Sustavi linearnih kongruencija

Karajko, Stjepan

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Studij
Sveučilišni prijediplomski studij Matematika

Sustavi linearnih kongruencija

Završni rad

Mentor:
prof. dr. sc. Ivan Matić

Student:
Stjepan Karajko

Osijek, 2024

Sadržaj

1 | Uvod

Sustavi linearnih kongruencija važan su dio teorije brojeva, grane matematike koja se bavi proučavanjem svojstava cijelih brojeva. Njemački matematičar Carl Friedrich Gauss smatra se ocem moderne teorije brojeva. Gauss je u svome djelu "Disquisitiones Arithmeticae" objavljenom 1801. godine razradio teoriju kongruencija. Uveo je koncept modula i kongruencija te simbol $\equiv$ koji olakšava proučavanje teorije djeljivosti te ima mnoge druge primjene. Jedan od najranijih i najznačajnijih rezultata vezanih uz sustave linearnih kongruencija jest Kineski teorem o ostacima. Taj teorem datira još iz 3. stoljeća, a pripisuje se kineskom matematičaru Sun Tzuu. Teorem se bavi rješavanjem sustava linearnih kongruencija s različitim modulima. Dokaz tog teorema poslužit će nam kao procedura za rješavanje sustava linearnih kongruencija.

Razvojem računalne znanosti, sustavi linearnih kongruencija pokazali su značajnu ulogu u kriptografiji, kodiranju te teoriji informacija. Principi rješavanja sustava linearnih kongruencija postali su vodeći alat za rješavanje složenih problema u mnogim područjima primjena, kao što su RSA kriptosustavi. Suvremeni matematičari i danas razvijaju i proučavaju metode za rješavanje sustava linearnih kongruencija, što puno govori o važnosti istih.

U prvom poglavlju uvest ćemo osnovne pojmove i svojstva djeljivosti i kongruencija na koja ćemo se pozivati tijekom rada. U drugom poglavlju uvest ćemo kongruencije koje sadrže nepoznatu varijablu. Najjednostavnije takve kongruencije poznate su pod nazivom linearne kongruencije. Navest ćemo temeljne rezultate koji će nam dati proceduru za njihovo rješavanje koju ćemo kasnije implementirati na sustave linearnih kongruencija. Nakon toga, u trećem poglavlju bavit ćemo se sustavima linearnih kongruencija. To su sustavi koji se sastoje od dvije ili više linearnih kongruencija s istim brojem varijabli. Najprije ćemo proučavati sustave linearnih kongruencija u jednoj varijabli x s u parovima relativno prostim modulima, a zatim ćemo preći na sustave po varijabli x s modulima koji nisu nužno relativno prosti. Konačno, u četvrtom poglavlju okrećemo se 2×2 linearnim sustavima u dvije varijable x i y s istim modulom.

2 | Djeljivost i kongruencije

Uvedimo najprije osnovne pojmove i svojstva djeljivosti i kongruencija koja ćemo koristiti tijekom čitavog rada.

2.1 Djeljivost

Definicija 1 (vidjeti [3, 1.1 Osnovni pojmovi]). *Neka su $a, b \in \mathbb{Z}$, $a \neq 0$. Kažemo da a dijeli b i pišemo $a \mid b$ ako postoji $d \in \mathbb{Z}$ takav da je $b = a \cdot d$.*

Ukoliko $a \mid b$, broj a nazivamo djeliteljem broja b, a broj b nazivamo višekratnikom broja a. Ukoliko a ne dijeli b, pišemo $a \nmid b$.

Primjer 1. *Kako je $6 = 2 \cdot 3$, prema definiciji djeljivosti $2 \mid 6$ pa je 2 djelitelj broja 6, a 6 je višekratnik broja 2.*

Primjer 2. *Broj 3 ne dijeli 8, tj. $3 \nmid 8$ jer ne postoji cijeli broj d takav da je $8 = 3 \cdot d$.*

Teorem 1 (Teorem o dijeljenju s ostatkom). (*vidjeti [3, Teorem 1.1.2]*) *Za $a \in \mathbb{N}$ i $b \in \mathbb{Z}$ postoje jedinstveni brojevi $q, r \in \mathbb{Z}$ takvi da je*

$$b = aq + r, \text{ pri čemu je } 0 \leq r < a.$$

Broj r iz prethodnog teorema nazivamo ostatak pri dijeljenju broja b brojem a, dok broj q nazivamo kvocijent cjelobrojnog dijeljenja broja b brojem a.

Napomena 1. *Iz Teorema o dijeljenju s ostatkom zaključujemo da se svaki cijeli broj b može prikazati u jednom od sljedećih oblika:*

$$aq, aq + 1, aq + 2, \ldots, aq + a - 1, \text{ za } a \in \mathbb{N} \text{ proizvoljan}.$$

Definicija 2 (vidjeti [1, Definicija 1.2.]). *Neka su $a, b, c \in \mathbb{Z}$ i $a \neq 0$. Broj a nazivamo zajedničkim djeliteljem brojeva b i c ukoliko a dijeli b i a dijeli c.*

Postoji samo konačno mnogo zajedničkih djelitelja brojeva b i c ukoliko je barem jedan od njih različit od nule. Najveći među svim zajedničkim djeliteljima nazivamo najveći zajednički djelitelj od b i c te označavamo s (b, c).

2.1.1 Euklidov algoritam

Euklidov algoritam je postupak za određivanje najvećeg zajedničkog djelitelja dva cijela broja, a bazira se na Teoremu o dijeljenju s ostatkom.
Neka je $a \in \mathbb{N}$ i $b \in \mathbb{Z}$. Pretpostavimo da smo uzastopnom primjenom Teorema o dijeljenju s ostatkom dobili sljedeći niz jednakosti:

$$\begin{aligned} b &= aq_1 + r_1, \quad 0 < r_1 < a, && (1)\\ a &= r_1q_2 + r_2, \quad 0 < r_2 < r_1, && (2)\\ r_1 &= r_2q_3 + r_3, \quad 0 < r_3 < r_2, && (3)\\ &\vdots \\ r_{n-2} &= r_{n-1}q_n + r_n, \quad 0 < r_n < r_{n-1}, && (n)\\ r_{n-1} &= r_nq_{n+1} + 0. && (n+1) \end{aligned}$$

Postupak završava kada dobijemo ostatak jednak nuli.
Kako je $a > r_1 > r_2 > r_3 > \cdots > r_{n-1} > r_n > 0$, niz ostataka je padajući i prema Teoremu o dijeljenju s ostatkom omeđen odozdo s nula pa postupak mora završiti u konačno mnogo koraka. Označimo $d = (a, b)$.
Uočimo,

$$\text{iz} \quad (n+1) \Rightarrow r_n \mid r_{n-1} \overset{(n)}{\Longrightarrow} r_n \mid r_{n-2} \Rightarrow \cdots \overset{(2)}{\Longrightarrow} r_n \mid a \overset{(1)}{\Longrightarrow} r_n \mid b.$$

Dakle, r_n je zajednički djelitelj brojeva a, b pa vrijedi $r_n \leq d$.
Nadalje,

$$\text{iz} \quad d = (a,b) \Rightarrow d \mid a \text{ i } d \mid b \overset{(1)}{\Longrightarrow} d \mid r_1 \overset{(2)}{\Longrightarrow} d \mid r_2 \Rightarrow \cdots \overset{(n)}{\Longrightarrow} d \mid r_n.$$

Kako je $r_n \in \mathbb{N}$, slijedi $d \leq r_n$.
Stoga, iz $r_n \leq d$ i $r_n \geq d$ zaključujemo da je $r_n = d$. Odnosno, najveći zajednički djelitelj brojeva a i b jednak je poslijednjem ostatku različitom od nule u Euklidovom algoritmu.
Uočimo još da je $r_1 = b - aq_1$ linearna kombinacija brojeva a i b pa je i r_2 i svaki $r_i, i \in \{1, 2, \ldots, n\}$ linearna kombinacija brojeva a i b. Stoga postoje $x, y \in \mathbb{Z}$ takvi da je

$$ax + by = (a, b)$$

i tu jednakost nazivamo Bezoutov identitet.

Primjer 3. *Odredimo* $(592, 162)$ *korištenjem Euklidovog algoritma.*
Rješenje.

$$\begin{aligned} 592 &= 162 \cdot 3 + 106\\ 162 &= 106 \cdot 1 + 56\\ 106 &= 56 \cdot 1 + 50\\ 56 &= 50 \cdot 1 + 6\\ 50 &= 6 \cdot 8 + \boxed{2}\\ 6 &= 2 \cdot 3 \end{aligned}$$

Dakle, broj 2 *je najveći zajednički djelitelj brojeva* 592 *i* 162.

Napomena 2. *Rješenja jednadžbe* $ax + by = (a, b)$ *možemo dobiti na sljedeći način: Ako je*

$$r_{-1} = a, \quad r_0 = b; \quad r_i = r_{i-2} - q_i r_{i-1};$$
$$x_{-1} = 1, \quad x_0 = 0; \quad x_i = x_{i-2} - q_i x_{i-1};$$
$$y_{-1} = 0, \quad y_0 = 1; \quad y_i = y_{i-2} - q_i y_{i-1};$$

pri čemu su r_i, q_i *iz Euklidova algoritma,* $i = 1, \ldots, n$*, onda je*

$$ax_n + by_n = (a, b).$$

Definicija 3 (vidjeti [1, Definicija 1.3.])**.** *Neka su* $a, b \in \mathbb{Z}$*. Kažemo da su* a *i* b *relativno prosti brojevi ako je* $(a, b) = 1$*.*

Primjer 4. $(5, 7) = 1, \quad (21, 10) = 1.$

Definicija 4 (vidjeti [1, Definicija 1.3.])**.** *Neka su* $a_1, a_2, \ldots, a_n \in \mathbb{Z}$*. Kažemo da su* $a_1, a_2, \ldots, a_n$ *u parovima relativno prosti ako vrijedi*

$$(a_i, a_j) = 1, \text{ za sve } i, j \text{ takve da } 1 \leq i, j \leq n, \ i \neq j.$$

Primjer 5. *Brojevi* $7, 11$ *i* 15 *su u parovima relativno prosti jer* $(7, 11) = 1$*,* $(7, 15) = 1$ *i* $(11, 15) = 1$*.*

2.2 Kongruencije

Relacija kongruencije jedna je od najznačajnijih relacija u teoriji brojeva. Uveo ju je i razvio njemački matematičar Carl Friedrich Gauss, jedan od najvećih matematičara svih vremena. Teoriju kongruencija predstavio je u svom djelu Disquisitiones Arithmeticae objavljenom 1801. godine.

Definicija 5 (vidjeti [3, 2.1 Definicija i osnovna svojstva])**.** *Neka je* $n \in \mathbb{N}$ *te neka su* $a, b \in \mathbb{Z}$*. Kažemo da je* a *kongruentan* b *modulo* n *te pišemo* $a \equiv b \pmod{n}$ *ukoliko* $n \mid a - b$*. Ukoliko* a *nije kongruentan* b *modulo* n*, pišemo* $a \not\equiv b \pmod{n}$*.*

Primjer 6.

$$46 \equiv 2 \pmod{4}, \text{ jer } 4 \mid 46 - 2, \qquad 26 \not\equiv 3 \pmod{4}, \text{ jer } 4 \nmid 26 - 3.$$

Teorem 2 (vidjeti [2, Theorem 4.1.])**.** *Neka je* $n \in \mathbb{N}$ *te neka su* $a, b \in \mathbb{Z}$*. Tada vrijedi*

$$a \equiv b \pmod{n} \text{ ako i samo ako je } a = b + kn \text{ za neki } k \in \mathbb{Z}.$$

Primjer 7.

$$78 \equiv 6 \pmod{9} + 4 \cdot 9 \Leftrightarrow 78 \equiv 6 \pmod{9}.$$

Teorem 3 (vidjeti [2, Theorem 4.2.]). *Neka je $n \in \mathbb{N}$ te neka su $a, b, c \in \mathbb{Z}$. Tada vrijedi:*

Refleksivnost $a \equiv a \pmod{n}$.

Simetričnost *Ako je* $a \equiv b \pmod{n}$, *onda je* $b \equiv a \pmod{n}$.

Tranzitivnost *Ako je* $a \equiv b \pmod{n}$ *i* $b \equiv c \pmod{n}$, *onda je* $a \equiv c \pmod{n}$.

Primjer 8.

$$4 \equiv 4 \pmod{3}.$$
$$7 \equiv 5 \pmod{2} \quad i \quad 5 \equiv 7 \pmod{2}.$$
$$15 \equiv -6 \pmod{7} \quad i \quad -6 \equiv 8 \pmod{7} \Rightarrow 15 \equiv 8 \pmod{7}.$$

Teorem 4 (vidjeti [2, Theorem 4.3.]). *Neka je $n \in \mathbb{N}$ te neka su $a, b \in \mathbb{Z}$. Tada vrijedi*

$a \equiv b \pmod{n}$ *ako i samo ako a i b daju isti ostatak pri dijeljenju s n.*

Primjer 9. *Vrijedi* $37 \equiv 17 \pmod{5}$, *jer pri dijeljenju s 5 oba broja daju ostatak 2.*

Korolar 1. [*vidjeti* [2, *Corollary 4.2*]] *Neka je $n \in \mathbb{N}$ te neka je $a \in \mathbb{Z}$. Cijeli broj r je ostatak pri dijeljenju broja a brojem n ako i samo ako je $a \equiv r \pmod{n}$, za $0 \leq r < n$. Broj r nazivamo najmanjim ostatkom modulo n.*

Primjer 10. *Kako je* $32 = 6 \cdot 5 + 2$, *najmanji ostatak od* 32 *modulo* 6 *je* 2 *pa vrijedi*

$$32 \equiv 2 \pmod{6}.$$

Korolar 2. *Svaki cijeli broj kongruentan je točno jednom od najmanjih ostataka $0, 1, 2, \ldots, n-1$ modulo n.*

Lema 1 (vidjeti [3, Lema 2.1.2.]). *Relacija ekvivalencije dijeli skup $\mathbb{Z}$ na disjunktne klase ekvivalencije.*

Za $a \in \mathbb{Z}$ i $n \in \mathbb{N}$ definirajmo klasu ekvivalencije $[a] = \{b \in \mathbb{Z} : b \equiv a \pmod{n}\}$.

$$[0] = \{b \in \mathbb{Z} : \underbrace{b \equiv 0 \pmod{n}}_{n|b-0 \Rightarrow \exists k \in \mathbb{Z} \quad b=kn} \} = \{kn : k \in \mathbb{Z}\} = [n] = n\mathbb{Z},$$
$$[1] = \{b \in \mathbb{Z} : \underbrace{b \equiv 1 \pmod{n}}_{n|b-1 \Rightarrow\ b-1=kn \Rightarrow b=kn+1} \} = \{kn+1 : k \in \mathbb{Z}\} = [n+1] = n\mathbb{Z}+1,$$
$$[2] = \{b \in \mathbb{Z} : b \equiv 2 \pmod{n} = \{kn+2 : k \in \mathbb{Z}\} = [n+2] = n\mathbb{Z}+2,$$
$$\vdots$$
$$[n-1] = \{b \in \mathbb{Z} : b \equiv n-1 \pmod{n} = \{kn+n-1 : k \in \mathbb{Z}\} = n\mathbb{Z}+n-1 = n\mathbb{Z}-1,$$
$$[n] = \{b \in \mathbb{Z} : b \equiv n \pmod{n} = \{kn+n : k \in \mathbb{Z}\} = n\mathbb{Z}+n = n\mathbb{Z} = [0].$$

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1].$$

Dakle, imamo n klasa ekvivalencije koje su određene s $0, 1, \ldots, n-1$ što su mogući ostaci pri dijeljenju cijelog broja s n. Općenito ne moramo odabrati najmanje ostatke za predstavnike klasa ekvivalencije. Prema Teoremu 4, dva cijela broja pripadaju istoj klasi ako i samo ako daju isti ostatak pri dijeljenju s n. Stoga bilo koji element klase može poslužiti kao odgovarajući predstavnik klase.

Primjer 11.

$$\begin{aligned}
&\cdots \equiv -9 \equiv -6 \equiv -3 \equiv 0 \equiv 3 \equiv 6 \equiv 9 \equiv \cdots \equiv 3k \pmod 3\\
&\cdots \equiv -8 \equiv -5 \equiv -2 \equiv 1 \equiv 4 \equiv 7 \equiv 10 \equiv \cdots \equiv 3k+1 \pmod 3\\
&\cdots \equiv -7 \equiv -4 \equiv -1 \equiv 2 \equiv 5 \equiv 8 \equiv 11 \equiv \cdots \equiv 3k+2 \pmod 3
\end{aligned}$$

Uočimo da su npr. $-6, 9, 0$ *predstavnici iste klase modulo* 3*, dok su npr.* $-5, 11$ *predstavnici različitih klasa modulo* 3*.*

Definicija 6 (vidjeti [3, 2.1.1 Potpuni i reducirani sustavi ostataka])**.** *Neka je* $n \in \mathbb{N}$*. Za skup* $S = \{a_1, a_2, \ldots, a_n\}$ *kažemo da je potpun sustav ostataka modulo* n *ako za svaki* $b \in \mathbb{Z}$ *postoji jedinstveni* $a_i \in S$ *takav da je* $b \equiv a_i \pmod n$*.*

Uočimo da skup S mora sadržavati sve moguće predstavnike klasa ekvivalencije modulo n i zbog toga što S ima n elemenata, a postoji i n klasa ekvivalencije, predstavnik klase je jedinstven.

Primjer 12. *Odredimo nekoliko potpunih sustav ostataka modulo* 3*.*
Rješenje.

$$S_1 = \{0, 1, 2\}, \quad S_2 = \{-9, 4, 8\}, \quad S_3 = \{3, -2, 2\}.$$

Potpunih sustava ostataka modulo n postoji beskonačno mnogo.

Napomena 3. *Neka su* $a, b \in \mathbb{Z}$ *te neka su* $c, n \in \mathbb{N}$*. Vrijedi sljedeće:*

1) n *dijeli* a *ako i samo ako je* $a \equiv 0 \pmod n$*.*

2) $a \equiv b \pmod n$ *ako i samo ako je* $ac \equiv bc \pmod{cn}$*.*

3) Ako je $a \equiv b \pmod{cn}$*, onda je* $a \equiv b \pmod n$*.*

Primjer 13. *Obrat tvrdnje 3) iz Napomene 3 općenito ne vrijedi.*

$$8 \equiv 3 \pmod 5, \quad \textit{ali} \quad 8 \not\equiv 3 \pmod{10}.$$

Propozicija 1 (vidjeti [3, Propozicija 2.1.3.])**.** *Neka je* $n \in \mathbb{N}$ *te neka su* $a, a', b, b', c \in \mathbb{Z}$*.*
1) Ako je $a \equiv a' \pmod n$ *i* $b \equiv b' \pmod n$*, onda vrijedi:*

$$a + b \equiv a' + b' \pmod n, \quad a - b \equiv a' - b' \pmod n, \quad a \cdot b \equiv a' \cdot b' \pmod n.$$

2) Neka je $(a, n) = 1$*. Ako je* $ab \equiv ac \pmod n$*, onda je i* $b \equiv c \pmod n$*.*

Napomena 4. *Primijetimo da je uvjet* $(a,n)=1$ *iz tvrdnje 2) Propozicije 1 nužan.*

Primjer 14.

$$28 \equiv 21 \pmod 7, \quad \textit{ali} \quad 4 \not\equiv 3 \pmod 7 \quad \textit{zbog} \quad (28,21)=7\neq 1.$$

Propozicija 2 (vidjeti [2, Theorem 4.5])**.** *Neka je* $n\in\mathbb{N}$ *te neka su* $a,b\in\mathbb{Z}$*. Ako je* $a\equiv b \pmod n$*, tada je* $a^m\equiv b^m \pmod n$*, za svaki* $m\in\mathbb{N}$*.*

Primjer 15.

$$5\equiv 3 \pmod 2 \Rightarrow 5^4\equiv 3^4 \pmod 2 \quad \textit{odnosno,} \quad 625\equiv 81 \pmod 2.$$

Teorem 5 (vidjeti [1, Teorem 2.4.])**.** *Neka je* $n\in\mathbb{N}$ *te neka su* $a,b,c\in\mathbb{Z}, a\neq 0$*. Tada vrijedi*

$$ab\equiv ac \pmod n \textit{ ako i samo ako } b\equiv c \left(\bmod \frac{n}{(a,n)}\right).$$

3 | Linearne kongruencije

Nakon što smo uveli pojam kongruencija i njihova osnovna svojstva, uvedimo kongruencije koje sadrže nepoznatu varijablu. Najjednostavnije takve kongruencije su linearne kongruencije.

Definicija 7 (vidjeti [2, 4.2 Linear Congruences]). *Neka je $n \in \mathbb{N}$ te neka su $a, b \in \mathbb{Z}, a \neq 0$. Kongruencijsku jednadžbu oblika*

$$ax \equiv b \pmod{n}$$

nazivamo linearna kongruencija.

Kao kod svih jednadžbi, prirodno nam se javljaju pitanja o postojanju, jedinstvenosti te pronalasku rješenja. Pod rješenjem linearne kongruencije podrazumijevamo cijeli broj x_0 takav da je $ax_0 \equiv b \pmod{n}$.
Pretpostavimo da je x_0 rješenje linearne kongruencije $ax \equiv b \pmod{n}$, tj.

$$ax_0 \equiv b \pmod{n}.$$

Dodatno, pretpostavimo da je

$$x_1 \equiv x_0 \pmod{n}.$$

Primjenom Teorema 5 na prethodnu kongruenciju, slijedi da je

$$ax_1 \equiv ax_0 \pmod{n}.$$

Nadalje, primjenom svojstva tranzitivnosti dobivamo da je

$$ax_1 \equiv b \pmod{n}$$

iz čega zaključujemo da je x_1 također rješenje linearne kongruencije.
Uočimo, x_0 i x_1 pripadaju istoj klasi ekvivalencije pa ako je x_0 rješenje dane kongruencije, onda su i svi članovi njegove klase također rješenja.

Primjer 16. *Kako je $4 \cdot 2 \equiv 5 \pmod{3}$, 2 je rješenje linearne kongruencije $4x \equiv 5 \pmod{3}$. Budući da je 2 rješenje linearne kongruencije $4x \equiv 5 \pmod{3}$, svaki član klase $[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}$ je također rješenje. Odnosno, sva rješenja dana su formulom $x = 2 + 3k$, pri čemu je k neki cijeli broj.*

$$\begin{aligned} 4 \cdot (2 + 3k) = 8 + 12k &\equiv 2 + 0 \pmod{3} \\ &\equiv 2 \pmod{3}. \end{aligned}$$

Primjer 17. *Linearna kongruencija* $6x \equiv 1 \pmod 3$ *nema rješenja jer* $3 \nmid 6x - 1$ *za bilo koji cijeli broj* x.

Dakle, ukoliko je linearna kongruencija $ax \equiv b \pmod n$ rješiva, ona ima beskonačno mnogo rješenja. Međutim, zanimaju nas samo međusobno nekongruentna rješenja modulo n.

Korolar 3 (vidjeti [2, Corollary 4.6]). *Linearna kongruencija* $ax \equiv b \pmod n$ *ima jedinstveno rješenje* [1] *modulo* n *ako i samo ako je* $(a, n) = 1$.

Dokaz. Egzistencija:
Budući da je $(a, n) = 1$, prema Bezoutovom identitetu postoje $u, v \in \mathbb{Z}$ takvi da vrijedi

$$au + nv = 1.$$

Djelovanjem s modulo n na prethodnu jednakost dobivamo

$$au \equiv 1 \pmod n. \tag{3.1}$$

Množenjem lijeve i desne strane linearne kongruencije $ax \equiv b \pmod n$ s ovako dobivenim u dobivamo

$$aux \equiv bu \pmod n.$$

Odnosno, zbog (3.1) slijedi

$$x \equiv bu \pmod n.$$

Jedinstvenost: Neka su x_0 i x_0' rješenja linearne kongruencije $ax \equiv b \pmod n$, tj.

$$ax_0 \equiv b \pmod n,$$
$$ax_0' \equiv b \pmod n.$$

Tada, primjenom svojstava simetričnosti i tranzitivnosti relacije "biti kongruentan modulo n" dobivamo

$$ax_0 \equiv ax_0' \pmod n.$$

Nadalje, prema Teoremu 5 slijedi

$$x_0 \equiv x_0' \pmod n.$$

Zaključujemo da x_0 i x_0' pripadaju istoj klasi modulo n pa je rješenje polazne linearne kongruencije jedinstveno modulo n. □

Napomena 5. *Dokaz prethodnog korolara je konstruktivan, tj. u njemu je ujedno dan postupak za rješavanje linearne kongruencije*

$$ax_0 \equiv b \pmod n, \text{ pri čemu je } (a, n) = 1.$$

[1] jedinstveno rješenje modulo n odnosi se na to da sva rješenja pripadaju istoj klasi modulo n.

Primjer 18. *Riješimo linearnu kongruenciju*

$$7x \equiv 6 \pmod{11}. \tag{3.3}$$

Rješenje.
Kako su koeficijent uz x i argument modula relativno prosti, tj. $(7,11) = 1$, prema prethodnom korolaru postoji jedinstveno rješenje modulo 11 linearne kongruencije (3.3). Prateći postupak za rješavanje linearnih kongruencija, najprije trebamo odrediti u. Budući da je $(7,11) = 1$, prema Bezoutovom identitetu postoje $u, v \in \mathbb{Z}$ takvi da

$$7u + 11v = 1.$$

Djelovanjem s modulo 11 na prethodnu jednakost dobivamo

$$7u \equiv 1 \pmod{11}.$$

Zatim, primjenom Euklidovog algoritma dobivamo

$$\begin{aligned} 11 &= 7 \cdot 1 + 4 \\ 7 &= 4 \cdot 1 + 3 \\ 4 &= 3 \cdot 1 + 1 \\ 3 &= 1 \cdot 3 \end{aligned}$$

pa u možemo odrediti primjenom rekurzivnih relacija prema Napomeni 2:

i	-1	0	1	2	3
q_i			1	1	1
u_i	0	1	-1	2	$\boxed{-3}$

Dakle,

$$u \equiv -3 \pmod{11} \equiv 8 \pmod{11}.$$

Množenjem lijeve i desne strane kongruencije (3.3) s $u = 8$ dobivamo

$$\begin{aligned} 7 \cdot 8x &\equiv 6 \cdot 8 \pmod{11} \\ 56x &\equiv 48 \pmod{11} \\ x &\equiv 4 \pmod{11} \\ x &= 4. \end{aligned}$$

Provjera:

$$7 \cdot 4 \equiv 6 \pmod{11} \Rightarrow 11 \mid 28 - 6 = 22.$$

Sljedeći teorem daje nam nužan i dovoljan uvjet da bi linearna kongruencija bila rješiva. Također, daje nam informaciju o broju međusobno nekongruentnih rješenja modulo n.

Teorem 6 (vidjeti [2, Theorem 4.9])**.** *Linearna kongruencija $ax \equiv b \pmod{n}$ je rješiva ako i samo ako $d \mid b$, pri čemu je $d = (a,n)$. Ako $d \mid b$, tada postoji d međusobno nekongruentnih rješenja modulo n.*

Teorem 7 (vidjeti [3, Teorem 2.1.9.]). *Neka su $a, n \in \mathbb{N}, b \in \mathbb{Z}$ te neka je $d = (a, n)$. Ako je x_0 rješenje kongruencije $\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$, onda su sva međusobno nekongruentna rješenja modulo n kongruencije $ax \equiv b \pmod{n}$ dana s:*

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

Napomena 6. *Dokaz prethodnog teorema je konstruktivan. Postupak za rješavanje linearne kongruencije*

$$ax \equiv b \pmod{n}, \text{ pri čemu je } d = (a, n)$$

je sljedeći:

1. *Prema Napomeni 5 pronađemo rješenje x_0 kongruencije*

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\bmod \frac{n}{d} \right).$$

2. *Sva rješenja modulo n polazne kongruencije dana su s*

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

Primjer 19. *Riješimo linearnu kongruenciju*

$$6x \equiv 9 \pmod{21}.$$

Rješenje.
Budući da je $(6, 21) = 3$ i $3 \mid 9$, prema prethodnom teoremu postoje tri klase rješenja modulo 21. Dijeljenjem polazne kongruencije s 3 dobivamo

$$2x \equiv 3 \pmod{7}. \tag{3.4}$$

Kako je sada $(2, 7) = 1$, prema Bezoutovom identitetu postoje $u, v \in \mathbb{Z}$ takvi da je

$$2u + 7v = 1.$$

Djelovanjem s modulo 7 na prethodnu jednakost dobivamo

$$2u \equiv 1 \pmod{7}.$$

Odavde lako uočavamo da je $u \equiv 4 \pmod{7}$. Ukoliko to ne uočimo odmah, u odredimo primjenom Euklidovog algoritma i rekurzivnih relacija kao u prethodnom primjeru. Nadalje, množenjem lijeve i desne strane kongruencije (3.4) s $u = 4$ dobivamo

$$8x \equiv 12 \pmod{7}.$$

Slijedi

$$x \equiv 5 \pmod{7}.$$

Pomoću ovoga rješenja možemo generirati sva rješenja linearne kongruencije (3.4) pa je rješenje početne kongruencije dano s

$$x \equiv 5, 5+7, 5+14 \equiv 5, 12, 19 \pmod{21}.$$

Primjer 20. *Odredimo jesu li kongruencije*

$$6x \equiv 8 \pmod 4, \quad 9x \equiv 2 \pmod 6 \quad i \quad 5x \equiv 6 \pmod 3$$

rješive te, ukoliko jesu, odredimo broj međusobno nekongruentnih rješenja.
Rješenje.

$(6,4) = 2$ *i* $2 \mid 8$ *pa kongruencija* $6x \equiv 8 \pmod 4$ *ima dva međusobno nekongruentna rješenja modulo* 4.

$(9,6) = 3$, *ali* $3 \nmid 2$ *pa kongruencija* $9x \equiv 2 \pmod 6$ *nema rješenja.*

$(5,3) = 1$ *pa prema Korolaru 3 kongruencija* $5x \equiv 6 \pmod 3$ *ima jedinstveno rješenje modulo* 3.

4 | Sustavi linearnih kongruencija

Sustav linearnih kongruencija sastoji se od dvije ili više linearnih kongruencija s istim brojem varijabli. Takvi sustavi u jednoj varijabli bili su poznati još u doba stare Kine, Indije i Grčke, a primarno su ih koristili astronomi za izradu kalendara. Jedan od najpoznatijih primjera korištenja sustava linearnih kongruencija je Sun-Tsuova zagonetka. Postavio ju je kineski matematičar Sun-Tsu, a spominje se u Matematičkom priručniku Učitelja Suna napisanom između 287. i 473. godine. Zagonetka glasi:

"Pronađite broj koji daje ostatak 1 *kada se podijeli s* 3*, ostatak* 2 *kada se podijeli s 5 i ostatak* 3 *kada se podijeli sa* 7*."*

Zapisano jezikom kongruencija, zagonetka je pronaći cijeli broj x koji zadovoljava sljedeće:

$$x \equiv 1 \pmod 3, \qquad x \equiv 2 \pmod 5, \qquad x \equiv 3 \pmod 7.$$

4.1 Metoda iteracija

Sustave linearnih kongruencija u jednoj varijabli koje susrećemo u kineskim problemima ostataka, kao što je npr. Sun-Tsuova zagonetka, često možemo izravno riješiti metodom iteracije. Metoda iteracija jednostavna je metoda kod koje uzastopno koristimo zamjenu za x dok ne dođemo do posljednje kongruencije. Spomenutu metodu demonstrirat ćemo na primjeru Sun-Tsuove zagonetke.

Primjer 21. *Riješimo Sun-Tsuovu zagonetku metodom iteracije.*
Rješenje.

$$x \equiv 1 \pmod 3, \qquad x \equiv 2 \pmod 5, \qquad x \equiv 3 \pmod 7.$$

Kako je $x \equiv 1 \pmod 3$*, prema Teoremu 4, x možemo zapisati u obliku*

$$x = 1 + 3k_1, \text{ pri čemu je } k_1 \text{ neki cijeli broj.}$$

Nadalje, zamjenom za x u kongruenciji $x \equiv 2 \pmod 5$ *dobivamo*

$$\begin{aligned} 1 + 3k_1 &\equiv 2 \pmod 5 \\ 3k_1 &\equiv 1 \pmod 5. \end{aligned}$$

Odavde se lako vidi da je

$$k_1 \equiv 2 \pmod 5,$$

odnosno, $k_1 = 2 + 5k_2$*, gdje je* k_2 *neki cijeli broj.*
Stoga,

$$\begin{aligned} x &= 1 + 3k_1 \\ &= 1 + 3(2 + 5k_2) \\ &= 7 + 15k_2. \end{aligned}$$

Sada zamjenom ove vrijednosti za x *u kongruenciji* $x \equiv 3 \pmod 7$ *dobivamo*

$$\begin{aligned} 7 + 15k_2 &\equiv 3 \pmod 7 \\ 15k_2 &\equiv 3 \pmod 7 \\ k_2 &\equiv 3 \pmod 7. \end{aligned}$$

Dakle, $k_2 = 3 + 7k$*, pri čemu je* k *neki cijeli broj.*
Stoga,

$$\begin{aligned} x &= 7 + 15k_2 \\ &= 7 + 15(3 + 7k) \\ &= 52 + 105k. \end{aligned}$$

Zaključujemo da je rješenje linearnog sustava svaki cijeli broj oblika $x = 52 + 105k$*, a to je ujedno opće rješenje početnog sustava. (Napomena:* $105 = 3 \cdot 5 \cdot 7$*.)*

4.2 Kineski teorem o ostacima

Kineski teorem o ostacima važan je rezultat u teoriji brojeva koji omogućava rješavanje sustava linearnih kongruencija s u parovima relativno prostim modulima.

Teorem 8 (Kineski teorem o ostacima)**.** *(vidjeti [1, Teorem 2.2]) Neka su* $m_1, \ldots, m_r$ *u parovima relativno prosti prirodni brojevi te neka su* $a_1, \ldots, a_r$ *cijeli brojevi. Tada sustav kongruencija*

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots \quad , x \equiv a_r \pmod{m_r} \tag{4.2}$$

ima jedinstveno rješenje modulo $m = m_1 m_2 \cdots m_r$*.*

Dokaz. Dokaz ćemo provesti u dva dijela. Najprije ćemo pokazati da rješenje postoji, a potom da je ono jedinstveno modulo $m_1 m_2 \cdots m_r$.
Egzistencija: Neka je $m = m_1 m_2 \cdots m_r$. Definirajmo

$$n_j = \frac{m}{m_j}, \quad j = 1, 2, \ldots, r.$$

Uočimo da je n_j zapravo jednak produktu brojeva $m_1, \ldots, m_{j-1}, m_{j+1}, \ldots, m_r$. Odnosno,

$$n_j = m_1 \cdots m_{j-1} m_{j+1} \cdots m_r.$$

Budući da su brojevi $m_1, \ldots, m_r$, prema pretpostavci teorema, u parovima relativno prosti tj. $(m_i, m_j) = 1$, za $i \neq j$, slijedi da je i $(n_j, m_j) = 1$ za $j = 1, 2, \ldots, r$. Stoga, prema Korolaru 3 postoje x_j sa svojstvom

$$n_j x_j \equiv a_j \pmod{m_j}, \quad j = 1, 2, \ldots, r$$

(jer kongruencije $n_j x \equiv a_j \pmod{m_j}, j = 1, 2, \ldots, r$ uvijek imaju rješenje).
Promotrimo sada broj $x_0 = n_1 x_1 + n_2 x_2 + \cdots + n_r x_r$. Budući da $m_j \mid n_i$, za $i \neq j$, vrijedi:

$$\begin{aligned} x_0 &\equiv n_1 x_1 + n_2 x_2 + \cdots + n_r x_r \pmod{m_j} \\ &\equiv 0 \cdot x_1 + \cdots + n_j x_j + \cdots + 0 \cdot x_r \pmod{m_j} \\ &\equiv a_j \pmod{m_j} \end{aligned}$$

pa je ovakav x_0 rješenje polaznog sustava.
Jedinstvenost: Pretpostavimo da su x_0 i x_0' rješenja sustava (4.2). Tada za svaki $j = 1, 2, \ldots, r$ imamo

$$\begin{aligned} x_0 &\equiv a_j \pmod{m_j}, \\ x_0' &\equiv a_j \pmod{m_j} \end{aligned}$$

pa je $x_0 \equiv x_0' \pmod{m_j}, j = 1, 2, \ldots, r$. Kako su $m_1, m_2, \ldots, m_r$ u parovima relativno prosti slijedi da je $x_0 \equiv x_0' \pmod{m}$. □

Napomena 7. *Dokaz prethodnog teorema je konstruktivan.*

Postupak za rješavanje sustava linearnih kongruencija

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \quad \ldots \quad , x \equiv a_r \pmod{m_r};$$

$$a_1, \ldots, a_r \in \mathbb{Z}, (m_i, m_j) = 1, i \neq j, i, j \in 1, 2, \ldots, r$$

je sljedeći:

1. Definiramo brojeve $m = m_1 m_2 \cdots m_r, n_j = \frac{m}{m_j}, j = 1, 2, \ldots, r$.
2. Riješimo kongruencije $n_j x_j \equiv a_j \pmod{m_j}, j = 1, 2, \ldots, r$.
3. Sva rješenja početne kongruencije su $x \equiv n_1 x_1 + n_2 x_2 + \cdots + n_r x_r \pmod{m}$.

Primjer 22. *Riješimo sustav linearnih kongruencija:*

$$x \equiv 4 \pmod 5, \qquad x \equiv 7 \pmod 8, \qquad x \equiv 6 \pmod{11}.$$

Rješenje.
Provjerimo najprije jesu li argumenti modula u parovima relativno prosti brojevi. Budući da su $m_1 = 5, m_2 = 8$ *i* $m_3 = 11$ *u parovima relativno prosti, prema Kineskom teoremu o ostacima možemo zaključiti da postoji jedinstveno rješenje linearnog sustava. Kako bismo ga pronašli, odredimo najprije* m *kao umnožak argumenata modula, tj.* $m = 5 \cdot 8 \cdot 11 = 440$ *i* n_1, n_2, n_3 *na idući način:*

$$n_1 = \frac{m}{5} = 88, \qquad n_2 = \frac{m}{8} = 55, \qquad n_3 = \frac{m}{11} = 40.$$

Sada tražimo rješenja linearnih kongruencija:

$$88x_1 \equiv 4 \pmod 5, \qquad 55x_2 \equiv 7 \pmod 8, \qquad 40x_3 \equiv 6 \pmod{11}.$$

Odnosno,

$$\begin{array}{lll} 3x_1 \equiv 4 \pmod 5 & 7x_2 \equiv 7 \pmod 8 & 7x_3 \equiv 6 \pmod{11} \\ & & \Updownarrow \text{ Primjer 18.} \\ x_1 \equiv 3 \pmod 5, & x_2 \equiv 1 \pmod 8, & x_3 \equiv 4 \pmod{11}. \end{array}$$

Stoga je rješenje polaznog sustava dano s

$$x \equiv 88x_1 + 55x_2 + 40x_3 \equiv 88 \cdot 3 + 55 \cdot 1 + 40 \cdot 4 \equiv 479 \pmod{440} \equiv 39 \pmod{440}.$$

Provjera:

$$\begin{array}{lll} 39 \equiv 4 \pmod 5; & 39 \equiv 7 \pmod 8; & 39 \equiv 6 \pmod{11}. \\ \Updownarrow & \Updownarrow & \Updownarrow \\ 5 \mid 39 - 4 = 35 & 8 \mid 39 - 7 = 32 & 11 \mid 39 - 6 = 33 \end{array}$$

Primjer 23. *Riješimo sustav linearnih kongruencija:*

$$x \equiv 3 \pmod 5, \qquad x \equiv 5 \pmod 6, \qquad x \equiv 2 \pmod 9.$$

Rješenje.
Budući da argumenti modula $5, 6$ *i* 9 *nisu u parovima relativno prosti, ne možemo direktno primijeniti Kineski teorem o ostacima pa je ideja generirati sustav na koji ćemo moći primijeniti Kineski teorem o ostacima. Uočimo sljedeće:*

$$\begin{aligned} x \equiv 3 \pmod 5, \qquad & x \equiv 5 \pmod 6, \qquad x \equiv 2 \pmod 9 \\ & \Updownarrow \text{ jer je } 6 = 2 \cdot 3 \text{ i } (2,3) = 1 \\ & x \equiv 5 \pmod 2 \\ & \quad i \\ & x \equiv 5 \pmod 3 \end{aligned}$$

odnosno, argument modula kongruencije $x \equiv 5 \pmod 6$ *prikazali smo u obliku produkta potencija prostih brojeva pa je početni sustav ekvivalentan sustavu:*

$$x \equiv 3 \pmod 5, \quad x \equiv 1 \pmod 2, \quad x \equiv 2 \pmod 3, \quad x \equiv 2 \pmod 9.$$

Kako argumenti modula 3 *i* 9 *nisu relativno prosti, još uvijek ne možemo primijeniti Kineski teorem o ostacima pa ćemo najprije riješiti podsustav:*

$$x \equiv 2 \pmod 3, \qquad x \equiv 2 \pmod 9.$$

Uočimo da iz kongruencije $x \equiv 2 \pmod 9$, *prema svojstvu 3) Napomene 3, slijedi* $x \equiv 2 \pmod 3$, *pri čemu obrat ne vrijedi pa će rješenje ovoga sustava biti*

$$x \equiv 2 \pmod 9.$$

Prema tome, zaključujemo da je početni sustav kongruencija ekvivalentan sustavu

$$x \equiv 3 \pmod 5, \qquad x \equiv 1 \pmod 2, \qquad x \equiv 2 \pmod 9.$$

Na ovaj sustav sada možemo primijeniti Kineski teorem o ostacima budući da su brojevi $5, 2$ *i* 9 *u parovima relativno prosti. Slijedimo postupak za rješavanje sustava linearnih kongruencija.*
Imamo sljedeće: $m = 5 \cdot 2 \cdot 9 = 90$,

$$n_1 = \frac{m}{5} = 18, \qquad n_2 = \frac{m}{2} = 45, \qquad n_3 = \frac{m}{9} = 10.$$

Tražimo rješenja linearnih kongruencija:

$$18x_1 \equiv 3 \pmod 5, \qquad 45x_2 \equiv 1 \pmod 2, \qquad 10x_3 \equiv 2 \pmod 9$$

tj.

$$\begin{aligned} 3x_1 \equiv 3 \pmod 5 \qquad & x_2 \equiv 1 \pmod 2, \qquad x_3 \equiv 2 \pmod 9. \\ x_1 \equiv 1 \pmod 5, & \end{aligned}$$

Stoga je rješenje polaznog sustava dano s

$$x \equiv 18x_1 + 45x_2 + 10x_3 \equiv 18 \cdot 1 + 45 \cdot 1 + 10 \cdot 2 \equiv 83 \pmod{90}.$$

Primjer 24. *Riješimo sustav linearnih kongruencija:*

$$x \equiv 10 \pmod{15}, \qquad x \equiv 19 \pmod{21}, \qquad x \equiv 25 \pmod{60}.$$

Rješenje.
Kako argumenti modula nisu u parovima relativno prosti brojevi, generirajmo najprije sustav na koji možemo primijeniti Kineski teorem o ostacima.

$$\begin{array}{lll}
x \equiv 10 \pmod{15}, & x \equiv 19 \pmod{21}, & x \equiv 25 \pmod{60}. \\
\Updownarrow (3,5) = 1 & \Updownarrow (3,7) = 1 & \Updownarrow (4,15) = 1 \\
x \equiv 10 \pmod{3} & x \equiv 19 \pmod{3} & x \equiv 25 \pmod{4} \\
\quad i & \quad i & \quad i \\
x \equiv 10 \pmod{5} & x \equiv 19 \pmod{7} & x \equiv 25 \pmod{15}
\end{array}$$

Odnosno,

$$\begin{array}{lll}
x \equiv 1 \pmod{3}, & x \equiv 1 \pmod{3}, & x \equiv 1 \pmod{4}, \\
x \equiv 0 \pmod{5}, & x \equiv 5 \pmod{7}, & x \equiv 10 \pmod{15} \\
 & & \Updownarrow (3,5) = 1 \\
 & & x \equiv 10 \pmod{3} \equiv 1 \pmod{3} \\
 & & \quad i \\
 & & x \equiv 10 \pmod{5} \equiv 0 \pmod{5}.
\end{array}$$

Početni sustav kongruencija ekvivalentan je sustavu

$$x \equiv 1 \pmod{3}, \qquad x \equiv 0 \pmod{5}, \qquad x \equiv 5 \pmod{7}, \qquad x \equiv 1 \pmod{4}.$$

Imamo sljedeće: $m = 3 \cdot 5 \cdot 7 \cdot 4 = 420$,

$$n_1 = \frac{m}{3} = 140, \qquad n_2 = \frac{m}{5} = 84, \qquad n_3 = \frac{m}{7} = 60, \qquad n_4 = \frac{m}{4} = 105.$$

Tražimo rješenja linearnih kongruencija

$$\begin{array}{llll}
140x_1 \equiv 1 \pmod{3} & 84x_2 \equiv 0 \pmod{5} & 60x_3 \equiv 5 \pmod{7} & 105x_4 \equiv 1 \pmod{4} \\
2x_1 \equiv 1 \pmod{3} & x_2 \equiv 0 \pmod{5}, & 4x_3 \equiv 5 \pmod{7} & x_4 \equiv 1 \pmod{4}. \\
x_1 \equiv 5 \pmod{3}, & & x_3 \equiv 3 \pmod{7}, &
\end{array}$$

Stoga je rješenje polaznog sustava dano s

$$x = 140 \cdot x_1 + 84 \cdot x_2 + 60 \cdot x_3 + 105 \cdot x_4 = 140 \cdot 5 + 84 \cdot 0 + 60 \cdot 3 + 105 \cdot 1$$

$$\equiv 985 \pmod{420} \equiv 145 \pmod{420}.$$

Primjer 25. *Riješimo sustav linearnih kongruencija:*

$$x \equiv 1 \pmod 3, \qquad x \equiv 3 \pmod 5, \qquad x \equiv 3 \pmod 6.$$

Rješenje.
Budući da argumenti modula $3, 5$ *i* 6 *nisu u parovima relativno prosti, generirajmo sustav na koji ćemo moći primijeniti Kineski teorem o ostacima.*
Uočimo sljedeće: Prema svojstvu 3) Napomene 3 iz

$$x \equiv 3 \pmod 6 \Rightarrow x \equiv 3 \pmod 3 \Rightarrow x \equiv 0 \pmod 3$$

pa dolazimo do kontradikcije s kongruencijom $x \equiv 1 \pmod 3$ *(jer ne postoji cijeli broj koji pri dijeljenju s* 3 *istovremeno daje ostatak* 0 *i* 1*, tj. ne postoji broj koji je istovremeno i paran i neparan). Prema tome, zaključujemo da ovaj sustav nema rješenja.*

5 | 2×2 linearni sustavi

U prethodnom poglavlju vidjeli smo kako rješavati sustave linearnih kongruencija s jednom varijablom. Okrenimo se sada rješavanju sustava linearnih kongruencija s dvije varijable po istom modulu.

Definicija 8 (vidjeti [2, 2×2 Linear Systems])**.** 2×2 *linearni sustav je sustav linearnih kongruencija oblika*

$$\begin{aligned} ax + by &\equiv e \pmod{m} \\ cx + dy &\equiv f \pmod{m}. \end{aligned}$$

Rješenje linearnog sustava je par $x \equiv x_0 \pmod{m}$, $y \equiv y_0 \pmod{m}$ *koji zadovoljava obje kongruencije.*

Primjer 26. *Pokažimo da je par* $x \equiv 10 \pmod{11}$, $y \equiv 2 \pmod{11}$ *rješenje sustava*

$$\begin{aligned} 4x + 5y &\equiv 6 \pmod{11} \\ 7x + 8y &\equiv 9 \pmod{11}. \end{aligned}$$

Rješenje.
Kako je $x \equiv 10 \pmod{11}$ *i* $y \equiv 2 \pmod{11}$*, uvrštavanjem u sustav dobivamo*

$$\begin{aligned} 4x + 5y &\equiv 4 \cdot 10 + 5 \cdot 2 \equiv 50 \equiv 6 \pmod{11} \\ 7x + 8y &\equiv 7 \cdot 10 + 8 \cdot 2 \equiv 86 \equiv 9 \pmod{11} \end{aligned}$$

Dakle, svaki par $x \equiv 10 \pmod{11}$, $y \equiv 2 \pmod{11}$ *je rješenje sustava. Odnosno, opće rješenje sustava dano je s* $x = 10 + 11k$, $y = 2 + 11k$*, gdje je* k *proizvoljan cijeli broj.*

U nastavku ćemo proučiti neke od metoda rješavanja 2×2 linearnih sustava. Jedna od njih je metoda eliminacije koju ćemo ilustrirati na sljedećem primjeru.

Metoda eliminacije je metoda kod koje eliminacijom jedne od varijabli sustav svodimo na linearnu kongruenciju koju zatim rješavamo. Nakon što pronađemo rješenje linearne kongruencije, uvrstimo ga u početni sustav kako bismo dobili drugu varijablu. Na taj način smo pronašli rješenje sustava.

Primjer 27. *Metodom eliminacije riješimo linearni sustav*

$$4x + 5y \equiv 6 \pmod{11} \tag{5.1}$$
$$7x + 8y \equiv 9 \pmod{11}. \tag{5.2}$$

Rješenje.
Kako bismo eliminirali jednu od nepoznanica, pomnožimo na primjer kongruenciju (5.1) sa 7 i kongruenciju (5.2) s -4. Dakle,

$$28x + 35y \equiv 42 \pmod{11}$$
$$-28x - 32y \equiv -36 \pmod{11}.$$

Zbrajanjem dobivamo

$$3y \equiv 6 \pmod{11}.$$

Dijeljenjem s 3 dobivamo

$$y \equiv 2 \pmod{11} \Rightarrow y = 2.$$

Zatim, da bismo dobili nepoznanicu x, uvrstimo $y = 2$ u npr. jednadžbu (5.1).

$$4x + 10 \equiv 6 \pmod{11}$$
$$4x \equiv -4 \pmod{11}$$
$$x \equiv -1 \equiv 10 \pmod{11}.$$

Dakle, rješenje polaznog sustava dano je s $x \equiv 10 \pmod{11}, y \equiv 2 \pmod{11}$.
(Primijetimo da se dobiveno rješenje podudara s onim iz Primjera 26.)

Idući teorem daje nam nužan i dovoljan uvjet kada će 2×2 linearni sustav imati jedinstveno rješenje po modulu.

Teorem 9 (vidjeti [2, Theorem 6.4])**.** *2×2 linearni sustav*

$$ax + by \equiv e \pmod{m}$$
$$cx + dy \equiv f \pmod{m}$$

ima jedinstveno rješenje ako i samo ako je $(\Lambda, m) = 1$, gdje je $\Lambda \equiv ad - bc \pmod{m}$.

Dokaz. Pretpostavimo da su $x \equiv x_0 \pmod{m}$ i $y \equiv y_0 \pmod{m}$ rješenja sustava

$$ax_0 + by_0 \equiv e \pmod{m} \tag{5.3}$$
$$cx_0 + dy_0 \equiv f \pmod{m}. \tag{5.4}$$

Množenjem jednadžbe (5.3) s d i jednadžbe (5.4) s b dobivamo

$$adx_0 + bdy_0 \equiv ed \pmod{m}$$
$$bcx_0 + bdy_0 \equiv bf \pmod{m}$$

Oduzimanjem dobivamo

$$(ad - bc)x_0 \equiv ed - bf \pmod{m}.$$

Prema Korolaru 3, x_0 ima jedinstvenu vrijednost po modulu m ako i samo ako je $(\Lambda, m) = 1$. Slično, y_0 ima jedinstvenu vrijednost po modulu m ako i samo ako je $(\Lambda, m) = 1$. Dakle, sustav će imati jedinstveno rješenje modulu m ako i samo ako je $(\Lambda, m) = 1$.

□

Prethodni teorem ilustrirat ćemo na primjeru.

Primjer 28. *Provjerimo ima li linearni sustav*

$$\begin{aligned} 4x + 5y &\equiv 6 \pmod{11} \\ 7x + 8y &\equiv 9 \pmod{11} \end{aligned}$$

jedinstveno rješenje modulo 11.
Rješenje.
Prema prethodnom teoremu, trebamo provjeriti je li $(\Lambda, 11) = 1$ *za dani linearni sustav.*

$$\Lambda \equiv ad - bc \equiv 4 \cdot 8 - 5 \cdot 7 \equiv -3 \equiv 8 \pmod{11}$$

Budući da je $(8, 11) = 1$, *prema Teoremu 9 polazni sustav ima jedinstveno rješenje modulo* 11.

Definicija 9 (vidjeti [2, Modular Inverses])**.** *Kažemo da je* a^{-1} *inverz cijelog broja a modulo m ukoliko vrijedi*

$$a \cdot a^{-1} \equiv 1 \pmod{m}.$$

Teorem 10 (vidjeti [2, Theorem 6.5])**.** *Jedinstveno rješenje modulo m linearnog sustava*

$$\begin{aligned} ax + by &\equiv e \pmod{m} \\ cx + dy &\equiv f \pmod{m} \end{aligned}$$

dano je s $x_0 \equiv \Lambda^{-1}(ed - bf) \pmod{m}$ *i* $y_0 \equiv \Lambda^{-1}(af - ce) \pmod{m}$, *gdje je* $\Lambda \equiv ad - bc \pmod{m}$, *a* Λ^{-1} *inverz od* Λ *modulo m.*

Dokaz. Prema Teoremu 9, budući da sustav ima jedinstveno rješenje modulo m, $(\Lambda, m) = 1$, prema Korolaru 3 postoji inverz od Λ modulo m. Kako linearni sustav ima jedinstveno rješenje, dovoljno je pokazati da x_0, y_0 zadovoljavaju sustav:

$$\begin{aligned} ax_0 + by_0 &\equiv a\Lambda^{-1}(de - bf) + b\Lambda^{-1}(af - ce) \pmod{m} \\ &\equiv (ad - bc)\Lambda^{-1}e + \Lambda^{-1}(abf - abf) \pmod{m} \\ &\equiv \Lambda\Lambda^{-1}e + 0 \pmod{m} \\ &\equiv e \pmod{m}, \text{ budući da je } \Lambda\Lambda^{-1} \equiv 1 \pmod{m}. \end{aligned}$$

Također,

$$\begin{aligned} cx_0 + dy_0 &\equiv c\Lambda^{-1}(de - bf) + d\Lambda^{-1}(af - ce) \pmod{m} \\ &\equiv (ad - bc)\Lambda^{-1}f + \Lambda^{-1}(cde - cde) \pmod{m} \\ &\equiv \Lambda\Lambda^{-1}f + 0 \pmod{m} \\ &\equiv f \pmod{m}, \text{ budući da je } \Lambda\Lambda^{-1} \equiv 1 \pmod{m}. \end{aligned}$$

Prema tome, par $x \equiv x_0 \pmod{m}, y \equiv y_0 \pmod{m}$ je jedinstveno rješenje linearnog sustava. □

Zapisano u obliku determinanti,

$$\Lambda \equiv ad - bc \equiv \begin{vmatrix} a & b \\ c & d \end{vmatrix} \pmod{m},$$
$$x_0 \equiv \Lambda^{-1}(ed - bf) \equiv \Lambda^{-1} \begin{vmatrix} e & b \\ f & d \end{vmatrix} \pmod{m},$$
$$y_0 \equiv \Lambda^{-1}(af - ce) \equiv \Lambda^{-1} \begin{vmatrix} a & e \\ c & f \end{vmatrix} \pmod{m},$$

formule za rješenje 2×2 linearnog sustava vrlo su slične onima za rješenje linearnog sustava Cramerovim pravilom pa je ova metoda poznata još kao **metoda determinanti**.
Prethodni teorem ilustrirat ćemo na primjeru.

Primjer 29. *Riješimo linearni sustav*

$$\begin{aligned} 4x + 15y &\equiv 9 \pmod{51} \\ 6x + 26y &\equiv 32 \pmod{51}. \end{aligned}$$

Rješenje. Budući da je

$$\Lambda = ad - bc = 4 \cdot 26 - 15 \cdot 6 \equiv 14 \pmod{51} \quad i \quad (14, 51) = 1$$

prema Teoremu 9 sustav ima jedinstveno rješenje modulo 51. *Odredimo sada* Λ^{-1}.

$$\begin{aligned} \Lambda\Lambda^{-1} &\equiv 1 \pmod{51} \\ 14\Lambda^{-1} &\equiv 1 \pmod{51}. \end{aligned} \tag{5.5}$$

Kako je $(14, 51) = 1$ *prema Bezoutovom identitetu postoje* $u, v \in \mathbb{Z}$ *takvi da*

$$14u + 51v = 1.$$

Djelovanjem s modulo 51 *dobivamo*

$$14u \equiv 1 \pmod{51}.$$

Primijetimo da je prethodna kongruencija ekvivalentna s (5.5). Odnosno, $u = \Lambda^{-1}$.
Primjenom Euklidovog algoritma dobivamo

$$\begin{aligned} 51 &= 14 \cdot 3 + 9 \\ 14 &= 9 \cdot 1 + 5 \\ 9 &= 5 \cdot 1 + 4 \\ 5 &= 4 \cdot 1 + 1 \\ 4 &= 1 \cdot 4 \end{aligned}$$

iz čega primjenom rekurzivnih relacija pronađemo u.

i	-1	0	1	2	3	4
q_i			3	1	1	1
u_i	0	1	-3	4	-7	$\boxed{11}$

Dakle,

$$u = \Lambda^{-1} \equiv 11 \pmod{51}.$$

Prema tome,

$$\begin{aligned} x_0 &\equiv \Lambda^{-1}(ed - bf) \pmod{51} \\ &\equiv 11 \cdot (9 \cdot 26 - 15 \cdot 32) \pmod{51} \\ &\equiv 11 \cdot (-246) \pmod{51} \\ &\equiv -2706 \pmod{51} \\ &\equiv 48 \pmod{51}; \end{aligned}$$

$$\begin{aligned} y_0 &\equiv \Lambda^{-1}(af - ce) \pmod{51} \\ &\equiv 11 \cdot (4 \cdot 32 - 6 \cdot 9) \pmod{51} \\ &\equiv 11 \cdot 74 \pmod{51} \\ &\equiv 814 \pmod{51} \\ &\equiv 49 \pmod{51}. \end{aligned}$$

Stoga je par $x \equiv 48 \pmod{51}, y \equiv 49 \pmod{51}$ *jedinstveno rješenje danog sustava.*

Literatura

[1] Andrej Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[2] Thomas Koshy, *Elementary number theory with applications*, Academic Press, New York, 2007.

[3] Ivan Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Osijek, 2013.

Sažetak

U ovome radu bavimo se sustavima linearnih kongruencija. Najprije uvodimo pojmove djeljivosti i kongruencija, elementarne pojmove teorije brojeva, te navodimo njihova osnovna svojstva. Nakon toga uvodimo linearne kongruencije i temeljne rezultate koji nam daju postupak za njihovo rješavanje koji kasnije primjenjujemo na sustave linearnih kongruencija. Zatim, dolazimo do sustava linearnih kongruencija za koje navodimo i dokazujemo jedan od najbitnijih rezultata pomoću kojega rješavamo takve sustave, kao i druge metode rješavanja. Na kraju se bavimo 2×2 linearnim sustavima.

Ključne riječi

djeljivost, kongruencije, linearne kongruencije, sustavi linearnih kongruencija, metoda iteracije, Kineski teorem o ostacima, 2×2 linearni sustav

Systems of linear congruences

Summary

In this paper, we deal with systems of linear congruences. First, we introduce the concepts of divisibility and congruence, elementary concepts of number theory, and state their basic characteristics. Subsequently, we introduce linear congruences and fundamental results that give us a procedure for solving them, which we later apply to systems of linear congruences. Afterwards, we come to systems of linear congruences for which we state and prove one of the most important results by means of which we solve such systems, as well as other solving methods. Finally, we deal with 2×2 linear systems.

Keywords

divisibility, congruences, linear congruences, systems of linear congruences, iteration method, Chinese remainder theorem, 2×2 linear systems

Životopis

Moje ime je Stjepan Karajko. Rođen sam 10. prosinca 2001. godine u Osijeku. Pohađao sam Osnovnu školu Stjepana Cvrkovića u Starim Mikanovcima. Nakon završetka osnovne škole upisujem Gimnaziju A. G. Matoša u Đakovu, prirodoslovno-matematički smjer, koju završavam 2020. godine. Svoje obrazovanje nastavljam upisom Prijediplomskog studija Matematike na Fakultetu primijenjene matematike i informatike.