Sustavi linearnih kongruencija i matrični račun

Grgić, Ivana; Čatipović, Marija

Source / Izvornik: **Acta mathematica Spalatensia. Series didactica, 2024, 7., 19 - 30**

Journal article, Published version
Rad u časopisu, Objavljena verzija rada (izdavačev PDF)

https://doi.org/10.32817/amssd.7.2

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:179:857310

ACTA MATHEMATICA SPALATENSIA
Series didactica
Vol.7 (2024) 19–30
https://doi.org/10.32817/amssd.7.2

Zaprimljen: 10. listopada 2023.
Prihvaćen: 14. veljače 2024.

Sustavi linearnih kongruencija i matrični račun

Ivana Grgić, Marija Čatipović

Sažetak

U ovom ćemo članku opisati metodu za rješavanje sustava linearnih kongruencija s n nepoznanica modulo m koristeći alate linearne algebre. Definirat ćemo kongruenciju matrica te što je inverz matrice modulo m. Iskazat ćemo teoreme o broju rješenja sustava n linearnih kongruencija s n nepoznanica te pokazati kako ih riješiti pomoću Gaussovih eliminacija i, u slučaju invertibilne matrice sustava, množenjem inverzne matrice modulo m i vektora slobodnih članova.

Ključni pojmovi: kongruencija, sustav linearnih kongruencija, kongruentne matrice, inverz modularne matrice

Abstract

In this article, we will describe a method for solving linear systems of congruences modulo m with n variables, using linear algebra tools. We will define congruence of matrices and what is the inverse of a matrix modulo m. We will present theorems on the number of solutions of the system of n linear congruences with n unknowns and show how to solve them using Gaussian eliminations and, in the case of an invertible system matrix, by multiplying the inverse matrix modulo m and the vector of free terms.

Keywords: congruence, system of linear congruences, congruent matrices, inverse of modular matrices

1. Osnovni pojmovi

Djeljivost je fundamentalni pojam teorije brojeva. Uz pojam djeljivosti veže se i pojam kongruencije. Teorija kongruencija nasljeđe je Carla Friedricha Gaussa koji je ovu tehniku, poznatu i kao modularna aritmetika, zasnovao u svom djelu *Disquisitiones Arithmeticae*, objavljenom 1801. godine.

Definicija 1. *Kažemo da su cijeli brojevi a i b* ***kongruentni po modulu*** *m (ili modulo m), $m \in \mathbb{N}$, ako je razlika $a - b$ djeljiva s m, tj. $m \mid a - b$. U tom slučaju pišemo*

$$a \equiv b \,(\mathrm{mod}\, m),$$

i čitamo a je kongruentan b po modulu m (modulo m) *[7].*

Također, možemo reći $a - b \in m\mathbb{Z}$.

Primjer 1. *Očigledno je* $14 \equiv 3 \,(\mathrm{mod}\, 11)$, $122 \equiv 2 \,(\mathrm{mod}\, 5)$, $-5 \equiv 7 \,(\mathrm{mod}\, 6)$.

Relacija *biti kongruentan modulo m* relacija je ekvivalencije na skupu $\mathbb{Z}$, tj. ona je refleksivna, simetrična i tranzitivna [7].

Sljedeće propozicije daju neka osnovna svojstva korisna u rješavanju sustava linearnih kongruencija.

Propozicija 2. *Ako je $a_1 \equiv b_1 \,(\mathrm{mod}\, m)$ i $a_2 \equiv b_2 \,(\mathrm{mod}\, m)$, gdje je $m \in \mathbb{N}$, onda vrijedi [7]:*

(i) $a_1 + a_2 \equiv b_1 + b_2 \,(\mathrm{mod}\, m)$,

(ii) $a_1 a_2 \equiv b_1 b_2 \,(\mathrm{mod}\, m)$.

Propozicija 3. *Neka su $a, b, k \in \mathbb{Z}$ i $m \in \mathbb{N}$ takvi da je $ak \equiv bk \,(\mathrm{mod}\, m)$ i $\mathrm{nzd}(k, m) = 1$. Tada vrijedi $a \equiv b \,(\mathrm{mod}\, m)$ [7].*

Propozicija 4. *Neka je $ax \equiv ay \,(\mathrm{mod}\, m)$. Tada vrijedi i $x \equiv y \left(\mathrm{mod}\, \frac{m}{d}\right)$, gdje je $d = \mathrm{nzd}(a, m)$ [2].*

Kao uvod u ono što slijedi navest ćemo uvjet rješivosti linearne kongruencije

$$ax \equiv b \,(\mathrm{mod}\, m) \tag{1}$$

za dane $a, b \in \mathbb{Z}$ i $m \in \mathbb{N}$. Ako je neki $x_0 \in \mathbb{Z}$ rješenje kongruencije (1), onda će i svi brojevi oblika $x_0 + mk$, $k \in \mathbb{Z}$ zadovoljavati tu kongruenciju. Dakle, ako linearna kongruencija (1) ima rješenja u skupu $\mathbb{Z}$, onda ih ima beskonačno mnogo. Pod pojmom broja rješenja kongruencije smatrat ćemo broj međusobno nekongruentnih (modulo m) rješenja [3].

Teorem 5. *Neka su a i b cijeli brojevi te m prirodan broj. Kongruencija* (1) *ima rješenja ako i samo ako $d = \text{nzd}(a, m)$ dijeli b. Ako je kongruencija* (1) *rješiva, onda je broj rješenja jednak d [6].*

Za male vrijednosti modula m, rješenje se može pronaći u nekom potpunom sustavu ostataka modulo m [5] što ćemo pokazati u sljedećem primjeru, no za veće vrijednosti od m koriste se metoda svođenja na diofantsku jednadžbu, Eulerova metoda ili metoda koja koristi Euklidov algoritam.

Primjer 2. *Promotrimo kongruenciju $3x \equiv 12 \pmod 6$. Uočimo $d = \text{nzd}(3, 6) = 3$, $b = 12$ i $d|b$, pa je kongruencija rješiva te ima $d = 3$ nekongruentnih rješenja. Iz dane kongruencije slijedi $3x - 6k = 12$, $k \in \{0, 1, 2, 3, 4, 5\}$. Odatle dobivamo nekongruentna rješenja:*
$x \equiv 0,\ 2,\ 4 \pmod 6$.

Promotrimo sada poseban slučaj kada je $b = 1$ u teoremu 5. Linearna kongruencija $ax \equiv 1 \pmod m$ ima jedno rješenje ako i samo ako $\text{nzd}(a, m) = 1$. Tada se za a kaže da je invertibilan, a x se naziva inverzom od a modulo m i označava s a^{-1} te vrijedi $a \cdot a^{-1} \equiv 1 \pmod m$ [5].

Teorem 6. *Neka su $a_1, \ldots, a_n$, b cijeli brojevi i m prirodan broj. Linearna kongruencija*

$$a_1x_1 + \cdots + a_nx_n \equiv b \pmod m \tag{2}$$

ima rješenja ako i samo ako $d = \text{nzd}(a_1, \ldots, a_n, m)|b$. Ako je linearna kongruencija (2), rješiva onda je broj nekongruentnih rješenja jednak $d \cdot m^{n-1}$ [6].

Primjer 3. *Riješimo sljedeću linearnu kongruenciju*

$$3x_1 - 7x_2 \equiv 11 \pmod{13}.$$

Uočimo $d = \text{nzd}(3, 7, 13) = 1$, $b = 11$ i $d|b$, pa je kongruencija rješiva te ima $d \cdot m^{n-1} = 1 \cdot 13^{2-1} = 13$ nekongruentnih rješenja. Iz dane kongruencije dobivamo jednadžbu $3x_1 - 7x_2 - 13k = 11$ koja ima opće rješenje za:

$$\begin{aligned} x_1 &= 7t_1 + 6 \pmod{13} \\ x_2 &= 3t_1 + 1 \pmod{13} \\ k &= 3t_2 \pmod{13} \end{aligned}$$

pri čemu su $t_1,\ t_2 \in \{0, \ldots, 12\}$. Kako t_1 postiže vrijednosti $\{0, \ldots, 12\}$, onda su sva nekongruentna rješenja linearne kongruencije dana tablicom:

x_1	6	0	7	1	8	2	9	3	10	4	11	5	12
x_2	1	4	7	10	0	3	6	9	12	2	5	8	11
t_1	0	1	2	3	4	5	6	7	8	9	10	11	12

Tablica 1. Nekongruentna rješenja linearne kongruencije $3x_1 - 7x_2 \equiv 11 \pmod{13}$.

2. Sustavi linearnih kongruencija s n nepoznanica

U nastavku ćemo opisati kako se rješavaju sustavi linearnih kongruencija s n nepoznanica modulo m. Sustav linearnih kongruencija sustav je oblika

$$\begin{aligned} a_{11}x_1 + a_{12}x_2 + \cdots + a_{1n}x_n &\equiv b_1 \pmod{m} \\ a_{21}x_1 + a_{22}x_2 + \cdots + a_{2n}x_n &\equiv b_2 \pmod{m} \\ &\vdots \\ a_{n1}x_1 + a_{n2}x_2 + \cdots + a_{nn}x_n &\equiv b_n \pmod{m} \end{aligned} \tag{3}$$

gdje su m i n prirodni brojevi, a a_{ij} i b_i cijeli brojevi za $i, j \in \{1, \ldots, n\}$. Skalare a_{ij} nazivamo koeficijentima sustava, skalare b_i slobodnim koeficijentima (ili članovima).
Zanima nas koliko rješenja ima ovaj sustav i kako ih izračunati koristeći postupak Gaussove eliminacije i osnovne pojmove modularne aritmetike. Za početak trebamo definirati pojam kongruentnih matrica [1].

Definicija 7. *Kažemo da su dvije $k \times p$ matrice A i B kongruentne modulo m ako vrijedi*

$$a_{ij} \equiv b_{ij} \pmod{m}, \text{ za svaki } i = 1, ..., k, \ j = 1, ..., p.$$

Primjer 4. $\begin{bmatrix} 9 & 1 & 5 \\ 1 & 0 & 4 \\ 2 & 0 & 12 \end{bmatrix} \equiv \begin{bmatrix} 6 & 7 & 8 \\ -2 & 9 & 1 \\ 11 & 15 & 0 \end{bmatrix} \pmod{3}$.

Sada gornji sustav kongruencija (3) jednostavnije možemo zapisati u matričnom obliku

$$AX \equiv B \pmod{m} \tag{4}$$

gdje je A matrica koeficijenata sustava, X vektor nepoznanica i B vektor slobodnih članova.

Označimo s $u(A, B, m)$ broj nekongruentnih rješenja modulo m sustava (4). Sljedećim teoremima dat ćemo uvid što se događa s brojem rješenja sustava (3).

Teorem 8. *Neka su A, B i m dani kao u (3) i (4). Tada je*

$$u(A, B, m) \leq (\text{nzd}(\det A,\, m))^n.$$

Ako je $\text{nzd}(\det A,\, m) = 1$ *onda je* $u(A, B, m) = 1$ *[4].*

Teorem 9. *Neka su A, B i m dani kao u (3) i (4). Pretpostavimo da je $m = m_1 \cdots m_k$ gdje su brojevi $m_1, \ldots, m_k$ u parovima relativno prosti. Onda je*

$$u(A, B, m) = u(A, B, m_1) \cdots u(A, B, m_k)\,[4].$$

Primjer 5. *Promotrimo sljedeći sustav*

$$\begin{aligned} 2x_1 + 7x_2 &\equiv 17 \,(\text{mod}\, 35) \\ 3x_1 + 8x_2 &\equiv 18 \,(\text{mod}\, 35). \end{aligned}$$

Prema teoremu 5 vrijedi $u(A, B, 35) \leq (\text{nzd}(\det A,\, 35))^2$ pri čemu je $A = \begin{bmatrix} 2 & 7 \\ 3 & 8 \end{bmatrix}$, $B = \begin{bmatrix} 17 \\ 18 \end{bmatrix}$. Kako je $\det A = -5$ to je $\text{nzd}(\det A,\, 35) = 5$ pa slijedi $u(A, B, 35) \leq 25$. Dakle, sustav ima najviše 25 rješenja. Uočimo da je $35 = 5 \cdot 7$, a 5 i 7 su u parovima relativno prosti pa po prethodnom teoremu 9 imamo $u(A, B, 35) = u(A, B, 5) \cdot u(A, B, 7)$. Sada promatramo isti sustav modulo 5 i modulo 7. Kako je $\text{nzd}(\det A,\, 5) = 5$ i $\text{nzd}(\det A,\, 7) = 1$ to je prema teoremu 8 $u(A, B, 5) \leq 25$, a $u(A, B, 7) = 1$. Rješavanjem sustava modulo 5 dobijemo točno 5 rješenja pa je

$$u(A, B, 35) = u(A, B, 5) \cdot u(A, B, 7) = 5 \cdot 1 = 5 \leq 25.$$

Rješavajući početni sustav modulo 35 postupkom koji ćemo opisati u nastavku, lako dolazimo do rješenja prikazanih tablicom:

x_1	33	26	19	12	5
x_2	0	10	17	24	31
x_3	0	1	2	3	4

Tablica 2. Nekongruentna rješenja zadanog sustava.

Iz linearne algebre znamo da se rješenje sustava linearnih jednadžbi ne mijenja ako na sustav primijenimo elementarne transformacije (množenje jednadžbe brojem različitim od nule, zamjena poretka jednadžbi,

pribrajanje jedne jednadžbe drugoj).
Vrijedi li isto i za sustave linearnih kongruencija?

Propozicija 10. *Elementarne operacije nad retcima matrice koje ne mijenjaju rješenje odgovarajućeg sustava linearnih kongruencija modulo m jesu [1]:*

1. *zamjena mjesta bilo koja dva retka*
2. *množenje jednog retka s brojem relativno prostim sa m (pomnoženi redak nazivamo višekratnikom retka),*
3. *zbrajanje višekratnika retka s drugim retkom matrice.*

Dokaz. Operacija (1), tj. mijenjanje redoslijeda kongruencija u sustavu ne utječe na rješenje sustava. Neka je dana kongruencija

$$acx + bcy \equiv dc \,(\mathrm{mod}\, m)$$

gdje je c relativno prost sa m. Pretpostavimo da je $x = x'$ i $y = y'$ rješenje ove kongruencije, tj.

$$acx' + bcy' \equiv dc \,(\mathrm{mod}\, m). \tag{5}$$

Onda prema propoziciji 3 vrijedi

$$ax' + by' \equiv d \,(\mathrm{mod}\, m)$$

pa je $x = x'\, y = y'$ rješenje kongruencije

$$ax + by \equiv d \,(\mathrm{mod}\, m). \tag{6}$$

Obratno, ako je $x = x_0$ i $y = y_0$ rješenje od (6), onda je i rješenje od (5). Dakle, rješenja od (5) i (6) identična su kada je $\mathrm{nzd}(c, m) = 1$ pa je dokazana i tvrdnja za operaciju (2). Operacija (3) je posljedica propozicije 2. □

Sada ćemo ilustrirati postupak rješavanja sustava 3 linearne kongruencije s 3 nepoznanice.

Primjer 6. *Promotrimo sustav kongruencija*

$$\begin{aligned} 5x_1 + 3x_2 + 2x_3 &\equiv 2 \,(\mathrm{mod}\, 7) \\ 3x_1 + 4x_2 + 6x_3 &\equiv 1 \,(\mathrm{mod}\, 7) \\ 2x_1 + x_2 + x_3 &\equiv 4 \,(\mathrm{mod}\, 7). \end{aligned}$$

Ovaj sustav u matričnom obliku možemo zapisati kao $AX \equiv B \pmod 7$, gdje je

$$A = \begin{bmatrix} 5 & 3 & 2 \\ 3 & 4 & 6 \\ 2 & 1 & 1 \end{bmatrix} \text{ matrica koeficijenata sustava,}$$

$$X = \begin{bmatrix} x_1 \\ x_2 \\ x_3 \end{bmatrix} \text{ vektor nepoznanica i } B = \begin{bmatrix} 2 \\ 1 \\ 4 \end{bmatrix} \text{ vektor slobodnih članova.}$$

Determinanta matrice A iznosi 7 pa je prema teoremu 9 $\operatorname{nzd}(\det A, 7) = 7$ i $u(A, B, 7) \leq 7^3$. Sada možemo riješiti prethodni sustav koristeći elementarne operacije nad retcima proširene matrice. Matricu ćemo svesti na gornji trokutasti oblik, odnosno provesti postupak poznat kao Gaussova eliminacija. Proširena matrica sustava jest

$$A|B = \left[\begin{array}{ccc|c} 5 & 3 & 2 & 2 \\ 3 & 4 & 6 & 1 \\ 2 & 1 & 1 & 4 \end{array}\right].$$

Pomnožimo prvi redak s 3. Ovo smijemo napraviti jer su 3 i 7 relativno prosti. Imajmo na umu da sve operacije radimo modulo 7. Dobijemo

$$A|B = \left[\begin{array}{ccc|c} 1 & 2 & 6 & 6 \\ 3 & 4 & 6 & 1 \\ 2 & 1 & 1 & 4 \end{array}\right].$$

Oduzmimo od drugog retka trostruki prvi redak, a od trećeg retka dvostruki prvi redak:

$$A|B = \left[\begin{array}{ccc|c} 1 & 2 & 6 & 6 \\ 0 & 5 & 2 & 4 \\ 0 & 4 & 3 & 6 \end{array}\right].$$

U sljedećem koraku htjeli bismo na mjestu $(2, 2)$ broj 1 pa riješimo kongruenciju $5x \equiv 1 \pmod 7$. Ona ima jedno rješenje, $x = 3$. Zato množimo drugi redak s 3 i dobijemo

$$A|B = \left[\begin{array}{ccc|c} 1 & 2 & 6 & 6 \\ 0 & 1 & 6 & 5 \\ 0 & 4 & 3 & 6 \end{array}\right].$$

Oduzimanjem od trećeg retka drugi redak pomnožen s 4 dobijemo sve nule u trećem retku:

$$A|B = \left[\begin{array}{ccc|c} 1 & 2 & 6 & 6 \\ 0 & 1 & 6 & 5 \\ 0 & 0 & 0 & 0 \end{array}\right].$$

Sada iz zadnje matrice možemo pročitati rješenje sustava:

$$\begin{aligned} x_2 &\equiv -6x_3 + 5 \equiv x_3 + 5 \,(\mathrm{mod}\, 7) \\ x_1 &\equiv -2x_2 - 6x_3 + 6 \equiv 5x_2 + x_3 + 6 \\ &\equiv 5(x_3 + 5) + x_3 + 6 \equiv 6x_3 + 3 \,(\mathrm{mod}\, 7). \end{aligned}$$

Kako je $x_3 \in \{0, \ldots, 6\}$, onda su sva rješenja sustava dana tablicom:

x_1	3	2	1	0	6	5	4
x_2	5	6	0	1	2	3	4
x_3	0	1	2	3	4	5	6

Tablica 3. Nekongruentna rješenja zadanog sustava.

Prethodni primjer pokazuje nam da sustav linearnih kongruencija može imati višestruka rješenja zbog linearne zavisnosti, isto kao i sustav linearnih jednadžbi u linearnoj algebri. No, kad radimo s kongruencijama tada je u pitanju konačno mnogo nekongruentnih rješenja, za razliku od beskonačno mnogo rješenja koja mogu postojati kada rješavamo sustave jednadžbi u skupu $\mathbb{R}$ [1].

Primjer 7. *Promotrimo sustav kongruencija*

$$\begin{aligned} 4x_1 + 3x_2 + x_3 &\equiv 2 \,(\mathrm{mod}\, 7) \\ x_2 + 3x_3 &\equiv 5 \,(\mathrm{mod}\, 7) \\ 2x_1 + 6x_2 + 3x_3 &\equiv 0 \,(\mathrm{mod}\, 7). \end{aligned}$$

Uočimo da je $\det A = -44$, tj. $\mathrm{nzd}(\det A, 7) = 1$ pa prema teoremu 8 sustav ima jedno rješenje, i to: $x_1 = 5$, $x_2 = 4$, $x_3 = 5$.

3. Inverz matrice modulo m

Ako je matrica A regularna i ako postoji njen inverz modulo m, rješenje sustava možemo naći tako da odredimo inverz matrice A i zatim ga pomnožimo s matricom B.
Neka je dana kvadratna $n \times n$ matrica A. Želimo pronaći matricu M takvu da je

$$AM \equiv MA \equiv I \,(\mathrm{mod}\, m)$$

gdje je I jedinična $n \times n$ matrica. Inverz modulo m matrice A, ako postoji, je upravo tražena matrica M i označavamo je s A^{-1}.

Sada nam je još potrebna propozicija iz koje proizlazi da množenje obiju strana kongruencije matrica s matricom čuva kongruenciju.

Propozicija 11. *Neka su A i B $n\times k$ matrice takve da je $A \equiv B \pmod m$. Onda je $AC \equiv BC \pmod m$ za neku $k\times p$ matricu C i $DA \equiv DB \pmod m$ za neku $p \times n$ matricu D [1].*

Na sljedećem primjeru, primjenom Gauss-Jordanovih eliminacija, pokazat ćemo računanje inverza modularne matrice.

Primjer 8. *Izračunajmo inverz matrice $A = \begin{bmatrix} 2 & 5 \\ 4 & 1 \end{bmatrix}$ modulo 7.*

Tražimo matricu A^{-1} takvu da je

$$AA^{-1} \equiv A^{-1}A \equiv I \pmod 7.$$

Proširimo matricu A jediničnom 2×2 matricom:

$$\left[\begin{array}{cc|cc} 2 & 5 & 1 & 0 \\ 4 & 1 & 0 & 1 \end{array}\right].$$

Na mjestu $(1,1)$ želimo 1 pa pomnožimo prvi redak s 4 jer je $x = 4$ rješenje kongruencije $2x \equiv 1 \pmod 7$. Imajmo na umu, sve operacije radimo modulo 7. Dobijemo

$$\left[\begin{array}{cc|cc} 1 & 6 & 4 & 0 \\ 4 & 1 & 0 & 1 \end{array}\right].$$

Sada pomnožimo prvi redak sa 4 i oduzmimo ga od drugog retka

$$\left[\begin{array}{cc|cc} 1 & 6 & 4 & 0 \\ 0 & 5 & 5 & 1 \end{array}\right].$$

Na mjestu $(2,2)$ želimo 1 pa pomnožimo drugi redak s 3 jer je $x = 3$ rješenje kongruencije $5x \equiv 1 \pmod 7$ pa imamo

$$\left[\begin{array}{cc|cc} 1 & 6 & 4 & 0 \\ 0 & 1 & 1 & 3 \end{array}\right].$$

Konačno, pomnožimo drugi redak sa 6 i oduzmimo ga od prvog retka:

$$\left[\begin{array}{cc|cc} 1 & 0 & 5 & 3 \\ 0 & 1 & 1 & 3 \end{array}\right].$$

Vidimo da je inverz A^{-1} modulo 7 matrice A matrica

$$\begin{bmatrix} 5 & 3 \\ 1 & 3 \end{bmatrix}.$$

Kako bismo provjerili da je A^{-1} uistinu inverz od A modulo 7 izračunajmo $A \cdot A^{-1}$ i uvjerimo se da ćemo dobiti jediničnu matricu:

$$\begin{bmatrix} 2 & 5 \\ 4 & 1 \end{bmatrix} \cdot \begin{bmatrix} 5 & 3 \\ 1 & 3 \end{bmatrix} \equiv \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix} \pmod 7.$$

Sljedećom propozicijom skraćujemo postupak računanja inverza 2×2 matrice modulo m.

Propozicija 12. *Neka je* $A = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ *matrica s cjelobrojnim elementima takva da je* $\Delta = \det A = ad - bc$ *relativno prost s* m, $m \in \mathbb{N}$. *Neka je* Δ^{-1} *inverz od* Δ *modulo* m. *Onda je matrica* $A^{-1} = \Delta^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix}$ *inverz matrice* A *modulo* m *[5].*

Primijenimo propoziciju 12 na prethodni primjer 8 te pronađimo inverz. Jednostavnim računom, imajući na umu da sve operacije računamo modulo 7, dobivamo $\Delta = \det A = 3$. Sada trebamo izračunati Δ^{-1}. Iz definicije inverza broja imamo $\Delta \cdot \Delta^{-1} \equiv 1 \pmod m$, tj. $3\Delta^{-1} \equiv 1 \pmod 7$. Odatle dobivamo $\Delta^{-1} = 5$ te je prema propoziciji 12 $A^{-1} = 5 \begin{bmatrix} 1 & -5 \\ -4 & 2 \end{bmatrix} = \begin{bmatrix} 5 & 3 \\ 1 & 3 \end{bmatrix} \pmod 7$.

Za poopćenje propozicije 12 trebamo uvesti pojam adjunkte matrice adj(A). Neka je sada A =$[a_{ik}]$ bilo koja kvadratna matrica, a $[A_{ik}]$ matrica algebarskih komplemenata elemenata matrice A. Transponiranu matricu te matrice, tj. matricu

$$\operatorname{adj}(A) = [A_{ik}]^\tau = [A_{ki}]$$

nazivamo adjunkta matrice A [8].

Propozicija 13. *Ako je* A $n \times n$ *matrica s cjelobrojnim elementima i* $m \in \mathbb{N}$ *takav da je* $\operatorname{nzd}(\det A, m) = 1$, *onda je matrica* $A^{-1} = \Delta^{-1} \cdot \operatorname{adj}(A)$ *inverz od* A *modulo* m, *gdje je* Δ^{-1} *inverz od* $\Delta = \det A$ *modulo* m *[5].*

Sada možemo iskoristiti inverz matrice A modulo m kako bismo riješili sustav

$$AX \equiv B \pmod m$$

gdje je $\text{nzd}(\det A, m) = 1$. Prema propoziciji 13, kad pomnožimo obje strane ove kongruencije s A^{-1} dobijemo

$$\begin{aligned} A^{-1}(AX) &\equiv A^{-1}B \,(\text{mod}\, m) \\ (A^{-1}A)X &\equiv A^{-1}B \,(\text{mod}\, m) \\ X &\equiv A^{-1}B \,(\text{mod}\, m). \end{aligned}$$

Primijenimo prethodno na primjeru.

Primjer 9. *Odredimo rješenje sustava*

$$\begin{aligned} 2x_1 + x_2 + x_3 &\equiv 1 \,(\text{mod}\, 5) \\ x_1 + 2x_2 + x_3 &\equiv 1 \,(\text{mod}\, 5) \\ x_1 + x_2 + 2x_3 &\equiv 1 \,(\text{mod}\, 5). \end{aligned}$$

Matrica sustava je $A = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 1 & 2 \\ 1 & 1 & 2 \end{bmatrix}$ i njena determinanta iznosi $\Delta = 4$. Vrijedi $\text{nzd}(\det A, 5) = 1$ pa sustav ima jedno rješenje. Inverz od $\Delta = 4$ modulo 5 je $\Delta^{-1} = 4$. Sada je

$$\begin{aligned} A^{-1} = 4\,\text{adj}(A) &= 4 \begin{bmatrix} 3 & -1 & -1 \\ -1 & 3 & -1 \\ -1 & -1 & 3 \end{bmatrix} = \begin{bmatrix} 12 & -4 & -4 \\ -4 & 12 & -4 \\ -4 & -4 & 12 \end{bmatrix} \\ &\equiv \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix} \,(\text{mod}\, 5) \end{aligned}$$

i

$$X = A^{-1}B = \begin{bmatrix} 2 & 1 & 1 \\ 1 & 2 & 1 \\ 1 & 1 & 2 \end{bmatrix} \begin{bmatrix} 1 \\ 1 \\ 1 \end{bmatrix} \equiv \begin{bmatrix} 4 \\ 4 \\ 4 \end{bmatrix} \,(\text{mod}\, 5).$$

Literatura

[1] D. Bishop, *Introduction to cryptography with Java applets*, Jones and Bartlett publishers, 2003.

[2] B. Ibrahimpašić, S. Ibrahimpašić, *Linearne kongruencije i sistemi linearnih kongruencija*, MAT-KOL (Banja Luka), ISSN 0354-6969 (p), ISSN 1986-5228 (o), Vol. XX (1)(2014), 27-36

[3] A. Matić, *Neke primjene kongruencija*, Diplomski rad, PMF Sveučilište u Zagrebu, 2018.

[4] M. Nilsson, R. Nyquist, *Number of solution of linear congruence systems*, 2021.

[5] K. H. Rosen, *Elementary number theory and its applications*, Addison-Wesley Publishing company, 1986.

[6] F. Smarandache, *Algorithms for solving linear congruences and systems of linear congruences*, SSRM Electronic Journal, 2007.

[7] D. Žubrinić, *Diskretna matematika*, Element, Zagreb, 2001.

[8] Web link, `https://www2.irb.hr/korisnici/zskoda/horvaticla.pdf`, datum zadnjeg pristupa: 2. 10. 2023.

Ivana Grgić
Sveučilište u Splitu, Fakultet elektrotehnike, strojarstva i brodogradnje, Ruđera Boškovića 32, 21 000 Split, Hrvatska
E-mail: `Ivana.Grgic@fesb.hr`

Marija Čatipović
Sveučilište u Splitu, Fakultet elektrotehnike, strojarstva i brodogradnje, Ruđera Boškovića 32, 21 000 Split, Hrvatska
E-mail: `mcatipov@fesb.hr`