

ARITMETICA ÎN \mathbb{Z} ȘI $K[X]$

1. DIVIZIBILITATE. ALGORITMUL LUI EUCLID.

Să începem prin a observa că inelele \mathbb{Z} și $K[X]$ (K corp comutativ) sunt domenii de integritate, $U(\mathbb{Z}) = \{-1, 1\}$ și $U(K[X]) = K^\times$.

Teorema 1.1. (Teorema de împărțire cu rest în \mathbb{Z}) Fie $a, b \in \mathbb{Z}$, $b \neq 0$. Atunci există $q, r \in \mathbb{Z}$ unice cu proprietatea că $a = bq + r$ și $0 \leq r < |b|$.

Proof. Existența. Fie $r = \min\{a - bx : x \in \mathbb{Z} \text{ și } a - bx \geq 0\}$. Scriem $r = a - bq$, $q \in \mathbb{Z}$. Dacă $r \geq |b|$, atunci $0 \leq a - b(q + \text{sgn}(b)) < r$, contradicție. Așadar $r < |b|$.

Unicitatea. Fie $q', r' \in \mathbb{Z}$ cu proprietatea că $a = bq' + r'$ și $0 \leq r' < |b|$. Atunci $b(q - q') = r' - r$ și de aici obținem $|b||q - q'| = |r' - r| < |b|$, deci $q = q'$ și $r = r'$. \square

Definiția 1.2. Numărul întreg q din teorema de mai sus se numește câtul împărțirii lui a la b , iar r se numește restul împărțirii lui a la b .

Exemplul 1.3. Fie $a = -17$ și $b = 2$. Scriem $-17 = 2(-9) + 1$, deci $q = -9$ și $r = 1$.

În cele ce urmează R va desemna \mathbb{Z} sau $K[X]$.

Definiția 1.4. Fie $a, b \in R$. Spunem că b divide a dacă există $c \in R$ astfel încât $a = bc$ și scriem $b \mid a$. Se mai spune că b este divizor al lui a sau că a este multiplu al lui b .

Remarca 1.5. (i) $1 \mid a$ și $a \mid 0$ pentru orice $a \in R$.

(ii) Dacă $b \neq 0$, atunci $b \mid a$ dacă și numai dacă restul împărțirii lui a la b este 0.

(iii) Dacă $b \mid a$, atunci $|b| \leq |a|$ pentru $R = \mathbb{Z}$, respectiv $\deg b \leq \deg a$ pentru $R = K[X]$.

Să enunțăm acum câteva proprietăți simple ale relației de divizibilitate.

Propoziția 1.6. (i) $a \mid b$ dacă și numai dacă $bR \subseteq aR$.

(ii) $a \mid a$ oricare ar fi $a \in R$.

(iii) $a \mid b$ și $b \mid c \Rightarrow a \mid c$.

(iv) $a \mid b_i, \forall i = 1, \dots, n \Rightarrow a \mid \sum_{i=1}^n \alpha_i b_i, \forall \alpha_i \in R$.

Definiția 1.7. Fie $a, b \in R$. Spunem că a și b sunt asociate în divizibilitate dacă $a \mid b$ și $b \mid a$.

Notăție: $a \sim b$.

Remarca 1.8. (i) " \sim " este o relație de echivalență pe R .

(ii) $a \sim 1$ dacă și numai dacă $a \in U(R)$.

Din propoziția 1.6(i) rezultă imediat că a este asociat în divizibilitate cu b dacă și numai dacă $aR = bR$.

Propoziția 1.9. Fie $a, b \in R$. Atunci a și b sunt asociate în divizibilitate dacă și numai dacă $b = \pm a$ pentru $R = \mathbb{Z}$, respectiv $b = au$, $u \in K^\times$ pentru $R = K[X]$.

Definiția 1.10. Fie $a, b \in R$. Spunem că un element $d \in R$ este un cel mai mare divizor comun al elementelor a, b dacă:

- (i) $d \mid a$ și $d \mid b$,
- (ii) $d' \mid a$ și $d' \mid b$ implică $d' \mid d$.

Notăție: c.m.m.d.c.(a, b) sau $\gcd(a, b)$ sau (a, b) .

Definiția 1.11. Fie $a, b \in R$. Spunem că un element $m \in R$ este un cel mai mic multiplu comun al elementelor a, b dacă:

- (i) $a \mid m$ și $b \mid m$,
- (ii) $a \mid m'$ și $b \mid m'$ implică $m \mid m'$.

Notăție: c.m.m.m.c.(a, b) sau $\text{lcm}(a, b)$ sau $[a, b]$.

Remarca 1.12. (i) Dacă $d_1, d_2 \in R$ sunt fiecare un cel mai mare divizor comun al elementelor a, b , atunci $d_1 \sim d_2$. Reciproc, dacă $d_1 \sim d_2$ și d_1 este un cel mai mare divizor comun al elementelor a, b , atunci și d_2 este un cel mai mare divizor comun al elementelor a, b . De aceea vom considera ca fiind c.m.m.d.c.(a, b) orice element al lui R care este un cel mai mare divizor comun al elementelor a, b și vom spune că c.m.m.d.c.(a, b) este unic până la o asociere în divizibilitate.

(ii) Considerații similare sunt valabile și pentru cel mai mic multiplu comun a două elemente $a, b \in R$.

Definiția 1.13. Două elemente $a, b \in R$ se numesc prime între ele sau relativ prime dacă $\text{c.m.m.d.c.}(a, b) = 1$.

Vom demonstra că în inelul R orice două elemente au un c.m.m.d.c.

Algoritmul lui Euclid. Fie $a, b \in R$, $b \neq 0$. Scriem $a = bq_1 + r_1$ cu $0 \leq r_1 < |b|$, respectiv $\deg r_1 < \deg b$. Dacă $r_1 \neq 0$, atunci scriem $b = r_1q_2 + r_2$ cu $0 \leq r_2 < r_1$, respectiv $\deg r_2 < \deg r_1$. Dacă $r_2 \neq 0$, atunci scriem $r_1 = r_2q_3 + r_3$ cu $0 \leq r_3 < r_2$, respectiv $\deg r_3 < \deg r_2$ și așa mai departe. Obținem astfel un șir strict descrescător de numere naturale $r_1 > r_2 > \dots$, respectiv $\deg r_1 > \deg r_2 > \dots$ care nu poate fi infinit, deci va exista un $n \in \mathbb{N}^*$ astfel încât $r_n \neq 0$ și $r_{n+1} = 0$.

Să arătăm că r_n este un c.m.m.d.c. al elementelor $a, b \in R$. Deoarece $r_{n+1} = 0$ avem $r_{n-1} = r_nq_{n+1}$, deci $r_n \mid r_{n-1}$. Din relația $r_{n-2} = r_{n-1}q_n + r_n$ deducem că $r_n \mid r_{n-2}$. Astfel obținem $r_n \mid r_i$ pentru orice $i = 1, \dots, n$. Din relația $b = r_1q_2 + r_2$ rezultă $r_n \mid b$ iar apoi din $a = bq_1 + r_1$ rezultă $r_n \mid a$. În concluzie, r_n este un divizor comun al lui a și b .

Fie acum d un divizor comun al lui a și b . Din relația $a = bq_1 + r_1$ deducem că $d \mid r_1$ și pas cu pas obținem $d \mid r_i$ pentru orice $i = 1, \dots, n$. În particular, $d \mid r_n$.

În concluzie, c.m.m.d.c.(a, b) este ultimul rest nenul din algoritmul lui Euclid aplicat perechii (a, b) .

Exemplul 1.14. Fie $a = 18$ și $b = 24$. Avem $18 = 24 \cdot 0 + 18$, $24 = 18 \cdot 1 + 6$, $18 = 6 \cdot 3$. Așadar $(18, 24) = 6$.

Exercițiul 1.15. Calculați $(24, 54)$ în \mathbb{Z} cu algoritmul lui Euclid.

Exercițiul 1.16. Calculați $(X^4 - 4X^3 + 1, X^3 - 3X^2 + 1)$ în $\mathbb{R}[X]$ cu algoritmul lui Euclid.

Propoziția 1.17. Fie $a, b, c \in R \setminus \{0\}$.

- (i) Dacă $d = (a, b)$, atunci există a', b' cu $a = da'$, $b = db'$ și $(a', b') = 1$.
- (ii) $(ac, bc) = (a, b)c$.
- (iii) $(a, b) = 1$ și $(a, c) = 1$ implică $(a, bc) = 1$.
- (iv) (Lema lui Euclid) $a \mid bc$ și $(a, b) = 1$ implică $a \mid c$.
- (v) $a \mid c$, $b \mid c$ și $(a, b) = 1$ implică $ab \mid c$.
- (vi) Există $[a, b]$ și $(a, b)[a, b]$ este asociat în divizibilitate cu ab .

Proof. (i) Fie $d' = (a', b')$. Deoarece $d' \mid a'$ și $d' \mid b'$ rezultă că $dd' \mid a$ și $dd' \mid b$, deci $dd' \mid d$ și cum $d \neq 0$ obținem $d' \mid 1$, adică $d' \sim 1$.

(ii) Egalitatea rezultă din algoritmul lui Euclid.

(iii) Fie $d = (a, bc)$. Din $d \mid a$ și $a \mid ac$ rezultă că $d \mid ac$, deci $d \mid (ac, bc)$. Din (ii) obținem $d \mid c$ și cum $d \mid a$ rezultă $d \mid 1$.

(iv) Din (ii) avem că $(ac, bc) = c$. Dar $a \mid ac$ și $a \mid bc$, deci $a \mid c$.

(v) Din (ii) avem că $(ac, bc) = c$. Dar $ab \mid ac$ și $ab \mid bc$, deci $ab \mid c$.

(vi) Fie $d = (a, b)$. Atunci există a', b' cu $a = da'$, $b = db'$ și $(a', b') = 1$. Fie $m = da'b'$. Deoarece $m = ab' = ba'$ rezultă $a \mid m$ și $b \mid m$. Fie $m' \in R$ astfel încât $a \mid m'$ și $b \mid m'$. Avem că $a' \mid \frac{m'}{d}$ și $b' \mid \frac{m'}{d}$. Din (v) rezultă $a'b' \mid \frac{m'}{d}$, deci $m \mid m'$. \square

Propoziția 1.18. Orice ideal al lui R este principal.

Proof. Fie I un ideal nenul al lui R . Fie $a \in I$, $a \neq 0$ cu $|a|$ minim dacă $R = \mathbb{Z}$, respectiv $\deg a$ minim dacă $R = K[X]$. Vom arăta că $I = aR$. Evident, $aR \subseteq I$. Reciproc, fie $b \in I$. Atunci $b = aq + r$ cu $0 \leq r < |a|$, respectiv $\deg r < \deg a$. Dar $r = b - aq \in I$ și atunci neapărat $r = 0$, deci $b = aq \in aR$. \square

Propoziția 1.19. Fie $a, b \in R$. Avem:

- (i) $aR + bR = (a, b)R$;
- (ii) $aR \cap bR = [a, b]R$.

Proof. (i) Deoarece R este inel principal, $aR + bR$ este ideal principal, deci există $d \in R$ cu proprietatea că $aR + bR = dR$. Cum $aR \subseteq dR$ și $bR \subseteq dR$ rezultă $d \mid a$ și $d \mid b$. Fie acum $d' \in R$ cu proprietatea că $d' \mid a$ și $d' \mid b$, echivalent $aR \subseteq d'R$ și $bR \subseteq d'R$. Avem $dR = aR + bR \subseteq d'R$, deci $d' \mid d$.

(ii) Deoarece R este inel principal, $aR \cap bR$ este ideal principal, deci există $m \in R$ cu proprietatea că $aR \cap bR = mR$. Cum $mR \subseteq aR$ și $mR \subseteq bR$ rezultă $a \mid m$ și $b \mid m$. Fie acum $m' \in R$ cu proprietatea că $a \mid m'$ și $b \mid m'$, echivalent $m'R \subseteq aR$ și $m'R \subseteq bR$. Avem $m'R \subseteq aR \cap bR = mR$, deci $m \mid m'$. \square

Corolarul 1.20. Fie $a, b \in R$ și $d = (a, b)$. Atunci există $r, s \in R$ astfel încât $d = ar + bs$.

Remarca 1.21. Folosind corolarul precedent putem da o altă demonstrație propoziției 1.17.

Exercițiul 1.22. Determinați $(X^2 - 1)\mathbb{Q}[X] \cap (X^3 - 1)\mathbb{Q}[X]$ și $(X^2 - 1)\mathbb{Q}[X] + (X^3 - 1)\mathbb{Q}[X]$.

2. ELEMENTE PRIME. ELEMENTE IREDUCTIBILE

În continuare R va desemna \mathbb{Z} sau $K[X]$.

Definiția 2.1. (i) Un element $p \in R$ se numește prim dacă $p \neq 0$, $p \notin U(R)$ și $p \mid ab$ implică $p \mid a$ sau $p \mid b$.

(ii) Un element $q \in R$ se numește ireductibil dacă $q \neq 0$, $q \notin U(R)$ și $q = ab$ implică $a \in U(R)$ sau $b \in U(R)$.

Un element care nu este ireductibil se numește reductibil.

Remarca 2.2. Un element asociat cu un element prim (ireductibil) este de asemenea element prim (ireductibil).

Propoziția 2.3. Orice element prim este ireductibil.

Proof. Dacă $p \in R$ este element prim și $p = ab$, atunci $p \mid ab$ și de aici rezultă $p \mid a$ sau $p \mid b$. Să presupunem că $p \mid a$. Atunci există $a' \in R$ astfel încât $a = pa'$ și înlocuind în $p = ab$ obținem $p = pa'b$, de unde $1 = a'b$, deci $b \in U(R)$. \square

Este adevărat și reciproc.

Propoziția 2.4. Orice element ireductibil este prim.

Proof. Fie $q \in R$ un element ireductibil. Să presupunem că $q \mid ab$. Fie $d = (q, a)$. Scriem $q = dq'$ și $a = da'$. Deoarece q este ireductibil rezultă $d \in U(R)$ sau $q' \in U(R)$. În primul caz $1 = (q, a)$ și din Lema lui Euclid obținem $q \mid b$. În cazul al doilea $q = (q, a)$ și astfel $q \mid a$. \square

Remarca 2.5. (i) Un număr $p \in \mathbb{Z}$ este prim dacă $p \notin \{-1, 0, 1\}$ și are ca divizori doar pe ± 1 și $\pm p$.

(ii) Un polinom $f \in K[X]$ este ireductibil dacă nu se poate scrie ca produs de două polinoame de grad ≥ 1 .

Definiția 2.6. Un număr întreg care nu este prim se numește compus, iar un polinom care nu este ireductibil se numește reductibil.

Exemplul 2.7. (i) Numerele $\pm 2, \pm 3, \pm 5, \dots$ sunt numere prime.

(ii) X este polinom ireductibil, iar X^2 este reductibil.

Propoziția 2.8. (i) Orice polinom de gradul întâi din $K[X]$ este ireductibil.

(ii) Un polinom de grad 2 sau 3 din $K[X]$ este ireductibil dacă și numai dacă nu are rădăcini în K .

Proof. (i) Evident.

(ii) În general, un polinom ireductibil $f \in K[X]$ nu are rădăcini în K . Aceasta rezultă imediat din lema lui Bézout. Reciproc, dacă $f \in K[X]$ cu $\deg f = 2, 3$ și nu are rădăcini în K , atunci f este ireductibil, altminteri s-ar descompune într-un produs de două polinoame dintre care cel puțin unul are gradul 1. Dar orice polinom de grad 1 din $K[X]$ are o rădăcină în K , contradicție. \square

Exemplul 2.9. (i) Polinomul $X^2 - 2$ este ireductibil în $\mathbb{Q}[X]$, dar este reductibil în $\mathbb{R}[X]$.

(ii) Polinoamele $X^2 + X + 1$ și $X^3 + X + 1$ sunt ireductibile în $\mathbb{Z}_2[X]$. Pe de altă

parte, polinomul $X^4 + X^2 + 1$ nu are rădăcini în \mathbb{Z}_2 , dar este reductibil în $\mathbb{Z}_2[X]$: $X^4 + X^2 + 1 = (X^2 + X + 1)^2$.

Exercițiul 2.10. Determinați polinoamele ireductibile de grad ≤ 5 din $\mathbb{Z}_2[X]$.

Exercițiul 2.11. Descompuneți polinomul $X^{56} - X^{49} - X^7 + 1$ în produs de polinoame ireductibile în $\mathbb{Z}_7[X]$.

Propoziția 2.12. Fie $p \in R$ element prim. Atunci inelul factor R/pR este corp.

Proof. Fie $\hat{a} \in R/pR$, $\hat{a} \neq \hat{0}$. Aceasta înseamnă că $a \notin pR$, adică $p \nmid a$. Așadar $(p, a) = 1$. Atunci există $u, v \in R$ cu proprietatea că $pu + av = 1$. Trecând la clase de resturi modulo idealul pR obținem $\hat{a}\hat{v} = \hat{1}$, deci \hat{a} este inversabil. \square

Remarca 2.13. Rezultatul de mai sus ne ajută să construim corpuri finite. De exemplu, $\mathbb{Z}_2[X]/(X^2 + X + 1)$ este corp finit cu 4 elemente.

Propoziția 2.14. Dacă $a \in R$ este un element nenul și neinvertibil, atunci acesta admite o descompunere în produs finit de elemente prime și această scriere este unică (până la o asociere în divizibilitate și abstracție făcând de ordinea factorilor).

Proof. Existența. Presupunem că există $a \in R$ nenul și neinvertibil care nu se scrie ca produs de numere prime, respectiv ca produs de polinoame ireductibile. Îl alegem pe a de modul, respectiv grad minim cu această proprietate. Cum a nu poate fi număr prim, respectiv polinom ireductibil, există $a_1, a_2 \in R$ nenule și neinvertibile astfel încât $a = a_1 a_2$. Atunci $|a_i| < |a|$, respectiv $\deg a_i < \deg a$ pentru $i = 1, 2$. Datorită alegerii lui a , elementele a_1, a_2 se pot scrie ca produs de numere prime, respectiv ca produs de polinoame ireductibile. Dar atunci și a este produs de numere prime, respectiv produs de polinoame ireductibile, contradicție.

Unicitatea. Fie $a = p_1 \cdots p_m = p'_1 \cdots p'_n$ cu $p_i, p'_j \in R$ elemente prime. Vom demonstra (prin inducție după m) că $m = n$ și există $\sigma \in S_n$ astfel încât $p_i \sim p'_{\sigma(i)}$ pentru orice $i = 1, \dots, m$.

Dacă $m = 1$, atunci $p_1 = p'_1 \cdots p'_n$. Deoarece p_1 este prim acesta este ireductibil și rezultă că $n = 1$.

Presupunem acum că $m > 1$. Din $p_m \mid p'_1 \cdots p'_n$ obținem că există j astfel încât $p_m \mid p'_j$ și cum p'_j este ireductibil rezultă $p_m \sim p'_j$. Să considerăm $j = n$, scriem $p_m = up'_n$ cu $u \in U(R)$ și prin simplificare obținem $p_1 \cdots (up_{m-1}) = p'_1 \cdots p'_{n-1}$. Acum aplicăm ipoteza de inducție și deducem că $m - 1 = n - 1$ și există $\sigma' \in S_{n-1}$ astfel încât $p_i \sim p'_{\sigma'(i)}$ pentru orice $i = 1, \dots, m - 1$. \square

Corolarul 2.15. Fie $a, b \in R$ nenule și neinvertibile. Dacă $a = \prod_{i=1}^r p_i^{k_i}$, $b = \prod_{i=1}^r p_i^{l_i}$, unde p_i sunt elemente prime, atunci $(a, b) = \prod_{i=1}^r p_i^{\min(k_i, l_i)}$ și $[a, b] = \prod_{i=1}^r p_i^{\max(k_i, l_i)}$.

Teorema 2.16. Mulțimea numerelor prime pozitive, respectiv mulțimea polinoamelor ireductibile și monice din $K[X]$ este infinită.

Proof. Presupunem că mulțimea numerelor prime pozitive, respectiv mulțimea polinoamelor ireductibile și monice din $K[X]$ este finită. Să notăm cu p_1, \dots, p_r elementele sale. Atunci $N = p_1 \cdots p_r + 1$ admite o descompunere în factori primi,

respectiv polinoame ireductibile și de aici rezultă că există $i \in \{1, \dots, r\}$ cu proprietatea că $p_i \mid N$. Dar cum $p_i \mid p_1 \cdots p_r$ rezultă $p_i \mid 1$, contradicție. \square

Exercițiul 2.17. Determinați c.m.m.d.c. și c.m.m.m.c. pentru polinoamele $f = (X-1)(X^2-1)(X^3-1)(X^4-1)$ și $g = (X+1)(X^2+1)(X^3+1)(X^4+1)$ din $\mathbb{Q}[X]$.

3. TEOREMA FUNDAMENTALĂ A ALGEBREI

Teorema 3.1. (Teorema lui Kronecker) *Fie K un corp și $f \in K[X]$ cu $\deg f \geq 1$. Atunci există o extindere L a lui K în care f are cel puțin o rădăcină.*

Proof. Deoarece f se descompune în produs de polinoame ireductibile este suficient să demonstrăm teorema pentru cazul în care f este ireductibil și de grad ≥ 2 . Fie $L = K[X]/(f)$. Știm că L este corp iar morfismul canonic $K \rightarrow L$ este injectiv, deci putem considera că L este o extindere a lui K . Fie $\alpha = X \bmod (f)$ (clasa lui X modulo idealul (f)). Este imediat că $\alpha \in L$ și $f(\alpha) = 0$. \square

Corolarul 3.2. *Fie K un corp și $f \in K[X]$ cu $\deg f \geq 1$. Atunci există o extindere L a lui K în care f are toate rădăcinile.*

Teorema 3.3. (Teorema fundamentală a algebrei) *Orice polinom $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$ are cel puțin o rădăcină în \mathbb{C} .*

Corolarul 3.4. (i) *Fie $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$. Atunci f este ireductibil dacă și numai dacă $\deg f = 1$.*

(ii) *Fie $f \in \mathbb{R}[X]$ cu $\deg f \geq 1$. Atunci f este ireductibil dacă și numai dacă $\deg f = 1$ sau $\deg f = 2$ și f nu are rădăcini reale.*

Corolarul 3.5. (i) *Fie $f \in \mathbb{C}[X]$ cu $\deg f \geq 1$. Atunci f se scrie în mod unic sub forma*

$$f = a(X - a_1)^{k_1} \cdots (X - a_m)^{k_m}$$

cu $a \in \mathbb{C}^\times$, $a_1, \dots, a_m \in \mathbb{C}$ distincte și $k_1, \dots, k_m \in \mathbb{N}^$.*

(ii) *Fie $f \in \mathbb{R}[X]$ cu $\deg f \geq 1$. Atunci f se scrie în mod unic sub forma*

$$f = a(X - a_1)^{k_1} \cdots (X - a_r)^{k_r} (X^2 + b_1X + c_1)^{l_1} \cdots (X^2 + b_sX + c_s)^{l_s}$$

cu $a \in \mathbb{R}^\times$, $a_1, \dots, a_r \in \mathbb{C}$ distincte, $b_1, c_1, \dots, b_s, c_s \in \mathbb{R}$ cu $b_i^2 < 4c_i$ pentru orice $i = 1, \dots, s$ și $k_1, \dots, k_r, l_1, \dots, l_s \in \mathbb{N}^$.*

Remarca 3.6. În $\mathbb{Q}[X]$ există polinoame ireductibile de orice grad. De exemplu, polinomul $X^n - 2$ este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Exercițiul 3.7. Arătați că polinomul $X^n - 2$ este ireductibil în $\mathbb{Q}[X]$ pentru orice $n \geq 1$.

Exercițiul 3.8. Descompuneți polinomul $X^n - 1$, $1 \leq n \leq 6$, în produs de polinoame ireductibile în $\mathbb{Q}[X]$, $\mathbb{R}[X]$, respectiv $\mathbb{C}[X]$.

4. TEOREMA CHINEZĂ A RESTURILOR

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

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

Vom arăta că sistemul dat are soluții și vom determina cea mai mică soluție pozitivă a acestuia.

Deoarece $(n_1, n_2) = 1$ avem că \hat{n}_1 este inversabil în $\mathbb{Z}/n_2\mathbb{Z}$, respectiv \hat{n}_2 este inversabil în $\mathbb{Z}/n_1\mathbb{Z}$. Așadar există $y_1, y_2 \in \mathbb{Z}$ cu proprietatea că $n_1 y_1 \equiv 1 \pmod{n_2}$, respectiv $n_2 y_2 \equiv 1 \pmod{n_1}$. Fie acum $x = a_1 n_2 y_2 + a_2 n_1 y_1$. Este evident că x este o soluție a sistemului de congruențe dat. Mai mult, sistemul are o infinitate de soluții, deoarece $x + kn_1 n_2$ este de asemenea soluție, oricare ar fi $k \in \mathbb{Z}$.

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

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

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

nu are soluții.

Exercițiul 4.1. Să se afle cea mai mică soluție pozitivă a sistemului de congruențe

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

Exercițiul 4.2. Rezolvați sistemul de congruențe

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

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

Teorema 4.3. (Teorema chineză a resturilor) Fie $s \geq 2$ și fie $n_1, \dots, n_s \geq 2$ numere întregi oricare două prime între ele. Fie a_1, \dots, a_s numere întregi fixate. Considerăm sistemul de congruențe

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ \dots\dots\dots \\ x \equiv a_s \pmod{n_s} \end{cases}$$

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