplu:

RSA fără LCR:

Textul clar (mesajul) :

364896564397011459724575230981320914472256689895283825736949671285945813416 96354706942814918 028461206078760419576264857826027092284914144780780178579 00999 65423415 165889627382848 490753196984483917921633 499173120483 80078921 81747 53482 435328041525968282689242448449908738367668775 6808250983298803378 215978241

Parametrii:

p=185078731400523062481441254377509455858583223247383377301344032467716615 3 94479165221010471 497948050956111729853739380662796534622032 53151628946347 4827 17349

q= 267555006214761824762350436240537518607679569699244254264924128354994854 9184532461156126642 1 975797211492947350804792680468942874570562 6 6805599795 4 53 1542783

n=4951874113008718246563764877823638477518291215696772123899429545707005362 90488450866636581 9163500270335 03520590165042451118 4728309504566139572183882 5 182 3817839618063383606331270868007199994101569204 79487110084 83131 97724 919863707 3 5178070440539339199488467331442197836969759922 86 90575040 50 3478 80295 257008984 2267

e =166955546873566405943

d=4113058132856990303207440829066756506737095935954805946015541770529275590 73441034057405225 5918347096676607455245438811889962163002823482 32642438569 71990 4468489402895376177381421241309 4692969677271378725699884 9857 09621 77 7443 073 31 5399832348842073472460444033155410993038278439491275547 53980703 4565431437 7543 097679

textul cifrat=4309806803004551571243529055103100691323093015616266228665 1969 2906 4983995171381743267074751119067424973487974548364196871115298821065461274668804847007286378034497802029030654067734912563568110 9104060 1916581 35442139 3941 3336518829979873903310013049936429396863299883 76690102899 270 227169 76434999 12469270040942711

textul decodat=364896564397011459724575230981320914472256689895283825736949671285945813416 96354706942814918 028461206078 760419576264857 826027092284914144780780178 57 9009 9965423415165889627382848490753196984483917 921633499173120483800789 0781 21 81 7475 348243532804152596828268924244844990873836766877568080250983 2988033 7 8215978241

RSA cu LCR:

Textul clar (mesajul) :

364896564397011459724575230981320914472256689895283825736949671285945813416 96354706942814918 028461206078 760419576264857 826027092284914144780780178 57 9009 9965423415165889627382848490753196984483917 921633499173120483800789 0781 21 81 7475 348243532804152596828268924244844990873836766877568080250983 2988033 7 8215978241

parametrii

p_1=203348092836732871144754439029953931368958698425634084429005176394229065 4950381705923948545984096870 220858090292091 881478338552738709 3734816832 86 26 66 480269

q_1=157359281576092611565867637602884304688976658191836251649407081811490132 15784181187471504 24785332 3491608819 7505642518979 25339269785978664 223 4625 356471 61271

n_1=319987097986568688516561467991940619925600055005148881200357523095545717 69302577500433622 37989030204552 162015402276191935720512262556353914281078058111 16634815181018825355744072757982 7123790533 4307486422998 505959999596325 41585 350821751456199914270271858756998786627316066437388090312299 39 3766 40 36029 734 982461899

e_1=96793620484551651428704035909150537691415559822529992641932845825398014868657604537299035 91298413638 3635012006461 6604941274827032 22402 86348 90 03 41916 67 37682296278870998147120825399150016479054 59104268930165575421 17 39 289874 0043 0903490662920682128834848619287099877800450043084167095 651900 34 80 43967519301 7447287

d_1=13000807100173770262325774950532580819678288838900669855034070742097228798543979594670979 477781241618 149236586384361 5727131160753526138 48705 27 77 8352 39 468055806228658865361299081808473430752 47214548050 3228568196836 770 27 1160617 5151907970972138787470395339832186467722882602129337372906 772 0818293162580159229143

p_2=191816707840332982137895843270557474232743846478402787547961443768848683 13478386925534025 2893274784 2336666135910 34021592443416 4392633596229006 40 152 858 92911

q_2=216612760372570517439180432981432372204029454655565658717298930054976639 53924460387283591 41705504745 11738646178 69177639094 98061895922 34777426369 8526 2 12 5097

n_2=41549946570873416673473276613020853574920730254296238329931698625869808808456050446342631 139451634562 5740268594148 13731668314326 72265669867930 73 240684 900524719573255783664403722878467265 6232247990 5486609934100705 14885 3452853 923715851183437848042435062512998077216721657897291121145587785 23 43 60093749 7027487367

e_2=135146536502394433895487372323006838246104757447027792522182781590542353 86079040939860387 0426392501070 732173435862109760 331828544858232123105088 1734 94 19710286040892703940511984222747867458 991651353662 6986363634 64510 26307 9144 0 185893491407782514034406976279860390939443841421 96630741173370 26684777852142 18380327

d_2=27438863311629338289438145005760040948953032770821014768010082582962189355415206403458317 46637351070 099318687315 455895994586893 676303002339561 54 335 04 52459850435135717567635635496129 869086 1610618 685195572 06575495546 14 834 355 13441810435999788043407054655361199743580084661811439431873603 437 19531 2561 4236176594503

cifrarea=15248790574093186962078242950293963317018072926227120748076221353288 33102299546546624842834 599539732537598 741481958506711452 9059 80847 3980 165 678 824 39859751060150681295345223806018427208178654561225656186 16958 512 7154 9640 217331 87708502028183457569123046272728866119705209 66338620891217313 77 29 78963018779 27761651091839239899928 892944329101 40047241434836 493 831 797

95739 2830642 000 18 60509837278178621936253443224 8191453756662755044 440 087 92879701931308265 7224 3 219332957816359223488028572904543249263051449 250 44 964043 0523155357804 2425 116 6329 454022 42885227 343628966 817604863 82276 55 771311288340199854 6861932 4964350 0 893610441493837269

descifrarea=364896564397011459724575230981320914472256689895283825736949671285945813416963547 069428149180 28461206078760 41957626485782 60270922849141 44780780 178579009996542341516588962738 2848490 75319698 448391792 16334991731 2048380 07 892181747534824353280415259682826892424484499087 383676687 756808250 98329 880 3378215978241

CAPITOLUL 3

Variante ale lemei chineze a resturilor și aplicații

În acest capitol vom prezenta atât varianta numerică cât și varianta polinomială a lemei chineze a resturilor, teorema de descompunere a fracțiilor raționale în fracții simple – ca o consecință a LCR precum și aaplicarea LCR în rezolvarea unor problme.

§3.1. Varianta numerică a LCR

Varianta numerică a LCR e din trei formulări:

(i) o formulare care utilizează doar elemente de teoria divizibilității,

(ii) o formulare care folosește conceptul de funcție,

(iii) o formulare cu ajutorul structurilor algebrice.

A. Tratarea LCR folosind elemente de teoria divizibilității

Notaţii şi elemente teoretice necesare

Fie dat un număr natural $m \geq 2$, număr numit *modul* (la plural *moduli*). Un număr natural *a* se poate reprezenta în mod unic sub forma:

(1) $a = m \cdot q + r,\ 0 \leq r \leq m$ (q, r numere naturale), conform teoriei de împărţire cu rest (pe scurt, TIR) pentru numere naturale.

Din (1) derivăm relaţiile:

$q_1 \leq \frac{a}{m} = q_1 + \frac{r_1}{m} < q_1 + 1$ care permit exprimarea câtului şi a restului împărţirii lui *a* la *m*:

$\left\lfloor \frac{a}{m} \right\rfloor$ este câtul (simbolul $\lfloor\ \rfloor$ desemnează partea întreagă), iar expresia $a - m\left\lfloor \frac{a}{m} \right\rfloor$, notată $a \bmod m$ (notaţie citită: „*a* modulo *m*”) este restul.

Se ştie că *m* divide pe *a* atunci şi numai atunci când $a \bmod m = 0$.

Fiind dat modulul m $(m \geq 2)$, putem aduce precizări privitoare la relaţia de egalitate a numerelor naturale şi putem introduce o nouă relaţie pentru numerele naturale, *relaţia de congruenţă modulo m*. Fie *a* şi *b* două numere naturale oarecare. Putem scrie în baza TIR:

(2) $a = mq_1 + r_1,\ 0 \leq r_1 \leq m$ (q_1, r_1 numere naturale),

(3) $b = mq_2 + r_2,\ 0 \leq r_2 \leq m$ (q_2, r_2 numere naturale).

- Pe unicitatea scrierilor (2) şi (3) se bazează echivalenţa logică:

  $a = b \Leftrightarrow (ii) q_1 + q_2$ şi $(ii) r_1 = r_2$.

- Proprietatea *a avea acelaşi rest faţă de modulul m* permite o identificare parţială a numerelor *a* şi *b* (identificare numită *congruenţă*): identificarea parţială are loc atunci şi numai atunci când are loc (ii). Formal,

(4) $a \equiv b(\mathrm{mod}\, m) :\Leftrightarrow a \bmod m = b \bmod m$,

unde simbolul $a \equiv b(\mathrm{mod}\, m)$ se citeşte: „*a* congruent cu *b* modulo *m*”.

Relaţia de congruenţă modulo *m* (introdusă de marele matematician C. F. Gauss (1777 – 1855)) are proprietăţi asemănătoare relaţiei de egalitate pentru numere naturale: (i) este reflexivă, simetrică şi tranzitivă, (ii) două congruenţe faţă de acelaşi modul se pot aduna, scădea şi înmulţi parte cu parte etc.

Caracterizări ale congruenţei modulo *m* sunt date de următoarea teoremă (care are o demonstraţie simplă):

Teoremă: *Cu notaţiile din (2) şi (3), următoarele condiţii:*

(c1) $r_1 = r_2$;

(c2) există un număr natural t *astfel încât* $a = b + m \cdot t$, *dacă* $a \geq b$;

(c3) m *divide diferenţa* $a - b$ *(dacă* $a \geq b$*)*

ori au loc toate, ori nu are loc niciuna, adică sunt echivalente.

Observaţie: a) Considerăm scrierea (2). Deoarece $r_1 < m$, avem:

$r_1 = m \cdot 0 + r_1,\ 0 \leq r_1 < m$**.** Prin urmare, $a \equiv a \bmod m$ (mod*m*), conform lui (4).

b) Reciproc, dacă *c* este un număr natural, cu $0 \le c < m$ şi dacă $a \equiv c(\mathrm{mod}\, m)$, atunci *c* este restul împărţirii numărului *a* la *m* (conform (c_2) din teorema de mai sus şi a unicităţii câtului cât şi a restului din TIR).

c) Lanţul de echivalenţe logice: *m* divide *a* $\Leftrightarrow r = 0 \Leftrightarrow a \equiv 0(\mathrm{mod}\, m)$ ne arată că relaţia de congruenţă generalizează relaţia de divizibilitate.

Prezentarea noţiunilor

[1] Următoarele precizări şi notaţii sunt utile. Fie date numerele naturale nenule *a* şi *b*.

i) Simbolul (a,b) desemnează pe cel mai mare element din mulţimea $D(a) \cap D(b)$ (unde $D(a)$ este notaţia pentru mulţimea formată din divizorii naturali ai numărului *a*, iar $D(b)$ este mulţimea divizorilor naturali ai numărului *b*), numit *cel mai mare divizor comun* (numit cmmdc) al numerelor *a* şi *b*.

ii) Dacă (a,b)=1, atunci spunem că numerele *a* şi *b sunt prime între ele*, caz în care folosim notaţia $a \perp b$.

[2] [Problematizare] Considerăm următoarea problemă de demonstrat:

Problema 1: *Fie date numerele naturale* m_1 *şi* m_2*, mai mari decât unitatea. Atunci* $m_1 \perp m_2$ *dacă şi numai dacă există un număr natural* a *cu proprietăţile* $a \bmod m_1 = 1 şi\ a \bmod m_2 = 0$.

Rezolvare:

- Dacă *a* este un număr natural cu proprietăţile: $a \bmod m_1 = 1$ şi $a \bmod m_2 = 0$, atunci $a = m_1 q_1 + 1$ şi $a = m_2 q_2$ (q_1, q_2 numere naturale). Putem scrie acum:

(5) $$m_2 q_2 = m_1 q_1 + 1$$

Dacă *d* este un element oarecare al mulţimii $D(m_1) \cap D(m_2)$ atunci din (5) se deduce că *d=1*, deci m_1 şi m_2 sunt numere relativ prime.

- Lucrăm acum în ipoteza că $m_1 \perp m_2$. Conform extinderii algoritmului lui Euclid (Euclid din Alexandria, cca. 450 – 380 î.H.), există doi întregi *u* şi *v* pentru care are loc relaţia

(6) $$um_1 + vm_2 = 1$$

Deoarece $m_1, m_2 \geq 2$, niciunul din numerele *u* şi *v* nu poate fi nul. Numerele *u* şi *v* nu pot avea acelaşi semn (ipoteza că *u* şi *v* au acelaşi semn conduce la concluzia absurdă că $1 \neq 1$, deoarece $1 = um_1 + vm_2 \neq 1$).

Cazul 1: $u < 0$ şi $v > 0$.

Luăm $a = vm_2$ şi obţinem din (6): $a \bmod m_1 = 1$ şi $a \bmod m_2 = 0$.

Cazul 2: $u > 0$ şi $v < 0$.

Alegem un număr natural *t* (de exemplu, $t = 1 + \max\left(\frac{u}{m_2}, \frac{-v}{m_1}\right)$) pentru care au loc relaţiile:

$u' = u - tm_2 < 0$ şi $v' = v + tm_2 > 0$.

Atunci

$$u'm_1 + v'm_2 = \left(um_1 - tm_1m_2\right) + \left(vm_2 + tm_1m_2\right) = um_1 + vm_2 = 1$$

Pentru întregii *u'* şi *v'* suntem acum în Cazul 1, deci se repetă argumentul de acolo.

[3] Ne reamintim următorul rezultat

Teoremă. *Fie date* t $(t \geq 3)$ *numere naturale nenule:* m_1, m_2, ..., m_t. *Dacă* $m_1 \perp m_2, m_1 \perp m_3, ..., m_1 \perp m_t$ *atunci* $m_1 \perp m_2 m_3 ... m_t$.

Fie daţi *t* $(t \geq 3)$ moduli: m_1, m_2, ..., m_t (m_1, m_2, ..., $m_t \geq 2$). Notăm şirul de moduli cu μ: $\mu := (m_1, m_2, ..., m_t)$. Introducem acum următorul concept:

Definiţie. Un şir de *t* numere naturale (b_1, b_2, ..., b_t) îl numim o μ-*bază* dacă au loc relaţiile:

$b_i \bmod m_j = \delta_{ij}$, oricare ar fi *i* şi *j* din $T := \{1, 2, ..., t\}$, unde simbolul δ_{ij} (numit *simbolul lui Kronecker*, Leopold Kronecker (1823 – 1891)) este definit prin: $\delta_{ij} = 0$ dacă $i \neq j$, respectiv $\delta_{ij} = 1$ dacă $i = j$.

Următoarea teoremă stabileşte legătura între existenţa unei μ-baze şi condiţia ca modulii să fie doi câte doi relativ primi.

Teoremă. *Există o μ-bază dacă şi numai dacă au loc relaţiile* $m_i \perp m_j$ *pentru toţi* $i \neq j$ *din* T.

Demonstraţie.

- În ipoteza că există μ-baze, fie (b_1, b_2, ..., b_t) una dintre ele. Fie *i* un element din T, fixat arbitrar. Pentru fiecare *j* din T-{*i*} avem: $b_i \bmod m_j = 0$. Cum $b_i \bmod m_i = 1$ deducem (conform Problema 1): $m_i \perp m_j$.

- Să presupunem acum că au loc relaţiile: $m_i \perp m_j$ pentru toţi $i \neq j$ din T. Introducem acum notaţiile (pe care le vom respecta şi în continuare):

$$M := m_1 m_2 ... m_t \quad \text{şi} \quad M_i := \frac{M}{m_j} \ (i=1, 2, ..., t).$$

Pentru construcţia unei μ-baze, fie *i* un element din T, fixat arbitrar. Deoarece $m_i \perp m_j$ pentru toţi *j* din T-{*i*}, deducem că $m_i \perp M_i$. Conform Problema 1, $m_i \perp M_i$ implică existenţa unui număr natural b_i pentru care au loc relaţiile: $b_i \bmod m_i = 1$ şi $b_i \bmod M_i = 0$.

Din $b_i \bmod M_i$ şi m_j divide M_i deducem că $b_i \bmod m_j = 0$, oricare ar fi *j* din T-{*i*}.

Deoarece $b_i \bmod m_j = \delta_{ij}$ pentru oricare *i* şi *j* din T, şirul (b_1, b_2, ..., b_t) este o μ-bază.

Notaţii:

$R_{m_i} := \{x \in \mathbb{N} : 0 \le x < m_i\}$ este mulţimea resturilor ce se pot obţine împărţind numerele naturale la m_i (i=1, 2, ..., t) şi $P := R_{m_1} \times R_{m_2} \times ... \times R_{m_t}$ (produs cartezian al mulţimii).

Definiţie. Fie *(r_1, r_2, ..., r_t)* un element oarecare din *P*. Spunem că *problema chinezească a resturilor are soluţie* pentru *(r_1, r_2, ..., r_t)* dacă există (cel puţin) un număr natural *n* pentru care au loc relaţiile: $n \bmod m_i = r_i$ (*i*=1, 2, …, *t*).

Următoarea teoremă poartă numele de *lema chinezească a resturilor*.

Teoremă (lema chinezească a resturilor, LCR). *Fie dat şirul de moduli $\mu=(m_1, m_2, ..., m_t)$. Atunci problema chinezească a resturilor are soluţie pentru fiecare$(r_1, r_2, ..., r_t)$ din P dacă şi numai dacă au loc relaţiile: $m_i \perp m_j$, oricare ar fi $i \neq j$ din T.*

Demonstraţie.

- Lucrăm în ipoteza că au loc relaţiile $m_i \perp m_j$ pentru toţi $i \neq j$ din T.

Relaţiile de mai sus implică existenţa a cel puţin unei μ-baze; fie $(b_1, b_2, ..., b_t)$ una dintre ele.

Fie acum $(r_1, r_2, ..., r_t)$ un element din *P*, fixat arbitrar. Definim numărul natural *n* prin: $n = r_1 b_1 + r_2 b_2 + ... + r_t b_t$.

Pentru *i* fixat în T avem:

$b_i = m_i q_i + 1$ (q_i număr natural) şi $b_j = m_i q_j$ (q_j număr natural), pentru toţi *j* din T-{*i*}.

Putem scrie $n = r_i \left(m_i q_i + 1\right) + \sum_{\substack{1 \le j \le t \\ j \neq i}} r_j q_j m_i = m_j \left(r_i q_i + \sum_{\substack{1 \le j \le t \\ j \neq i}} r_j q_j \right) + r_i$,

deci $n \bmod m_i = r_i$ (*i*=1, 2, …, *t*) şi prin urmare, *n* este o soluţie corespunzătoare lui $(r_1, r_2, ..., r_t)$.

- Presupunem că problema chinezească a resturilor (pe scurt, PCR) are soluţie pentru fiecare element din P. Alegem următoarele elemente din P: $E_1 = \left(1,0,0,...,0\right)$, $E_2 = \left(0,1,0,...,0\right)$, …, $E_t = \left(0,0,0,...,0,1\right)$

Conform ipotezei de lucru, există un număr natural b_i care este soluţie a PCR corespunzătoare lui E_i (*i*=1, 2, ..., *t*). Urmează că au loc relaţiile: $b_i \bmod m_j = \delta_{ij}$ pentru toţi *i* şi *j* din T, deci $(b_1, b_2, ..., b_t)$ este o μ-bază şi prin urmare $m_i \perp m_j$ pentru toţi $i \neq j$ din T.

Algoritm de construcţie a unei μ-baze. *Dacă se dă şirul de moduli $\mu = (m_1, m_2, ..., m_t)$, cu $m_i \perp m_j$ pentru toţi $i \neq j$ din T, să se afle o μ-bază $(b_1, b_2, ..., b_t)$.*

Pentru *i*=1, 2, ..., *t* se efectuează următoarele acţiuni şi se iau următoarele decizii:

(j) se atribuie variabilei *x* valoarea 1;

(jj) se efectuează algoritmul de împărţire curent, cu deîmpărţitul=xM_i şi împărţitorul=m_i, şi se obţine: $xM_i \bmod m_i = v_x$;

(jjj) dacă $v_x = 1$, atunci $c_i = x$ şi se înlocuieşte i cu i+1 (dacă $i \neq t$) altfel se înmulţeşte x cu x+1 (dacă $x \neq m_i - 1$) şi se revine la pasul (jj).

După execuţia algoritmului de mai sus se dispune de şirul $(c_1M_1, c_2M_2, ..., c_tM_t)$, despre care vom demonstra că este o μ-bază.

Fie i un element din T, fixat arbitrar. Atunci $M_i \perp m_i$. În baza TIR, putem scrie:

$1 \cdot M_i = m_i \cdot x_1 \cdot y_1$, $0 \le y_1 < m_i$ (x_1, y_1 numere naturale)

$1 \cdot M_i = m_i \cdot x_2 \cdot y_2$, $0 \le y_2 < m_i$ (x_2, y_2 numere naturale)

……

$1 \cdot M_i = m_i \cdot x_s \cdot y_s$, $0 \le y_s < m_i$ (x_s, y_s numere naturale) unde numărul m_i -1 s-a notat cu s.

Niciunul dintre resturile y_1, y_2, …, y_s nu poate fi nul: în ipoteza că $y_k=0$, $1 \le k \le s$, avem: $kM_i = m_i \cdot x_k$, de unde urmează că m_i divide produsul kM_i şi cum $m_i \perp M_i$ urmează în continuare că m_i divide numărul k, concluzie absurdă deoarece $1 \le k \le m_i - 1$.

Resturile y_1, y_2, …, y_s sunt distincte două câte două: dacă $y_a=y_b$, cu $1 \le a < b \le s$, atunci prin scăderea relaţiilor obţinem: $(b-a)M_i = m_i(x_b - x_a)$.

Din nou se ajunge la concluzia absurdă că m_i divide numărul natural b-a, unde $1 \le b - a \le s - 1 = m_i - 2$.

Din cele demonstrate mai sus rezultă că unul şi numai unul din resturile y_1, y_2, …, y_s este egal cu 1, să zicem că $y_l=1$ $(1 \le l \le s)$; atunci $c_i=l$, unde $1 \le l \le s = m_i - 1$.

Deci, algoritmul „lucrează bine”.

Să arătăm că algoritmul furnizează o μ-bază. Pentru fiecare i din T avem:

$c_iM_i = m_ix_i + 1$, iar pentru fiecare j din T- $\{i\}$ avem $c_iM_i = m_jx_j$, deoarece m_j divide M_i.

În continuare, ne punem următoarea problemă.

Problema 2. *Fie dat şirul de moduli* $\mu = (m_1, m_2, ..., m_t)$, *cu* $m_i \perp m_j$ *pentru toţi* $i \neq j$ *din T={1,2, ..., t}. Pentru fiecare element din* $P = R_{m_1} \times R_{m_2} \times ... \times R_{m_t}$, *câte soluţii are problema chinezească a resturilor?*

Rezolvare. Ipoteza că $m_i \perp m_j$ pentru toţi $i \neq j$ din T permite folosirea algoritmului descris mai sus. Se obţine μ-baza: (c_1M_1, …, c_tM_t) pe care o vom numi în continuare *μ-baza standard.*

Fie *(r_1, r_2, ..., r_t)* un element oarecare din P, fixat arbitrar. Ştim atunci că numărul natural *n* definit prin $n := r_1c_1M_1 + ... + r_tc_tM_t$, este una din soluţiile PCR, deci $n \bmod m_i = r_i$ pentru *i*=1, 2, .., *t*.

Să admitem că mai există soluţii; fie *n** una dintre ele. Din $n^* \bmod m_i = r_i = n \bmod m_i$ deducem că $n^* \equiv n (\bmod m_i)$ deci m_i divide diferenţa $|n^* - n|$ $(i \in T)$.

Cum diferenţa $|n^* - n|$ se divide cu fiecare modul din μ şi $m_i \perp m_j$, oricare ar fi $i \neq j$ din T, se deduce concluzia că $M = m_1m_2...m_t$ divide diferenţa $|n^* - n|$, deci există un număr natural *p* pentru care avem:

(i) $n^* = n + pM$, dacă $n^* \geq n$, respectiv

(ii) $n = n^* + pM$, dacă $n > n^*$.

Dacă *p* este un număr natural, atunci numărul $n + pM$ este soluţie a PCR, aşa cum se poate uşor verifica.

La fel, dacă $n > M$ şi dacă *p* este un număr natural pentru care *n-pM* este tot număr natural, *n-pM* este soluţia PCR.

Concluziile problemei propuse sunt (pentru *(r_1, r_2, ..., r_t)* din P):

- PCR are o infinitate de soluţii;

- Dacă n_0 este cea mai mică soluţie a PCR (unde $n_0=n$, dacă$n < M$, respectiv $n_0=n$ mod$M$, dacă $n \geq M$ - cu observaţia că $n_0=0$ dacă şi numai dacă $(r_1, r_2, \ldots, r_t)=(0,0,\ldots, 0)$), atunci mulţimea tuturor soluţiilor a PCR este $\{n_0 + pM : p \in \mathbb{N}\}$;

- Pentru orice număr natural a, în mulţimea $[a, a+M) \cap \mathbb{N}$ PCR are exact o singură soluţie. Într-adevăr, echivalenţa următoarelor relaţii

$a \leq n_0 + pM < a + M$,

$a - n_0 \leq pM < a - n_0 + M$ şi

$$\frac{a-n_0}{M} \leq p < 1 + \frac{a-n_0}{M}$$

ne permite să formulăm următoarea concluzie:

i) dacă $a \leq n_0$, atunci în $[a, a+M) \cap \mathbb{N}$ singura soluţie a PCR este n_0;

ii) dacă $a > n_0$, atunci în $[a, a+M) \cap \mathbb{N}$ singura soluţie a PCR este n_0+pM, unde

$$p = \left\lfloor \frac{a-a_0}{M} \right\rfloor .$$

APLICAŢII

[1]. Pentru prezentarea unei aplicaţii a LCR următoarea teoremă este utilă.

Teoremă. (teorema bazelor de numeraţie). *Fie dat un număr natural* b*, cu* $b \geq 2$. *Atunci fiecare număr natural* $a \geq b$ *se poate reprezenta în mod unic ca un polinom în* b*:*

$a = c_0 b^0 + c_1 b^1 + \ldots + c_n b^n$,

unde $n \geq 1$ este un număr natural, $c_0, c_1, \ldots, c_n \in \mathbb{R}_b = \{0,1,\ldots,b-1\}$ şi $c_n \neq 0$.

Demonstraţia teoremei va fi dată deoarece există o variantă a sa şi pentru polinoame.

Existenţa. Numerele a şi b $(a \geq b)$ le putem asocia următorul şir de relaţii:

$a = bq_0 + c_0$, $0 \leq c_0 < b$ ($q_0 \neq 0$ şi c_0 numere naturale)

$q_0 = bq_1 + c_1$, $0 \leq c_1 < b$ ($q_1 \neq 0$ şi c_1 numere naturale)

……

$q_{n-2} = bq_{n-1} + c_{n-1},\ 0 \le c_{n-1} < b$ ($q_{n-1} \neq 0$ şi c_{n-1} numere naturale)

$q_{n-1} = b \cdot 0 + c_n,\ 0 \le c_n = q_{n-1} < b$ (c_n număr natural)

Putem scrie:

$q_{i-1}b^i - q_i b^{i+1} = c_i b_i$,

unde i=0,1, …, n (numărul a este notat q_{-1}).

Prin însumare se obţine $q_{-1}b^0 - q_n b^{n+1} = c_0 b^0 + c_1 b^1 + ... + c_n b^n$ şi în continuare avem (deoarece $q_{-1}=a$ şi $q_n=0$)

(*) $a = c_0 b^0 + c_1 b^1 + ... + c_n b^n$, scriere ce îndeplineşte condiţiile din teoremă.

Din (*) se obţine în continuare:

$b^n \le c_n b^n \le a \le (b-1)b^0 + (b-1)b^1 + ... + (b-1)b^n = b^{n+1} - 1 < b^{n+1}$, deci $b^n \le a < b^{n+1}$.

Unicitatea. Presupunem că în afară de scrierea (*) ar mai exista şi scrierea:

(**) $a = x_0 b^0 + x_1 b^1 + ... + x_m b^m$, unde $m \ge 1$ este un număr natural, $x_0, x_1, ..., x_m \in \mathbb{R}_b$ şi $x_m \neq 0$.

Din (**) se deduce că $b^m \le a < b^{m+1}$.

Scrierile (*) şi (**) au aceeaşi lungime, adică $m=n$. Dacă, spre exemplu, ar avea relaţia $n<m$, atunci din lanţul de ordonări: $b^n \le a < b^{n+1} \le b^m \le a < b^{m+1}$ se extrage concluzia absurdă că $a<a$. La aceeaşi concluzie se ajunge şi când se pleacă de la ipoteza $m<n$.

Din scrierea (**) , cu $m=n$, se obţine aplicând TIR:

$c_0 = x_0$ şi $q_0 = x_1 b^0 + x_2 b^1 + ... + x_n b^{n-1}$

$c_1 = x_1$ şi $q_1 = x_2 b^0 + x_3 b^1 + ... + x_n b^{n-2}$

……

$c_n = x_n$ şi $q_n = 0$.

APLICAŢII

A1. Vom prezenta o aplicaţie a LCR strâns legată de descompunerea unei fracții în fracții simple.

Fie date numerele naturale *a* şi *M*, cu $1 \le a < M$, $a \perp M$, *M* fiind un număr compus. Presupunem că *M* se descompune într-un produs de numere naturale: $M=m_1\ m_2\ \ldots m_t$, unde $t \ge 2$, $m_i \ge 2$ (i=1, 2, …, t) şi $m_i \perp m_j$, oricare ar fi $i \ne j$ din T={1,2, …, t}.

Notăm $r_i := a \bmod m_i$ (i=1, 2, …, t).

Determinăm pentru $\mu := (m_1, m_2, ..., m_t)$ μ-baza standard (c_1M_1, …, c_tM_t) şi pentru (r_1, …, r_t), soluţia standard $n = r_1c_1M_1 + ... + r_tc_tM_t$ a PCR. Din relaţiile $1 \le r_i \le m_i - 1$ şi $1 \le c_i \le m_{i-1}$ rezultă relaţiile $1 \le r_ic_i \le m_i(m_i - 2) + 1$, deci putem scrie $r_ic_i = m_ix_i + y_i$ (x_i, y_i numere naturale), unde $0 \le x_i \le m_i - 2$ şi $y_i \in \mathbb{R}_{m_i}$ (i=1, 2, …, t).

Atunci $n = n_1 + (x_1 + x_2 + ... + x_t)M$ unde $n_1 := y_1M_1 + ... + y_tM_t$. Deoarece $n \equiv n_1 (\bmod M)$, n_1 este soluţie a PCR.

Acum $a \bmod m_i = r_i = n_1 \bmod m_1$ (i=1, 2, …, t), deci $a \equiv n_1 (\bmod M)$ şi prin urmare, există un număr natural *p* pentru care $a + pM = n_1$, relaţie care se scrie succesiv: $\frac{a}{M} = \frac{n_1}{M} + k$,

(++) $\frac{a}{M} = \frac{y_1}{m_1} + ... + \frac{y_t}{m_t} + k$, unde *k* este număr întreg şi $y_i \in \mathbb{R}_{m_i}$ (i=1, 2, …, t).

Să admitem că fracţia ordinară $\frac{a}{M}$ se mai poate scrie încă şi sub forma:

(+++) $\frac{a}{M} = \frac{z_1}{m_1} + ... + \frac{z_t}{m_t} + l$, unde *l* este număr întreg şi $z_i \in \mathbb{R}_{m_i}$ (i=1, 2, …, t).

Din (++) obţinem:

$$a = y_1M_1 + ... + y_tM_t + kM \text{ , (deci } a \equiv n_1 (\bmod M)\text{), iar din (+++),}$$

$$a = z_1M_1 + ... + z_tM_t + lM \text{ ,}$$

deci $a \equiv n_2 (\mathrm{mod}\, M)$, unde $n_2 = z_1 M_1 + ... + z_t M_t$.

Folosind tranzitivitatea $a \equiv n_1 (\mathrm{mod}\, M)$ şi $a \equiv n_2 (\mathrm{mod}\, M)$ implică $n_2 \equiv n_1 (\mathrm{mod}\, M)$, deci şi n_2 este soluţia PCR.

Fie i un element din T, fixat arbitrar. Deoarece m_i divide M, $n_2 \equiv n_1 (\mathrm{mod}\, M)$ implică $n_2 \equiv n_1 (\mathrm{mod}\, m_i)$. Cum m_i divide M_j, pentru fiecare j din T-{i}, avem: $n_2 (\mathrm{mod}\, m_i) = r_i = n_1 (\mathrm{mod}\, m_i)$, deci $y_i M_i \equiv z_i M_i (\mathrm{mod}\, m_i)$, de unde deducem că m_i divide numărul natural $|y_i - z_i| \cdot M_i$. Cum $m_i \perp M_i$, urmează că m_i divide numărul natural $|y_i - z_i|$, unde $0 \le |y_i - z_i| < m_i$, deci $y_i = z_i$. Din egalitatea: $\frac{y_1}{m_1} + ... + \frac{y_t}{m_t} = \frac{z_1}{m_1} + ... + \frac{z_t}{m_y}$ şi din relaţiile (++) şi (+++) se mai poate deduce că $l=k$, deci reprezentarea (++) pentru fracţia ordinară $\frac{a}{M}$ este unică.

În continuare tratăm cazul special $m_i = p_i^{e_i}$, (i=1, 2, ..., t), unde p_1, p_2, …, p_t sunt numere prime diferite două câte două, iar $e_i \ge 1$ este număr natural (i=1, 2, ..., t).

Fie i fixat în T. Numărul y_i din (++) se poate reprezenta ca un polinom în p_i:

$y_i = c(i,e_i) p_i^0 + c(i,e_i - 1) p_i^1 + ... + c(i,1) p_i^{e_i - 1}$, unde $c(i,j) \in R_{p_i}$ (j=1, 2, …, e_i). În consecinţă:

$$\frac{y_i}{p_i^{e_i}} = \frac{c(i,1)}{p_i^1} + \frac{c(i,2)}{p_i^2} + ... + \frac{c(i,e_i)}{p_i^{e_i}}.$$

Putem scrie acum (++) în forma:

$$\frac{a}{p_1^{e_1} p_2^{e_2} ... p_t^{e_t}} = k + \sum_{i=1}^{t} \sum_{j=1}^{e_i} \frac{c(i,j)}{p_i^j},$$

unde $c(i,j) \in R_{p_i}$ (j=1, 2, …, e_i) pentru i=1, 2, .., t. Este uşor de arătat (aşa cum am procedat pentru scrierile (++) şi (+++)) că ultima scriere este unică.

Numim *fracţie simplă* orice fracţie ordinară de forma

$$\frac{c}{p^e},$$

unde p este număr natural prim, iar c şi e sunt numere naturale cu proprietăţile $1 \le c < p$ şi $e \ge 1$.

Am demonstrat următoarea teoremă:

Teoremă (Gauss, 1801) – **teorema de descompunere în fracţii simple**

Fie fracţia ordinară $\frac{a}{b}$, *unde* a *şi* b *sunt numere naturale, cu* $1 \le a < b$ *şi* $b = p_1^{b_1} p_2^{b_2} ... p_t^{b_t}$ *(*$t \ge 2$*;* $p_1 < p_2 < ... < p_t$ *numere prime şi* $b_i \ge 1$ *număr natural pentru* i=*1, 2, ..., t). Atunci fracţia ordinară subunitară* $\frac{a}{b}$ *se descompune în mod unic sub forma:* $\frac{a}{b} = \sum_{i=1}^{t} \sum_{j=1}^{b_i} \frac{c(i,j)}{p_i^j}$, *unde* k *este număr întreg şi* $c(i,j) \in R_{p_i}$ *(*j=*1, 2, ...,* b_i*) pentru* i=*1, 2, ..., t.*

Exemple.

E1. Pentru a=35 şi b=72= $2^3 \cdot 3^2$ obţinem $\frac{35}{72} = \frac{35}{2^3 \cdot 3^2} = \frac{1}{2^2} + \frac{1}{2^3} + \frac{1}{3^2} = \frac{1}{4} + \frac{1}{8} + \frac{1}{9}$.

Justificare. Avem M=72, m_1=8, m_2=9, M_1=9, M_2=8. Pentru M_1=9 şi m_1=8 avem: $1 \cdot M_1 = 8 \cdot 1 + 1$ deci c_1=1.

Pentru M_2=8 şi m_2=9 avem: $1 \cdot M_1 = 9 \cdot 0 + 8$, …, $8 \cdot M2 = 9 \cdot 7 + 1$, deci c_2=8.

Acum

$$r_1 = a \bmod m_1 = 35 \bmod 8 = 3,$$

$$r_2 = a \bmod m_2 = 35 \bmod 9 = 8$$

şi prin urmare soluţia standard a PCR este $n = r_1 c_1 M_1 + r_2 c_2 M_2 = 3 \cdot 1 \cdot 8 + 8 \cdot 8 \cdot 8$.

Din $r_1 c_1 = m_1 x_1 + y_1$ şi $3 = 8 \cdot 0 + 3$ obţinem x_1=0 şi y_1=1. Din $r_2 c_2 = m_2 x_2 + y_2$ şi $64 = 9 \cdot 7 + 1$ obţinem x_2=7 şi y_2=1.

Deoarece

$$n_1 = y_1 M_1 + y_2 M_2 = 3 \cdot 9 + 1 \cdot 8 = 35 = a \text{ rezultă}$$

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

E2. Fie a=13 şi b=60=$3\cdot 4\cdot 5$. Atunci M=b=60, m_1=3, m_2=4, m_3=5, $M_1=\frac{M}{m_1}=20$, $M_2=\frac{M}{m_2}=15$ şi $M_3=\frac{M}{m_3}=12$.

Găsim:

$$c_1=2,\ c_2=3,\ c_3=3;$$

$$x_1=0,\ y_1=2;\ x_2=0,\ y_2=3;\ x_3=1,\ y_3=4.$$

Atunci $n_1=y_1M_1+y_2M_2+y_3M_3=2\cdot 20+3\cdot 15+4\cdot 12=133=2M+a$, de unde $\frac{13}{60}=\frac{a}{b}=\frac{n_1-2M}{M}=\frac{2\cdot 20+3\cdot 15+4\cdot 12}{60}-2=(-2)+\frac{2}{3}+\frac{3}{4}+\frac{4}{5}=(-2)+\frac{2}{3}+\frac{2+1}{4}+\frac{4}{5}$ deci $\frac{13}{60}=(-2)+\frac{1}{2}+\frac{1}{4}+\frac{2}{3}+\frac{4}{5}$.

A2. La întrebarea: **Cum putem folosi LCR în rezolvarea de probleme?** răspundem… prin două probleme:

Problema 1. *Într-un tablou cu 3 linii şi 210 coloane sunt scrise numere naturale astfel: (i) pe prima linie apare secvenţa 1, 2, 3, 4, 5 scrisă repetat de 42 de ori, (ii) pe a doua linie apare secvenţa 1, 2, 3, 4, 5, 6 scrisă repetat de 35 de ori şi (iii) pe a treia linie apare secvenţa 1, 2, 3, 4, 5, 6, 7 scrisă repetat de 30 de ori. Să se afle:*

1) *Care sunt numerele scrise pe a 123-a coloană;*
2) *Pe a câta coloană sunt scrise de sus în jos numerele 3, 4 şi 4.*

Rezolvare. TATONARE: Încercând să scriem o parte a tabloului, am observa următoarele fapte: dacă j este numărul de ordine al unei coloane ($1\le j\le 210$) şi dacă în coloana j sunt scrise numerele:

	Coloana j
Linia 1:	a
Linia 2:	b
Linia 3:	c

atunci j-a este multiplu de 5, j-b este multiplu de 6 şi j-c este multiplu de 7.

SCHIMBAREA PROBLEMEI: Pentru a obţine resturile de la împărţirea cu 5 (pentru prima linie), cu 6 (pentru a doua linie), respectiv cu 7 (pentru a treia linie), înlocuim tabloul iniţial T_i cu tabloul final T_f obţinut din T_i scăzând o unitate din fiecare din cele 630 de numere din T_i. acum situaţia de mai sus capătă forma:

	Coloana j
Linia 1:	a-1
Linia 2:	b-1
Linia 3:	c-1

Mai este deci necesară încă o schimbare: folosind drept numere ordinale pentru coloanele din T_f pe: 0, 1, …, 209. Acum avem în T_f:

	Coloana j
Linia 1:	$j \bmod 5$
Linia 2:	$j \bmod 6$
Linia 3:	$j \bmod 7$

situaţie care face trimitere la LCR, deci putem formula răspunsurile:

(1) pe a 123-a coloană din T_i sunt numerele:

$$122 \bmod 5 = 2$$

$$122 \bmod 6 = 2$$

$$122 \bmod 7 = 4$$

(2) pentru modulii 5, 6 şi 7 (care sunt relativ primi doi câte doi), LCR ne furnizează soluţia:

$$88 \bmod 5 = 3$$

$$88 \bmod 6 = 4$$

$$88 \bmod 7 = 4$$

deci numerele 3, 4 şi 4 sunt în a 89-a coloană din T_i.

Problema 2. *Într-o clasă sunt n elevi. Aşezaţi în bănci câte trei, în una din bănci se află 2 elevi. Aşezaţi în bănci câte 4, în una din bănci sunt 3 elevi. Aşezaţi în bănci câte 5, în una din bănci sunt 3 elevi. Aflaţi valoarea lui n ştiind că* $n \le 40$.

Analiza problemei şi conversaţia euristică trebuie să conducă la următoarele constatări:

- Problema prezentată este o problemă de aflat (se cere aflarea lui *n*).
- Aflarea lui *n* se bazează pe condiţiile: împărţind succesiv pe n la numerele 3, 4 şi 5, se obţin resturile 2, 3 şi respectiv 3 (pentru LCR astfel de condiţii sunt caracteristice).
- Condiţia $n \le 40$ (necesară enunţului, în baza experienţei organizării elevilor în clase) are un rol de „descurajare" pentru cei care doresc o rezolvare brută: *n*=1 nu satisface condiţiile, *n*=2 nu satisface condiţiile, ..., *n*=40 nu satisface condiţiile, doar *n*=23 satisface condiţiile.

B. Prezentarea lemei chinezeşti a resturilor folosind conceptul de funcţie.

Mai întâi să precizăm câţiva termeni din teoria funcţiilor.

Fie dată o funcţie $f : D \to \mathbb{R}$. Îi putem asocia lui *f* următoarele mulţimi:

i) *imaginea lui* f: $im(f) := \{ f(a) : a \in D \} \subseteq \mathbb{R}$

ii) *clasele lui* f: fiecărui element *i* din mulţimea *im(f)* îi asociem clasa $D_i := \{ a \in D : f(a) = i \} \subseteq D$.

iii) *nucleul lui* f: $\ker(f) := \{ D_i : i \in im(f) \} =$ partiţie a mulţimii *D*.

Obiecte date: se consideră date $t (t \ge 2)$ numere naturale mai mari decât unitatea: a_1, a_2, …, a_t.

Notaţii:

$$T := \{1, 2, ..., t\}$$

$A := a_1 a_2 ... a_t$

$A_i := \frac{A}{a_i}$ (i=1, 2, …, t)

$R_{a_i} := \{0,1,...a_i - 1\}$ (i=1, 2, …, t) şi $R_A := \{0,1,..., A-1\}$

$P := R_{a_1} \times R_{a_2} \times ... \times R_{a_t}$ (produs cartezian)

$m := [a_1, a_2, ..., a_t]$ (cel mai mic multiplu comun)

Fapte: Se ştie că:

- $m := [a_1, a_2, ..., a_t] \Leftrightarrow M(a_1) \cap M(a_2) \cap ... \cap M(a_t) = M(m)$
  (unde $M(m) := \{kn : k \in \mathbb{N}^*\}$ pentru oricare n din $\mathbb{N}^*$);
- $m = A \Leftrightarrow a_i \perp a_j$, oricare ar fi $i \neq j$ din T;
- $a_i \perp a_j$ (j=2, 3, …, t) $\Leftrightarrow a_1 \perp A_1$.

Funcţia: Definim funcţia $\varphi : R_A \to P$ prin $\varphi(x) := (x \bmod a_1, x \bmod a_2, ..., x \bmod a_t,)$.

Motivaţia: Observăm că: (i) m divide pe A şi (ii) mulţimile R_A şi P au fiecare A elemente.

Putem pune elevilor întrebarea: *Ce legături logice există între condiţiile?*

(1) φ bijecţie;
(2) φ injecţie;
(3) φ surjecţie?

Răspunsul dorit este acela că cele trei condiţii de mai sus sunt echivalente (datorită observaţiei (ii)). Dirijarea învăţării este asigurată de cerinţa ca elevii (individual sau pe grupe) să rezolve succesiv următoarele probleme:

Problema 1. *Fie* $x_1 \le x_2$ *elemente din* R_A. *Arătaţi că au loc echivalenţele logice:* $\varphi(x_1) = \varphi(x_2) \Leftrightarrow x_2 - x_1$ *este multiplu de* a_i, *oricare ar fi* i *din* T $\Leftrightarrow x_2 - x_1$ *este multiplu de* m.

Problema 2. *Să se arate că:*

1) *Im(*φ) *conţine* m *elemente;*

2) *Ordonând crescător elementele din fiecare clasă a lui* φ*, se obţin* m *progresii aritmetice, fiecare având raţia egală cu* m*;*

3) *Ker(*φ) *este o echipartiţie a mulţimii* R_A (adică toate clasele lui φ au acelaşi cardinal).

Dacă elevii cunosc noţiunea de congruenţă numerică, atunci rezolvarea problemei 1 nu ridică mari dificultăţi. Rezolvarea problemei 2 este mai dificilă. Putem da aici următoarele indicaţii:

- arătaţi că $\varphi(0),\varphi(1),...,\varphi(m-1)$ sunt elemente diferite din *Im(*φ);
- dacă $x\in\mathbb{R}$ şi $x\geq m$ atunci din $x=mq+r$, $r<m$ (q, r numere naturale), rezultă că $\varphi(x)=\varphi(r)$.

Când s-a încheiat rezolvarea problemei 2, elevii trebuie să obţină următoarele rezultate: clasele funcţiei φ sunt:

$$\left\{0,m,2m,...,\left(\frac{A}{m}-1\right)m\right\}$$
$$\left\{1,m+1,2m+1,...,\left(\frac{A}{m}-1\right)m+1\right\}$$
.....
$$\left\{(m-1),m+(m-1),...,\left(\frac{A}{m}-1\right)m+(m-1)\right\}$$

deci fiecare este o progresie aritmetică de lungime $\frac{A}{m}$ şi raţie m. Acest rezultat conduce la formularea următoarei probleme: *Ce se întâmplă în cazul în care* m=A*?*

Răspunsul la această întrebare poate fi formulat astfel: Dacă $A=m$, atunci în fiecare clasă a lui φ se află exact un singur element. În consecinţă, φ este injecţie. Dar atunci φ=injecţie=surjecţie=bijecţie.

În baza răspunsului dat mai sus, obiectivul urmărit în continuare este enunţarea şi demonstrarea unei teoreme importante a aritmeticii modulare, teoremă cunoscută sub numele de *LCR*.

Cu precizarea că împărţitorii folosiţi la TIR se mai numesc şi *moduli* (de aici şi denumirea de *aritmetică modulară*), LCR răspunde la următoarea întrebare: dacă se cunosc

resturile $x \bmod a_1$, $x \bmod a_2$, ..., $x \bmod a_t$, atunci se poate reconstitui numărul (natural, respectiv întreg) *x*?

Din rezolvările de mai sus reiese ca fiind important cazul *m=A*, adică $a_i \perp a_j$, oricare ar fi $i \neq j$ din *T*.

Enunţul şi demonstrarea LCR

Teoremă (lema chinezească a resturilor) *Fiind date numerele naturale* $a_1, a_2, \ldots, a_t \geq 2$ *(t≥2), se defineşte funcţia* $\varphi: \mathbb{N} \to P, \varphi(x) = (x \bmod a_1, x \bmod a_2, ..., x \bmod a_t)$. *Atunci* φ *este surjecţie dacă şi numai dacă* a_i *este relativ prim cu* a_j, *oricare ar fi* $i \neq j$ *din* T.

Demonstraţie. Următoarele elemente din *P* sunt importante: $E_1=(1, 0, 0, \ldots, 0)$, $E_2=(0,1, 0, \ldots, 0)$, ..., $E_t=(0, 0, 0, \ldots, 1)$.

1) [implicaţia $\Rightarrow$] Din ipoteza că φ este surjecţie rezultă că există în domeniul de definiţie $\mathbb{N}$ *t* elemente: $n_1, n_2, \ldots, n_t$ astfel încât $\varphi(n_1) = E_1, \varphi(n_2) = E_2, ..., \varphi(n_t) = E_t$.

Să studiem consecinţele relaţiei $\varphi(n_1) = E_1$. Avem:
$$\begin{aligned} n_1 &= a_1 q_1 + 1 \quad (q_1 \text{ număr natural}) \\ n_1 &= a_2 q_2 \quad (q_2 \text{ număr natural}) \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ n_1 &= a_t q_t \quad (q_t \text{ număr natural}) \end{aligned}$$

Fie *j* un element oarecare din *T-{1}*. Relaţiile $n_1 = a_1 q_1 + 1$ şi $n_1 = a_j q_j$ conduc la scrierea: $a_1 q_1 + 1 = a_j q_j$, din care rezultă uşor că a_1 şi a_j sunt numere naturale relativ prime.

Analog se procedează cu relaţiile $\varphi(n_2) = E_2, ..., \varphi(n_t) = E_t$.

2) [implicaţia $\Leftarrow$] Vom da o demonstraţie constructivă (acesta este şi motivul pentru care am formulat separat LCR şi nu ne-am rezumat la problema 2). Ideea fundamentală este aceea de a arăta că elementele $E_1, E_2, \ldots, E_t$ sunt în imaginea lui φ.

Construcţia unui element n_1 din domeniul de definiţie al funcţiei φ pentru care să aibă loc relaţia $\varphi(n_1) = E_1$.

Deoarece $a_1 \perp a_j$ (j=2, 3, … t), deducem că $a_1 \perp A$. Împărţim cu rest multiplii succesivi $1A_1$, $2A_1$, …, $(a_1\text{-}1)A_1$ ai lui A_1 la a_1:

$$\begin{aligned} &1A_1 = a_1q_1 + r_1, r_1 < a_1; \\ &2A_1 = a_1q_2 + r_2, r_2 < a_1; \\ &\ldots\ldots\ldots\ldots\ldots\ldots \\ &(b-1)A_1 = a_1q_{b-1} + r_{b-1}, r_{b-1} < a_1. \end{aligned}$$

Atunci resturile $r_1, r_2, \ldots, r_{b-1}$ sunt nenule (în caz contrar a_1 divide A_1, absurd) şi distincte două câte două (dacă $r_i=r_j$, cu $i<j$, atunci $(j\text{-}i)A_1=a_1(q_j\text{-}q_i)$, relaţie care conduce la consecinţa a_1 divide A_1, deoarece $j\text{-}i$ şi a_1 sunt relativ prime, absurd). În consecinţă, există un unic element nenul c_1 în R_{a_1} pentru care avem $(c_1A_1) \bmod a_1 = 1$. Luăm $n_1=c_1A_1$ şi atunci: n_1 este număr natural şi $\varphi(n_1) = E_1$. Procedând analog, găsim un element nenul c_j în R_{a_1} pentru care avem $(c_jA_j) \bmod a_j = 1$ şi $\varphi(n_j) = E_j$, unde $n_j = c_jA_j$ (j=2, 3, …, t).

Fie (r_1, …, r_t) un element oarecare din P. Calculăm:

(*) $n:=r_1c_1A_1+\ldots+r_tc_tA_t$.

Deoarece a_1 divide A_j (j=2, 3, .., t) şi $c_1A_1=a_1q_1+1$, deci $r_1c_1A_1=a_1(r_1q_1)+r_1$, deducem că $n \bmod a_1 = r_1$. Analog $n \bmod a_i = r_i$ pentru i=2, 3, …, t. Deci $\varphi(n) = (r_1, \ldots, r_t)$ de unde tragem concluzia că φ este surjecţie. Încheiem demonstraţia teoremei cu următoarea observaţie: putem scrie (*) sub forma: $n:=r_1c_1A_1+\ldots+r_tc_tA_t=Aq+r$, $r<A$ (q, r numere naturale).

Atunci a_i divide A (i=1, 2, …, t) şi prin urmare, $r \in R_A$ şi
$r \bmod a_i = (n - Aq) \bmod a_i = r_i \quad (i = 1, 2, \ldots, t)$ deci $\varphi(r) = (r_1, \ldots, r_t)$.

COMENTARIU

1) Observaţia finală din LCR şi rezultatele furnizate de problema 1 şi problema 2 ne conduc la concluzia că R_A este un sistem complet şi independent de reprezentanţi pentru partiţia $\ker(\varphi)$ a mulţimii $\mathbb{N}$.

2) Clasele funcţiei φ sunt:

$$\begin{aligned} &\{0 + kA : k \in \mathbb{N}\}; \\ &\{1 + kA : k \in \mathbb{N}\}; \\ &\ldots\ldots\ldots\ldots\ldots \\ &\{(A-1) + kA : k \in \mathbb{N}\} \end{aligned}$$

Consecinţă: Dacă ($r_1, ..., r_t$) este un element în P, fixat arbitrar, atunci, oricare ar fi numărul natural x, în mulţimea $[x, x+A) \cap \mathbb{N}$ există un unic element n pentru care are loc relaţia $\varphi(n) = (r_1, ..., r_t)$. Într-adevăr fie $x \geq A$ un număr natural şi fie $r \in R_A$ pentru care avem $\varphi(r) = (r_1, ..., r_t)$. Pentru $s \in \mathbb{N}$ avem: $x \leq r + As < x + A \Leftrightarrow \frac{x-r}{A} \leq s < 1 + \frac{x-r}{A} \Leftrightarrow s = \left\lfloor \frac{x-r}{A} \right\rfloor$. Numărul natural $n := A \cdot \left\lfloor \frac{x-r}{A} \right\rfloor + r$ satisface condiţiile $n \in [x, x+A) \cap \mathbb{N}$ şi $\varphi(n) = (r_1, ..., r_t)$.

3) Restricţia φ / R_A este o bijecţie şi $(\varphi / R_A)^{-1}(r_1, ..., r_t) = (r_1 c_1 A_1 + ... + r_t c_t A_t) \bmod A$ (a se vedea observaţia finală din demonstraţia LCR).

APLICAŢIE. *Fie date numerele naturale* $a_1, a_2, \ldots, a_t \geq 2 (t \geq 2)$ *cu* $a_i \perp a_j$, *oricare ar fi* $i \neq j$ *din {1, 2, ..., t}. Se defineşte un tablou cu* t *linii şi* $A = a_1 a_2 \ldots a_t$ *coloane astfel: pentru fiecare* i=*1, 2, ...,* t, *pe linia* i *a tabloului se scrie un şir de lungime* A, *periodic de perioadă* ai *şi cu termenii iniţiali 1, 2, ...,* a1. *Să se precizeze elementele de pe coloana* j $(1 \leq j \leq A)$.

Rezolvarea foloseşte ideile din aplicaţia *A2* de la paragraful 1.A.

Probleme din concursuri

P1. *Arătaţi că există un şir crescător* $(a_n)_{n \geq 1}$ *de numere naturale astfel încât, pentru orice întreg* $k \geq 0$, *şirul* $(k + a_n)_{n \geq 1}$ *conţine un număr finit de numere prime.*

(1997 Czech and Slovak Mathematical Olympiad)

Soluţie. Fie p_k numărul prim de rang k, $k \geq 1$. Luăm $a_1 := 2$. Pentru $n \geq 1$, fie a_{n+1} cel mai mic întreg mai mare strict ca a_n care este congruent cu $-k$ modulo p_{k+1} pentru toţi $k \leq n$. Întregul a_{n+1} există în baza LCR. Atunci, pentru toţi $k \geq 0$, $k + a_n \equiv 0 (\bmod p_{k+1})$ pentru $n \geq k+1$, deci cel mult $k+1$ termeni din şirul $(k+a_n)$ sunt numere prime (începând cu al *(k+2)-lea* termen din şir numerele sunt multipli de p_{k+1}).

P2. *Un punct laticeal* X *din plan se spune că este vizibil din originea* O *dacă segmentul* OX *nu conţine un alt punct laticeal aflat între* O *şi* X. *Arătaţi că oricare ar fi un întreg pozitiv* n,

există un pătrat cu n^2 *puncte laticeale (cu laturile paralele cu axele de coordonate) astfel încât niciun punct din interiorul pătratului să nu fie vizibil din origine.*

(2002 Taiwanese Mathematical Olympiad)

Soluţie. Considerăm o matrice $P = \begin{pmatrix} p_{11} & p_{12} & \cdots & p_{1n} \\ p_{21} & p_{22} & \cdots & p_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ p_{n1} & p_{n2} & \cdots & p_{nn} \end{pmatrix}$

cu toate elementele numere prime, distincte două câte două. Notăm:

$$L_i = \prod_{j=1}^{n} p_{ij} \quad (i = 1, 2, ..., n) \quad \text{şi}$$

$$C_j = \prod_{i=1}^{n} p_{ij} \quad (j = 1, 2, ..., n).$$

Fie x_1 o soluţie întreagă a congruenţelor:

$$x_1 \equiv 0 (\mathrm{mod}\, L_1)$$

$$x_1 + 1 \equiv 0 (\mathrm{mod}\, L_2)$$

.....

$$x_1 + n - 1 \equiv 0 (\mathrm{mod}\, L_n)$$

Şi fie y_1 o soluţie a congruenţelor:

$$y_1 \equiv 0 (\mathrm{mod}\, C_1)$$

$$y_1 + 1 \equiv 0 (\mathrm{mod}\, C_2)$$

.....

$$y_1 + n - 1 \equiv 0 (\mathrm{mod}\, C_n)$$

Ambii întregi (adică x_1 şi y_1) există prin LCR. Punctul (x_1,y_1) este colţul din stânga-jos al pătratului, celelalte puncte sunt (x_1+i, y_1+i) $(i=0,1,...,n-1; j=0,1,...,n-1)$.

Se observă că ambele coordonate ale unui punct din interiorul pătratului sunt divizibile printr-un element din matricea P, deci nu este vizibil din origine.

C. Prezentarea LCR cu ajutorul structurilor algebrice

Studiul structurilor algebrice (grup, inel) permite stabilirea unor legături (în ambele sensuri) între algebra abstractă şi aritmetica lui $\mathbb{Z}$. Aceste legături le vom pune în evidenţă (sub formă de schiţă) în cele ce urmează, punând accentul pe legătura:

Algebră abstractă $\rightarrow$ aritmetica lui $\mathbb{Z}$

1. Folosirea teoriei funcţiilor

Fie $m\geq 2$ un întreg fixat. Definim funcţia surjectivă $f:\mathbb{Z}\rightarrow R_m := \{0,1,...,m-1\}$ prin $f(z) := z \bmod m$. Pentru fiecare *i* din *Rm*, avem *f-clasa*: $C_i := \{z\in\mathbb{Z} : f(z)=i\} = \{m\cdot c + i : c\in\mathbb{Z}\}$

deci $\{C_0, C_1, ..., C_{m-1}\} =: \mathbb{Z}_m$ este nucleul funcţiei *f*, şi este o partiţie a lui $\mathbb{Z}$.

Partiţiei $\mathbb{Z}_m$ a lui $\mathbb{Z}$ îi corespunde relaţia *a fi în aceeaşi f-clasă*:

$z_1 \equiv z_2 (\bmod m) \Leftrightarrow z_1 \bmod m = z_2 \bmod m$ care este o echivalenţă pe $\mathbb{Z}$, numită *relaţia de congruenţă modulo m.*

Deoarece este validă următoarea teoremă:

Teoremă. *Fie z1 şi z2 numere întregi. Atunci condiţiile:*

(i) $z_1 \bmod m = z_2 \bmod m$ *;*

(ii) m divide diferenţa z_1-z_2*;*

(iii) există un întreg t *astfel încât* $z_1=z_2+mt$

sunt echivalente.

Putem demonstra uşor următoarele rezultate:

Regula adunării: *Dacă* $z_1 \equiv z_2 (\mathrm{mod}\, m)$, *atunci* $u_1 \equiv u_2 (\mathrm{mod}\, m)$, *atunci* $az_1 + bz_2 \equiv au_1 + bu_2 (\mathrm{mod}\, m)$ *oricare ar fi întregii a, b.*

Regula înmulţirii: *Dacă* $z_1 \equiv z_2 (\mathrm{mod}\, m)$ şi $u_1 \equiv u_2 (\mathrm{mod}\, m)$, *atunci* $z_1 u_1 \equiv z_2 u_2 (\mathrm{mod}\, m)$.

Noţiunea abstractă de *congruenţă a unei structuri* s-a obţinut din noţiunea de congruenţă modulo m reţinând doar următoarele proprietăţi:

- Este o relaţie de echivalenţă pe suportul structurii;
- Deoarece $(\mathbb{Z},+)$=grup ($(\mathbb{Z},\cdot)$=monoid) şi regula adunării, cu $a=b=1$ (respectiv, regula înmulţirii) permite introducerea conceptului de *compatibilitate* a relaţiei de echivalenţă cu operaţia grupală (respectiv, cu operaţia monoidală);
- Deoarece $(\mathbb{Z},+,\cdot)$=inel, compatibilitatea relaţiei de echivalenţă cu operaţiile inelare este asigurată de data asta de ambele reguli.

În încheierea acestui paragraf venim cu următoarele precizări:

- Elementele partiţiei $\mathbb{Z}_m$ se numesc *clase de resturi modulo m*.
- (caracterizarea unei clase de resturi modulo m) Dacă $A \subset \mathbb{Z}, A \neq \emptyset$ atunci $A \in \mathbb{Z}_m$ dacă şi numai dacă sunt satisfăcute condiţiile:

(j) $x \equiv y (\mathrm{mod}\, m)$, oricare ar fi x şi y din A;

(jj) $x \in A, y \in \mathbb{Z}$ şi $x \equiv y (\mathrm{mod}\, m)$ implică $y \in A$.

- (caracterizarea relaţiei de egalitate pe $\mathbb{Z}_m$). Deoarece $\mathbb{Z}_m$ este o partiţie al lui $\mathbb{Z}$, pentru fiecare z din $\mathbb{Z}$, există şi este unică o clasă de resturi $A \in \mathbb{Z}_m$ astfel încât $z \in A$; notăm clasa de resturi A cu $\hat{z}$ şi spunem că z este un *reprezentant* a lui A. Fie acum $A, B \in \mathbb{Z}_m$ şi $z, u \in \mathbb{Z}$ cu $A=\hat{z}$ şi $B=\hat{u}$. Atunci $A=B$ dacă şi numai dacă $z = u (\mathrm{mod}\, m)$.

2. Monoizi

Presupunem (aşa cum o să procedăm şi mai jos) că s-a introdus noţiunea de monoid şi s-au stabilit regulile de calcul într-un monoid. Scopul urmărit aici este acela de a introduce operaţiile cu clase de resturi modulo m.

2.1. Monoidul ($\mathbb{Z}$,+)

Relativ la monoidul ($\mathbb{Z}$,+) (care este de fapt un grup abelian) introducem operaţia de adunare în $P^*(\mathbb{Z}) := \{A : A \subseteq \mathbb{Z} \text{ şi } A \neq \phi\}$ prin următoarea definiţie:

$A \oplus B := \{a+b : a \in A \text{ şi } b \in B\}$ unde $A, B \in P^*(\mathbb{Z})$.

Este uşor de arătat că $\left(P^*(\mathbb{Z}), \oplus\right)$=monoid abelian, unde identitatea aditivă este {0}.

Fie acum dat întregul $m \geq 2$. Ne punem problema:

Dacă $A, B \in \mathbb{Z}_m$, *atunci* $A \oplus B = ?$.

Fie $a \in A$ şi $y \in B$. Deoarece $\mathbb{Z}_m$ este o partiţie al lui $\mathbb{Z}$, există un element unic C în $\mathbb{Z}_m$ astfel încât $a+b \in C$. Dacă $a \in A$ şi $y \in B$, atunci $x = a(\mathrm{mod}\, m)$ şi $y = b(\mathrm{mod}\, m)$. În baza regulii adunării, $x + y = a + b(\mathrm{mod}\, m)$ şi deoarece $a+b \in C$ avem $x + y \in C$, deci $A \oplus B \subseteq C$.

Mai mult, dacă $c \in C$, atunci definim

$$d := c - a$$

şi obţinem acum:

$$a + b = a + d(\mathrm{mod}\, m),$$

relaţie din care rezultă (după adunarea cu $(-a)$ în ambii membri),

$$b = d(\mathrm{mod}\, m),$$

Deci *b* şi *d* sunt în *B* şi prin urmare,

$c = a + d$, cu $a \in A$ şi $d \in B$, adică $c \in A \oplus B$. În concluzie, $A \oplus B = C \in \mathbb{Z}_m$, relaţie care se scrie cu ajutorul reprezentanţilor:

$$\hat{a} \oplus \hat{b} = \widehat{a+b}.$$

Se demonstrează uşor faptul că $(\mathbb{Z}_m, \oplus)$ este grup abelian, unde elementul neutru este $\hat{0}$, iar simetrica clasei $\hat{a}$ este clasa $\widehat{(-a)}$.

2.2. Monoidul $(\mathbb{Z}, \cdot)$

Ca şi mai sus, fie $A, B \in \mathbb{Z}_m$ şi $a \in A$, $y \in B$. Produsul $a \cdot b$ al celor doi reprezentanţi se află într-o clasă $D \in \mathbb{Z}_m$. Aşa cum am procedat în 2.1 obţinem:

(*) $A \odot B \subseteq D$, unde

$$A \odot B := \{x \cdot y : x \in A, y \in B\}.$$

Considerarea unor exemple particulare ne atrage atenţia că nu este obligatoriu ca să aibă loc şi relaţia $D \subseteq A \odot B$.

În concluzie, via (*), putem introduce o nouă operaţie cu clasele A şi B din $\mathbb{Z}_m$:

$$A \boxdot B := D,$$

adică $A \boxdot B$ este acea clasă de resturi modulo m care include submulţimea $A \odot B := \{x \cdot y : x \in A, y \in B\}$ nevidă, a lui $\mathbb{Z}$; în baza definiţiei cu reprezentanţi,

(**) $\hat{a} \boxdot \hat{b} := \widehat{a \cdot b}$.

Se demonstrează uşor şi aici că $(\mathbb{Z}_m, \boxdot)$ este un monoid abelian care are ca identitatea multiplicativă pe $\hat{1}$.

O problemă importantă este următoarea:

Să se determine unităţile (adică elementele inversabile) monoidului $(\mathbb{Z}_m, \boxdot)$.

Pentru rezolvarea acestei probleme, aşa cum arată şi (**), vom folosi reprezentanţi ai claselor de resturi din $\mathbb{Z}_m$.

- Fie a unul dintre reprezentanţii unei clase inversabile din monoidul $(\mathbb{Z}_m, \boxdot)$. Atunci există o unică clasă $C \in \mathbb{Z}_m$ astfel încât

$$\hat{a} \boxdot C = \hat{1}.$$

Fie *b* un element oarecare din C. din

$$\hat{a} \boxdot \hat{b} = \hat{1}$$

deducem că

(***) $$a \cdot b \equiv 1 (\mathrm{mod}\, m)$$

şi prin urmare, $a \cdot b = 1 + tm$ pentru un anumit întreg *t*. Ultima relaţie ne arată că

$$(a, m) = (|a|, |m|) = (|a|, m) = 1,$$

deci $a \perp m$ (scriere simbolică a faptului că *a* şi *m* sunt întregi relativ primi). Deci $\hat{a} \in U(\mathbb{Z}_m)$ implică $a \perp m$.

În baza relaţiei (***) putem introduce următorul concept aritmetic: Fie $a \in \mathbb{Z}$. Spunem că numărul întreg *a* este *inversabil* modulo m, dacă există un întreg *b* astfel încât $b \cdot a \equiv 1 (\mathrm{mod}\, m)$.

- Fie acum cazul $a \perp m$. Folosind extinderea algoritmului lui Euclid, există doi întregi *u* şi *v* pentru care are loc relaţia:

$$u \cdot a + v \cdot m = 1$$

Putem scrie ultima relaţie în forma:

$$u \cdot a = 1 + (-v)m$$

deci

$$u \cdot a \equiv 1 (\mathrm{mod}\, m).$$

Din ultima relaţie deducem că

$$\hat{u} \cdot \hat{a} = \hat{1},$$

deci $\hat{a} \in U(\mathbb{Z}_m)$.

În rezumat,

$\hat{a} \in U(\mathbb{Z}_m)$ dacă şi numai dacă $a \perp m$.

Concluzii la subparagraful 2.2

- Din cele prezentate deducem că:

$a \perp m$ şi $x \equiv a(\mathrm{mod}\, m)$ implică $x \perp m \quad (x \in \mathbb{Z})$

- Deoarece $R_m = \{0,1,...,m-1\}$ este un sistem complet şi independent de reprezentanţi ai partiţiei $\mathbb{Z}_m$ a lui $\mathbb{Z}$, putem scrie $\mathbb{Z}_m = \{\hat{0}, \hat{1}, \ldots, \widehat{m-1}\}$.

- Avem pentru mulţimea U ($\mathbb{Z}_m$) a unităţile din monoidul ($\mathbb{Z}_m$, $\boxdot$):

$$U(\mathbb{Z}_m) = \{\hat{r} : r \in R_m \text{ şi } r \perp m\}$$

- Ultimul rezultat motivează deplin introducerea funcţiei φ (*indicatorul lui Euler*):
  funcţia $\varphi : \mathbb{N}^* \to \mathbb{N}^*$ este definită prin $\varphi(1) := 1$ (prin definiţie) şi
  $\varphi(m) := |\{r \in R_m : r \perp m\}| = |U(\mathbb{Z}_m)|$

- Deoarece:

În orice monoid, mulţimea unităţilor împreună cu operaţia indusă pe această mulţime de către operaţia monoidală, formează un grup.

Avem că ($U(\mathbb{Z}_m)$, $\boxdot$)=grup abelian, unde operaţia indusă de $\boxdot$ pe $U(\mathbb{Z}_m)$ s-a notat cu acelaşi simbol. Folosim acum acest grup pentru a demonstra teorema lui Euler.

Teoremă. (teorema lui Euler) *Fie întregii* $m \geq 2$ *şi a, cu* $m \perp a$. *Atunci* $a^{\varphi(m)} = 1(\mathrm{mod}\, m)$.

Demonstraţie. Relaţia $m \perp a$ ne arată că $\hat{a} \in U(\mathbb{Z}_m)$. Notăm: $\mathbb{Z}_m = \{\alpha_1, \alpha_2, ..., \alpha_s\}$ unde $s = \varphi(m)$

Din relaţiile:

$$\alpha_1 \boxdot \hat{a} = \alpha_{i_1}$$

$$\alpha_2 \boxdot \hat{a} = \alpha_{i_2}$$

.....

$$\alpha_s \boxdot \hat{a} = \alpha_{i_s}$$

deducem: $$p \boxdot (\hat{a})^s = p$$

unde produsul de clase $\alpha_1, \alpha_2, ..., \alpha_s$ s-a notat cu p. După simplificarea cu p se obţine:

$$(\hat{a})^s = \hat{1}, \text{ adică } \widehat{a^s} = \hat{1}$$

relaţie din care se obţine congruenţa

$$a^s \equiv 1 (\mathrm{mod}\, m).$$

- Demonstraţia de mai sus se foloseşte şi pentru următoarea generalizare:

Teoremă. (teorema lui Euler) *Fie* $(G, \cdot)$ *un grup abelian cu* s *elemente. Dacă* a *este un element din mulţimea* G*, atunci* $a^s = 1$*, unde 1 este identitatea grupului* $(G, \cdot)$*.*

- În încheierea acestor concluzii dăm o demonstraţie algebrică următoarei teoreme:

Teoremă. (Euclid, Gauss) *Fie întregii* m*,* a *şi* b *cu proprietăţile:*

i) $m \geq 2$

ii) $m \mid ab$

iii) $m \perp a$.

Atunci $m \mid b$.

Demonstaţie.

1) Algebrică:

$\hat{a} \in U(\mathbb{Z}_m)$, deci există $\hat{c} \in U(\mathbb{Z}_m)$ astfel încât $\hat{a} \boxdot \hat{c} = \hat{1}$.

În monoidul $(\mathbb{Z}_m, \boxdot)$ putem scrie acum succesiv

$$\hat{a} \boxdot \hat{b} = \hat{0},$$

$$\hat{c} \boxdot (\hat{a} \boxdot \hat{b}) = \hat{0},$$

$$(\hat{c} \boxdot \hat{a}) \boxdot \hat{b} = \hat{0},$$

$$\hat{1} \boxdot \hat{b} = \hat{0},$$

$$\hat{b} = \hat{0},$$

Deci $m \mid b-0=b$.

2) „Aritmetică”:

Deoarece $a \perp m$, a este inversabil *modulo m,* deci există un întreg c pentru care are loc relaţia:

$$c \cdot a \equiv 1 (\mathrm{mod}\, m).$$

Din $a \cdot b \equiv 1 (\mathrm{mod}\, m)$ deducem că $c \cdot a \cdot b \equiv 0 (\mathrm{mod}\, m)$

dar $c \cdot a \cdot b \equiv b (\mathrm{mod}\, m)$ (din $c \cdot a \equiv 1 (\mathrm{mod}\, m)$ şi $b \equiv b (\mathrm{mod}\, m)$),

deci $b \equiv 0 (\mathrm{mod}\, m)$

relaţie din care se deduce că *m* divide pe *b*.

Concluzii la paragraful 2.

FAPTE:

- Perechea $(\mathbb{Z},+)$ este un grup abelian. Relaţia de congruenţă modulo m ($m \geq 2$ întreg) este o relaţie de echivalenţă pe $\mathbb{Z}$ care este compatibilă cu operaţia grupală (adică, operaţia de adunare a numerelor întregi). Pentru fiecare *a* şi *b* din $\mathbb{Z}$, avem:

(+) $$\hat{a} \oplus \hat{b} = \widehat{a+b},$$

egalitate de mulţimi.

- Perechea $(\mathbb{Z},\cdot)$ este un monoid abelian și, pentru fiecare *a* și *b* din $\mathbb{Z}$ avem:

(++) $$\hat{a} \boxdot \hat{b} \subseteq \widehat{a \cdot b},$$

incluziune de mulţimi. În această structură avem, prin definiţie,

$$\hat{a} \boxdot \hat{b} \coloneqq \widehat{a \cdot b},$$

relaţie de definiţie (notată ca de obicei cu simbolul „:=”).

Concluzii: Fie „*” una din operaţiile „+”, respectiv „$\cdot$”. Avem: $(\mathbb{Z},*)$=monoid abelian. Pentru $m \geq 2$ dat, relaţia de congruenţă modulo *m* este compatibilă cu operaţia monoidală:

$z_1 \equiv z_2 (\mathrm{mod}\, m)$ şi $u_1 \equiv u_2 (\mathrm{mod}\, m)$ implică $z_1 * u_1 \equiv z_2 * u_2 (\mathrm{mod}\, m)$, deci relaţia de congruenţă modulo *m* este o relaţie de congruenţă a monoidului $(\mathbb{Z},*)$. Putem extinde operaţia monoidală pe $\mathbb{Z}$ la o operație monoidală pe $P^*(\mathbb{Z})$, prin definiţia:

$$A * B := \{a * b : a \in A, b \in B\}$$

unde operaţia pe $P^*(\mathbb{Z})$ s-a notat (pentru simplitate) cu acelaşi simbol, cu * (fără încercuire, respectiv fără încadrare).

Dacă $A, B \in \mathbb{Z}_m$, atunci

(+++) $$A * B \subseteq C,$$

unde $C \in \mathbb{Z}_m$ şi *C*=unic cu proprietatea (+++).

Prin urmare, putem lua prin definiţie:

(++++) $$A * B := C,$$

şi atunci $(\mathbb{Z}_m,*)$=monoid abelian, cu identitatea dată de elementul identitate din $(\mathbb{Z},*)$:

$\hat{0}$, respectiv $\hat{1}$. Mai mult, deci $a \in A$ şi $b \in B$ atunci (++++) se scrie:

(+++++) $$\hat{a} * \hat{b} := \widehat{a * b},$$

unde relaţia de definiţie „:=” este o egalitate de mulţimi, ca în (+), sau o incluziune, ca în (++). Folosind reprezentanţi (++++) şi (+++++) ne arată că C este acea clasă din $\mathbb{Z}_m$ care conţine elementul a*b. Definiţia (++++), respectiv (+++++) se bazează pe (+++). În loc să spunem că „(+++) implică (+++++)”, spunem că „operaţia (+++++) nu depinde de alegerea reprezentanţilor”. Validarea ultimei sintagme se bazează pe următorul text demonstrativ:

„Alegem $a \in A$ şi $b \in B$. Compusul a*b (care este fie o sumă, fie un produs) este un element din $\mathbb{Z}$. Cum $\mathbb{Z}_m$ este o partiţie a lui $\mathbb{Z}$, există un element C în $\mathbb{Z}_m$ astfel încât $a * b \in C$.

Fie acum o altă alegere: $x \in A$ şi $y \in B$. Au loc următoarele fapte:

- Cum $x, a \in A$, avem $x \equiv a (\mathrm{mod}\, m)$;
- Cum $y, b \in B$, avem $y \equiv b (\mathrm{mod}\, m)$.

Deoarece relaţia de congruenţă modulo *m* este o relaţie de congruenţă în monoidul ($\mathbb{Z}$,*), mai avem şi relaţia

$$x * y \equiv a * b (\mathrm{mod}\, m),$$

deci $x * y \in C$. Prin urmare, operaţia cu clase din $\mathbb{Z}_m$ dată de definiţia (++++) nu depinde de alegerea reprezentanţilor."

3. Grupuri.

UN MODEL PENTRU GRUPURI FACTOR

Perechea ($\mathbb{Z}$,+) este un grup abelian. Se ştie din teoria generală a grupurilor că:

- Dacă $a \in \mathbb{Z}$, atunci $\langle a \rangle$ (subgrupul generat de *a*) este dat de:

$$\langle a \rangle = \{ z \cdot a : z \in \mathbb{Z} \} =: a\mathbb{Z}$$

- Dacă $a \in \mathbb{Z}$, atunci $\langle a \rangle = \langle -a \rangle$, *-a* fiind simetricul lui *a*.

Folosind TIR, se demonstrează că $\{0\mathbb{Z} = \{0\}, 1\mathbb{Z} = \mathbb{Z}, 2\mathbb{Z}, 3\mathbb{Z}, ...\} = \{n\mathbb{Z} : n \in \mathbb{N}\}$ este familia tuturor subgrupurilor grupului ($\mathbb{Z}$,+).

Fie dat întregul $m \geq 2$. Atunci $m\mathbb{Z}$ este subgrup al grupului abelian ($\mathbb{Z}$,+) (pentru grupurile neabeliene considerăm divizorii normali). Faptul demonstrat în paragraful 2, că ($\mathbb{Z}_m$,+) devine grup, are următoarea prezentare:

i) Se introduce relaţia de congruenţă în raport cu subgrupul (respectiv, divizorul normal):

$$z_1 \equiv z_2 (\mathrm{mod}\, m\mathbb{Z}) :\Leftrightarrow z_1 - z_2 \in m\mathbb{Z}$$

care este o relaţie de congruenţă, adică o relaţie de echivalenţă pe suportul grupului (pe $\mathbb{Z}$) şi este compatibilă cu operaţia grupală:

$z_1 \equiv z_2 (\mathrm{mod}\, m\mathbb{Z})$ şi $u_1 \equiv u_2 (\mathrm{mod}\, m\mathbb{Z})$ implică $z_1 + u_1 \equiv z_2 + u_2 (\mathrm{mod}\, m\mathbb{Z})$.

ii) Se introduce notaţia: Dacă $x \in \mathbb{Z}$, atunci

$$\hat{x} := \{ y \in \mathbb{Z} : y \equiv x (\mathrm{mod}\, m\mathbb{Z}) \}$$

este clasa lui *x* în raport cu relaţia de echivalenţă definită la (i). Se arată că

$\hat{x} = \hat{y} \Leftrightarrow x \equiv y (\mathrm{mod}\, m\mathbb{Z})$

oricare a fi $x, y \in \mathbb{Z}$.

iii) Se introduce operaţia cu clase de echivalenţă:

$$\hat{x} + \hat{y} := \widehat{x + y}.$$

iv) Se arată că operaţia definită la (iii) nu depinde de alegerea reprezentanţilor.

v) Mulţimea de clase se notează cu:

$$\frac{\mathbb{Z}}{m\mathbb{Z}} = \frac{\text{suport grup}}{\text{suport subgrup}} =: \mathbb{Z}_m .$$

Se arată că $(\mathbb{Z}_m, +)$ este grup abelian, numit *grup factor*. În plus, $\hat{0} = m\mathbb{Z}$.

Pentru *m=0*, relaţia de congruenţă modulo $0\mathbb{Z} = \{0\}$ este chiar relaţia de egalitate pe $\mathbb{Z}$. Deci $\hat{x} = \{x\}$, oricare ar fi *x* din $\mathbb{Z}$. În plus, $(\mathbb{Z}_0, +) \cong (\mathbb{Z}, +)$, caz banal.

Pentru *m*=1, relaţia de congruenţă modulo $1\mathbb{Z} = \mathbb{Z}$ este relaţia universală pe $\mathbb{Z}$, adică orice element din $\mathbb{Z}$ este în relaţie cu orice element din $\mathbb{Z}$. Deci $\hat{0} = \mathbb{Z}$ şi prin urmare, $(\mathbb{Z}_1, +)$ este un grup cu un singur element, şi anume $\hat{0}$, caz neinteresant.

FOLOSIREA HOMOMORFISMELOR

a) Epimorfism canonic. Fie $m \geq 2$ un întreg şi fie funcţia *p* definită pe $\mathbb{Z}$ cu valori în $\mathbb{Z}_m$, dată de:

$$p(z) = \hat{z},$$

unde $\hat{z}$ este unica clasă din $\mathbb{Z}_m$ ce conţine pe *z* din $\mathbb{Z}$. Atunci *p* este un homomorfism al grupului $(\mathbb{Z}_m, +)$, adică:

$p(x + y) = p(x) + p(y)$, oricare ar fi *x,y* din $\mathbb{Z}$, şi *p*=surjecţie.

Spunem că *p* este epimorfism al grupului $(\mathbb{Z}, +)$ pe grupul factor $(\mathbb{Z}_m, +)$. Următoarele observaţii sunt utile:

- $p(x+y)=p(x)+p(y)$ înseamnă că $\widehat{x+y}=\hat{x}+\hat{y}$;
- Mulţimea $\left\{x\in\mathbb{Z}: p(x)=\hat{0}\right\}$ se numeşte nucleul homomorfismului *p* şi se notează cu $\ker(p)$. Deoarece $\ker(p)=m\mathbb{Z}$ şi $\frac{\mathbb{Z}}{m\mathbb{Z}}=\mathbb{Z}_m$, nucleul algebric al lui *p* este echivalent cu nucleul funcţional al lui *p*, adică $m\mathbb{Z}$ este echivalent cu $\mathbb{Z}_m$;
- Mulţimea $\left\{p(x): x\in\mathbb{Z}\right\}$ se numeşte imaginea homomorfismului *p* şi se notează cu $Im(p)$. Deoarece $Im(p)=\mathbb{Z}_m$, adică *p* (ca funcţie) este o surjecţie, spunem că grupul $(\mathbb{Z}_m,+)$ este imaginea homomorfă a grupului $(\mathbb{Z},+)$.

b) Ordinul unui element dintr-un grup. Fie a un element dintr-un grup oarecare (G, ·), unde elementul neutru al grupului se notează cu simbolul *e*. Se ştie că:

$$< a >=\left\{a^z : z\in\mathbb{Z}\right\}.$$

Ultima relaţie ne sugerează introducerea funcţiei $f(z):\mathbb{Z}\to G,\ f(z):=a^z$. Atunci *f* este un homomorfism de la grupul $(\mathbb{Z},+)$ la grupul (G, ·), adică:

$f(z_1+z_2)=f(z_1)\cdot f(z_2)$, conform relaţiei:

$$a^{z_1+z_2}=a^{z_1}\cdot a^{z_2},(z_1,z_2\in\mathbb{Z}).$$

Atunci:

$$Im(f)=< a >=\text{subgrup al grupului (G, ·)}$$

şi

$$\ker(f)=\left\{z\in\mathbb{Z}: f(z)=e\right\}=\left\{z\in\mathbb{Z}: a^z=e\right\}=m\mathbb{Z}$$

deoarece $\ker(f)=$subgrup al grupului $(\mathbb{Z},+)$, cu $m\in\mathbb{N}$. Se defineşte ordinul lui *a* în grupul (G, ·) prin:

$ord(a)=m$,

unde $m\mathbb{Z}=\ker(f)$ şi $m\in\mathbb{N}$. Prin urmare:

- $ord(a)=0 \Leftrightarrow a^z = e$ implică $z=0$, oricare ar fi $z \in \mathbb{Z}$;
- $ord(a)=1 \Leftrightarrow a=e$;
- $ord(a)=m \geq 2 \Leftrightarrow a^1 \neq e, a^2 \neq e, ..., a^{m-1} \neq e$ şi $a^m \neq e \Leftrightarrow a^m = e$ şi $a^z = e$ implică m/z, oricare ar fi z din $\mathbb{Z}$, echivalenţe ce se pot demonstra direct sau prin folosirea teoremei fundamentale de izomorfism pentru grupuri:

$$\frac{\mathbb{Z}}{\ker(f)} = \frac{\mathbb{Z}}{m\mathbb{Z}} = \mathbb{Z}_m = im(f) =< a >.$$

4. **Inele**

Tripletul $(\mathbb{Z},+,\cdot)$ este un inel unitar şi comutativ (mai exact, un domeniu de integritate). Fie $m \geq 2$ un întreg. Deoarece $(\mathbb{Z}_m,+)$=grup abelian şi $(\mathbb{Z}_m,\cdot)$=monoid abelian şi încă $\hat{a}\cdot\left(\hat{b}+\hat{c}\right)=\hat{a}\cdot\hat{b}+\hat{a}\cdot\hat{c}\ (a,b,c\in\mathbb{Z})$, deducem că $(\mathbb{Z},+,\cdot)$ este inel unitar şi comutativ, numit inelul claselor de resturi modulo m. Dacă relativ la grupul $(\mathbb{Z},+)$ mulţimea $m\mathbb{Z} := \{m\cdot z : z\in\mathbb{Z}\}$ este divizor normal, relativ la inelul $(\mathbb{Z},+,\cdot)$, mulţimea $m\mathbb{Z}$ este un ideal bilateral. Deci putem da încă un model de a construi inelul factor $(\mathbb{Z}_m,+,\cdot)$ plecând de la inelul $(\mathbb{Z},+,\cdot)$ şi de la idealul bilateral $m\mathbb{Z}$, construcţie pe care nu o mai detaliem.

Funcţia $p:\mathbb{Z}\to\mathbb{Z}_m$ definită prin $p(z)=\hat{z}$ devine un epimorfism de inele, numită *epimorfismul canonic*. Aşa cum am arătat la celelalte paragrafe, $U(\mathbb{Z}_m)=\{\hat{r} : r\in R_m$ şi r $\perp$ m$\}$. În particular, $(\mathbb{Z}_m,+,\cdot)$=corp dacă şi numai dacă *m*=număr natural prim.

5. Lema chinezească a resturilor.

Fie daţi întregii: $m_1, m_2, ..., m_t \geq 2$, numiţi *moduli* ($t \geq 2$), avem inele factor: $(\mathbb{Z}_{m_i},+,\cdot)$ $(i=1,2,...,t)$. Deoarece $\mathbb{Z}_{m_i}=\{0+m_i\mathbb{Z}, 1+m_i\mathbb{Z},,..., (m_i-1)+m_i\mathbb{Z}\}$, adică clasa lui 0 modulo idealul $m_i\mathbb{Z}$, …, clasa lui m_i-1 modulo idealul $m_i\mathbb{Z}$ (nu avem suficiente simboluri diacritice pentru a nota clasele de resturi modulo m_i), *i*=1, 2, …, *t*, deducem că produsul cartezian de mulţimi $P := \mathbb{Z}_{m_1}\times\mathbb{Z}_{m_2}\times...\times\mathbb{Z}_{m_t}$ are $m_1, m_2, ...m_t =: M$ elemente. Pe mulţimea *P* se introduc operaţiile:

1) De adunare, $\alpha+\beta := (x_1+y_1, x_2+y_2, ..., x_n+y_n)$;
2) De înmulţire, $\alpha\cdot\beta := (x_1\cdot y_1, x_2\cdot y_2, ..., x_n\cdot y_n)$;

pentru *n*-uplele: $\alpha = (x_1, x_2, ..., x_n)$ şi $\beta = (y_1, y_2, ..., y_n)$ din *P* (deci, elementele din α şi din β sunt clase de resturi).

Se demonstrează uşor că $(P, +, \cdot)$ este un inel unitar şi comutativ, numit *produsul inelelor* $(\mathbb{Z}_{m_i}, +, \cdot)$ $(i = 1, 2, .., t)$, unde elementul nul din *P* este uplul:

$$(0 + \mathbb{Z}_{m_1}, 0 + \mathbb{Z}_{m_2}, ..., 0 + \mathbb{Z}_{m_t}) =: 0_P,$$

iar elementul identitate din *P* este uplul: $(1 + \mathbb{Z}_{m_1}, 1 + \mathbb{Z}_{m_2}, ..., 1 + \mathbb{Z}_{m_t}) =: 1_P$.

Cu notaţiile astfel introduse, următoarea teoremă o vom numi *lema chinezească a resturilor*.

Teoremă (LCR)

1) *Funcţia* $\varphi : \mathbb{Z} \to P$ *definită prin* $\varphi(z) = (z + m_1\mathbb{Z}, z + m_2\mathbb{Z}, ..., z + m_t\mathbb{Z},)$ *este un homomorfism de la inelul* $(\mathbb{Z}, +, \cdot)$ *la inelul* $(P, +, \cdot)$ *şi* $\ker(\varphi) = \mu$, *unde* μ *este cel mai mic multiplu comun al numerelor naturale* $m_1, m_2, ...m_t$.
2) *Funcţia* φ *este un epimorfism al inelului* $(\mathbb{Z}, +, \cdot)$ *pe inelul* $(P, +, \cdot)$ *dacă şi numai dacă* $m_i \perp m_j$, *oricare ar fi* $i \neq j$ *din mulţimea* $\{1, 2, ..., t\}$.

Demonstraţie.

(1) Demonstraţia faptului că φ este un homomorfism de la inelul $(\mathbb{Z}, +, \cdot)$ în inelul $(P, +, \cdot)$ nu ridică mari probleme.

Fie acum *z* din $\ker(\varphi)$. Atunci $\varphi(z) = 0_P$, deci *z* este un multiplu de m_i $(i = 1, 2, .., t)$, de unde se deduce că *z* este un multiplu al lui μ, deci $z \in \mu\mathbb{Z}$ şi prin urmare, $\ker(\varphi) \leq \mu\mathbb{Z}$. Reciproc, dacă $z \in \mu\mathbb{Z}$, atunci $m_i \mid \mu \mid \mathbb{Z}$ $(i = 1, 2, .., t)$ şi deci, $\varphi(z) = 0_P$, adică $\mu\mathbb{Z} \leq \ker(\varphi)$. În concluzie, $\ker(\varphi) = \mu\mathbb{Z}$.

(2) Necesitatea. Deoarece φ este o funcţie surjectivă, elementele din P:

$$E_1 := (1 + m_1\mathbb{Z}, 0 + m_2\mathbb{Z}, ..., 0 + m\mathbb{Z}_t),$$
$$E_2 := (0 + m_1\mathbb{Z}, 1 + m_2\mathbb{Z}, ..., 0 + m\mathbb{Z}_t),$$
$$.....$$
$$E_t := (0 + m_1\mathbb{Z}, 0 + m_2\mathbb{Z}, ..., 1 + m\mathbb{Z}_t)$$

sunt în imaginea lui ϕ. Deci există în $\mathbb{Z}$ t elemente $z_1, z_2, ..., z_t$ astfel încât

$$\phi(z_i) = E_i \ (i = 1, 2, ..., t).$$

Din $\phi(z_i) = E_i$ deducem egalitatea:

$$(z_1 + m_1\mathbb{Z}, z_1 + m_2\mathbb{Z}, ..., z_1 + m_t\mathbb{Z}) = (1 + m_1\mathbb{Z}, 0 + m_2\mathbb{Z}, ..., 0 + m_t\mathbb{Z})$$

de unde se obţin congruenţele: $z_1 \equiv 1 (\mathrm{mod}\, m_1)$ şi $z_1 \equiv 0 (\mathrm{mod}\, m_i)$ cu $(i = 1, 2, ..., t)$. Prin urmare $z_1 = 1 + m_1 \cdot k = m_i \cdot c_i$ relaţii ce implică faptul că $m_1 \perp m_i$ $(i = 2, 3, ..., t)$.

Analog, $m_j \perp m_i$, oricare ar fi *i* din mulţimea $\{1, 2, ..., t\} - \{j\}$ pentru $j = 2, 3, ..., t$.

Suficienţa. Folosim metoda constructivă. Introducem notaţiile:

$$M_i := \frac{M}{m_i} \ (i = 1, 2, ..., t).$$

Deoarece $m_1 \perp m_i$ $(i = 2, 3, ..., t)$, deducem că $m_1 \perp M_1$, deci întregul *M1* este inversabil modulo *M1* şi prin urmare, există şi este unic întregul $\mu_1 \in \mathbb{R}_{m_1} = \{0, 1, ..., m_1 - 1\}$ astfel încât

$$\mu_1 M_1 \equiv 1 (\mathrm{mod}\, m_1).$$

Faptul că μ_1 este în $\mathbb{R}_{m_1}$ are următoarea demonstraţie: cum $M_1 \perp m_1$, există un întreg *a* pentru care avem $aM_1 \equiv 1 (\mathrm{mod}\, m_1)$. Atunci μ_1 este restul împărţirii întregului *a* la modulul *m1*. Unicitatea lui μ_1 se justifică astfel: dacă şi *b* este în $\mathbb{R}_{m_1}$ şi dacă $bM_1 \equiv 1 (\mathrm{mod}\, m_1)$, atunci $\mu_1 M_1 \equiv bM_1 (\mathrm{mod}\, m_1)$ şi prin urmare, $\mu_1 \equiv b (\mathrm{mod}\, m_1)$, adică $b = \mu_1$. (algebric: $\widehat{\mu_1} \cdot \widehat{M_1} = \hat{1} = \hat{b} \cdot \widehat{M_1}$ implică, după simplificarea cu $\widehat{M_1} \in U(\mathbb{Z}_{m_1})$, $\widehat{\mu_1} = \hat{b}$, deci $\mu_1 = b$, unde $\hat{z}$ este clasa lui *z* din $\mathbb{Z}$)

Analog, există un unic μ_i în $\mathbb{R}_{m_1} = \{0, 1, ..., m_i - 1\}$ astfel încât

$$\mu_1 M_i \equiv 1 (\mathrm{mod}\, m_i), \text{ unde } (i = 2, 3, ..., t).$$

Fie acum elementul oarecare $\rho := \left(r_1 + m_1\mathbb{Z}, r_2 + m_2\mathbb{Z}, ..., r_t + m_t\mathbb{Z}\right)$ din P unde $r_1, r_2, ..., r_t \in \mathbb{Z}$. Definim elementul z din $\mathbb{Z}$ prin $z := r_1\mu_1 M_1 + ... + r_t\mu_t M_t$. Pentru fiecare $i = 1, 2, ..., t$ avem:

- $\mu_i M_i \equiv 1 \left(\mathrm{mod}\, m_i\right)$, deci $r_i\mu_i M_i \equiv r_i \left(\mathrm{mod}\, m_i\right)$ şi
- $\mu_i M_i \equiv 0 \left(\mathrm{mod}\, m_j\right)$, deoarece m_j divide M_i ($j \in \{1, 2, ...t\} - \{i\}$). Deci, $\varphi(z) = \rho$.

Consecinţe. În baza teoremei fundamentale de izomorfism pentru inele, avem izomorfismul:

$$\frac{\mathbb{Z}}{\ker(\varphi)} \cong im(\varphi), \text{ adică } \frac{\mathbb{Z}}{\mu\mathbb{Z}} = \mathbb{Z}\mu \cong im(\varphi).$$

Consecinţa 1. *Imaginea* $im(\varphi)$ *este dată de*

$$im(\varphi) = \left\{\left(i + m_1\mathbb{Z}, i + m_2\mathbb{Z}, ..., i + m_t\mathbb{Z},\right) : i = 0, 1, ..., \mu - 1\right\}.$$

Consecinţa 2. *Are loc izomorfismul:* $\frac{\mathbb{Z}}{M\mathbb{Z}} = \mathbb{Z}_M \cong P$.

Deoarece $\varphi(z_1) = \varphi(z_2) \Leftrightarrow z_1 - z_2 \in \ker(\varphi)$ $\left(z_1, z_2 \in \mathbb{Z}\right)$, pentru Consecinţa 2 putem da următoarea formulare:

Teoremă (forma clasică a LCR). *Fie daţi modulii* m_i $\left(i = 1, 2, ..., t\right)$ *cu* $m_i \perp m_j$ *pentru orice* $i \neq j$ *din* $\{1, 2, ..., t\}$. *Atunci, oricare ar fi întregii* $a_1, a_2, ..., a_t$, *sistemul de congruenţe*

$$\begin{cases} x \equiv a_1 \left(\mathrm{mod}\, m_1\right) \\ \quad\vdots \\ x \equiv a_t \left(\mathrm{mod}\, m_t\right) \end{cases}$$

are exact o soluţie în mulţimea $[z, z + M) \cap \mathbb{Z}$, *oricare ar fi întregul* z.

§3.2. Varianta polinomială a LCR

Pentru dezvoltarea acestei secţiuni, reactualizăm termeni şi rezultate privitoare la polinoamele într-o nedeterminată şi cu coeficienţi reali. De asemenea, mai precizăm şi

principalele structuri algebrice necesare. Modelul ce trebuie urmat este domeniul de integritate euclidian $(\mathbb{Z},+,\cdot)$.

(A) $\mathbb{R}$ – algebra $\mathbb{R}[x]$

(1) $\mathbb{R}$ – algebra $\mathbb{R}[x]$

- se consideră fixate următoarele obiecte:
  - x = nedeterminată;
  - $\mathbb{R}[x]$ = mulţimea polinoamelor în x cu coeficienţi reali.
- un polinom nenul f(x) din $\mathbb{R}[x]$ are *forma algebrică standard* (care este unică):

(*) $f(x)=a_0x^0+a_1x^1+...+a_nx^n$, unde

  - $m\geq 0$ este număr întreg, numit *gradul* polinomului f(x) (în notaţie, $n=grad(f(x))$);
  - elementele $a_0,a_1,...,a_n$ (numite *coeficienţii* lui f(x)) sunt numere reale;
  - $a_n\neq 0$ este numit *coeficientul dominant* al lui f(x).
- Operaţia de extragere a coeficientului puterii k a lui x se notează cu simbolul $[x^k]$ şi se defineşte prin (conform (*)): $[x^k]f(x):=a_k$ ($k\in\mathbb{N}$).

Evident, $k>n$ implică $[x^k]f(x)=0$ ($k\in\mathbb{N}$).

Polinomul nul, notat cu $\theta(x)$, este caracterizat de condiţiile:

$[x^k]\theta(x)=0$, oricare ar fi $k\in\mathbb{N}$, motiv pentru care luăm $grad(\theta(x))=-\infty$.

- $\mathbb{R}[x]$ se organizează ca $\mathbb{R}$-algebră în baza următoarelor definiţii, dacă $f(x),g(x)\in\mathbb{R}[x]$ şi $r\in\mathbb{R}$, atunci:
  - $[x^k](f(x)+g(x)):=[x^k]f(x)+[x^k]g(x)$, oricare ar fi $k\in\mathbb{N}$;
  - $[x^k](f(x)\cdot g(x)):=\sum_{i+j=k}[x^i]f(x)\cdot[x^j]g(x)$, oricare ar fi $k\in\mathbb{N}$;
  - $[x^k](r\cdot f(x)):=r\cdot[x^k]f(x)$, oricare ar fi $k\in\mathbb{N}$

Tripletul $\left(\mathbb{R}[x],+,\cdot\right)$ este un inel unitar şi comutativ; elementul de identitate este $e(x):=1x^0$, iar elementul nul este $\theta(x)=0\cdot e(x)$. Inelul $\left(\mathbb{R}[x],+,\cdot\right)$ este o $\mathbb{R}$-algebră.

(2) Funcţia grad

- Structura de monoid ordonat arhimedian $\left(\mathbb{N},+,\leq\right)$ se extinde la $\overline{\mathbb{N}}$ introducând relaţiile:
  - $(-\infty)+(-\infty):=-\infty$ şi $(-\infty)+n=n+(-\infty):=-\infty$ oricare ar fi $n\in\mathbb{N}$.
  - $-\infty=-\infty$ şi $-\infty<n$ oricare ar fi $n\in\mathbb{N}$.

Noua structură $\left(\overline{\mathbb{N}},+,\leq\right)$ este un monoid ordonat (dar nu arhimedian, deoarece $k(-\infty)=\underbrace{(-\infty)+(-\infty)+\ldots+(-\infty)}_{k\text{ termeni}}=-\infty<n$, oricare ar fi $k\in\mathbb{N}^*$ şi $n\in\mathbb{N}$).

- *Funcţia grad*, notată grad, se defineşte astfel: $grad:\mathbb{R}[x]\to\mathbb{N}$, şi pentru un element oarecare *f(x)* din $\mathbb{R}[x]$ avem:

  (i) $grad\left(f(x)\right)=-\infty$, dacă *f(x)* este polinom nul, respectiv

  (ii) $grad\left(f(x)\right)=\max\left\{k\in\mathbb{N}:\left[x^k\right]f(x)\neq 0\right\}\in\mathbb{N}$, dacă *f(x)* nu este polinom nul.

- Următoarele relaţii relative la $\left(\overline{\mathbb{N}},+,\leq\right)$ constituie proprietăţile algebrice ale funcţiei grad:
  - $grad\left(f(x)+g(x)\right)\leq\max\left(grad\left(f(x)\right),grad\left(g(x)\right)\right)$;
  - $grad\left(-g(x)\right)=grad\left(g(x)\right)$
  - $grad\left(f(x)\cdot g(x)\right)=grad\left(f(x)\right)+grad\left(g(x)\right)$ (relaţie numită *teorema gradului*)
  - $grad\left(r\cdot f(x)\right)=gradf(x)$ m dacă $r\neq 0$, respectiv $grad\left(r\cdot f(x)\right)=-\infty$, dacă $r=0$

$\left(f(x),g(x)\in\mathbb{R}[x];r\in\mathbb{R}\right)$

(3) Relaţia de egalitate pe $\mathbb{R}[x]$

(i) (egalitatea după grad şi coeficienţi) Fie *f(x)* şi *g(x)* din $\mathbb{R}[x]$. Spunem că polinoamele *f(x)* şi *g(x) sunt egale după coeficienţi* dacă şi numai dacă $\left[x^k\right]f(x)=\left[x^k\right]g(x)$, oricare ar fi $k\in\mathbb{N}$.

(ii) (egalitatea după valori) Fie *f(x)* un polinom nenul din $\mathbb{R}[x]$ care are forma algebrică standard exprimată în (*). Pentru fiecare *r* din (*), expresia numerică

$$a_0r^0+a_1r^1+\ldots+a_nr^n\in\mathbb{R}$$

(ce se obţine din (*) prin substituţia $x\leftarrow r$) se numeşte *valoarea* polinomului *f(x) în r* şi se notează cu simbolul *f(r)* (prin convenţie, $r^0=1$, oricare ar fi $r\in\mathbb{R}$)

Dacă $r\in\mathbb{R}$, atunci $\theta(r):=0$.

În baza precizărilor de mai sus dăm următoarea definiţie: fie *f(x)* şi *g(x)* din $\mathbb{R}[x]$. Spunem că polinoamele *f(x)* şi *g(x) sunt egale după valori* dacă și numai dacă *f(r)=g(r)*, oricare ar fi $r\in\mathbb{R}$.

Se ştie că cele două relaţii de egalitate sunt echivalente pe $\mathbb{R}[x]$, motiv pentru care le notam pe ambele prin simbolul =.

(4) Rădăcini ale unui polinom

- Fie dat un polinom *f(x)* din $\mathbb{R}[x]$. Un element oarecare $r\in\mathbb{R}$ *este o rădăcină* a polinomului *f(x)* dacă *f(r) =0*.

Deoarece $\theta(r)=0$, oricare ar fi $r\in\mathbb{R}$, urmează că polinomul nul $\theta(x)$ are rădăcină pe orice element din $\mathbb{R}$. Dacă a_0 este un număr real nenul şi dacă $f(x)=a_0x^n$, atunci $f(r)=a_0$, oricare ar fi $r\in\mathbb{R}$, deci *f(x)* nu are nicio rădăcină reală.

Polinoamele care au gradul egal cu $-\infty$ sau egal cu 0 se numesc *polinoame constante*. Celelalte polinoame din $\mathbb{R}[x]$ se numesc *polinoame neconstante*.

- **Teoremă** (teorema lui Descartes) *Orice polinom neconstant* f(x) *din* $\mathbb{R}[x]$ *are în* $\mathbb{R}$ *cel mult* n *rădăcini distincte, unde* $grad\left(f(x)\right)=n\geq 1$.

- **Teoremă** (consecinţă a teoremei lui Descartes) *Fie* f(x) *şi* g(x) *din* $\mathbb{R}[x]$*, cu* $grad(f(x)), grad(g(x)) \le n \quad (n \in \mathbb{N})$*. Dacă există în* $\mathbb{R}$ n+1 *elemente:* $r_1 < r_2 < ... < r_n < r_{n+1}$ *astfel încât* $f(r_i) = g(r_i)$ *(*$i = 1, 2, \ldots, n+1$*), atunci* f(x)=g(x) *(şi prin urmare,* f(r)=g(r)*, oricare ar fi* $r \in \mathbb{R}$*).*

(5) Teorema de împărţire cu rest (TIR)

Teoremă (numită încă şi teorema de împărţire euclidiană). *Fie* f(x) *şi* g(x) *polinoame din* $\mathbb{R}[x]$*, cu* $g(x) \neq \theta(x)$*. Atunci există şi sunt unice polinoamele* c(x) *(*numit *câtul) şi* r(x) *(*numit *restul) din* $\mathbb{R}[x]$ *care satisfac relaţiile:*

(i) (proba împărţirii) $f(x) = g(x) \cdot c(x) + r(x)$*;*

(ii) (condiţia restului) $grad(r(x)) < grad(g(x))$.

Notaţie: $f(x) \bmod g(x) := r(x)$.

(6) Structuri algebrice cu mulţimea suport $\mathbb{R}[x]$

1) $(\mathbb{R}[x], +, \cdot)$ este o $\mathbb{R}$ - algebră.

2) $(\mathbb{R}[x], +, \cdot)$ este un domeniu de integritate (proprietatea de integritate: $f(x) \neq \theta(x)$ şi $g(x) \neq \theta(x)$ implică $f(x)g(x) \neq \theta(x)$ este o consecinţă a teoremei gradului) euclidian (în baza TIR), aşa cum este şi $(\mathbb{Z}, +, \cdot)$.

3) $(\mathbb{R}[x], +)$ este un $\mathbb{R}$ - spaţiu vectorial de dimensiune infinită. Baza standard este $\sigma = (x^0, x^1, x^2, ...) = (x^n) \ n \ge 0$.

(B) Aritmetica domeniului de integritate euclidian $\mathbb{R}[x]$

(1) Relaţia de divizibilitate în $\mathbb{R}[x]$

- Fie *f(x)* şi *g(x)* din $\mathbb{R}[x]$. Spunem că *f(x) divide* pe *g(x)* dacă există în $\mathbb{R}[x]$ un polinom *h(x)* pentru care are loc relaţia $h(x)f(x) = g(x)$, deci „factorul divide produsul”.

Notaţie simbolică: $f(x)\big|g(x)$.

- Dacă $f(x)\neq\theta(x)$, atunci $f(x)\big|g(x)$ dacă şi numai dacă $g(x)\bmod f(x)=\theta(x)$.
- Dacă $g(x)=\theta(x)$, luând $h(x)=\theta(x)$, atunci $f(x)\big|g(x)$, oricare ar fi *f(x)* din $\mathbb{R}[x]$.
- Relaţia de divizibilitate în $\mathbb{R}[x]$ este o preordine (este reflexivă şi tranzitivă)

▪ Relaţia de divizibilitate din $\mathbb{R}[x]$ se extinde la o relaţie de echivalenţă pe $\mathbb{R}[x]$ (numită *relaţia de asociere în divizibilitate*) pe baza definiţiei:

$$f(x)\sim g(x):\Leftrightarrow f(x)\big|g(x)\ \text{şi}\ g(x)\big|f(x).$$

- Se demonstrează uşor că: *Fie* f(x) *şi* g(x) *din* $\mathbb{R}[x]$. *Atunci* $f(x)\sim g(x)$ *dacă şi numai dacă există un scalar real nenul* r *astfel încât* f(x) = c·g(x) *(sau echivalent* $g(x)=\frac{1}{c}f(x)$*).*
- Clasele de echivalenţă ale relaţiei de asociere în divizibilitate sunt aşadar:

$\widehat{\theta(x)}=\{\theta(x)\}$ şi $f(x)=\{rf(x):r\in\mathbb{R}\}$, dacă *f(x)* este un polinom nenul din $\mathbb{R}[x]$. În particular, clasa de echivalenţă a identităţii $e(x)=1x^0$ este

$$\widehat{e(x)}=\{re(x):r\in\mathbb{R}^*\}=U(\mathbb{R}[x]),$$

adică mulţimea unităţilor (elementele inversabile) din $\mathbb{R}[x]$.

- Mulţimea de clase $\frac{\mathbb{R}[x]}{\sim}$ se ordonează în baza definiţiei:

$$\widehat{f(x)}\leq\widehat{g(x)}:\Leftrightarrow f(x)\big|g(x)\ \ (f(x),g(x)\in\mathbb{R}[x])$$

care nu depinde de alegerea reprezentanţilor. În mulţimea parţial ordonată: $\left(\frac{\mathbb{R}[x]}{\sim}, \leq\right)$,

primul element este clasa $e(x) = U\left(\mathbb{R}[x]\right)$, iar ultimul element este clasa $\widehat{\theta(x)} = \{\theta(x)\}$.

Observăm că $\widehat{e(x)} \cup \widehat{\theta(x)}$ = mulţimea polinoamelor constante.

- Spunem că o proprietate (P) este *proprietate aritm*etică dacă din faptul că o are un polinom *f(x)* din $\mathbb{R}[x]$ rezultă că o are orice polinom din clasa sa de echivalenţă, $\widehat{f(x)}$.
  - Fie $f(x) = a_0x^0 + a_1x^1 + ... + a_nx^n$ forma algebrică standard a unui polinom *f(x)* din $\mathbb{R}[x]$.

Atunci definim polinomul

$$f^*(x) := \frac{1}{a_n} f(x) = \frac{a_0}{a_n}x^0 + \frac{a_1}{a_n}x^1 + ... + \frac{a_{n-1}}{a_n}x^{n-1} + 1 \cdot x^n,$$

numit *polinomul monic asociat lui f(x)* (un polinom nenul se numeşte monic dacă coeficientul său dominant este egal cu numărul real 1). Un produs finit de polinoame monice este un polinom monic. Dacă *n=0*, atunci $f(x) = a_0x^0$ şi $f^*(x) = e(x)$ $(a_0 \neq 0$ din $\mathbb{R})$. Prin definiţie, $\theta^*(x) := \theta(x)$.

(2) Proprietăţi aritmetice

Fie *f(x)* un polinom neconstant din $\mathbb{R}[x]$. Spunem:

(i) că *f(x) este polinom ireductibil (în* $\mathbb{R}[x]$*)* dacă $f(x) = g(x)h(x)$ implică $g^*(x) = e(x)$ sau $h^*(x) = e(x)$, oricare ar fi $g(x), h(x) \in \mathbb{R}[x]$;

(ii) că *f(x) este polinom reductibil (în* $\mathbb{R}[x]$*)* dacă există în $\mathbb{R}[x]$ două polinoame *g(x)* şi *h(x)* cu proprietăţile $f(x) = g(x) \cdot h(x)$, $g^*(x) \neq e(x)$ şi $h^*(x) \neq e(x)$ (deci *g(x)* şi *h(x)* sunt polinoame neconstante);

(iii) că *f(x) este un polinom prim* (în $\mathbb{R}[x]$) dacă $f(x) \mid g(x)h(x)$ implică $f(x) \mid g(x)$ sau $f(x) \mid h(x)$, oricare ar fi polinoamele $g(x), h(x) \in \mathbb{R}[x]$.

Observaţii.

a) Proprietăţile: „a fi polinom ireductibil”, „a fi polinom reductibil” şi „a fi polinom prim” sunt proprietăţi aritmetice, aşa cum lesne se poate demonstra.

b)Proprietăţile: „a fi polinom ireductibil” şi „a fi polinom prim” sunt echivalente.

c) Avem analogiile:

- Polinom ireductibil în $\mathbb{R}[x] \leftrightarrow$ număr prim în $\mathbb{N}$ (sau în $\mathbb{Z}$)
- Polinom reductibil în $\mathbb{R}[x] \leftrightarrow$ număr compus în $\mathbb{N}$

d) Proprietăţile: „a fi polinom ireductibil” şi „a fi polinom reductibil” sunt în relaţia logică de contradicţie relativ la mulţimea de polinoame neconstante din $\mathbb{R}[x]$. În concluzie, dacă *f(x)* este un polinom neconstant din $\mathbb{R}[x]$, atunci pentru $f^*(x)$ (deci şi pentru *f(x)*) are loc una şi numai una din situaţiile:

i) $f^*(x)$ este ireductibil

ii) $f^*(x)$ este reductibil.

(3) Cel mai mare divizor comun

Pentru un polinom nenul *f(x)* din $f^*(x)$ notăm

$D^*(f(x)) := \{g(x) \in \mathbb{R}[x] : g(x)$ este nenul, este monic şi $g(x) | f(x)\}$ deci $D^*(f(x))$ este mulţimea divizorilor monici ai polinomului *f(x)*. Fie *f(x)* şi *g(x)* două polinoame nenule din $\mathbb{R}[x]$. Mulţimea $D^*(f(x)) \cap D^*(g(x))$ conţine divizorii comuni monici ai polinoamelor f(x) şi g(x). Cel mai mare polinom în grad din $D^*(f(x)) \cap D^*(g(x))$ se numeşte *cel mai mare divizor comun (monic) al polinoamelor f(x) şi g(x)* şi se notează cu simbolul (*f(x),g(x)*). Dacă *(f(x),g(x)) = e(x)*, spunem că polinoamele *f(x)* şi *g(x) sunt relativ prime*, şi notăm acest fapt cu simbolul $f(x) \perp g(x)$.

- În baza TIR se obţine algoritmul lui Euclid în varianta polinomială. Ca şi în $(\mathbb{Z},+,\cdot)$, se obţine rezultatul: *Fie* f(x) *şi* g(x) *două polinoame nenule din* $\mathbb{R}[x]$. *Dacă (*f(x),g(x)) = d(x)*, atunci* $D^*(f(x))\cap D^*(g(x))=D^*(d(x))$.

Plecând de la acest rezultat se obţin şi celelalte rezultate analoge aritmeticii lui $(\mathbb{Z},+,\cdot)$.

- $(f(x)h(x),g(x)h(x))=h(x)(f(x)g(x))$ (*f(x)* şi *g(x)* polinoame nenule din $\mathbb{R}[x]$; *h(x)* polinom nenul şi monic din $\mathbb{R}[x]$).
- $(f(x),g(x))=e(x)$ implică $(f(x),g(x)|h(x))=(f(x),h(x))$ (*f(x), g(x), h(x)* polinoame nenule din $\mathbb{R}[x]$).
- Dacă $(f(x),g_i(x))=e(x)$ ($i=1,2,\ldots,n$), atunci $(f(x),g_1(x),...,g_n(x))=e(x)$ (*f(x)* şi g_i(x) polinoame nenule din $\mathbb{R}[x]$).
- Dacă $f(x)|g(x)h(x)$ şi $(f(x),g(x))=e(x)$ atunci $f(x)|h(x)$ (*f(x), g(x), h(x)* polinoame nenule din $\mathbb{R}[x]$).
- Dacă $f(x)|h(x),g(x)|h(x)$ şi $(f(x),g(x))=e(x)$ atunci $f(x)g(x)|h(x)$ (*f(x), g(x), h(x)* polinoame nenule din $\mathbb{R}[x]$).
- Dacă $(f(x),g(x))=d(x)\neq e(x)$, atunci $\left(\frac{f(x)}{d(x)},\frac{g(x)}{d(x)}\right)=e(x)$ (*f(x), g(x)* polinoame nenule din $\mathbb{R}[x]$).

(4) Polinoame monice ireductibile. Teorema fundamentală a aritmeticii lui $\mathbb{R}[x]$.

- **O clasificare a polinoamelor nenule din $\mathbb{R}[x]$**

Pentru fiecare polinom nenul *f(x)* din $\mathbb{R}[x]$ are loc doar una din următoarele situaţii:

(i) *f(x)* este polinom constant, şi atunci $D^*(f(x))=\{e(x)\}$, deci polinomul identitate $e(x)=1x^0$ este singurul divizor monic;

(ii) *f(x)* este polinom ireductibil, şi atunci *f(x)* este polinom neconstant şi $D^*(f(x))=\{e(x)\}, f^*(x)$, deci *f(x)* are exact doi divizori monici;

(iii) *f(x)* este polinom ireductibil, şi atunci *f(x)* este polinom neconstant şi $D^*\left(f\left(x\right)\right)=\left\{d_1\left(x\right)=e\left(x\right),d_2\left(x\right),...,d_t\left(x\right)=f^*\left(x\right)\right\}$, deci *f(x)* are exact $t\geq 3$ divizori monici distincţi.

- **Polinoame monice ireductibile**
  - Exemple: Se demonstrează uşor faptul că:

a) Polinoamele monice ireductibile de gradul întâi sunt de forma $m'_a\left(x\right)=x-ax^0$, unde $a\in\mathbb{R}$;

b) Polinoamele monice ireductibile de gradul doi sunt de forma $m''_{b,c}\left(x\right)=x^2+bx^1+cx^0$ unde $b,c\in\mathbb{R}$ şi $\Delta=b^2-4c<0$

În baza teoremei fundamentale a algebrei (care poate fi formulată astfel: *În domeniul de integritate euclidian* $\left(\mathbb{C}\left[x\right],+,\cdot\right)$*, singurele polinoame ireductibile monince sunt cele de forma* $m'_\alpha\left(x\right)=x-\alpha$*, cu* $\alpha\in\mathbb{C}$.) rezultă că alte polinoame monice ireductibile nu mai există în $\mathbb{R}\left[x\right]$.

- **O proprietate a polinoamelor reductibile:** *Dacă f(x) este un polinom reductibil, atunci polinomul reductibil are un divizor polinom monic ireductibil*.

Demonstraţie. Este suficient să luăm în (iii) pe $d_j\left(x\right)$ cu proprietăţile $d_j\left(x\right)\neq e\left(x\right)$ şi $gradd_j\left(x\right)\leq grad\left(d\left(x\right)\right)\ \left(j=2,3,...,t\right)$.

- **O generalizare a unei proprietăţi a polinoamelor ireductibile.**

Fie p(x) *un polinom ireductibil (monic sau nu). Dacă* p(x) *divide un produs* $f_1\left(x\right)f_2\left(x\right)...f_t\left(x\right)$ *de polinoame din , atunci p(x) divide cel puţin un factor:* $\mathbb{R}\left[x\right]\left(t\geq 2\right)$ *pentru cel puţin un* i *din {1, 2, ..., t}.*

Demonstraţie. Avem $p^*\left(x\right)=\left(p\left(x\right),f_1\left(x\right)f_2\left(x\right)...f_t\left(x\right)\right)$. Din ipoteza $\left(p\left(x\right),f_i\left(x\right)\right)=e\left(x\right)\ \left(i=1,2,...,t\right)$ se obţine concluzia absurdă $p^*\left(x\right)=\left(p\left(x\right),f_1\left(x\right)f_2\left(x\right)...f_t\left(x\right)\right)=e\left(x\right)$. Cu observaţia: Fie *p(x)* un polinom ireductibil din $\mathbb{R}\left[x\right]$ şi fie $f\left(x\right)\in\mathbb{R}\left[x\right]$. Atunci:

$$D^*\left(p\left(x\right)\right)\cap D^*\left(f\left(x\right)\right)=\left\{e\left(x\right)\right\},\ \text{dacă}\ p\left(x\right)\nmid f\left(x\right);$$

respectiv $D^*\left(p\left(x\right)\right)\cap D^*\left(f\left(x\right)\right)=\left\{e\left(x\right),p^*\left(x\right)\right\}$ dacă $p\left(x\right)\mid f\left(x\right)$.

- **Teorema fundamentală a aritmeticii lui $\mathbb{R}[x]$.**

Fie $f(x)=a_0x^0+a_1x^1+...+a_nx^n$ *forma algebrică standard a unui polinom reductibil din* $\mathbb{R}[x]$. *Atunci există şi sunt unice polinoamele monice ireductibile* $m_1(x),m_2(x),...,m_t(x)$ $(t\geq 2)$ *astfel încât*

$$(*)\ f(x)=a_n\cdot m_1(x)\cdot m_2(x)\cdot...\cdot m_t(x).$$

Demonstraţia Existenţei şi **Unicităţii** descompunerii (*) este analoagă celei privitoare la numerele compuse din $\mathbb{N}$: (j) pentru demonstraţia **Existenţei** ne folosim de proprietatea că orice polinom reductibil are cel puţin un divizor polinom monic şi ireductibil şi de proprietatea de bună ordonare a lui $\mathbb{N}$ prin ordinea naturală şi (jj) pentru demonstraţia **Unicităţii** ne folosim de proprietatea prezentată mai sus privind polinoamele ireductibile.

- **Descompunerea standard a unui polinom ireductibil**

Relaţia (*) se mai scrie încă în forma:

$$(**)\ f(x)=a_n\left(m_1(x)\right)^{k_1}\left(m_2(x)\right)^{k_2}...\left(m_s(x)\right)^{k_s},$$

formă numită **descompunerea standard**, unde $s\geq 1$ este întreg; $m_1(x),m_2(x),...,m_s(x)$ sunt polinoame ireductibile monice, distincte două câte două, iar numerele $k_1\geq 1$, $k_2\geq 1$, …, $k_s\geq 1$ numite *multiplicităţi*, sunt numere întregi. Ca şi la numerele naturale compuse, din (**) se pot deduce rezultate cum ar fi:

(+) numărul de divizori din $D^*(f(x))$ este egal cu $(1+k_1)(1+k_2)...(1+k_s)$;

(++) condiţia necesară şi suficientă ca un polinom *g(x)* să se dividă cu *f(x)* este ca $(m_i(x))^{k_1}\mid g(x)$ pentru $i=1,2,..,s$;

(+++) dacă $g(x)=b_\beta\cdot\left(m_1(x)\right)^{l_1}\left(m_2(x)\right)^{l_2}...\left(m_s(x)\right)^{l_s}$ atunci

$$\left(f(x),g(x)\right)=\left(m_1(x)\right)^{\min(k_1,l_1)}\cdot\left(m_s(x)\right)^{\min(k_s,l_s)},\ \text{unde}\ k_i,l_i\geq 0\ \text{şi}\ k_i+l_i\geq 1\ \ (i=1,2,...,s).$$

(5) Criterii de divizibilitate prin polinoame monice ireductibile

- Fie $f(x)\in\mathbb{R}[x]$ şi fie polinomul monic ireductibil de gradul întâi $m'_a(x)=x-a$. În baza TIR avem $f(x)=m'_a(x)c(x)+r(x)$, unde $c(x),r(x)\in\mathbb{R}[x]$ şi $r(x)$ este polinom constant: $r(x)=kx^0$. Substituim $x\leftarrow a$ (unde a este rădăcina

polinomului monic ireductibil $m'_a(x)$) şi obţinem $f(a)=0\cdot c(a)+k$, deci $f(x)\bmod(x-a)=f(a)x^0\equiv f(a)$.

Urmează criteriul de divizibilitate cu $x-a$ (numit teorema lui Bézout): $x-a\mid f(x)$ dacă şi numai dacă $f(a)=0$.

- Fie $f(x)\in\mathbb{R}[x]$ şi fie polinomul monic ireductibil de gradul doi: $m''_{b,c}(x)=x^2+bx+c$ $\left(b,c\in\mathbb{R}\text{ şi }b^2<4c\right)$. Există un element α în $\mathbb{C}-\mathbb{R}$ astfel încât $m''_{b,c}(x)=(x-\alpha)\left(x-\overline{\alpha}\right)$, descompunere în $\mathbb{C}[x]$. Folosind TIR în $\mathbb{C}[x]$ obţinem criteriul $m''_{b,c}(x)=x^2+bx+c=(x-\alpha)\left(x-\overline{\alpha}\right)$ divide pe *f(x)* dacă şi numai dacă $f(\alpha)=0$ (cu observaţia $f(\alpha)=0$ implică $f\left(\overline{\alpha}\right)=0$).
- Pentru divizibilitatea cu puteri naturale de polinoame monice ireductibile folosim teorema de descompunere în baza un polinom neconstant din $\mathbb{R}[x]$.

Fie $m(x)$ un polinom monic ireductibil şi fie $f(x)$ un polinom neconstant din $\mathbb{R}[x]$.

Aplicăm TIR cât timp câturile succesive (care sunt din ce în ce mai mici în grad) nu sunt polinoame nule:

$$\begin{aligned}
&(\text{pasul }0)\text{ cum }f(x)\neq\theta(x),f(x)=m(x)c_0(x)+r_0(x)\\
&(\text{pasul }1)\text{ cum }c_0(x)\neq\theta(x),c_0(x)=m(x)c_1(x)+r_1(x)\\
&(\text{pasul }2)\text{ cum }c_1(x)\neq\theta(x),c_1(x)=m(x)c_2(x)+r_2(x)\\
&\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\ldots\\
&\left(\text{pasul }(t-1)\right)\text{ cum }c_{t-2}(x)\neq\theta(x),c_{t-2}(x)=m(x)c_{t-1}(x)+r_{t-1}(x)\\
&\left(\text{pasul }(t-2)\right)\text{ cum }c_{t-1}(x)\neq\theta(x),c_{t-1}(x)=m(x)\theta(x)+r_t(x)
\end{aligned}$$

unde $r_0(x)\ldots r_t(x)$ sunt polinoame de grad $<gradm(x)$ şi $c_{t-1}(x)=r_t(x)$ este polinom nenul.

Din relaţiile de mai sus obţinem forma de scriere

(+) $f(x)=r_0(x)+r_1(x)\cdot m(x)+r_2(x)\cdot\left(m(x)\right)^2+\ldots+r_t(x)\cdot\left(m(x)\right)^t$.

Descompunerea (+) este unică.

Observaţii.

(a) Dacă $m(x)$ este un polinom monic ireductibil de gradul întâi, atunci relaţia (+) se mai numeşte şi **formula lui Taylor**.

(b) Dacă *i* este un întreg, cu $1 \le i \le t$, atunci $\left(m(x)\right)^i$ divide pe $f(x)$ dacă şi numai dacă au loc relaţiile: $r_j(x) = \theta(x)$ pentru $j = 0,1,...,i-1$. Mai exact, $\left(m(x)\right)^i$ divide pe $f(x)$ şi $\left(m(x)\right)^{i+1}$ nu divide pe $f(x)$ $(1 \le i \le t)$ dacă şi numai dacă au loc relaţiile

$$r_j(x) - \theta(x) \text{ pentru } j = 0,1,...,i-1 \text{ şi}$$

$$r_i(x) \neq \theta(x).$$

A. Lema chinezească a resturilor în varianta polinomială

A1. Varianta aritmetică a LCR

Noţiuni pregătitoare. Dacă $m(x)$ este un polinom neconstant din $\mathbb{R}[x]$, numit şi aici *modul*, atunci *relaţia de congruenţă modulo* $m(x)$ se defineşte pe $\mathbb{R}[x]$ prin:
$f(x) \equiv g(x)\left(\bmod m(x)\right) :\Leftrightarrow f(x) \bmod m(x) = g(x) \bmod m(x)$, adică $f(x)$ şi $g(x)$ au acelaşi rest la împărţirea cu $m(x)$ ($f(x), g(x) \in \mathbb{R}$). Relaţia de congruenţă modulo $m(x)$ pe $\mathbb{R}[x]$ are aceleaşi proprietăţi ca şi relaţia de congruenţă modulo m ($m \ge 2$ întreg) pe $\mathbb{Z}$.

- În continuare identificăm polinomul constant $re(x) = rx^0$ cu numărul real *r*, pentru fiecare $r \in \mathbb{R}$ (deoarece, aşa cum se ştie, corpul $(\mathbb{R}, +, \cdot)$ se poate scufunda în inelul $(\mathbb{R}[x], +, \cdot)$ via morfismul $u(r) = re(x)$).
- Algoritmul lui Euclid în varianta polinomială are o extindere aşa cum are şi algoritmul lui Euclid în $\mathbb{Z}$. Prin urmare, dacă $f(x)$ şi $g(x)$ sunt polinoame neconstante din $\mathbb{R}[x]$ şi dacă $\left(f(x), g(x)\right) = d(x)$, atunci există două polinoame $u(x)$ şi $v(x)$ în $\mathbb{R}[x]$ pentru care are loc relaţia $u(x)f(x) + v(x)g(x) = d(x)$. În baza acestei proprietăţi mai spunem că $(\mathbb{R}[x], +, \cdot)$ *este un domeniu de integritate Bézout* (orice domeniu de integritate euclidian este un domeniu de integritate Bézout).
- Fie $f(x)$ şi $g(x)$ două polinoame neconstante din $\mathbb{R}[x]$. Dacă există un polinom $h(x) \in \mathbb{R}[x]$ astfel încât $h(x)f(x) \equiv 1\left(\bmod g(x)\right)$, atunci spunem:

i) că $f(x)$ *este inversabil modulo* $g(x)$;

ii) că $h(x)$ *este un invers modulo* $g(x)$ al lui $f(x)$;

iii) că $h(x)$ *este inversul redus modulo* $g(x)$ al lui $f(x)$, dacă $gradh(x) < gradg(x)$.

Evident, $f(x)$ este inversabil modulo $g(x)$ dacă şi numai dacă $f(x) \perp g(x)$.

Dacă $f(x) \perp g(x)$, atunci există $u(x), v(x) \in \mathbb{R}[x]$ astfel încât $u(x)f(x) + v(x)g(x) = 1$ de unde rezultă că $u(x)f(x) \equiv 1 \pmod{g(x)}$.

În baza TIR avem: $u(x) = g(x)c(x) + r(x)$ şi atunci are loc relaţia $r(x)f(x) \equiv 1 \pmod{g(x)}$, cu $gradr(x) < gradg(x)$. Dacă $s(x) \in \mathbb{R}[x]$ are şi el proprietăţile: $grads(x) < gradg(x)$ şi $s(x)f(x) \equiv 1 \pmod{g(x)}$, obţinem prin scădere $(r(x) - s(x))f(x) \equiv 0 \pmod{g(x)}$, relaţie din care rezultă că $g(x)$ divide produsul $(r(x) - s(x))f(x)$, şi cum $g(x) \perp f(x)$, avem că $g(x)$ divide diferenţa $r(x) - s(x)$. Acest ultim fapt ne permite să scriem:

$$r(x) = r(x) \bmod g(x) = s(x) \bmod g(x) = s(x),$$

deci inversul redus modulo $g(x)$ al polinomului $f(x)$ este unic.

Enunţul LCR în $\mathbb{R}[x]$ - varianta aritmetică

Aceste enunţ este analog LCR în $\mathbb{Z}$. Fie date polinoamele neconstante: $m_1(x), m_2(x), ..., m_t(x)$ $(t \geq 2)$, cu $m_i(x) \perp m_j(x)$ pentru $i \neq j$. Notăm:

$$M(x) := m_1(x)m_2(x)...m_t(x) \text{ şi}$$

$$M_j(x) = \prod_{\substack{1 \leq j \leq t \\ j \neq i}} m_j(x) \quad (i = 1, 2, ..., t).$$

Introducem următorii termeni:

- dacă $f(x) \in \mathbb{R}[x]$, atunci t-uplul de polinoame din $\mathbb{R}[x]$:

$$\rho(f(x)) = (f(x) \bmod m_1(x), ..., f(x) \bmod m_t(x))$$

se numeşte *reducerea modulară* a polinomului $f(x)$.

- Orice polinom din $\mathbb{R}[x]$ de grad mai mic strict decât $grad(m_i(x))$ se numeşte *un rest modulo* $m_i(x)$ $(i=1,2,...,t)$.

Teoremă (LCR în varianta polinomială) *Fie daţi modulii* $m_1(x), m_2(x), ..., m_t(x)$ $(t \geq 2)$ *cu* $m_i(x) \perp m_j(x)$ *pentru* $i \neq j$ *şi fie t-uplul de polinoame din* $\mathbb{R}[x]$*:* $(r_1(x), ..., r_t(x))$*, unde* $r_i(x)$ *este un rest modulo* $m_i(x)$ $(i=1,2,...,t)$.

i) *Există atunci un polinom* $f(x)$ *în* $\mathbb{R}[x]$ *cu proprietatea că* $\rho(f(x)) = (r_1(x), ..., r_t(x))$.

ii) *Dacă* $g(x)$ *este un polinom oarecare din* $\mathbb{R}[x]$*, atunci* $\rho(g(x)) = \rho(f(x))$ *dacă şi numai dacă* $g(x) \equiv f(x) (\mathrm{mod}\, M(x))$.

Demonstraţie.

(i) Pentru fiecare $i=1,2,...,t$ avem: $M_i(x) \perp m_i(x)$, deci

(*) $c_i(x) M_i(x) \equiv 1 (\mathrm{mod}\, m_i(x))$,

unde $c_i(x)$ este inversul redus modulo $m_i(x)$ al polinomului $M_i(x)$. Înmulţim cu $r_i(x)$ în (*) şi obţinem:

(**) $r_i(x) c_i(x) M_i(x) \equiv r_i (\mathrm{mod}\, m_i(x))$.

Definim polinomul $f(x) \in \mathbb{R}[x]$ prin

$f(x) := r_1(x) c_1(x) M_1(x) + ... + r_t(x) c_t(x) M_t(x)$ (numit soluţia standard).

Cum $m_j(x)$ divide pe $M_i(x)$ pentru $j \neq i$, atunci pentru fiecare $i=1,2,...,t$ avem: $f(x) \equiv r_i(x) c_i(x) M_i(x) \overset{(**)}{\equiv} r_i(x) (\mathrm{mod}\, m_i(x))$ şi cum $grad(r_i(x)) < grad(m_i(x))$ deducem că $f(x) \mathrm{mod}\, m_i(x) = r_i(x)$. În consecinţă, $\rho(f(x)) = (r_1(x), ..., r_t(x))$.

(ii)

- Dacă $g(x) \equiv f(x) (\mathrm{mod}\, M(x))$, atunci $g(x) \equiv f(x) \equiv r(x) (\mathrm{mod}\, m_i(x))$ pentru $i=1,2,...,t$, deci $\rho(g(x)) = \rho(f(x))$.

- Dacă $\rho\left(g\left(x\right)\right)=\rho\left(f\left(x\right)\right)$, atunci $g\left(x\right)\bmod m_i\left(x\right)=f\left(x\right)\bmod m_i\left(x\right)$, deci $m_i\left(x\right)$ divide $g\left(x\right)-f\left(x\right)$ pentru $i=1,2,...,t$.

Cum $m_i\left(x\right)\perp m_j\left(x\right)$ pentru $i\neq j$, deducem că şi $M\left(x\right)$ divide $g\left(x\right)-f\left(x\right)$ şi prin urmare, $g\left(x\right)\equiv f\left(x\right)\left(\bmod M\left(x\right)\right)$.

Dacă $f\left(x\right)$ este soluţia standard, redusul modulo $M\left(x\right)$ al polinomului $f\left(x\right)$:
$f\left(x\right)\bmod M\left(x\right)$ = restul împărţirii lui $f\left(x\right)$ prin $M\left(x\right)$ o numim *soluţie principală* (termen analog perioadei principale a unei funcţii periodice). Deci,

$$grad\left(f\left(x\right)\bmod M\left(x\right)\right)<gradM\left(x\right) \text{ şi}$$

$$\rho\left(f\left(x\right)\bmod M\left(x\right)\right)=\rho\left(f\left(x\right)\right)$$

adică $f\left(x\right)\bmod M\left(x\right)$ este cel mai mic polinom în grad care satisface

$$\rho\left(f\left(x\right)\bmod M\left(x\right)\right)=\left(r_1\left(x\right),...,r_t\left(x\right)\right).$$

COROLAR. *Folosind datele din LCR, fie* $\left(a_1\left(x\right),...,a_t\left(x\right)\right)$ *un t-uplu de polinoame din* $\mathbb{R}\left[x\right]$. *Atunci:*

i) *Există cel puţin un polinom în* $\mathbb{R}\left[x\right]$ *care satisface sistemul de congruenţe:*

$$(s)\begin{cases}f\left(x\right)\equiv a_1\left(x\right)\left(\bmod m_1\left(x\right)\right)\\ .....\\ f\left(x\right)\equiv a_t\left(x\right)\left(\bmod m_t\left(x\right)\right)\end{cases}$$

ii) *Dacă* $f\left(x\right)$ *este o soluţie a lui* (s) *şi dacă* $g\left(x\right)\in\mathbb{R}\left[x\right]$, *atunci* $g\left(x\right)$, *este o soluţie al lui* (s) *dacă şi numai dacă* $g\left(x\right)\equiv f\left(x\right)\left(\bmod M\left(x\right)\right)$.

Demonstraţie. Facem reducerile: $r_i\left(x\right):=a_i\left(x\right)\bmod m_i\left(x\right)$ $\left(i=1,2,...,t\right)$. Acum se aplică LCR t-uplului $\left(r_1\left(x\right),...,r_t\left(x\right)\right)$ şi se foloseşte faptul că $a_i\left(x\right)\equiv r_i\left(x\right)\left(\bmod m_i\left(x\right)\right)$ pentru orice $i=1,2,...,t$.

A2. Varianta algebrică a LCR

Această variantă este analogă celei prezentate în paragraful **1.C**.

Teoremă. *Fie date polinoamele neconstante din* $\mathbb{R}[x]: m_1(x),...,m_t(x)$ $(t \geq 2)$, *cu* $m_i(x) \perp m_j(x)$ *pentru* $i \neq j$. *Se defineşte funcţia* $\varphi: \mathbb{R}[x] \to \frac{\mathbb{R}(x)}{(m_1(x))} \times ... \times \frac{\mathbb{R}(x)}{(m_t(x))}$ *prin* $\varphi(f(x)) = (f(x) mod(m_1(x)), \dots, f(x) mod(m_t(x)))$, *unde simbolul* $(m_i(x))$ *desemnează idealul principal generat de polinomul* $m_i(x)$ *în inelul* $(\mathbb{R}[X], +.\cdot), (i = 1,2, \dots, t)$. *Atunci*

i) φ *este un epimorfism de la inelul* $(\mathbb{R}[X], +.\cdot)$ *pe inelul produs* $\left(\frac{\mathbb{R}[X]}{(m_1(x))} \times ... \times \frac{\mathbb{R}[X]}{(m_t(x))}, +, \cdot\right)$.

ii) *are loc izomorfismul* $\left(\frac{\mathbb{R}[X]}{(M(x))}, +, \cdot\right) \cong \left(\frac{\mathbb{R}[X]}{(m_1(x))} \times ... \times \frac{\mathbb{R}[X]}{(m_t(x))}, +, \cdot\right)$.

B. Polinomul de interpolare al lui Lagrange este LCR în formă polinomială

- Rezultate pregătitoare

Fie $x - a$ un polinom monic ireductibil din $\mathbb{R}[X]$ $(a \in \mathbb{R})$.

- Dacă $b \in \mathbb{R}$ şi$b \neq a$, atunci

i) $x - b \perp x - a$, deoarece $x - b\big|_{x=a} = a - b \neq 0$;

ii) din relaţia $(x - b) - (x - a) = a - b$ deducem că $\frac{1}{a-b}(x - b) + \frac{1}{b-a}(x - a) = 1$, deci $\frac{1}{a-b}(x - b) \equiv 1(mod(x - a))$, relaţie care ne arată că polinomul constant $\frac{1}{a-b}$ este inversul redus modulo $(x - a)$ al polinomului $(x - b)$.

- Mai general, fie $f(x) \epsilon \mathbb{R}[X]$ cu $f(x) \perp x - a$. Atunci

  j) $f(a) \neq 0$ (în caz contrar, $x - a \,|\, f(x)$, absurd);

  jj) $f(x) = (x - a)c(x) + f(a)$ implică $\frac{1}{f(a)} f(x) \equiv 1(mod(x - a))$

  jjj) polinomul constant $\frac{1}{f(a)}$ este inversul redus modulo $(x - a)$ al polinomului $f(x)$.

- **Polinomul de interpolare al lui Lagrange**

Fie date numerele reale $a_1 < a_2 < \dots < a_n$ respectiv $b_1, b_2, \dots, b_n$ ($n \geq 2$ natural). Avem tabelul de interpolare

x	a_1	a_2	…	a_n
$y = f(x)$	b_1	b_2	…	b_n

şi problema de interpolare: *Să se arate că există un polinom unic* $f(x) \in \mathbb{R}[X]$ *cu proprietăţile:*

i) $gradf(x) \leq n-1$;

ii) $b_i = f(a_i)\,, (i = 1,2, \dots, t)$.

- **Interpretarea folosind aritmetica lui** $\mathbb{R}[X]$

- Şirul strict crescător $a_1 < a_2 < \cdots < a_n$ ne conduce la concluzia că pentru modulii $m_1(x) = x - a_1, m_2(x) = x - a_2, \dots, m_n(x) = x - a_n$ avem $m_i(x) \perp m_j(x)$ pentru $i \neq j$.
- Condiţiile din (ii) se traduc prin congruenţele: $f(x) \equiv b_i\big(mod(x - a_i)\big), (i = 1,2, \dots, n)$ deoarece $b_i = f(x)\big(mod(x - a_i)\big) = f(a_i)$.
- Definim sistemul de congruenţe algebrice (deoarece polinomul $f(x)$ îl presupunem necunoscut):

(c)
$$\begin{cases} f(x) \equiv b_1\big(mod(x - a_1)\big) \\ f(x) \equiv b_2\big(mod(x - a_2)\big) \\ \dots\dots\dots\dots\dots\dots\dots\dots \\ f(x) \equiv b_n\big(mod(x - a_n)\big) \end{cases}$$

Introducem notaţiile standard $M(x) \coloneqq (x - a_1)(x - a_2) \dots (x - a_n)$.

$$M_i(x) \coloneqq \prod_{\substack{1 \leq j \leq n \\ j \neq i}} (x - a_j)$$

Polinomul $f(x)$ din enunţul problemei de interpolare este soluţia principală a sistemului (c) (această soluţie există în baza LCR).

Determinarea soluţiei standard pentru LCR descrisă de (c)

Pentru fiecare $i = 1,2,..,n$ avem $M_i(x) \perp m_i(x) = x - a_i$ şi $\frac{1}{M_i(x_i)}\, M_i(x) \equiv 1\big(mod(x - a_i)\big)$.

Soluţia standard este dată de $s(x) \coloneqq b_1 \frac{1}{M_1(a_1)} M_1(x) + \cdots + b_n \frac{1}{M_n(a_n)} M_n(x) =$

$\frac{b_1}{M_1(a_1)} M_1(x) + \cdots + \frac{b_n}{M_n(a_n)} M_n(x)$ şi coincide cu soluţia principală deoarece $grad\big(s(x)\big) \leq$

$\max\left(grad\left(\frac{b_1}{M_1(a_1)} M_1(x)\right), \dots, grad\left(\frac{b_n}{M_n(a_n)} M_n(x)\right)\right) \leq n-1 < n = grad(M(x))$.

În concluzie, $f(x) = s(x)$. Unicitatea lui $f(x)$se demonstrează:

Clasic: dacă şi $g(x) \in \mathbb{R}[x]$, cu $gradg(x) < n$ satisface (ii), atunci $f(a_i) = b_i = g(a_i)(i = 1,2, \dots, n)$, relaţii care conduc la concluzia că $g(x) = f(x)$.

Aritmetic – conform LCR: dacă şi $g(x) \in \mathbb{R}[x]$ satisface (i) şi (ii), atunci $g(x) \equiv f(x)(modM(x))$, deci $g(x) = f(x) + h(x)M(x)$, cu $h(x) \in M[x]$. Dacă $h(x)$ nu este polinom nul, se obţine concluzia absurdă că: $n \leq grad\big(f(x) + h(x)M(x)\big) = grad\big(g(x)\big) \leq n-1$, adică $n \leq n-1$. Prin urmare, $h(x)$ este polinom nul şi atunci $g(x) = f(x)$.

Noi explorări

Soluţia $f(x)$ a problemei de interpolare este dată de

(1) $f(x) = \frac{b_1}{M_1(a_1)} M_1(x) + \cdots + \frac{b_n}{M_n(a_n)} M_n(x)$

Şi este la fel exprimată ca şi în rezolvarea clasică (fără LCR).

Din punctul de vedere al LCR, (1) ne dă soluţia standard a LCR exprimată prin sistemul de congruenţe algebrice (c). Ne amintim că algoritmul lui Garner furnizează soluţia principală pentru LCR în varianta numerică. Să încercăm să traducem acest algoritm în varianta polinomială.

- Punerea problemei. Fie modulii $m_1(x) = x - a_1, m_2(x) = x - a_2, \dots, m_n(x) = x - a_n$ cu $m_i(x) \perp m_j(x)$ pentru $i \neq j$ (deoarece $a_1 < a_2 < \cdots < a_n$). Pentru $j =$

$2,3,\dots,n$ şi fiecare $i = 1,2,..,j-1$ determinăm inversul redus modulo $m_j(x)$ a polinomului $m_i(x)$: $\frac{1}{a_j-a_i}(x-a_j) \equiv 1(mod(x-a_j))$, deci $c_{ij} = \frac{1}{a_j-a_i}$.

Punerea algoritmică:

INPUT: sunt date numerele reale $b_1, b_2, \dots, b_n$.

OUTPUT: se determină polinomul $f(x)$ din $\mathbb{R}[x]$ cu proprietăţile:

i)$gradf(x) < grad(M(x))$;

ii)$f(x)mod(x-a_i) = b_i$, adică $f(a_i) = b_i$ pentru fiecare $i = 1,2,\dots,n$.

Algoritmul lui Garner:

Pas iniţial: $r_1 \coloneqq b_1$

Pas curent: pentru $i = 1,2,\dots,n$ calculăm $r_{i+1} := \left(b_{i+1}\prod_{k=1}^{i} c_{k,i+1} - \sum_{l=1}^{i} r_l \prod_{k=l}^{i} c_{k,i+1}\right)modm_{i+1}(x) = \frac{b_{i+1}}{(a_{i+1}-a_1)(a_{i+1}-a_2)\dots(a_{i+1}-a_i)} - \frac{r_1}{(a_{i+1}-a_1)(a_{i+1}-a_2)\dots(a_{i+1}-a_i)} - \frac{r_2}{(a_{i+1}-a_2)(a_{i+1}-a_3)\dots(a_{i+1}-a_i)} - \dots - \frac{r_i}{(a_{i+1}-a_i)}$

Pas final:

(2) $f(x) = r_1 + r_2(x-a_1) + r_3(x-a_1)(x-a_2) + \dots + r_n(x-a_1)(x-a_2)\dots(x-a_{n-1})$ este polinomul cerut.

Evident, (2) ne furnizează o altă formă a polinomului de interpolare.

CONCLUZII

Dacă constantele reale $r_1, r_2, \dots, r_n$ din (2) sunt nedeterminate, atunci aflarea lor se poate realiza dacă se rezolvă sistemul:

$$\begin{cases} b_1 = f(a_1) = r_1 \\ b_2 = f(a_2) = r_1 + r_2(a_2 - a_1) \\ b_3 = f(a_3) = r_1 + r_2(a_3 - a_1) + r_3(a_3 - a_1)(a_3 - a_2) \\ \dots\dots\dots\dots\dots\dots\dots\dots\dots \\ b_n = f(a_n) = r_1 + r_2(a_n - a_1) + \cdots + r_n(a_n - a_1)(a_n - a_2)\dots(a_n - a_{n-1}) \end{cases}$$

care este un sistem liniar de tip Gauss.

Formulei (2) îi dăm următoarea interpretare vectorială. Ştim că $(\mathbb{R}[x],\cdot)$ este un $\mathbb{R}$ - spaţiu vectorial şi că $\sigma := (1, x, x^2, \dots) = (x^k)_{k\geq 1}$ este o bază a sa (numită baza standard). Fie acum dat un şir crescător de numere reale$(a_k)_{k\geq 1}$. Atunci şirul de polinoame $\alpha := (1, x - a_1, (x - a_1)(x - a_2), (x - a_1)(x - a_2)(x - a_3), \dots)$ este tot o bază a spaţiului vectorial $\mathbb{R}[x]$ (deoarece polinoamele din α se ordonează strict crescător după grade). Atunci (2) exprimă scrierea vectorului $f(x) \in \mathbb{R}[x]$ cu $grad\big(f(x)\big) \leq n - 1$ relativ la baza α.

Particularizăm şirul $(a_k)_{k\geq 1}$ din (2) luând $a_k = k - 1$ $(k \geq 1)$. Atunci $x^{(0)} := 1, x^{(1)} := x, x^{(2)} := x(x - 1), x^{(3)} := x(x - 1)(x - 2), \dots$ reprezintă şirul puterilor factoriale în descreştere al nedeterminatei x. Baza spaţiului vectorial $\mathbb{R}[x]$ $\varphi := (x^{(k)})_{k\geq 0}$ se numeşte baza puterilor factoriale în descreştere ale lui x. Din combinatorică se ştie că (2) devine pentru $f(x) = x^{n-1}$: $x^{n-1} = \sum_{k=1}^{n-1} \left\{ {n-1 \atop k} \right\} x^{(k)}$ unde coeficientul $r_k = \left\{ {n-1 \atop k} \right\}$ reprezintă numărul de partiţii cu k clase ale unei mulţimi ce conţine $n - 1$ elemente (acest număr se numeşte numărul lui Stirling de a doua speţă de indici $n - 1$ şi k).

În corpul de fracţii $K(\mathbb{R}[x])$ al domeniului de integritate $(\mathbb{R}[x], +, \cdot)$, unde $K(\mathbb{R}[x]) = \left\{ \frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x], g(x) nenul \right\}$ putem obţine următoarele rezultate:

Din (1) obţinem:

(1') $\frac{f(x)}{(x-a_1)(x-a_2)\dots(x-a_n)} = \frac{\frac{b_1}{M_1(a_1)}}{x-a_1} + \frac{\frac{b_2}{M_2(a_2)}}{x-a_2} + \cdots + \frac{\frac{b_n}{M_n(a_n)}}{x-a_n}$, formulă care constituie un caz special al teoremei de descompunere a fracţiilor din $K(\mathbb{R}_n[x])$ în sumă de fracţii simple.

Din (2) obţinem:

(2') $\frac{f(x)}{(x-a_1)(x-a_2)\dots(x-a_{n-1})} = r_n + \frac{r_{n-1}}{x-a_{n-1}} + \frac{r_{n-2}}{(x-a_{n-1})(x-a_{n-2})} + \cdots + \frac{r_1}{(x-a_1)(x-a_2)\dots(x-a_{n-1})}$ sau

după substituţia $c_k = r_{n-k}$ $(k = 1,2,\dots,n)$ şi permutarea factorilor $x-a_1,\dots,x-a_2$,

(2'') $\frac{f(x)}{(x-a_1)(x-a_2)\dots(x-a_n)} = c_0 + \frac{c_1}{x-a_1} + \frac{c_2}{(x-a_1)(x-a_2)} + \cdots + \frac{c_{n-1}}{(x-a_1)(x-a_2)\dots(x-a_{n-1})}$ unde ne

reamintim că $grad\big(f(x)\big) \leq n-1$. Formula (2'') ne arată că fracţia

$$\frac{f(x)}{M(x)} \text{ din corpul } K(\mathbb{R}_n[x])$$

poate avea şi alte descompuneri în sumă de „fracţii simple".

Descompunerea (1') poate fi utilizată (datorită simplităţii sale) şi în alte domenii ale matematicii. Funcţia cu valori reale dată prin $\varphi(t) = \frac{f(t)}{M(t)} = \frac{f(t)}{(t-a_1)(t-a_2)\dots(t-a_n)}$ şi definită pe mulţimea de numere reale $D \coloneqq \mathbb{R} - \{a_1,\dots,a_n\}$ se numeşte funcţie reală raţională şi este asociată fracţiei $\frac{f(x)}{M(x)}$ din corpul $K(\mathbb{R}_n[x])$. În baza relaţiei de egalitate după valori pe mulţimea $\mathbb{R}[x]$, deducem din (1') relaţia

(1'') $\varphi(t) = \frac{\frac{b_1}{M_1(a_1)}}{t-a_1} + \frac{\frac{b_2}{M_2(a_2)}}{t-a_2} + \cdots + \frac{\frac{b_n}{M_n(a_n)}}{t-a_n}$ oricare ar fi t din D. În baza formulei (1'') putem calcula, de exemplu, integrala nedefinită a funcţiei φ pe un interval fixat $I \subseteq D$:

$$\int \varphi(t)dt = \sum_{i=1}^{n} \frac{b_i}{M_i(a_i)} \ln|t-a_i| + \mathcal{C} \quad (t \in I).$$

Observăm că pentru a calcula $\int \varphi(t)dt$ formula (2'') este inutilizabilă (dacă se doreşte un calcul rapid al integralei).

Exerciţiu rezolvat. Fie $a < b < c$ numere reale. Să se demonstreze egalităţile:

1) $\frac{a}{(a-b)(a-c)} + \frac{b}{(b-c)(b-a)} + \frac{c}{(c-a)(c-b)} = 0$;

2) $\frac{a^2}{(a-b)(a-c)} + \frac{b^2}{(b-c)(b-a)} + \frac{c^2}{(c-a)(c-b)} = 1.$

Rezolvare. Produsele de la numitorii fracţiilor ne sugerează o problemă de interpolare (adică LCR). Avem

$M(x) = (x-a)(x-b)(x-c),$

$M_1(x) = (x-b)(x-c)$ și $m_1(x) = x-a,$

$M_2(x) = (x-a)(x-c)$ și $m_2(x) = x-b,$

$M_3(x) = (x-a)(x-b)$ și $m_3(x) = x-c.$

Atunci

$$\frac{1}{M_1(a)} M_1(x) = \frac{1}{(a-b)(a-c)} (x-b)(x-c)$$

$$\frac{1}{M_2(b)} M_2(x) = \frac{1}{(b-a)(b-c)} (x-a)(x-c)$$

$$\frac{1}{M_3(c)} M_3(x) = \frac{1}{(c-a)(c-b)} (x-a)(x-b)$$

reprezintă polinoame care se folosesc la obţinerea soluţiei principale $f(x)$, cu $grad(f(x)) \leq 2$.

Dacă avem inspiraţia să sesizăm că expresiile din membrul stâng din 1) şi 2) sunt coeficienţi extraşi din $f(x)$: $[x^k]f(x)$ pentru valori convenabile ale lui k, atunci obţinem tabelul de interpolare:

x	a	b	c
$y = f(x)$	a^2	b^2	c^2

cu soluţia directă: $f(x) = x^2$. Aşadar, polinomul $f(x)$ are două forme diferite de scriere:

$f(x) = x^2 = \frac{a^2}{(a-b)(a-c)}(x-a)(x-b) + \frac{b^2}{(b-c)(b-a)}(x-a)(x-b) + \frac{c^2}{(c-a)(c-b)}(x-a)(x-b)$.

(1) revine la faptul că $[x^0]f(x) = 0 = \frac{a^2bc}{(a-b)(a-c)} + \frac{b^2ac}{(b-c)(b-a)} + \frac{c^2ab}{(c-a)(c-b)}$ de unde se deduce că $\frac{a}{(a-b)(a-c)} + \frac{b}{(b-c)(b-a)} + \frac{c}{(c-a)(c-b)} = 0$. Acum $[x^2]f(x) = 1 = \frac{a^2}{(a-b)(a-c)} + \frac{b^2}{(b-c)(b-a)} + \frac{c^2}{(c-a)(c-b)}$.

C. Teorema de descompunere în sumă de fracţii simple a fracţiilor din corpul $K(\mathbb{R}[x])$

Din nou vom folosi LCR în varianta polinomială. Vom obţine varianta polinomială a teoremei lui Gauss de descompunere a fracţiilor ordinare din $\mathbb{Q}^* - \mathbb{N}$ în sumă de fracţii simple.

Precizări

- Aşa cum s-a mai spus şi mai sus, $K(\mathbb{R}[x]) = \left\{\frac{f(x)}{g(x)} : f(x), g(x) \in \mathbb{R}[x], g(x) nenul\right\}$ este corpul de fracţii al domeniului de integritate $(\mathbb{R}[x], +, \cdot)$.

Proprietatea de integritate a inelului $(\mathbb{R}[x], +, \cdot)$ are următoarea consecinţă: *Dacă* $f(x), g(x), h(x) \in \mathbb{R}[x]$ *şi dacă* $f(x)$ *nu este polinom nul, atunci* $f(x)g(x) = f(x)h(x)$ *implică* $g(x) = h(x)$ *(proprietatea de simplificare).*

- Se confundă „nedeterminata” x cu o variabilă reală: lui x nu i se pot „da valori”. De exemplu, fie polinomul $f(x) = 3 - 2x + 3x^2$. Unui element din $\mathbb{R}$, cum ar fi numărul real 4 i se asociază – via polinomul $f(x)$ - expresia $3 - 2 \cdot 4 + 3 \cdot 4^2 = 43$, notată $f(4)$. Spunem că expresia $f(4)$ **este asociată** perechii de obiecte $(f(x), 4)$ şi că nu este **rezultatul unui calcul obţinut** din polinomul $f(x)$ prin substituţia $x := 4$.

Această „nuanţare” este pusă în evidenţă în manualele şcolare (şi în alte lucrări de uz şcolar) prin folosirea simbolului X pentru a desemna nedeterminata (şi care se defineşte în construcţia cu şiruri reale prin

$$X = (0, 1, 0, 0, \dots), \text{ deci}$$

un temei pentru a nu da lui X valori, fiind un obiect fixat). Astfel, polinomul de mai sus capătă forma:

$$f = 3 - 2X + 3X^2, \text{ iar}$$

$f(4)$ este f – expresia asociată lui 4: $f(4) = 3 - 2 \cdot 4 + 3 \cdot 4^2 = 43$ şi, în general, $f = 3 - 2x + 3x^2$ reprezintă f – expresia asociată unui element arbitrar x din $\mathbb{R}$. În continuare vom folosi şi noi simbolul X pentru a desemna nedeterminata, deci $\mathbb{R}[X]$ va fi notaţia pentru mulţimea tuturor polinoamelor în X cu coeficienţi reali. Polinomului $f = 3 - 2X + 3X^2$ îi putem asocia funcţia polinomială $\tilde{f}: \mathbb{R} \to \mathbb{R}$ definită prin $\tilde{f}(t) = 3 - 2t + 3t^2$ (sau $\tilde{f}(x) = 3 - 2x + 3x^2$, deoarece „numele” variabilei nu este semnificativ).

Proprietatea de universalitate a inelului $(\mathbb{R}[X], +, \cdot)$ are formularea: Fie morfismul $\mathbb{R} \xrightarrow{i} (\mathbb{R}[X], X)$, unde $(\mathbb{R}, +, \cdot)$ = corp, i este monomorfism (numit *de incluziune*) de la corpul $(\mathbb{R}, +, \cdot)$ în inelul $(\mathbb{R}[X], +, \cdot)$, iar perechea $(\mathbb{R}[X], X)$ formată dintr-un inel şi un element fixat în mulţimea suport a inelului se numeşte inel punctat.

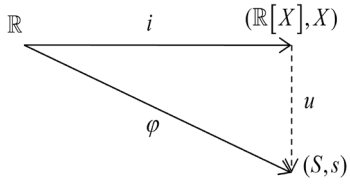
Tot morfism se numeşte obiectul $\mathbb{R} \xrightarrow{\varphi} (S, s)$ alcătuit din:

- S = inel comutativ şi unitar;
- s un element fixat în mulţimea S;
- φ un homomorfism unitar de la inelul $\mathbb{R}$ = corp la inelul S (operaţiile inelare se subînţeleg).

Mai exact, φ *este un morfism* de la inelul $\mathbb{R}$ la inelul punctat (S, s).

Formulare: *Morfismul* $\mathbb{R} \xrightarrow{i} (\mathbb{R}[X], X)$ *are următoarea proprietate: oricare ar fi morfismul* $\mathbb{R} \xrightarrow{\varphi} (S, s)$ *, atunci există un unic homomorfism unitar* u *de la inelul* $\mathbb{R}[X]$ *la inelul* S *cu proprietăţile:*

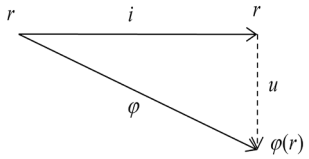
i) diagrama



comută, adică $u \circ i = \varphi$*;*

ii) $u(X) = s$ *(elementele fixate se corespund prin* u*)*

Deoarece



şi $u(X) = s$, deducem că *u* pune în corespondenţă un polinom $g = a_0x^0 + a_1x^1 + \cdots + a_nx^n$din $\mathbb{R}[X]$ cu elementele din *S*: $\varphi(a_0) + \varphi(a_1)s + \cdots + \varphi(a_n)s^n$ notat g^u. Deci *u* transformă pe *g* în g^u transformând coeficienţii lui *g* (după regula $a_i \xrightarrow{u} \varphi(a_i)$), nedeterminata *X* în elementul *s* şi operaţiile inelare din $\mathbb{R}[X]$ în operaţiile inelare din *S*: $(f + g)^u = f^u + g^u$ şi $(f \cdot g)^u = f^u \cdot g^u$.

De exemplu, dacă $g = 4 + 3X + 9X^2$, $\varphi = i$, $S = \mathbb{R}[X]$ şi $s = X^2 + X + 1$, atunci $g(X^2 + X + 1) \coloneqq 4 + 3(X^2 + X + 1) + 9(X^2 + X + 1)^2 = 9X^4 + 18X^3 + 30X^2 + 21X + 16$

- Fie polinomul $X - 4$ din $\mathbb{R}[X]$. Fracţiei $\frac{1}{X-4}$ din $K(\mathbb{R}[X])$ nu i se pun condiţii, cum ar fi $X \neq 4$, deoarece X nu poate primi valori. În schimb, dacă x este o variabilă reală, atunci pentru funcţia reală $\frac{1}{x-4}$ punem condiţia $x \neq 4$.
- Dacă x este o variabilă reală şi dacă $\mathbb{R}[x]$ desemnează mulţimea funcţiilor polinomiale (operaţia de înmulţire a funcţiilor fiind înlocuită de operaţia analogă celei de la polinoame), atunci $(\mathbb{R}[x], +, \cdot)$ este inel şi $(\mathbb{R}[x], +, \cdot) \cong (\mathbb{R}[X], +, \cdot)$ (un astfel de izomorfism nu are loc pentru orice inel de polinoame).

Formularea.

Fie date polinoamele neconstante $m_1, m_2, \dots, m_t$ $(t \geq 2)$, cu $m_i \perp m_j$ pentru $i \neq j$. Folosim şi aici notaţiile standard: $M = m_1 m_2 \dots m_t$ şi $M_i = \prod_{\substack{1 \leq j \leq t \\ i \neq j}} m_j$. Pentru fiecare $i = 1,2, \dots, t$ avem $M_i \perp m_i$, deci putem determina inversul redus $modulo\ m_i$ al polinomului M_i: $c_i M_i \equiv 1 (\mathrm{mod} m_i)$ şi $grad(c_i) < grad(m_i)$.

Fie acum un polinom f din $\mathbb{R}[X]$, cu $grad(f) < grad(M)$.. Folosim reprezentarea modulară a lui f: $\rho(f) = (r_1, r_2, \dots, r_t)$ unde $r_i := f \mathrm{mod} m_i$ $(i = 1,2, \dots, t)$.

Construim soluţia standard: $s := r_1 c_1 M_1 + r_2 c_2 M_2 + \cdots + r_t c_t M_t$.

Construim soluţia principală: $p := p_1 M_1 + p_2 M_2 + \cdots + p_t M_t$, unde

$$p_i := (r_i c_i) mod(m_i)\ (i = 1,2, \dots, t),$$

unde $grad(p) \leq \max(grad(p_1 M_1), \dots, grad(p_t M_t)) < grad(M)$.

Avem: $p \equiv s (mod M)$ şi $p \equiv s \equiv p_1 M_1 + p_2 M_2 + \cdots + p_t M_t \equiv p_i M_i \equiv r_i c_i M_i \equiv r_i (mod(m_i))$ adică $p\ mod(m_i) = p_i$. Deoarece $f\ mod(m_i) = p\ mod(m_i)$ $(i = 1,2, \dots, t)$ se deduce că $f \equiv p (mod M)$, deci $f (mod M) = f = p = p (mod M)$. Aşadar, $f = p_1 M_1 + p_2 M_2 + \cdots + p_t M_t$ de unde se obţine descompunerea

(D) $\frac{f}{m} = \frac{p_1}{m_1} + \cdots + \frac{p_t}{m_t}$, unde $grad(p_i) < grad(m_i)$ $(i = 1,2, \dots, t)$.

Tratăm în continuare cazul special: $M \in \mathbb{R}[X]$ şi

(S) $M = c \cdot p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_t^{k_t}$, unde $c \neq 0$ este o constantă reală, iar $P_1, P_2, \dots, P_t$ sunt polinoame monice ireductibile din $\mathbb{R}[X]$ şi $k_1, k_2, \dots, k_t \geq 1$ sunt numere întregi (multiplicităţile). Deci (S) este descompunerea standard a polinomului *M*. Factorul constant *c* se elimină luând $M^* = p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_t^{k_t}$. Înlocuim în (D) pe *M* cu *M** şi m_i cu $p_i^{k_i}$ $(i = 1,2, \dots, t)$ obţinem:

(D') $\frac{f}{M^*} = \frac{p_1}{p_1^{k_1}} + \cdots + \frac{p_t}{p_t^{k_t}}$. Pentru fiecare $i = 1,2, \dots, t$ putem scrie $p_i = c_{i1} + c_{i2} p_i + c_{i3} p_i^2 + \cdots + c_{i\alpha_i} p_i^{\alpha_i}$, unde $c_{ij} \in \mathbb{R}[X]$ şi $grad(c_{ij}) < grad(p_i) (j = 1,2, \dots, \alpha_i), \alpha_i \leq k_i - 1$.

Atunci $\frac{p_i}{p_i^k} = \frac{c_{i1}}{p_i^k} + \frac{c_{i2}}{p_i^{k-1}} + \cdots + \frac{c_{i,k_i-1}}{p_i^1}$, sau după reindexarea polinoamelor de la numărător, $\frac{p_i}{p_i^k} = \frac{c_{i1}}{p_i^1} + \frac{c_{i2}}{p_i^2} + \cdots + \frac{c_{i,k_i}}{p_i^{k_i}}$.

Acum (D') devine

(D'') $\frac{f}{M^*} = \frac{c_{11}}{p_1^1} + \frac{c_{12}}{p_1^2} + \cdots + \frac{c_{1,k_1}}{p_1^{k_1}} + \cdots + \frac{c_{t1}}{p_t^1} + \frac{c_{t2}}{p_t^2} + \cdots + \frac{c_{t,k_t}}{p_t^{k_t}} = \sum_{i=1}^{t} \sum_{j=1}^{k_i} \frac{c_{ij}}{p_i^j}$. Deci

(D''') $\frac{f}{M} = \sum_{i=1}^{t} \sum_{j=1}^{k_i} \frac{\frac{1}{c} c_{ij}}{p_i^j}$.

Fracţiile din corpul $K(\mathbb{R}[X])$ de forma $\frac{p}{p^k}$, unde P = polinom (monic) ireductibil din $\mathbb{R}[X]$, $k \geq 1$ întreg şi $P \in \mathbb{R}[X]$, cu $grad(p) < grad(P)$ se numeşte *fracţie simplă*. Fracţiile simple din $K(\mathbb{R}[X])$ sunt de două tipuri (după cum sunt şi polinoamele monice ireductibile din $\mathbb{R}[X]$):

i) fracţie simplă de primul tip $\frac{b}{(x-a)^k}$ (unde $a, b \in \mathbb{R}, b \neq 0$ şi $k \geq 1$ întreg)

ii) fracţie simplă de al doilea tip $\frac{rX+s}{(X^2+bX+c)^k}$ (unde $r, s, b, c \in \mathbb{R}$ cu proprietăţile $b^2 < 4c$ şi $r^2 + s^2 \neq 0$)

Formula (D’’’) ne arată că fracţia $\frac{f}{M}$ cu $0 \leq grad(f) < grad(M)$ se descompune în sumă finită de fracţii simple.

Unicitatea descompunerii (D’’’). Admitem că $\frac{f}{M}$ mai are şi descompunerea:

(U) $\frac{f}{M} = \sum_{i=1}^{t} \sum_{j=1}^{k_i} \frac{g_{ij}}{p_i^k}$, unde $grad(g_{ij}) < grad(p_i)$ $(j = 1,2, \dots, k_i)$ pentru fiecare $i = 1,2, \dots, t$. Din (U) se obţine relaţia

$$\frac{f}{M} = \frac{g_1}{p_1^{k_1}} + \cdots + \frac{g_t}{p_1^{k_t}}, \text{ unde } grad(g_i) < grad({p_i}^{k_i})(i = 1,2, \dots, t).$$

Notăm pentru simplitate: ${m_i = {p_i}^{k_i}}$ $(i = 1,2, \dots, t)$ şi atunci

$$\frac{f}{M} = \frac{g_1}{m_1} + \cdots + \frac{g_t}{m_t},$$

relaţie care se scrie încă şi sub forma

$f = g_1 M_1 + \cdots + g_t M_t$, cu $grad(g_i) < grad(m_i)(i = 1,2, \dots, t)$.

Acum $f(x) \equiv g_1 M_1 + \cdots + g_t M_t \equiv g_i M_i (mod\ m_i)$ şi $f(x) \equiv r_i (mod\ m_i)$, deci $g_i M_i \equiv r_i \equiv r_i c_i M_i (mod\ m_i)$. Dar $M_i \perp m_i$, deci putem simplifica prin M_i şi obţinem $g_i \equiv r_i c_i \equiv p_i (mod\ m_i)$, deci $g_i = g_i (mod\ m_i) = p_i (mod\ m_i) = p_i$ pentru fiecare $i = 1,2, \dots, t$. În consecinţă, descompunerea (U) coincide cu descompunerea (D’’’). am demonstrat deci următoarea teoremă:

Teoremă. *Orice fracţie* $\frac{f}{M}$ *din corpul* $K(\mathbb{R}[X])$ *, cu* $f, g \in \mathbb{R}[X]$ *şi* $0 \leq grad(f) < grad(M)$ *se descompune în mod unic într-o sumă finită de fracţii simple. Dacă polinomul* M *are descompunerea standard* $M = c \cdot p_1^{k_1} \cdot p_2^{k_2} \cdot \dots \cdot p_t^{k_t}$*, atunci de scompunerea fracţiei* $\frac{f}{M}$ *în sumă finită de fracţii simple are formula*

(*)$\frac{f}{M} = \sum_{i=1}^{t} \sum_{j=1}^{k_i} \frac{c_{ij}}{p_i^j}$*, unde* $grad(c_{ij}) < grad(p_i)$ *pentru* $i = 1,2, \dots, t$ *şi* $j = 1,2, \dots, k_i$.

Dacă $grad(f) \geq grad(M)$, atunci avem conform TIR: $f = M \cdot q + f^*$, unde $g, f^* \in \mathbb{R}[X]$, şi $grad(f^*) < grad(M)$. Putem scrie: $\frac{f}{M} = q + \frac{f^*}{M} = q + \sum_{i=1}^{t} \sum_{j=1}^{k_i} \frac{c_{ij}}{p_i^j}$, o formă de

descompunere mai aproape de teorema lui Gauss dacă $\frac{f}{M} = h + \sum_{i=1}^{t}\sum_{j=1}^{k_i}\frac{g_{ij}}{p_i^j}$, cu $h \in \mathbb{R}[X]$ şi $grad(g_{ij}) < grad(p_i)$ $(i = 1,2,\dots,t$ *şi* $j = 1,2,\dots,k_i)$, atunci $\sum_{i=1}^{t}\sum_{j=1}^{k_i}\frac{g_{ij}}{p_i^j} = \frac{g}{M}$, unde $grad(g) < grad(M)$ şi deci, $\frac{f}{M} = h + \frac{g}{M}$, de unde se obţine relaţia $f = Mh + g$. Folosind partea de unicitate a TIR, deducem că $h = q$ şi $g = f^*$, şi aşa cum s-a demonstrat mai sus, $g_{ij} = c_{ij}$ $(i = 1,2,\dots,t\ ;\ j = 1,2,\dots,k_i)$.

Aplicaţii.

A1. (în analiza matematică, clasa a XII-a)

Să se calculeze integrala nedefinită: $\int \frac{x^3+x^2+1}{(x+1)(x^2+1)^2}dx, x \in (-1,+\infty)$.

Rezolvare. Notăm cu $f(x)$ integrantul. Funcţia reală f este o funcţie raţională. Ea se asociază în mod natural cu fracţia din $K(\mathbb{R}[X])$: $F \coloneqq \frac{X^3+X^2+1}{(X+1)(X^2+1)^2}$, unde $X + 1$ şi $X^2 + 1$ sunt polinoame monice şi ireductibile în $\mathbb{R}[X]$.

Teorema de descompunere a fracţiilor nenule şi neîntregi (adică fracţiile care au la numitor un polinom constant şi nenul) din corpul $K(\mathbb{R}[X])$ aplicată fracţiei nenule şi neîntregi *F* se transpune şi funcţiei f : are loc egalitatea de funcţii: $f(x) = \frac{x^3+x^2+1}{(x+1)(x^2+1)^2} = \frac{a}{x+1} + \frac{bx+c}{x^2+1} + \frac{dx+e}{(x^2+1)^2}$, unde *a*, *b*, *c*, *d* şi *e* sunt constante reale nedeterminate ($x \in (-1,+\infty)$). Eliminăm numitorii şi obţinem egalitatea

$(*)x^3 + x^2 + 1 = a(x^2 + 1)^2 + (bx + c)(x + 1)(x^2 + 1) + (dx + e)(x + 1)$, pentru orice x din $(-1,+\infty)$ şi prin urmare, pentru orice x din $\mathbb{C}$ (deoarece polinoamele $X^3 + X^2 + 1$ şi $a(X^2 + 1)^2 + (bX + c)(X + 1)(X^2 + 1) + (dX + e)(X + 1)$ au valori egale în mai mult de 4 puncte reale, mai exact au valori egale în toate punctele intervalului $(-1,+\infty)$).

Luăm $x = -1$ în (*) şi obţinem:$-1 = 4a$, deci $a = -\frac{1}{4}$.

Luăm $x = i$ în (*) şi obţinem $1(di + e)(i + 1)$.

Cum $(di + e)(i + 1) = -d + ei + di + e = (-d + e) + (e + d)i$, ultima relaţie conduce la sistemul: $\begin{cases} -d + e = 1 \\ d + e = 0 \end{cases}$, cu soluţia $e = \frac{1}{2}$ şi $d = -\frac{1}{2}$.

Pentru $x = 0$ obţinem: $1 = a + c + e$, deci $1 = -\frac{1}{4} + c + \frac{1}{2}$, de unde aflăm că $c = \frac{3}{4}$. În final, pentru $x = 1$ se obţine $3 = 4a + 4b + 4c + 2d + 2e = -1 + 4b + 3 - 1 + 1$, deci $b = \frac{1}{2}$. Putem scrie deci

$$\int f(x)dx = \int\left(-\frac{1}{4}\cdot\frac{1}{x+1} + \frac{\frac{1}{4}x+\frac{3}{4}}{x^2+1} + \frac{-\frac{1}{2}x+\frac{1}{2}}{(x^2+1)^2}\right)dx = \int\left(-\frac{1}{4}\cdot\frac{1}{x+1} + \frac{1}{8}\cdot\frac{(x^2+1)'}{x^2+1} + \frac{3}{4}\cdot\frac{1}{x^2+1} - \frac{1}{4}\cdot\frac{(x^2+1)'}{(x^2+1)^2} + \frac{1}{2}\frac{1}{(x^2+1)^2}\right)dx = \int\left(-\frac{1}{4}\cdot\frac{1}{x+1} + \frac{1}{8}(\ln(x^2+1))' + \frac{3}{4}\cdot\frac{1}{x^2+1} + \frac{1}{4}\cdot((x^2+1)^{-1})' +$$

$\left(\frac{1}{4}\cdot\frac{x}{x^2+1}-\frac{1}{4}arctg\,x\right)'\Big)dx=-\frac{1}{4}\ln(x+1)+\frac{1}{8}\ln(x^2+1)+\frac{3}{4}arctg\,x+\frac{1}{4}\cdot\frac{1}{x^2+1}+\frac{1}{4}\cdot\frac{x}{x^2+1}-\frac{1}{4}arctg\,x+\mathcal{C}==-\frac{1}{4}\ln(x+1)+\frac{1}{8}\ln(x^2+1)+\frac{1}{2}arctg\,x+\frac{1}{4}\cdot\frac{x+1}{x^2+1}+\mathcal{C},(x\in(-1,+\infty))$.

A2. (analiză matematică, clasa a XI-a)

Să se calculeze derivatele succesive ale funcţiei $f(x)=\frac{2x-1}{x^2-1},x\in\mathbb{R}-\{-1,1\}$.

Rezolvare. Descompunem în sumă de fracţii simple: $f(x)=\frac{3}{2}\cdot\frac{1}{x-1}+\frac{1}{2}\cdot\frac{1}{x+1}=\frac{3}{2}(x-1)^{-1}+\frac{1}{2}(x+1)^{-1},x\in\mathbb{R}-\{-1,1\}$.

A *n*-a derivată a funcţiei *f* este funcţia $f^{(n)}(x)=\frac{3}{2}((x-1)^{-1})^{(n)}+\frac{1}{2}((x+1)^{-1})^{(n)}=\frac{3}{2}(-1)^n n!\,(x-1)^{-1-n}+\frac{1}{2}(-1)^n n!\,(x+1)^{-1-n}$.

A3. (funcţii generatoare)

Folosind funcţii generatoare să se determine formula generală a termenilor din şirul lui Fibonacci: $(F_n)_{n\geq 0}$ *dat de relaţiile* $F_0=0$, $F_1=1$ *şi* $F_{n+2}-F_{n+1}-F_n=0$ *oricare ar fi* n *din* $\mathbb{N}$.

Rezolvare. Definim funcţia generatoare a şirului lui Fibonacci $G(z):=\sum_{n\geq 0}F_n z^n$. Înmulţim relaţia $F_{n+2}-F_{n+1}-F_n=0$ cu z^{n+2} şi obţinem $F_{n+2}z^{n+2}-F_{n+1}z^{n+2}-F_n z^{n+2}=0$. Însumăm: $\sum_{n\geq 0}F_{n+2}z^{n+2}-\sum_{n\geq 0}F_{n+1}z^{n+2}-\sum_{n\geq 0}F_n z^{n+2}=0$ deci $\sum_{n\geq 2}F_n z^n-z\sum_{n\geq 1}F_n z^n-\sum_{n\geq 0}F_n z^n=0$, de unde $-z+\sum_{n\geq 0}F_n z^n-z\sum_{n\geq 0}F_n z^n-z^2\sum_{n\geq 0}F_n z^n=0$, deci $(1-z-z^2)G(z)=z$, adică $G(z)=\frac{z}{1-z-z^2}$.

Luăm $\emptyset=\frac{1+\sqrt{5}}{2}$ (raportul de aur) şi $\widetilde{\emptyset}=\frac{1-\sqrt{5}}{2}$ şi obţinem $\emptyset+\widetilde{\emptyset}=1$ şi $\emptyset\cdot\widetilde{\emptyset}=-1$. Prin urmare, $(1-\emptyset z)\left(1-\widetilde{\emptyset}z\right)=1-\left(\emptyset+\widetilde{\emptyset}\right)z+\left(\emptyset\cdot\widetilde{\emptyset}\right)z^2=1-z-z^2$.

Putem scrie

$$\frac{z}{1-z-z^2}=\frac{z}{(1-\emptyset z)(1-\widetilde{\emptyset}z)}=\frac{a}{1-\emptyset z}+\frac{b}{1-\widetilde{\emptyset}z}.$$

Eliminăm numitorii $z=a\left(1-\widetilde{\emptyset}z\right)+b(1-\emptyset z)$, identitate pe $\mathbb{C}$.

Pentru $z=0$ avem $0=a+b$, deci $z=a\left(1-\widetilde{\emptyset}z\right)-a(1-\emptyset z)=a\left(\emptyset-\widetilde{\emptyset}\right)z=a\sqrt{5}\cdot z$, deci $=\frac{1}{\sqrt{5}}$.

Acum $G(z)=\frac{1}{\sqrt{5}}\cdot\frac{1}{1-\emptyset z}-\frac{1}{\sqrt{5}}\cdot\frac{1}{1-\widetilde{\emptyset}z}=\frac{1}{\sqrt{5}}\sum_{n\geq 0}\emptyset^n z^n-\frac{1}{\sqrt{5}}\sum_{n\geq 0}\widetilde{\emptyset}^n z^n$, deci

$G(z)=\sum_{n\geq 0}F_n z^n=\sum_{n\geq 0}\frac{\emptyset^n-\widetilde{\emptyset}^n}{\sqrt{5}}z^n$, de unde se găseşte *formula lui Binet*,

$$F_n=\frac{\emptyset^n-\widetilde{\emptyset}^n}{\sqrt{5}}=\frac{\left(\frac{1+\sqrt{5}}{2}\right)^n-\left(\frac{1-\sqrt{5}}{2}\right)^n}{\sqrt{5}},n\geq 0.$$

BIBLIOGRAFIE

1. Albu, T., Ţena, M., **Descompunerea în fracţii simple**, G.M. 3/1987, p.104-114.
2. Becheanu, M., Dincă, A., Ion, D., Niţă, C., Purdea, I., Radu, N., Ştefănescu C., **Algebră pentru perfecţionarea profesorilor**, E.D.P. Bucureşti, 1983.
3. Becheanu, M., Niţă, C., Ştefănescu, M., Dincă, A., Purdea, I., Radu, N., Vraciu, C., **Algebra**, Ed. All Educational, 1998.
4. Băeţică, C., Dăscălescu, S., **Probleme de algebră**, Tipografia Uniersităţii Bucureşti,1993.
5. Borevici, Z.I., Şafarevici, I.R., **Teoria numerelor**, Ed. Ştiinţifică şi Enciclopedică, Bucureşti, 1985.
6. Cucurezeanu, I., **Probleme de aritmetică şi teoria numerelor**, Ed. Tehnică, 1976
7. Dumitrescu, T., **Algebra**, Ed. Universităţii din Bucureşti, 2006.
8. Ion, I.D., **Algebra**, E.D.P.,Bucureşti, 1991.
9. Ion, I.D., Niţă, C., Popescu, D., Radu,N., **Probleme de algebră**, E.D.P.,Bucureşti, 1981
10. Ion, I.D., Niţă, C., Buzeţeanu, Ş., **Capitole speciale de algebră modernă**, Tipografia Uniersităţii Bucureşti, 1984.
11. Kostrikin, A., **Introduction à l' algèbre**, Ed. Mir, 1981.
12. Miron, R., Brânzei, D., **Fundamentele aritmeticii şi geometriei**, Ed. Academiei, Bucureşti, 1983.
13. Năstăsescu, C., Niţă, C., Vraciu, C., **Bazele algebrei**, vol I, Ed. Academiei, Bucureşti, 1986.
14. Năstăsescu, C., Niţă, C., Vraciu, C., **Aritmetică şi algebră**, E.D.P.,Bucureşti, 1992.
15. Purdea, I., Pic, I., **Tratat de algebră modernă**, Vol. I, Ed. Academiei, 1977.
16. Purdea, I., **Tratat de algebră modernă**, Vol. II, Ed. Academiei, 1982.
17. Purdea, I., Pop, I., **Algebra**, Ed.Gil, Zalău, 2003.
18. Radu, N. şi colab. **Algebră pentru perfecţionarea profesorilor**, E.D.P. Bucureşti, 1983.
19. Radu, N., şi colectiv, **Algebra**, Editura All, 1998.
20. Rivest, R.L.; Shamir, A.; Adleman, L., **A Method for Obtaining Digital Signatures and Public-Key Cryptosystems**
21. Rivest, R.L.; Shamir, A.; Adleman, L., *Communications of the ACM* **21** (2), 2008, pp. 120–126.doi:10.1145/359340.359342. http://theory.lcs.mit.edu/~rivest/rsapaper.pdf.
22. Şafarevici, I.R., **Noţiunile fundamentale ale algebrei**, Ed. Academiei, 1989.