Др Бернадин Ибрахимпашић, др Ариф Золић

ЧЕТИРИ МЕТОДЕ ЗА РЈЕШАВАЊЕ ЛИНЕАРНИХ КОНГРУЕНЦИЈА

Теорију конгруенција је увео Гаус у свом дјелу *Disquisitiones Arithmeticae* 1801. године. Он је увео и ознаку за конгруенције $\equiv$ која је и данас у употреби. Као што је и ознака за конгруенције слична знаку једнако, тако и саме конгруенције имају доста сличности с једнакостима. Истакнимо да је релација „бити конгруентан модуло m“ релација еквиваленције на скупу $\mathbb{Z}$, тј. она је рефлексивна, симетрична и транзитивна.

Дефиниција 1. Ако цијели број $m \neq 0$ дијели разлику $a - b$ онда кажемо да је *a конгруентан b* модуло m и пишемо $a \equiv b \pmod{m}$. У противном кажемо да *a није конгруентан b* модуло m и пишемо $a \not\equiv b \pmod{m}$.

Треба напоменути да, како је $a - b$ дјељиво с m ако и само ако је дјељиво с $-m$, то је довољно разматрати само случајеве када је m позитиван цијели број, тј. када је m природан. Такође треба уочити да постоји разлика између конгруенција и остатака при дијељењу природним бројем. Ако је a цијели и m природан број, тада $a \bmod m$ представља остатак при дијељењу броја a бројем m. Тако имамо да је $23 \equiv 13 \pmod{5}$, али је $23 \bmod 5 \neq 13$.

Једна карактеризација конгруенција је директна посљедица Теореме о дијељењу с остатком.

Теорема 1. [Теорема о дијељењу с остатком] *За произвољан природан број b и цијели број a постоје јединствени цијели бројеви q и r такви да је $a = qb + r$, $0 \leqslant r < b$.*

Број q се зове количник а r се зове остатак.

Сада из дефиниције релације бити конгруентан и претходне теореме закључујемо да ако је $a \equiv b \pmod{m}$, то значи да постоји цијели број k такав да је $a = km + b$.

Ми ћемо анализирати рјешивост линеарне конгруенције с једном непознатом, тј. конгруенције облика

$$ax \equiv b \pmod{m},$$

гдје су a и m природни бројеви, а b цијели број.

Прије него наведемо методе за рјешавање линеарних конгруенција, наведимо неке особине конгруенција.

Теорема 2. *Нека су a, b, c, d цијели бројеви, $m, m_1, m_2, \ldots, m_r$ природни бројеви и f полином с цјелобројним коефицијентима.*

1. $a \equiv b \pmod{m} \Leftrightarrow a - b \equiv 0 \pmod{m}$.
2. *Ако је* $a \equiv b \pmod{m}$ *и* $c \equiv d \pmod{m}$, *онда је* $ac \equiv bd \pmod{m}$, $a + c \equiv b + d \pmod{m}$ *и* $a - c \equiv b - d \pmod{m}$.
3. *Ако је* $a \equiv b \pmod{m}$ *и* $d \mid m$, *онда је* $a \equiv b \pmod{d}$.
4. *Ако је* $a \equiv b \pmod{m}$, *онда је* $ac \equiv bc \pmod{mc}$ *за сваки* $c > 0$.
5. $a \equiv b \pmod{m_i}, i = 1, \ldots, r \Leftrightarrow a \equiv b \pmod{\operatorname{nzs}(m_1, \ldots, m_r)}$.
6. *Ако је* $a \equiv b \pmod{m}$ *онда је* $f(a) \equiv f(b) \pmod{m}$.
7. $ax \equiv ay \pmod{m} \Leftrightarrow x \equiv y \pmod{\frac{m}{\operatorname{nzd}(a,m)}}$.
8. *Ако је* $m > 1$, $\operatorname{nzd}(a, m) = \operatorname{nzd}(b, m) = 1$, *те вриједи* $a^c \equiv b^c \pmod{m}$ *и* $a^d \equiv b^d \pmod{m}$, *тада је* $a^{\operatorname{nzd}(c,d)} \equiv b^{\operatorname{nzd}(c,d)} \pmod{m}$.

1. Рјешење линеарне конгруенције

Рјешење конгруенције $f(x) \equiv 0 \pmod{m}$, гдје је $f(x)$ полином с цјелобројним коефицијентима, јесте сваки цијели број x који је задовољава. Ако је x_1 неко рјешење конгруенције $f(x) \equiv 0 \pmod{m}$, и $x_2 \equiv x_1 \pmod{m}$, онда је и x_2 такође рјешење те конгруенције. За два рјешења x и x' кажемо да су *еквивалентна* ако је $x \equiv x' \pmod{m}$. Под бројем рјешења конгруенције подразумијевамо број нееквивалентних рјешења.

Теорема 3. *Нека су a и m природни бројеви, те b цијели број. Конгруенција*

$$ax \equiv b \pmod{m} \tag{1}$$

има рјешења ако и само ако $d = \operatorname{nzd}(a, m)$ дијели b. Ако је овај услов испуњен, онда горња конгруенција има тачно d рјешења модуло m, и то

$$x_0 + t \cdot \frac{m}{d}, \quad t = 0, 1, \ldots d - 1,$$

гдје је x_0 јединствено рјешење конгруенције

$$\frac{a}{d}\, x \equiv \frac{b}{d} \pmod{\frac{m}{d}}.$$

У раду ће бити описане четири методе за рјешавање линеарних конгруенција с једном непознатом, и то:

1. метода свођења на диофантску једначину,
2. метода трансформације коефицијената,
3. Ојлерова метода,
4. метода која користи Еуклидов алгоритам

Примјер 1. Ријешити конгруенцију $4x \equiv 7 \pmod{10}$.

Рјешење. Како $\operatorname{nzd}(4, 10) = 2$ не дијели 7, то посматрана конгруенција нема рјешења. $\triangle$

2. Метода свођења на диофантску једначину

Ако је $ax \equiv b \pmod{m}$, онда број m дијели разлику $ax-b$, тј. мора постојати цијели број y такав да је $\dfrac{ax-b}{m} = y$ или у еквивалентном облику

$$ax - my = b. \tag{2}$$

Видимо да ће конгруенција (1) имати рјешење ако диофантска једначина (2) има рјешење. Ако је x_0 рјешење конгруенције (1), тј. ако је (x_0, y_0) рјешење диофантске једначине (2), онда мора бити

$$ax_0 - my_0 = b. \tag{3}$$

Одузмемо ли од једначине (2) једначину (3) добијамо да је

$$y - y_0 = \frac{a(x-x_0)}{m}.$$

Како $d = \mathrm{nzd}(a, m)$ дијели a и m, то вриједи

$$y - y_0 = \frac{\frac{a}{d}(x-x_0)}{\frac{m}{d}},$$

а како су бројеви a/d и m/d релативно прости, те како је лијева страна цијели број, то да би и десна страна била цијели број мора бити $x - x_0$ дјељиво с m/d. Тако добијамо да је

$$x - x_0 = t \cdot \frac{m}{d} \quad \text{па је} \quad x = x_0 + t \cdot \frac{m}{d},\ t \in \mathbb{Z}.$$

Тако добијамо d неконгруентних рјешења модуло m конгруенције (1), и то:

$$x_0, x_0 + \frac{m}{d}, x_0 + \frac{2m}{d}, \ldots, x_0 + \frac{(d-1)m}{d}.$$

Примјер 2. Ријешити методом свођења на диофантску једначину конгруенције

а) $3x \equiv 5 \pmod{7}$, б) $2x \equiv 6 \pmod{10}$.

Рјешење. а) Како је $\mathrm{nzd}(3, 7) = 1$ и како $1 \mid 5$, то наша конгруенција има јединствено рјешење. Из дате конгруенције слиједи да број $3x - 5$ мора бити дјељив са 7, тј. постоји цијели број y такав да је $\dfrac{3x-5}{7} = y$. То значи да је

$$3x - 7y = 5. \tag{4}$$

Очито је једно партикуларно рјешење ове једначине $(x_0, y_0) = (4, 1)$ и вриједи

$$3x_0 - 7y_0 = 5. \tag{5}$$

Одузимајући једначине (4) и (5) добијамо $3(x-x_0)-7(y-y_0) = 0$, одакле слиједи да је $x - x_0 = 7t$, $t \in \mathbb{Z}$. Закључујемо да је рјешење полазне конгруенције

$$x = 7t + 4,\ t \in \mathbb{Z}, \quad \text{тј.} \quad x \equiv 4 \pmod{7}.$$

б) Сада је $\mathrm{nzd}(2,10) = 2$, па како $2 \mid 6$, то полазна конгруенција има 2 рјешења. Аналогно претходном примјеру, добијамо придружену диофантску једначину $2x - 10y = 6$ чије је једно партикуларно рјешење $(8,1)$, па јој је рјешење

$$x = 8 + \frac{-10}{2} \cdot t = 8 - 5t,\ t \in \mathbb{Z},$$

тј. $x = 8 + 5w$, $w \in \mathbb{Z}$. Добили смо да је рјешење дате конгруенције $x \equiv 8 \pmod 5$, што можемо записати као

$$x = 10t + 3 \quad \text{или} \quad x = 10t + 8,\ t \in \mathbb{Z}. \quad \triangle$$

3. Метода трансформације коефицијената

Користећи чињеницу да је релација бити конгруентан једна релација еквиваленције, те њене наведене особине, ми заданој конгруенцији додајемо (одузимамо) неку прикладно одабрану истиниту конгруенцију како бисмо поједноставили поступак рјешавања.

Примјер 3. Методом трансформације коефицијената ријешити конгруенције
а) $7x \equiv 3 \pmod{11}$, б) $17x \equiv 25 \pmod{28}$.

Рјешење. а) Како је $\mathrm{nzd}(7,11) = 1$ и како $1 \mid 3$, то наша конгруенција има јединствено рјешење. Додамо ли задатој конгруенцији конгруенцију $0 \equiv 11 \pmod{11}$, која је очигледно истинита, добијамо конгруенцију $7x \equiv 14 \pmod{11}$. Скратимо ли ову конгруенцију са 7 (што је дозвољено) добијамо

$$x \equiv 2 \pmod{11},$$

што и представља рјешење полазне конгруенције.

б) Због $\mathrm{nzd}(17,28) = 1$ и ова конгруенција има јединствено рјешење. Додамо ли јој конгруенцију $28x \equiv 0 \pmod{28}$ добијамо конгруенцију $45x \equiv 25 \pmod{28}$ коју можемо скратити с 5. Након скраћивања имамо конгруенцију $9x \equiv 5 \pmod{28}$, којој додајемо конгруенцију $0 \equiv -140 \pmod{28}$ и добијамо $9x \equiv -135 \pmod{28}$. Након скраћивања с 9 добијамо конгруенцију $x \equiv -15 \pmod{28}$, тј.

$$x \equiv 13 \pmod{28}. \quad \triangle$$

4. Ојлерова метода

За рјешавање линеарних конгруенција Ојлеровом методом потребна нам је Ојлерова теорема.

Дефиниција 2. Функција $\varphi\colon \mathbb{N} \to \mathbb{N}$, која природном броју m придружује број природних бројева мањих или једнаких m, који су релативно прости с m, назива се *Ојлерова функција*.

Ојлерова функција је мултипликативна, тј. ако су m и n релативно прости природни бројеви, онда за Ојлерову функцију вриједи $\varphi(mn) = \varphi(m) \cdot \varphi(n)$. Ако

је $n = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_r^{\alpha_r}$ растављање природног броја $n > 1$ на просте факторе, онда вриједи

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

Специјално имамо да за прост број p вриједи $\varphi(p) = p - 1$.

Пример 4. Израчунати вриједност Ојлерове функције за 13 и 778635.

Рјешење. Како је 13 прост број, то је $\varphi(13) = 13 - 1 = 12$. Одредимо ли канонско растављање броја 778635 добијамо

$$\begin{aligned}\varphi(778635) &= \varphi\left(3^2 \cdot 5 \cdot 11^3 \cdot 13\right) \\ &= 778635 \cdot \left(1 - \frac{1}{3}\right) \cdot \left(1 - \frac{1}{5}\right) \cdot \left(1 - \frac{1}{11}\right) \cdot \left(1 - \frac{1}{13}\right) \\ &= 348480. \quad \triangle\end{aligned}$$

Теорема 4. [Ојлер] *Нека су a и m природни бројеви. Ако је* $\operatorname{nzd}(a, m) = 1$*, онда је*

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

Према Ојлеровој теореми имамо да је $a^{\varphi(m)} \equiv 1 \pmod{m}$, а због рефлексивности релације конгруенције вриједи $b \equiv b \pmod{m}$. Измножимо ли ове двије конгруенције добијамо да је $a^{\varphi(m)} \cdot b \equiv b \pmod{m}$, тј.

$$a \cdot \left(a^{\varphi(m)-1} \cdot b\right) \equiv b \pmod{m}.$$

Упоредимо ли ову конгруенцију с конгруенцијом (1), чије рјешење тражимо, видимо да је њено рјешење

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

Пример 5. Ојлеровом методом ријешити конгруенцију $5x \equiv 4 \pmod{12}$.

Рјешење. Како је $\operatorname{nzd}(5, 12) = 1$, то наша конгруенција има јединствено рјешење. Искористимо ли Ојлерову теорему и описану методу добијамо да је рјешење полазне конгруенције

$$\begin{aligned}x &\equiv 5^{\varphi(12)-1} \cdot 4 \pmod{12} \equiv 5^{4-1} \cdot 4 \pmod{12} \\ &\equiv 125 \cdot 4 \pmod{12} \equiv 5 \cdot 4 \pmod{12} \\ &\equiv 20 \pmod{12} \equiv 8 \pmod{12}. \quad \triangle\end{aligned}$$

5. Метода која користи Еуклидов алгоритам

Еуклидов алгоритам за одређивање највећег заједничког дјелиоца два природна (цијела) броја први пут је описан у Еуклидовим *Елементима*, античком дјелу о математици које је настало око 300. године пр.н.е, иако се вјерује да је алгоритам био познат бар 200 година раније. У VII књизи *Елемената* је исказан за природне бројеве, а у X књизи је дата његова примјена на дужи.

Еуклидов алгоритам је први нетривијални алгоритам који је преживио до данас. Врло је ефикасан за рачунање највећег заједничког дјелиоца два природна броја који не захтијева њихову претходну факторизацију, за коју треба напоменути да представља један од тешких математичких проблема.

Алгоритам има велику и теоријску и практичну примјену. У [4] су описане неке од практичних примјена као што су рјешавање линеарних диофантских једначина, рјешавање линеарних конгруенција, одређивање мултипликативног инверза у коначном пољу и за развој рационалног броја у верижни разломак. У [3] је описана методичка обрада наставне теме Еуклидов алгоритам.

Еуклидов алгоритам је заснован на Теореми о дијељењу с остатком и на чињеници исказаној у сљедећој теореми.

Теорема 5. *Нека су a, b, q и r цијели бројеви такви да је $b > 0$, $0 \leqslant r < b$ и $a = bq + r$. Тада је* $\operatorname{nzd}(a, b) = \operatorname{nzd}(b, r)$.

Теорема 6. [Еуклидов алгоритам] *Нека су a и $b > 0$ цијели бројеви. Претпоставимо да је узастопном примјеном Теореме о дијељењу с остатком добијен низ једнакости*

$$\begin{aligned} a &= bq_1 + r_1, & 0 < r_1 < b,\\ b &= r_1q_2 + r_2, & 0 < r_2 < r_1,\\ r_1 &= r_2q_3 + r_3, & 0 < r_3 < r_2,\\ &\dots\\ r_{j-2} &= r_{j-1}q_j + r_j, & 0 < r_j < r_{j-1},\\ r_{j-1} &= r_jq_{j+1}. \end{aligned}$$

Тада је $\operatorname{nzd}(a, b)$ *једнак r_j, тј. посљедњем остатку различитом од нуле. Вриједности за x_0 и y_0 у изразу* $\operatorname{nzd}(a, b) = ax_0 + by_0$ *могу се добити изражавањем сваког остатка r_i као линеарне комбинације од a и b.*

Рјешење конгруенције (1) добијамо примјеном рекурзивне релације

$$x_{-1} = 1, \quad x_0 = 0, \quad x_i = x_{i-2} - q_ix_{i-1}, \quad i = 1, 2, \dots, j,$$

гдје је j индекс посљедњег остатка у Еуклидовом алгоритму који је различит од 0, а q_i су количници из Еуклидовог алгоритма. У том случају рјешење конгруенције (1) је

$$x \equiv x_j \pmod m.$$

Кроз примјере ћемо показати рјешавање конгруенције $ax \equiv b \pmod m$ у 4 случаја:

1. $\operatorname{nzd}(a, m) = b = 1$,
2. $\operatorname{nzd}(a, m) = 1$, $b > 1$,
3. $\operatorname{nzd}(a, m) = b \neq 1$,
4. $b > \operatorname{nzd}(a, m) > 1$.

Примјер 6. Ријешити конгруенцију $5x \equiv 1 \pmod 7$.

Рјешење. Одредимо $\operatorname{nzd}(5, 7)$ Еуклидовим алгоритмом.

$$5 = 7 \cdot 0 + 5, \quad 7 = 5 \cdot 1 + 2, \quad 5 = 2 \cdot 2 + 1, \quad 2 = 1 \cdot 2.$$

Добили смо да је $\mathrm{nzd}(5,7)=1$, па наша конгруенција има јединствено рјешење које добијамо примјеном наведене рекурзивне релације.

i	-1	0	1	2	3
q_i			0	1	2
x_i	1	0	1	-1	3

Добили смо да је $x\equiv 3 \pmod 7$ рјешење полазне конгруенције. $\triangle$

Примјер 7. Рјешити конгруенцију $7x\equiv 5 \pmod 9$.

Рјешење. Одредимо $\mathrm{nzd}(7,9)$ Еуклидовим алгоритмом.

$$7=9\cdot 0+7,\quad 9=7\cdot 1+2,\quad 7=2\cdot 3+1,\quad 2=1\cdot 2.$$

Добили смо и овдје да је $\mathrm{nzd}(7,9)=1$ па наша конгруенција има јединствено рјешење.

i	-1	0	1	2	3
q_i			0	1	3
x_i	1	0	1	-1	4

Аналогно претходном примјеру је $x'\equiv 4 \pmod 9$ рјешење конгруенције $7x\equiv 1 \pmod 9$, па је рјешење полазне конгруенције

$$x\equiv 5\cdot 4\equiv 20\equiv 2 \pmod 9. \quad \triangle$$

Примјер 8. Ријешити конгруенцију $24x\equiv 3 \pmod{39}$.

Рјешење. Примијенимо Еуклидов алгоритам.

$$24=39\cdot 0+24,\quad 39=24\cdot 1+15,\quad 24=15\cdot 1+9,$$
$$15=9\cdot 1+6,\quad 9=6\cdot 1+3,\quad 6=3\cdot 2.$$

Видимо да је $d=\mathrm{nzd}(24,39)=3$, па како $3\mid 3$ то конгруенција има 3 рјешења. Рјешење полазне конгруенције је

$$x\equiv x_j+t\cdot\frac{m}{d} \pmod m,\ t=0,1,\dots,d-1,$$

гдје је k индекс посљедњег ненултог остатка у Еуклидовом алгоритму.

i	-1	0	1	2	3	4	5
q_i			0	1	1	1	1
x_i	1	0	1	-1	2	-3	5

Добили смо да је рјешење наше конгруенције $24x\equiv 3 \pmod{39}$ дато с

$$x\equiv 5+t\cdot\frac{39}{3}\equiv 5+13t,\quad t=0,1,2,$$

тј. $x\equiv 5,18,31 \pmod{39}$. $\triangle$

Пример 9. Ријешити конгруенцију $195x \equiv 57 \pmod{231}$.

Рјешење. Примијенимо Еуклидов алгоритам да одредимо $\mathrm{nzd}(231, 195)$.

$$195 = 231 \cdot 0 + 195, \quad 231 = 195 \cdot 1 + 36, \quad 195 = 36 \cdot 5 + 15,$$
$$36 = 15 \cdot 2 + 6, \quad 15 = 6 \cdot 2 + 3, \quad 6 = 3 \cdot 2.$$

Добили смо да је $d = \mathrm{nzd}(195, 231) = 3$. Како $3 \mid 57$ то дата конгруенција има рјешење (има 3 рјешења).

Формирајмо конгруенцију $a'u \equiv b' \pmod{m'}$, гдје је $a' = a/d$, $b' = b/d$ и $m' = m/d$. Како је $\mathrm{nzd}(a', m') = 1$, то посљедња конгруенција има јединствено рјешење. У нашем примјеру имамо да је $a' = 195/3 = 65$, $b' = 57/3 = 19$ и $m' = 231/3 = 77$. Напоменимо да су количници у Еуклидовом алгоритму за одређивање $\mathrm{nzd}(a', m')$ једнаки количницима из Еуклидовог алгоритма за одређивање $\mathrm{nzd}(a, m)$. Искористимо ту чињеницу и примијенимо наведену рекурзивну релацију да ријешимо конгруенцију $65u \equiv 19 \pmod{77}$.

i	-1	0	1	2	3	4	5
q_i			0	1	5	2	2
u_i	1	0	1	-1	6	-13	32

Имамо да је

$$u \equiv u_j \cdot b' \equiv 32 \cdot 19 \equiv 608 \equiv 69 \pmod{77}$$

рјешење конгруенције $65u \equiv 19 \pmod{77}$. На крају, користећи формулу

$$x \equiv u + t \cdot m' \pmod{m}, \ t = 0, 1, \ldots, d-1,$$

добијамо рјешења полазне конгруенције.

$$x \equiv 69, 69 + 77, 69 + 2 \cdot 77 \equiv 69, 146, 223 \pmod{231}. \quad \triangle$$

ЛИТЕРАТУРА

[1] B. Ibrahimpašić, *Uvod u teoriju brojeva*, Pedagoški fakultet, Bihać, 2014.

[2] B. Ibrahimpašić, S. Ibrahimpašić, *Linearne kongruencije i sistemi linearnih kongruencija*, MAT–KOL, XX (1) (2014), 27–36.

[3] B. Ibrahimpašić, K. Pjanić, *Euklidov algoritam za određivanje najvećeg zajedničkog djelioca*, MAT–KOL, XX (1) (2014), 15–25.

[4] B. Ibrahimpašić, A. Zolić, *Euklidov algoritam i njegove primjene*, Nastava matematike, LVIII 1–2 (2013), 14–23.

[5] B. Pavković, B. Dakić, P. Mladinić, *Elementarna teorija brojeva*, Element, Zagreb, 1994.

Б.И: Педагошки факултет, Универзитет у Бихаћу, Луке Марјановића бб, 77000 Бихаћ, Босна и Херцеговина

E-mail: bernadin@bih.net.ba

А.З: Математички факултет, Универзитет у Београду, Студентски трг 16, 11000 Београд, Србија

E-mail: azolic@diginaut.com