CZU 511.2(072.8)

TEHNICI DE REZOLVARE A CONGRUENȚELOR LINIARE ÎN RAPORT CU MODUL COMPUS

Doina BARGAN, *studentă, Facultatea de Științe Reale, Economice și ale Mediului, Universitatea de Stat „Alecu Russo" din Bălți*
Conducător științific: **Tatiana ROTARI,** *asist. univ.*

Abstract: *The concept of linear congruence is studied in the university course of Algebra and Number Theory, as a fundamental notion of study in the Mathematics and Computer Science specialty. During the course, some learning difficulties arise, which are influenced by various factors. One of these factors is the limited number of exercises provided in the problem sets for the given topic, as well as the wide variety of methods used to solve them.*

Keywords: *residue class, linear congruence, evidence method, multiple of module, Euler's theorem,*

Teoria numerelor este cea mai veche ramură a matematicii, fiind o ramură pură dedicată în primul rând studiului numerelor întregi. Numerele întregi pot fi luate fie ca atare, fie ca soluții ale ecuațiilor. Întrebările din teoria numerelor sunt deseori înțelese cel mai bine prin studiul obiectelor analitice care codifică proprietățile numerelor întregi, prime sau altor obiecte teoretice numerice.

Termenul mai vechi pentru teoria numerelor este aritmetică. La începutul secolului al XX-lea, el a fost înlocuit de „teoria numerelor". Utilizarea termenului „aritmetică" pentru teoria numerelor a recâștigat un anumit nivel în a doua jumătate a secolului XX, probabil datorită influenței franceze.

Conceptul de congruență liniară se aseamănă destul de mult cu acela de ecuație liniară, atât ca formă, dar și ca sens. În continuare se va descrie și se va caracteriza acest concept.

Definiția 1. Două numere a și b se numesc congruente după modulul m dacă fiind împărțite la m dau același rest [1].

De exemplu, numerele 13 și 16 sunt congruente după modulul 3, deoarece restul împărțirii acestor numere la 3 este 1 pentru fiecare din ele.

Definiția 2. Expresia de forma

$$ax \equiv b \ (mod\ m) \qquad (1)$$

se numește congruența liniară cu o necunoscută [1, 2].

A rezolva o congruență liniară înseamnă a determina clasa de numere care fiind înmulțite cu a, iar mai apoi să fie împărțite la m să dea restul egal cu b. Congruețele liniare pot avea 0, 1 sau mai multe soluții. Pentru a determina numărul de soluții ale congruenței liniare se verifică următoarele condiții:

1. dacă $(a, m) = 1$, atunci congruența are o singură soluție.
2. dacă $(a, m) = d$ și $d \nmid b$, atunci congruența nu are soluții.

3. dacă $(a, m) = d$ și $d \mid b$, atunci congruența are d soluții.

Exemplul 1. Congruența

$$3x \equiv 4 \ (mod\ 11)$$

congruența are o singură soluție, deoarece numerele 3 ,si 11 sunt reciproc prime.

Exemplul 2. Congruența

$$6x \equiv 13 \ (mod\ 24).$$

Deoarece cel mai mare divizor comun al numerelor 6 și 24 este 2, iar 13 nu se divide prin 2, reiese că congruența nu admite soluții.

Este de evidențiat faptul că, soluția unei congruențe liniare nu este un număr, ci o clasă de rest (o mulțime de numere care fiind împărțite la m da același rest).

Metoda probelor. Una din cele mai cunoscute și folosite metodă de rezolvare a congruențelor liniare este metoda probelor. Această metodă constă în următoarele:

1. se determinăm numărul de soluții;
2. se determină sistemul complet de resturi;
3. se substituie treptat clasele de resturi în congruență până se determină toate soluțiile.

Spre deosebire de cazul când modulul este prim, în cazul în care modulul este compus, este necesar de ținut cont de faptul că nu orice clasă de rest poate fi soluție a congruenței liniare, precum și de faptul că congruența poate avea mai multe soluții. Dacă congruența are soluție unică, termenul liber și modulul nu sunt numere reciproc prime, atunci soluția congruenței la fel nu este reciproc primă cu modulul. Dacă însă congruența liniară are mai multe soluții, atunci se procedează astfel:

1. se determină numărul de soluții ale congruenței (1).
2. se împart ambele părți ale congruenței și modulul la numărul de soluții. Congruența nouă obținută poate fi atât o congruență liniară în raport cu modulul prim, cât și în raport cu modulul compus.
3. se determină soluția congruenței prin metoda probelor descrisă sus, apoi se generează soluțiile congruenței în felul următor:
   a) după simplificarea congruenței (1) prin k obținem:
   $$a'x = b' \ (mod\ m'), \qquad (2)$$
   unde $a = a'k, b = b'k, m = m'k$.
   b) fie $x' \equiv c \ (mod\ m')$, atunci
   $$x \equiv c \ (mod\ m)$$
   este o soluție a congruenței inițiale.
4. se generează celelalte $k - 1$ soluții:
$$\begin{cases} x \equiv c + m' (mod\ m), \\ x \equiv c + 2m' \ (mod\ m), \\ \dots\ \dots\ \dots \\ x \equiv c + (k-1)m' \ (mod\ m). \end{cases} \qquad (3)$$

Exemplul 3. Rezolvați congruența: $2x \equiv 7\ (mod\ 21)$.

Rezolvare. Deoarece 2 și 21 sunt numere reciproc prime, iar $(7, 21) = 7$, reiese că soluția congruenței este generată de un număr ce nu este prim cu modulul și nici cu 7, adică se caută soluția congruenței printre 7 și 14.

$$x \equiv 7 \Longrightarrow 2 \cdot 7 \equiv 14\ (mod\ 21),$$
$$x \equiv 14 \Longrightarrow 2 \cdot 14 \equiv 7\ (mod\ 21).$$

Deoarece congruența are o singură soluție, reiese să soluția a fost găsită și anume:

$$x \equiv 14\ (mod\ 21) \Leftrightarrow x = 14 + 24t, t \in \mathbb{Z}$$

Răspuns. $S = \{14 + 21t, t \in \mathbb{Z}\}$

Exemplul 4. Rezolvați congruența: $38x \equiv 4\ (mod\ 26)$. [4]

Rezolvare. Deoarece $(38, 26) = 2$ și 4 se divide prin 2, reiese că ecuația are două soluții. Simplificând congruența prin 2, se obține:

$$19x \equiv 2\ (mod\ 13)$$

Deoarece $(13, 19) = 1$, reiese că congruența nouă obținută posedă soluție unică. Se determină clasele de rest modulul 13:

$$Z_{13} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12\}.$$

Prin substituții succesive se determină soluția congruenței în raport cu modulul 13 și anume:

$$x = 5 \Longrightarrow 19 \cdot 5 = 95 - 7 \cdot 13 = 4 \equiv 4\ (mod\ 13).$$

Deoarece congruența inițială a avut soluții multiple, se generează soluțiile în raport cu modulul 26.

$$x_1 \equiv 5\ (mod\ 26),$$
$$x_2 \equiv 5 + 13\ (mod\ 26) \Longrightarrow x_2 \equiv 18\ (mod\ 26).$$

Răspuns. $S = \{5 + 26t_1, 18 + 26t_2, \forall t_1, t_2 \in \mathbb{Z}\}$.

Metoda adunări unui multiplu al modulului la partea dreaptă a congruenței.

Această metodă se bazează pe următoarele două proprietăți ale relației de congruență:

1. la orice parte a congruenței poate fi adunat sau scăzut un multiplu al modulului;
2. ambele părți ale congruențe pot fi simplificate printr-un număr ce este reciproc prim cu modulul.

Pentru a rezolva congruența liniară în raport cu modul compus prin această metodă, este necesar mai întâi de studiat numărul de soluții ale congruenței liniare. Metoda poate fi aplicată dacă congruența are o singură soluție. Pentru a rezolva congruența prin metoda adunării unui multiplu al modulului la partea dreaptă a congruenței, se parcurg după următorii pași: se adună la partea dreaptă a congruenței un multiplu al modulului, astfel încât numărul $b + mt, t \in \mathbb{Z}$ să se devidă prin a, anume $b + mt = ak$, unde $mt \in \mathbb{Z}$. În rezultat se va obține următoarea:

$$ax \equiv ab'\ (mod\ m). \qquad (4)$$

Deoarece $(a, m) = 1$, după simplificarea ambele părți ale congruenței a relație (4) de forma:

$$x \equiv b' \ (mod\ m) \Leftrightarrow x = b' + mt, t \in \mathbb{Z}. \quad (6)$$

Exemplul 5. Rezolvați congruența $15x \equiv 21\ (mod\ 18)$ [8]:

Rezolvare. Deoarece $(15, 18) = 3$ și 21 se divide prin 3, reiese că congruența are trei soluții. După simplificarea songruenței și modulului prin 3, se obține:

$$5x \equiv 7\ (mod\ 6).$$

Deoarece partea stângă a congruenței este un multiplu al lui 5, relația de congruență este posibilă doar dacă partea dreaptă a congruenței la fel este un multiplu al lui 5. Adunând la partea dreaptă a congruenței trei module, se obține:

$$5x \equiv 7 + 18\ (mod\ 6) \Leftrightarrow 5x \equiv 25 (mod\ 6).$$

Simplificând ambele părți ale congruenței prin 5, se obține:

$$x \equiv 5\ (mod\ 6).$$

Se generează soluțiile congruenței în raport cu modulul 18.

$$\begin{bmatrix} x \equiv 5\ (mod\ 18), \\ x \equiv 5 + 6\ (mod\ 18), \\ x \equiv 5 + 12\ (mod\ 18) \end{bmatrix} \Leftrightarrow \begin{bmatrix} x \equiv 5\ (mod\ 18), \\ x \equiv 11\ (mod\ 18), \\ x \equiv 17\ (mod\ 18) \end{bmatrix} \Leftrightarrow \begin{bmatrix} x = 5 + 18\,t_1, \\ x = 11 + 18t_2,\ t_1, t_2, t_3 \in \mathbb{Z}. \\ x = 17 + 18t_3, \end{bmatrix}$$

Răspuns. $S = \{5 + 18t_1, 11 + 18t_2, 17 + 18t_3, \forall t_1, t_2, t_3 \in \mathbb{Z}\}$

Utilizarea teoremei lui Euler în rezolvarea congruenței liniare. Una din cele mai importante teoreme cu referire la teoria congruențelor este teorema lui Euler sau se mai numește și teorema Fermat-Euler. Analizei și demonstrări acestei teoreme a fost dedicate multe lucrări. În una din aceste lucrări [9], teorema este formă astfel:

Teoremă. Dacă $n \geq 2$ este un număr natural, iar $a \in \mathbb{Z}$ astfel încât $(a, n) = 1$. atunci $a^{\varphi(n)} \equiv 1\ (mod\ n)$ (φ fiind indicatorul lui Euler).

Indicatorul lui Euler reprezintă una dintre funcțiile numerice ce determină numerele de numere naturale ce sunt mai mici decât n și sunt reciproc prime cu n. Dacă numărul natural n are descompunerea canonică

$$n = p_1^{k_1} \cdot p_2^{k_2} \cdot \ldots \cdot p_s^{k_s},$$

atunci

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

În continuare, descriem algoritmul de rezolvare a congruențelor liniare, utilizând teorema lui Euler. După cum este cunoscut, teorema lui Euler reliefează că:

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

unde cum am spus mai sus $\varphi(m)$ este indicatori lui Euler. Înmulțind congruența generală cu aceasta, parte cu parte obținem:

$$ax \equiv b \cdot a^{\varphi(m)}\ (mod\ m)$$

sau

$$x \equiv b \cdot a^{\varphi(m)-1} \ (mod\ m).$$

Exemplul 6. Rezolvați congruența

$$7x \equiv 9 \ (mod\ 25).$$

Rezolvare. Pentru a rezolva congruența liniară, se determină mai întâi indicatorul lui Euler pentru $m = 25$. Deoarece $25 = 5^2$, se obține:

$$\varphi(25) = 25\left(1 - \frac{1}{5}\right) = 25 \cdot \frac{4}{5} = 20.$$

Atunci soluția congruenței este

$$x \equiv 9 \cdot 7^{19} \ (mod\ 25)$$

Determinăm în continuare restul împărțirii numărului $9 \cdot 7^{19}$ la 25, folosind proprietățile congruețelor numerice.

$$7^2 = 49 \equiv -1 \ (mod\ 25)$$

Ridicăm albele părți ale congruenței la puterea a 9-a:

$$7^{18} \equiv -1 \ (mod\ 25)$$

Înmulțim ambele părți ale congruenței la 63:

$$9 \cdot 7^{19} \equiv -63 \ (mod\ 25)$$

Adunăm la partea întreagă un multiplu al modulului și anume 75. În rezultat obținem:

$$9 \cdot 7^{19} \equiv 12 \ (mod\ 25)$$

sau

$$x \equiv 12 \ (mod\ 25)$$

Răspuns. S=$\{12 + 25t \mid t \in \mathbb{Z}\}$

Bibliografie:

1. ROTARI, T. *Algebra și teoria numerelor:* Suport de curs, Bălți, 2019. – 167 p. ISBN 978-9975-3369-7-0
2. УЛИКОВ Л. Я. Алгебра и теория чисел. Москва, Изд.: Высшая школа, 1979. – 559 стр.
3. ГРИБАНОВ, В. И., Сборник упражнений по теорий чисел. Москва, Издательство Просвещение, 1964. – 144 стр.
4. НЕСТЕРЕНКО, Ю. Теория чисел, М., Изд, Академия, 2008, – 272 стр. ISBN 978-5-7695-4646
5. ROTARU D, Utilizarea teoremei lui Fermat la rezolvarea congruențelor liniare. În Interuniversitaria, Bălți, Editura Universității de Stat 2019. pp. 29-32. ISBN 978-9975-50-234-4
6. КАЗАЧЕК Н., Алгебра и теория чисел. Москва, Изд. Просвещение, 1974. – 196 стр. ISBN 60406-705-103-03-7
7. VOLCOV, N. F., Elemente de teoria numerelor Chișinău, Ed. Școala Sovietică, 1958.
8. КОЧЕВА А. А., Задачник-практикум по алгебре и теории чисел. Ч. III. Москва, Изд.: Просвещение 1984. – 41 стр.
9. BOBOC F., PICIU D., *Aritmetica și teoria numerelor,* Craiova, Ed. Universitaria, 1999. 216 p. ISBN: 973-927-73-1