Sustavi kongruencija

Špoljarić, Kristina

Undergraduate thesis / Završni rad

2023

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, School of Applied Mathematics and Informatics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Fakultet primijenjene matematike i informatike**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:544439

Sveučilište J. J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni prijediplomski studij Matematika

Kristina Špoljarić

Sustavi kongruencija

Završni rad

Osijek, 2023.

Sveučilište J. J. Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike
Sveučilišni prijediplomski studij Matematika

Kristina Špoljarić

Sustavi kongruencija

Završni rad

Mentor: izv. prof. dr. sc. Ivan Soldo

Osijek, 2023.

Sažetak

U ovom radu proučavat ćemo kongruencije te sustave kongruencija. Na početku ćemo pomoću djeljivosti, što nam je jedan od najvažnijih pojmova u teoriji brojeva, doći do definicije kongruencija. Proći ćemo kroz načine riješavanja kongruencija te doći do sustava kongruencija. Spomenut ćemo najbitnije teoreme, pokazati kada sustav ima rješenja te na koje sve načine možemo riješiti sustav. Na kraju ćemo spomenuti neke primjene sustava kongruencija.

Ključne riječi

djeljivost, kongrunecije, sustavi kongruencija, linearne kongruencije, RSA kriptosustav

System of congruences

Summary

In this paper, we will discuss congruences and systems of congruences. At the beginning, using divisibility, which is one of the most important concepts in number theory, we will arrive at the definition of congruences. We will go through methods of solving congruences and reach systems of congruences. We will mention the most essential theorems, demonstrate when a system has solutions, and explore various approaches to solving the system. Finally, we will touch upon some applications of systems of congruences.

Keywords

divisibility, congruences, systems of congruences, linear congruences, RSA cryptosystem

Sadržaj

Uvod

Teorija brojeva, matematička je cjelina, koja najvećim djelom proučava svojstva cijelih brojeva. Neka od tih svojstava su djeljivost, rješivost jednadžbi te rastav na proste faktore. U ovom radu proučavat ćemo kongruencije i sustave kongruencija. Teorija kongruencija veoma nam je bitna za riješavanje problema o djeljivosti brojeva. Njenu teoriju, teoriju kongrunecija, uveo je njemački matematičar Carl Friedrich Gauss u svojoj knjizi *Disquisitiones Arithmeticae* koju je objavio 1801.godine. Tom teorijom, Gauss je pojednostavio mnoge probleme o djeljivosti brojeva. Gauss je također uveo oznaku za kongruenciju $\equiv$ koja se i dalje koristi. Vidimo kako je oznaka veoma slična oznaci jednakosti, čime je Guass htio istaknuti njihovu sličnost.

U prvom poglavlju ćemo se prisjetiti pojma djeljivosti i najbitnijeg teorema vezanog za djeljivost. U drugom poglavlju ćemo definirati kongruencije i neka njena osnovna svojstva. Pokazat ćemo kako se kongruencije riješavaju i kada rješenja postoje. U trećem poglavlju doći ćemo do sustava kongruencija. Prvo ćemo proći kroz par primjera sustava dviju kongruencija, te pokazati u kojem slučaju takvi sustavi imaju rješenje. Nadalje ćemo se baviti sustavima n linearnih kongruencija. Pomoću kineskog teorema o ostatcima pokazat ćemo kada sustav ima rješenja te kako ga pronaći. Proći ćemo kroz nekoliko primjera riješavanja sustava. U posljednjem djelu spomenut ćemo neke primjene sustava kongruencija.

1 Djeljivost

Prije nego uvedemo pojam kongruencija, prisjetit ćemo se definicije djeljivosti. Djeljivost nam je jedan temeljnih pojmova u teoriji brojeva.

Definicija 1. *Neka su $a \neq 0$ i b cijeli brojevi. Kažemo da je b djeljiv s a, odnosno da a dijeli b ako postoji cijeli broj x takav da je $b = ax$. To zapisujemo $a \mid b$. Ako b nije djeljiv s a, onda pišemo $a \nmid b$.*

Ako $a \mid b$, onda još kažemo da je a djelitelj od b te da je b višekratnik od a.

Promotrimo zapis djeljivosti na sljedećem primjeru.

Primjer 1. *Kažemo da $2 \mid 6$ zato što $\exists\, x \in \mathbb{Z}$ t.d. je $6 = 2 \cdot x$. U ovom slučaju $x = 3$, zato što je $6 = 2 \cdot 3$.*

Kažemo da $2 \nmid 7$ zato što $\nexists$ broj $x \in \mathbb{Z}$ t.d. je $7 = 2 \cdot x$.

Možemo primjetiti da $x \mid 0$ $\forall x \in \mathbb{Z} \setminus \{0\}$ jer je $0 = 0 \cdot x$. Također vrijedi i $1 \mid y$ $\forall y \in \mathbb{Z}$ jer je $y = y \cdot 1$.

Kada govorimo o djeljivosti, svakako moramo spomenuti jedan od najbitnijih nam teorema u teoriji brojeva, teorem o dijeljenju s ostatkom.

Teorem 1 (vidjeti [1, Teorem 2.2.])**.** *(Teorem o dijeljenju s ostatkom) Neka je $a \in \mathbb{N}$ te $b \in \mathbb{Z}$, tada kažemo da $\exists!\ r, q \in \mathbb{Z}$ takvi da je $b = qa + r$, $0 \leq r < a$.*

Dokaz. Dokaz možemo pronaći u [1, Teorem 2.2.]. □

Broj r iz prethodnog teorema nazivamo ostatak, a broj q nazivamo kvocijent pri dijeljenju b s a. Kažemo da je ostatak $r = 0$ akko a dijeli b.

Kada govorimo o djeljivosti, jedan od bitnijih pojmova nam je i zajednički djelitelj dvaju ili više brojeva. Pogledajmo sljedeću definiciju i primjer.

Definicija 2. *Neka su $b, c \in \mathbb{Z}$. Za $a \in \mathbb{Z}$ kažemo da je zajednički djelitelj brojeva b i c ukoliko $a \mid b$ i $a \mid c$.*

Ukoliko barem jedan od brojeva a i b nije nule, onda imamo konačno mnogo zajedničkih djelitelja tih brojeva. Najveći od njih se naziva ***najveći zajednički djelitelj*** *od b i c i označavamo s $nzd(b, c)$ tj. (b, c).*

Primjer 2.

$$(90, 7) = 1$$
$$(36, 6) = 6.$$

Analogno definiramo najvećeg zajedničkog djelitelja brojeva $k_1, k_2, ..., k_n \in \mathbb{Z}$ te ga označavamo s $(k_1, k_2, ..., k_n)$.

Kada govorimo o najvećem zajedničkom djelitelju, veoma je bitno napomenuti da brojevi čiji je najveći zajednički djelitelj 1 nazivamo **relativno prosti**.

Definicija 3. *Za $a, b \in \mathbb{Z}$ kažemo da su relativno prosti ukoliko je $(a, b) = 1$. Za $b_1, b_2, ..., b_n \in \mathbb{Z}$ kažemo da su relativno prosti ukoliko je $(b_1, b_2, ..., b_n) = 1$. Za $b_1, b_2, ..., b_n \in \mathbb{Z}$ kažemo da su u parovima relativno prosti ukoliko je $(b_i, b_j) = 1$ $\forall\ 1 \leq i, j \leq n, i \neq j$.*

Primjer 3. *Za brojeve 5 i 73 kažemo da su relativno prosti brojevi, zato što je $(5, 73) = 1$.*

Možemo primjetiti kako za sve u parovima relativno proste brojeve vrijedi da su i relativno prosti, no obrat ne vrijedi. Dakle, za brojeve koji su relativno prosti ne mora vrijediti da su i u parovima relativno prosti. Pogledajmo na sljedećem primjeru.

Primjer 4. *Brojevi 5, 8 i 16 su relativno prosti brojevi, zato što je $(5, 8, 16) = 1$, ali vidimo kako nisu u parovima relativno prosti jer $(8, 16) = 8 \neq 1$.*

Sada kada smo definirali najvećeg zajedničkog djelitelja, pitamo se kako ćemo ga odrediti. A odgovor na to pitanje će nam reći sljedeći teorem.

Teorem 2 (vidjeti [4, Theorem 1.15])**.** *(Euklidov algoritam)*
Neka su $a, b \in \mathbb{N}$ te $b \neq a$.Nadalje, neka je $a = r_0$, $b = r_1$. Uzastopnom primjenom teorema o dijeljenju s ostatkom dobili smo niz jednakosti:

$$\begin{aligned}
r_0 &= r_1 q_1 + r_2, 0 < r_2 < r_1, \\
r_1 &= r_2 q_2 + r_3, 0 < r_3 < r_2, \\
&\vdots \\
r_{n-2} &= r_{n-1} q_{n-1} + r_n, 0 < r_n < r_{n-1}, \\
r_{n-1} &= r_n q_n + r_{n+1}, r_{n+1} = 0.
\end{aligned}$$

Tada je r_n, posljednji ostatak u ovom procesu, jednak najvećem tajedničkom djelitelju brojeva a i b, tj. $r_n = (a, b)$.

Euklidov algoritam smatra se gotovo najvažnijim algoritmom u teoriji brojeva. Njega je prvi naveo i dokazao Euklid u sedmoj knjizi *Elemenata*. Pogledajmo dokaz ovog teorema.

Dokaz. Uzastopnom primjenom teorema o dijeljenju s ostatkom, doći ćemo do trenutka kada će nam $r_{n+1} = 0$, zato što nam se ostatci r_i smanjuju te su nenagitivni. Zadnja relacija $r_{n-1} = r_n q_n + r_{n+1}$ nam pokazuje da $r_n \mid r_{n-1}$. Predzadnja nam pokazuje da $r_n \mid r_{n-2}$. Dalje indukcijom vidimo kako $r_n \mid r_i$, $\forall i$. Dakle, $r_n \mid r_1 = b$ i $r_n \mid r_0 = a$, što znači da je r_n zajednički djelitelj brojeva a i b. Sada želimo pokazati kako je on najveći od svih zajedničkih djelitelja. Neka je d proizvoljni zajednički djelitelj brojeva a i b. Definicija od r_2 nam govori da $d \mid r_2$. Sljedeća relacija nam govori da $d \mid r_3$. Indukcijom vidimo da $d \mid r_i$ pa tako i $d \mid r_n$. Odavde zaključujemo da je onda r_n najveći od svih zajedničkih djelitelja brojeva a i b. □

Pogledajmo na primjeru kako funkcionira Euklidov algoritam.

Primjer 5. *Odredite* $(663, 168)$

$$\begin{aligned} 663 &= 168 \cdot 3 + 159 \\ 168 &= 159 \cdot 1 + 9 \\ 159 &= 9 \cdot 17 + 6 \\ 9 &= 6 \cdot 1 + 3 \\ 6 &= 3 \cdot 2 + 0. \end{aligned}$$

Odavde slijedi da je $(663, 168) = 3$.

Kada bismo prošli primjer krenuli od zadnjeg koraka i unazad išli korak po korak, dobili bi sljedeće jednakosti:

$$
\begin{aligned}
3 &= 9 - 6 \\
3 &= 9 - (159 - 9 \cdot 17) \\
3 &= (168 - 159) \cdot 18 - 159 \\
3 &= 168 \cdot 18 - 159 \cdot 19 \\
3 &= 168 \cdot 18 - (663 - 168 \cdot 3) \cdot 19 \\
3 &= 168 \cdot 75 - 663 \cdot 19.
\end{aligned}
$$

Odnosno, vidimo kako smo najvećeg zajedničkog djelitelja brojeva 663 i 168 zapisali upravo kao linearnu kombinaciju tih dvaju brojeva.

Ovime smo dobili postupak za pronalaženje cjelobrojnih rješenja jednadžbe $ax + by = (a, b)$. Ovaj izraz nazivamo **Bezoutov identitet**. Možemo vidjeti kako Euklidov postupak završava kada dobijemo ostatak 0. Postupak će završiti u konačno mnogo koraka zato što nam vrijedi da $a > r_1 > r_2 > ...$

Sada kada smo se prisjetili definicije djeljivosti i dijeljenja s ostatkom, možemo započeti s temom ovoga rada, odnosno s kongruencijama te sustavima kongruencija.

2 Kongruencije

Definicija 4. *Neka su* $a, b \in \mathbb{Z}$ *te* $n \in \mathbb{N}$. *Ako broj* $n \neq 0$ *dijeli razliku brojeva* $a - b$, *odnosno* $n \mid (a - b)$, *tada kažemo da je* a *kongruentan* b *modulo* n *i pišemo* $a \equiv b \pmod{n}$.

Suprotno kažemo kako a *nije kongruentan* b *modulo* n. *To zapisujemo kao* $a \not\equiv b \pmod{n}$.

Ukoliko je a kongruentan b modulo n, znači da $\exists\, y \in \mathbb{Z}$ t.d. je $ny = a - b$. Broj n u ovom slučaju nazivamo modulom kongruencije.

Ilustrirajmo to sljedećim primjerom.

Primjer 6. *Kažemo da je* $9 \equiv 2 \pmod{7}$ *zato što* 7 *dijeli razliku brojeva* 9 *i* 2, *odnosno* $7 \mid 9 - 2$.

Također, kažemo da $9 \not\equiv 2 \pmod{5}$ *zato što* 5 *ne dijeli razliku brojeva* 9 *i* 2, *odnosno* $5 \nmid 9 - 2$.

Primjer 7. *Kažemo da je* $a \equiv b \pmod{1}$, $\forall a, b$.

Uočima da nam kongruencija $a \equiv 0 \pmod{n}$ govori kako n dijeli broj a. Upravo je to ono za što kongruencije koristimo, da bismo dokazali je li nešto djeljivo s n ili nije.

2.1 Osnovna svojstva kongruencija

Spomenut ćemo neka najvažnija svojstva kongruencija. Svakako jedni od najbitnijih slijede iz sljedećeg teorema.

Teorem 3 (vidjeti [1, Propozicija 3.1.])**.** *Relacija "biti kongruentan modulo n" je relacija ekvivalencije.*

Dokaz. Da bismo dokazali da je nešto relacija ekvivalencije, moramo dokazati refleksivnost, simetričnost i tranzitivnosti.

- (refleksivnost) : Pogledajmo vrijedi li da je $k \equiv k \pmod{n}$, odnosno vrijedi li da n dijeli 0. Prema svojstvima djeljivosti znamo da je 0 djeljiv sa svakim brojem, odakle zaključujemo kako refleksivnost vrijedi.

- (simetričnost) : Iz kongruencije $k \equiv l \pmod{n}$ slijedi da $\exists\, y \in \mathbb{Z}$ t.d. je $ny = k - l$. Pomnožimo li to s (-1) slijedi: $-ny = l - b$ tj. $l \equiv k \pmod{n}$.

- (tranzitivnost) : Iz kongruencija $k \equiv l \pmod{n}$ i $l \equiv m \pmod{n}$ slijedi da $\exists\, y, z \in \mathbb{Z}$ t.d. je $ny = k - l$ i $nz = l - m$. Zbrojimo li te dvije jednadžbe, dobivamo da je $n(y + z) = k - m$, tj. $k \equiv m \pmod{n}$.

□

U daljnjem radu s kongruencijama, također su nam bitna i svojstva vezana za zbrajanje, oduzimanje, množenje i dijeljenja. U sljedećim teoremima ćemo upravo njih obraditi.

Teorem 4 (vidjeti [2, Theorem 2.2.]). *Neka su $a, b, c, d \in \mathbb{Z}$. Ako je $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$, onda je $a + c \equiv b + d \pmod{n}$, $a - c \equiv b - d \pmod{n}$ te $ac \equiv bd \pmod{n}$.*

Dokaz. Iz kongruencija $a \equiv b \pmod{n}$ i $c \equiv d \pmod{n}$ slijedi da $\exists\, y, z \in \mathbb{Z}$ t.d. je $ny = a - b$ i $nz = c - d$.

Zbrojimo li te dvije jednadžbe dobit ćemo: $(a + c) - (b + d) = n(y + z)$, tj. $a + c \equiv b + d \pmod{n}$.

Oduzmemo li te dvije jednadžbe dobit ćemo: $(a - c) - (b - d) = n(y - z)$, tj. $a - c \equiv b - d \pmod{n}$.

Množenjem tih dviju jednadžba dobit ćemo: $ac - bd = n(yz)$,
tj. $a - c \equiv b - d \pmod{n}$. □

Teorem 5 (vidjeti [1, Propozicija 3.2.]). *Neka su $a, b, c, d \in \mathbb{Z}$.*

1. *Ako $a \equiv b \pmod{n}$ te $d \mid n$, onda je $a \equiv b \pmod{d}$.*
2. *Ako $a \equiv b \pmod{n}$, onda je $ac \equiv bc \pmod{nc}$, $\forall c \neq 0$.*

Dokaz. Dokaz možemo pronaći u [1, Propozicija 3.2.]]. □

Vidimo kako za kongruencije vrijede svojstva asocijativnosti, distributivnosti i komutativnosti te da ih možemo zbrajati, oduzimati i množiti. Važno je napomenuti da to vrijedi samo za one s istim modulom. A što nam se dešava s dijeljenjem? Možemo li obje strane kongruencija podijeliti zajedničkim faktorom? Pogledajmo sljedeći primjer.

Primjer 8. *Podijelimo kongruenciju $36 \equiv 6 \pmod{6}$ brojem 6.Sada naša kongrunecija glasi $6 \equiv 1 \pmod{6}$. Vidimo kako to ne vrijedi jer $6 \nmid (6 - 1)$, tj. $6 \nmid 5$.*

Vidimo kako kongruencije ne možemo dijeliti na takav način. No sljedeći teorem će nam pokazati na koji način ih možemo dijeliti.

Teorem 6 (vidjeti [1, Teorem 3.4.]). *Kongruencija* $ac \equiv bc \pmod{n}$ *je ekvivalentna s kongruencijom* $a \equiv b \pmod{\frac{n}{nzd(c,n)}}$.

Dokaz. Dokaz se može naći u [1, Teorem 3.4.]]. □

Pogledajmo sada primjenu Teorema 6 na Primjeru 8.

Primjer 9. *Kongruencija* $36 \equiv 6 \pmod{6}$ *ekvivalentna je kongruencija* $6 \equiv 1 \pmod{\frac{6}{6}}$, *odnosno kongruenciji* $6 \equiv 1 \pmod{1}$.

Posebni slučaj prethodnog teorema vrijedi kada je $(c, n) = 1$. Tada vrijedi sljedeće:

Teorem 7 (vidjeti [3, Theorem 5.2.1.]). *Ako vrijedi da je* $(c, n) = 1$ *i* $ac \equiv bc \pmod{n}$ *onda je* $a \equiv b \pmod{n}$.

Dokaz. Iz $ac \equiv bc \pmod{n}$ znamo da n dijeli razliku brojeva $(ac - bc)$ tj. n dijeli $c(a-b)$. Obzirom da je $(c, n) = 1$, slijedi da n dijeli $(a-b)$, tj. $a \equiv b \pmod{n}$. □

Primjer 10. *Kongruencija* $36 \equiv 6 \pmod{11}$ *ekvivalentna je kongruencija* $6 \equiv 1 \pmod{11}$, *odnosno kongruenciji* $6 \equiv 1 \pmod{1}$.

2.2 Potpun sustav ostataka modulo n

Definicija 5. *Skup* $\{x_1, x_2, ..., x_n\}$ *zovemo potpuni sustav ostataka modulo* n *ako* $\forall y \in \mathbb{Z}\ \exists! x_j$ *takav da je* $y \equiv x_j \pmod{n}$.

Potpun sustav ostataka modulo n dobit ćemo na način da uzmemo iz svake klase ekvivalencije modulo n po jedan član. Vidimo kako postoji beskonačno mnogo potpunih sustava ostataka modulo n, te da svaki sadržu upravo n međusobno nekongruentnih brojeva. U sljedećem primjeru ćemo vidjeti jednog od najčešće korištenog potpunog sustava ostataka modulo n.

Primjer 11. *Jedan od potpunih sustava ostataka modulo n je skup:* $\{0, 1, ..., n-1\}$.

Pogledajmo kako to izgleda na konkretnim primjerima.

Primjer 12. *Pogledajmo potpun sustav ostataka modulo 5. Kada bismo ga tražili pomoću prethodnog primjera, on bi glasio:* $\{0, 1, 2, 3, 4\}$. *No kako imamo beskonačno mnogo potpunih sustava ostataka modulo 5, tako su također i skupovi:* $\{-4, -3, -2, -1, 0\}$, $\{15, 16, 17, 18, 19\}$ *potpuni sustavi ostataka modulo 5.*

2.3 Linearne kongruencije

Definicija 6. *Linearna kongruencija je kongruencija oblika* $ax \equiv b \pmod{n}$*, gdje su* $a, n \in \mathbb{N}$*,* $b \in \mathbb{Z}$*.*

Sljedeći teorem će nam reći više o postojanju i jedinstvenosti rješenja linearne kongrunecije.

Teorem 8 (vidjeti [1, Teorem 3.6.])**.** *Linearna kongrunecija ima rješenja akko* $d \mid b$*, gdje je* $d = nzd(a, n)$ $ax \equiv b \pmod{n}$*. Ukoliko kongrunecija zadovoljava ovaj uvjet, slijedi da ona ima točno* d *rješenja modulo* n*.*

Dokaz. Kažemo da ako postoje rješenja kongruencije $ax \equiv b \pmod{n}$, onda $\exists y \in \mathbb{Z}$ takav da je $ax - ny = b$. Očito vrijedi kako $nzd(a, n)$ dijeli b. Sada pretpostavljamo da $d = nzd(a, n)$ dijeli b. Neka je $a' = \frac{a}{d}, b' = \frac{b}{d}, n' = \frac{n}{d}$. Dobivamo kongruenciju oblika $a'x \equiv b' \pmod{n'}$. koja ima točno jedno rješenje modulo n'. Iz $nzd(a', n') = 1$, kada x prolazi potpunim sustavom ostataka modulo n' slijedi da $a'x$ također prolazi potpunim sustavom ostataka modulo n'. Odnosno tada vrijedi da se svaki ostatak modulo n' dobiva točno za jedan x iz potpunog sustava ostataka modulo n'. To također vrijedi i za b'. Neka je x' rješenje od $a'x' \equiv b' \pmod{n'}$.Sva ostala rješenja kongruencije $ax \equiv b \pmod{n}$ tada su dana s $x = x' + kn'$ za $k \in \mathbb{Z}$. Dok je svako međusobno neekvivalentno rješenje dano s $x = x' + kn'$ za $k = 0, 1, ..., d - 1$. Zaključujemo da ukoliko d dijeli b, tada je d ukupan broj rješenja modulu n kongruencije $ax \equiv b \pmod{n}$. □

Prethodni teorem nam želi pokazati da ako vrijedi relativna prostost brojeva a i n, odnosno, ukoliko je $nzd(a, n) = 1$, kongruencija uvijek ima točno jedno rješenje. Također, ukoliko vrijedi da $d \nmid b$, onda kongruencija nema rješenja.

Ukoliko je x_1 rješenje neke kongruencije, a $x_1 \equiv x_2 \pmod{n}$, tada je također i x_2 rješenje te iste kongruencije. Za rješenje x_1, x_2 za koja vrijedi $x_1 \equiv x_2 \pmod{n}$ kažemo da su ekvivalentna rješenja. Broj rješenja neke kongrunecije modulo n smatramo broj neekvivalentnih rješenja.

2.3.1 Riješavanje linearnih kongruencija

Sada kada smo definirali linearnu kongruneciju i rekli nešto o postojanju njenih rješenja, zanima nas kako pronaći ta rješenja. Za male module je to jednostavno, pokušali bismo sa svim brojevima iz skupa potpunog sustava ostataka i vidjeli koji

brojevi bi zadovoljavali danu kongruenciju te bi to bilo rješenje. Pogledajmo na primjeru.

Primjer 13. *Riješimo kongruenciju* $3x \equiv 2 \pmod 5$. *Prvo ćemo pronaći potpun sustav ostataka modulo* 5. *To je skup* $\{0, 1, 2, 3, 4\}$. *Pogledajmo koji od članova tog skupa će zadovoljavati ovu kongruenciju.*

$$\begin{aligned} x = 0 &\Rightarrow 0 \not\equiv 2 \pmod 5 \\ x = 1 &\Rightarrow 3 \not\equiv 2 \pmod 5 \\ x = 2 &\Rightarrow 6 \not\equiv 2 \pmod 5 \\ x = 3 &\Rightarrow 9 \not\equiv 2 \pmod 5 \\ x = 4 &\Rightarrow 12 \equiv 2 \pmod 5. \end{aligned}$$

Vidimo kako jedino $x = 4$ *zadovoljava zadanu kongruenciju, te je to rješenje. Kako je* $(a, n) = (3, 5)$ *slijedi da je to jedino rješenje ove linearne kongruencije.*

No što ako se radi o velikom modulu? Recimo o nekom dvoznamenkastom ili troznamenkastom broju. E tada više nebi bilo tako jednostavno. Dokaz iz Teorema 8 je konstruktivan za riješavanje takvih problema. Pogledajmo na sljedećem primjeru.

Primjer 14. *Riješimo linarnu kongruenciju* $10x \equiv 15 \pmod{25}$. *Prvo ćemo izračunati* d, $d = nzd(10, 25) = 5$. *Vidimo da* $5 \mid 15$ *što znači da kongruencija ima 5 rješenja modulo* n. *Uzmimo sada* $a' = \frac{10}{5}, b' = \frac{15}{5}, n' = \frac{25}{5}$. *Odavde dobivamo novu kongruenciju* $2x \equiv 3 \pmod 5$. *Množeći sada obje strane s* 3 *dobit ćemo kongruneciju* $6x \equiv 9 \pmod 5$. *Budući da znamo da je* $6 \equiv 1 \pmod 5$ *te* $9 \equiv 4 \pmod 5$, *slijedi kako je* $x' \equiv 4 \pmod 5$ *jedno rješenje ove kongruencije, odnosno sva rješenja su:* $x \equiv 4 \pmod{25}$, $x \equiv 9 \pmod{25}$, $x \equiv 14 \pmod{25}$, $x \equiv 19 \pmod{15}$, $x \equiv 24 \pmod{25}$.

Primjer 15. *Riješimo linearnu kongruenciju* $9x \equiv 11 \pmod{21}$. *Prvo ćemo izračunati* d, $d = nzd(9, 21) = 3$. *Vidimo da* $3 \not| 11$ *što znači da kongruencija nema rješenja.*

Još jedan način kako riješiti linearnu kongruenciju je pomoću euklidovog algoritma. Ukoliko pogledamo linearnu kongruenciju $ax \equiv b \pmod n$, za koju vrijedi da je

$nzd(a,n) = 1$, vidimo da onda vrijedi da $\exists u, v \in \mathbb{Z}$ takvi da je $au + nv = 1$, a u i v možemo pronaći pomoću Euklidovog algoritma. Tada vrijedi da je $au \equiv 1 \pmod{n}$ pa je $ax \equiv ub \pmod{n}$.

Pogledajmo kako bismo riješili kongruenciju iz Primjera 14 pomoću Euklidovog algoritma.

Primjer 16. *Riješimo linearnu kongruenciju* $10x \equiv 15 \pmod{25}$*, kako je* $nzd(a,n) = 5 \neq 1$*, i* $5 \mid 15$*, ovu kongruenciju možemo zapisati kao* $2x' \equiv 3 \pmod{5}$*. Primjenimo sada euklidov algoritam:*

$$5 = 2 \cdot 2 + 1$$
$$2 = 1 \cdot 2 + 0.$$

Pomoću tablice izračunajmo vrijednosti koje nam nedostaju.

i	-1	0	1
q_i			2
y_i	0	1	-2

.

Pomnožimo li kongruenciju $2u \equiv 1 \pmod{5}$ *s* 3 *dobivamo rješenje* $u \equiv 3 \pmod{5}$*, odavde slijedi da je* $2x' \equiv 3 \pmod{5}$ *množeći s* 3 *dobivamo rješenje* $x' \equiv 9 \equiv 4 \pmod{5}$*. Sva rješenja početne kongruencije dana su s:* $x \equiv 4, 9, 14, 19, 24 \pmod{25}$.

3 Sustavi kongruencija

Sada smo naučili što su linearne kongruencije i kako ih riješavati, no što ako imamo sustav linearnih kongruencije? Kako bismo ih onda riješili i postoji li uopće rješenje?

3.1 Sustavi dviju linearnih kongruencija

Pogledajmo prvo što se događa kada imamo sustav dviju linearnih kongruencija.

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2}. \end{aligned}$$

Primjer 17. *Riješimo sustav kongruencija*

$$\begin{aligned} x &\equiv 6 \pmod{7} \\ 3x &\equiv 3 \pmod{8}. \end{aligned}$$

Rješenje: Koristit ćemo metodu supstitucije. Prvu jednadžbu možemo zapisati kao: $x = 6 + 7k, k \in \mathbb{Z}$. *Sada ubacimo supstituciju u drugu jednadžbu:*

$$\begin{aligned} 3x &\equiv 3 \pmod{8} \\ 3(6+7k) &\equiv 3 \pmod{8} \\ 18 + 21k &\equiv 3 \pmod{8} \\ 2 + 5k &\equiv 3 \pmod{8} \\ 5k &\equiv 1 \pmod{8}. \end{aligned}$$

Množeći s 5 *dobivamo:*

$$25k \equiv k \equiv 5 \pmod{8}.$$

Sada imamo da je $k = 5+8l, l \in \mathbb{Z}$. *Vratimo li to u* x *dobivamo:* $x = 6+7(5+8l) = 7 + 35 + 56l = 42 + 56l$, *tj.rješenje ovog sustava je*

$$x \equiv 42 \pmod{56}.$$

Primjer 18. *Pronađimo rješenje sljedećeg sustava kongruencija*

$$\begin{aligned} x &\equiv 2 \pmod 4 \\ x &\equiv 1 \pmod 6. \end{aligned}$$

Rješenje: Metodom supstitucije prvu jednadžbu možemo zapisati kao: $x = 2 + 4k, k \in \mathbb{Z}$. *Sada ubacimo supstituciju u drugu jednadžbu:*

$$\begin{aligned} x &\equiv 1 \pmod 6 \\ 2 + 4k &\equiv 1 \pmod 6 \\ 4k &\equiv -1 \equiv 5 \pmod 6. \end{aligned}$$

Kako je $nzd(4, 6) = 2$, *a* $2 \nmid 5$, *slijedi da ova kongruencija nema rješenje, tj.ovaj sustav nema rješenje.*
Vidimo kako ne mora svaki sustav imati rješenje, iako svaka od jednadžbi zasebno ima. Sljedeći teorem će nam reći više o postojanju i jedinstvenosti rješenja.

Teorem 9 (vidjeti [2, Theorem 7.1.])**.** *Neka je* m *najmanji zajednički višekratnik brojeva* m_1 *i* m_2. *Uvjet za rješenje sustava kongruencija*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2} \end{aligned}$$

je

$$(m_1, m_2) \mid a_1 - a_2.$$

Ukoliko to vrijedi, tada sustav ima jedinstveno rješenje modulo m.

Dokaz. Za dokaz [vidjeti [2, Theorem 7.1.]] □

Kada dobijemo sustav kongruencija, prvo ćemo provjeriti prethodnim teoremom postoji li rješenje sustava. Ukoliko postoji, sljedeći korak nam je riješiti sustav. Jedna od metoda koju smo već spomenuli je metoda supstitucije.

Primjer 19. *Riješimo sustav kongruencija metodom supstitucije*

$$\begin{aligned} x &\equiv 53 \pmod{57} \\ x &\equiv 10 \pmod{13}. \end{aligned}$$

Rješenje: Pomoću prethodnog teorema provjerimo postoji li rješenje.
Kako je $(57, 13) = 1$, *a* $1 \mid 43$, *slijedi da sustav ima jedinstveno rješenje. Sada ćemo metodom supstitucije riješiti zadani sustav, Prvu jednadžbu možemo zapisati kao*

$$x = 53 + 57 \cdot p, p \in \mathbb{Z}.$$

Uvrstimo li taj x *u drugu jednadžbu dobivamo*

$$53 + 57 \cdot p \equiv 10 \pmod{13}.$$

Skratimo li 53 *i* 57 *modulo* 13, *dobivamo*

$$\begin{aligned} 1 + 5 \cdot p &\equiv 10 \pmod{13} \\ 5 \cdot p &\equiv 9 \pmod{13}. \end{aligned}$$

Množeći s 8 dobivamo:

$$40 \cdot p \equiv 72 \pmod{13}.$$

tj. skratimo li s modulo 13 *dobivamo*

$$p \equiv 7 \pmod{13}.$$

Tj. $p = 7 + 13r, r \in \mathbb{Z}$. *Vratimo li se u* x, *dobivamo*

$$\begin{aligned} x &= 53 + 57(7 + 13r) \\ x &= 53 + 399 + 741r \\ x &= 452 + 741r. \end{aligned}$$

Dakle, opće rješenje sustava je

$$x \equiv 452 \pmod{741}.$$

3.2 Sustavi n linearnih kongruencija

A što ako imamo sustav n linearnih kongruencije? Kako bismo ih onda riješili te postoji li uopće rješenje?

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{n_1} \\ a_2 x &\equiv b_2 \pmod{n_2} \\ &\vdots \\ a_n x &\equiv b_n \pmod{n_n}. \end{aligned}$$

Odgovor na to pitanje, daje nam sljedeći teorem.

3.2.1 Kineski teorem o ostatcima

Kada govorimo o sustavima kongruencija, jedno od najbitnijih pitanja je postoji li rješenje sustava. Odgovor na to pitanje, prvi nam je dao kineski matematičar Sun Tzua u teoremu kojeg nazivamo kineski teorem o ostatcima. Kažemo da je to jedan od fundamentalnih rezultata teorije brojeva. Teorem je u to vrijeme služio za prebrojavanje vojnika. Vojska bi se stala u blokove po $3, 4, 5, 7, 9, 11$ osoba. Tada bi se pomoću broja preostalnih vojnika iz posljednjeg reda dobivao sustav kongruencija modulo $3, 4, 5, 7, 9, 11$. Riješavajući takav sustav dobili bi kongruenciju iz koje bi dobili ukupan broj vojnika. Broj osoba u pojedinim redovima mogao se je promjeniti no trebalo je pripaziti da brojevi budu međusobno relativno prosti.Također produkt tih brojeva je trebao biti dovoljno velik kako bi se iz završne kongruencije mogao iščitati ispravan broj vojnika.
Sljedeći teorem, kineski teorem o ostatci upravo nam govori o postojanju rješenja sastava linearnih kongruencija.

Teorem 10 (vidjeti [4, Theorem 5.26.]). *(Kineski teorem o ostatcima) Neka su* $m_1, m_2, ..., m_r \in \mathbb{N}$ *u parovima relativno prosti, tj.*$(m_i, m_k) = 1$*, za* $i \neq k$*.*

Neka su $b_1, ..., b_r \in \mathbb{Z}$ *proizvoljni. Tada sustav kongruencija*

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_r \pmod{m_r} \end{aligned}$$

ima točno jedno rješenje modulo $m_1 \cdot m_2 \cdots m_r$

Dokaz. Prvo ćemo definirati $M = m_1 \cdot m_2 \cdots m_r$ te $M_k = M/m_k$. Tada $(M_k, m_k) = 1$ pa za $\forall M_k$ vrijedi da ima jedinstveni inverz M_k' modulo m_k. Neka je sada $x = b_1 M_1 M_1' + b_2 M_2 M_2' + \cdots + b_r M_r M_r'$. Pogledajmo sada članove prethodne sume modulo k. Kako vrijedi da je $M_i \equiv 0(\mod m_k)$ za $i \neq k$, slijedi da $x \equiv b_k M_k M_k' \equiv b_k \pmod{m_k}$. Iz ovoga možemo zaključiti kako x zadovoljava svaku kongruenciju u sustavu. Preostalo nam je sada pokazati da je to rješenje modulo M jedinstveno. Kada bi postojala dva rješenja, x i y, imala bismo $x \equiv y \pmod{m_k}$ $\forall k$. S obzirom na uvjet znamo da je $(m_i, m_k) = 1$ za $i \neq k$, iz toga slijedi kako je $x \equiv y \pmod{M}$. □

Dokaz Teorema 10 je konstruktivan i on govori kako da pronađemo rješenje sustava linearnih kongruencija. Sljedeći teorem je poopćenje prethodnog teorema.

Teorem 11 (vidjeti [4, Theorem 5.27.]). *Neka su $m_1, m_2, ..., m_r \in \mathbb{N}$ u parovima relativno prosti. Neka su $b_1, ..., b_r \in \mathbb{Z}$ proizvoljni te neka $a_1, ..., a_r$ zadovoljavaju $(a_k, m_k) = 1$ za $k = 1, 2, ..., r$. Tada linearan sustav kongruencija*

$$\begin{aligned} a_1 x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ a_r x &\equiv b_r \pmod{m_r} \end{aligned}$$

ima točno jedno rješenje modulo $m_1 \cdot m_2 \cdots m_r$.

Dokaz. Neka je a'_k recipročna vrijednost od broja a_k modulo m_k. Znamo da recipročna vrijednost postoji jer je $(a_k, m_k) = 1$. Iz toga znamo da je kongruencija $a_k x \equiv b_k \pmod{m_k}$ jednaka kongruenciji $x \equiv b_k a'_k \pmod{m_1}$ pa primijenimo prethodni teorem. □

Pogledajmo na sljedećem primjeru

Primjer 20. *Pronađimo rješenje sljedećeg sustava kongruencija:*

$$\begin{aligned} x &\equiv 2 \pmod 5 \\ x &\equiv 6 \pmod 7 \\ x &\equiv 1 \pmod 3. \end{aligned}$$

Rješenje: Vidimo kako je $(5, 7) = (7, 3) = (5, 3) = 1$. Sada primijenimo Teorem 10. $M = 5 \cdot 7 \cdot 3$.
$M_1 = \frac{5 \cdot 7 \cdot 3}{5} = 21$, $M_2 = \frac{5 \cdot 7 \cdot 3}{7} = 15$, $M_3 = \frac{5 \cdot 7 \cdot 3}{3} = 35$. Sada imamo linearne kongruencije:

$$\begin{aligned} 21x_1 \equiv 2 \pmod 5 &\iff x_1 \equiv 2 \pmod 5 \\ 15x_2 \equiv 6 \pmod 7 &\iff x_2 \equiv 6 \pmod 7 \\ 35x_3 \equiv 1 \pmod 3 &\iff 2x_3 \equiv 1 \pmod 3 \iff x_3 \equiv 3 \pmod 3. \end{aligned}$$

Dakle, rješenje polaznog sustava kongruencija je

$$\begin{aligned} x &\equiv 21 \cdot 2 + 15 \cdot 6 + 35 \cdot 3 \pmod{105} \\ x &\equiv 237 \pmod{105} \equiv 27 \pmod{105}. \end{aligned}$$

Ali što kada dobijemo zadatak gdje nam moduli kongruencija nisu u parovima relativno prosti brojevi? Pogledajmo na sljedećem primjeru.

Primjer 21. *Pronađimo rješenje sljedećeg sustava kongruencija:*

$$\begin{aligned} x &\equiv 14 \pmod{15} \\ x &\equiv 17 \pmod{21} \\ x &\equiv 24 \pmod{35}. \end{aligned}$$

Rješenje: Vidimo kako brojevi $15, 21, 35$ *nisu u parovima relativno prosti, pa ne smijemo koristiti kineski teorem o ostatcima dikrektno, ali možemo naći ekvivalentan sustav našemu ukoliko module razdvojimo kao potencije prostih brojeva:*

$$\begin{aligned} x \equiv 14 \pmod 3, x \equiv 17 \pmod 7, x \equiv 24 \pmod 5 \\ x \equiv 14 \pmod 5, x \equiv 17 \pmod 3, x \equiv 24 \pmod 7. \end{aligned}$$

Module smo zapisali u obliku potencija prostih brojeva. Sada nam još preostaje usporediti kongruencije koje imaju isti modul.
Ukoliko gledamo modulo 3 *imamo sljedeće:*

$$\begin{aligned} x \equiv 14 \pmod 3 &\iff x \equiv 2 \pmod 3 \\ x \equiv 17 \pmod 3 &\iff x \equiv 2 \pmod 3 \\ \Rightarrow x &\equiv 2 \pmod 3. \end{aligned}$$

Pogledajmo modulo 5*.*

$$\begin{aligned} x \equiv 14 \pmod 5 &\iff x \equiv 4 \pmod 5 \\ x \equiv 24 \pmod 5 &\iff x \equiv 4 \pmod 5 \\ \Rightarrow x &\equiv 4 \pmod 5. \end{aligned}$$

I još nam preostaje pogledati modulo 7*.*

$$\begin{aligned} x \equiv 17 \pmod 7 &\iff x \equiv 3 \pmod 7 \\ x \equiv 24 \pmod 7 &\iff x \equiv 3 \pmod 7 \\ \Rightarrow x &\equiv 3 \pmod 7. \end{aligned}$$

Sada smo dobili sustav:

$$\begin{aligned} x &\equiv 2 \pmod 3 \\ x &\equiv 4 \pmod 5 \\ x &\equiv 3 \pmod 7. \end{aligned}$$

Vidimo da su brojevi $3, 5, 7$ *u parovima relativno prosti brojevi pa možemo iskoristiti kineski teorem o ostatcima.* $M = 3 \cdot 5 \cdot 7 = 105$. $M_1 = 35, M_2 = 21, M_3 = 15$. *Iz ovoga dobivamo sljedeći sustav*

$$\begin{aligned} 35x_1 &\equiv 2 \pmod 3 \iff x_1 \equiv 1 \pmod 3 \\ 21x_2 &\equiv 4 \pmod 5 \iff x_2 \equiv 4 \pmod 5 \\ 15x_3 &\equiv 3 \pmod 7 \iff x_3 \equiv 3 \pmod 7. \end{aligned}$$

Dakle, naše rješenje jednako je $x \equiv 35 \cdot 1 + 21 \cdot 4 + 15 \cdot 3 \pmod{105}$ *tj.* $x \equiv 59 \pmod{105}$.

Inače, za sustav kongruencija $x \equiv a_i \pmod{n_i}$, *gdje je* $i = 1, 2, ..., r$ *te u kojem* n_i *nisu u parovima relativo prosti brojevi, kažemo da može, ali i ne mora imati rješenje.*

Pogledajmo sljedeći sustav.

Primjer 22. *Riješimo sustav kongruencija:*

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

Riješimo prvo prvu jednadžbu. Pomnožimo li je s 2 *dobivamo:*

$$\begin{aligned} 12x &\equiv 18 \pmod{11} \\ x &\equiv 7 \pmod{11}. \end{aligned}$$

Riješimo sada drugu jednadžbu. Množeći s 4 *dobivamo:*

$$\begin{aligned} 28x &\equiv 16 \pmod 9 \\ x &\equiv 7 \pmod 9. \end{aligned}$$

Sada nam je početni sustav istovjetan sljedećem sustavu

$$\begin{aligned} x &\equiv 7 \pmod{11} \\ x &\equiv 7 \pmod 9. \end{aligned}$$

Vidimo da je $(9, 11) = 1$ *što znači da možemo koristiti kineski teorem o ostatcima.* $M = 11 \cdot 9$. $M_1 = \frac{9 \cdot 11}{11} = 9$, $M_2 = \frac{9 \cdot 11}{9} = 11$. *Sada imamo linearne kongruencije:*

$$\begin{aligned} 9x_1 &\equiv 7 \pmod{11} \iff x_1 \equiv 2 \pmod{11} \\ 11x_2 &\equiv 7 \pmod{9} \iff x_2 \equiv 8 \pmod{9}. \end{aligned}$$

Dakle, rješenje polaznog sustava kongrunecija je $x \equiv 9 \cdot 2 + 11 \cdot 8 \pmod{99}$ *tj.* $x \equiv 106 \pmod{99} \equiv 7 \pmod{99}$.

Vidimo kako nam kineski teorem omugućava da računanje s velikim modulom zamjenimo s više neovisnih računanja s manjim modulom, što nam dosta pojednostavljuje računanje.
Kod riješavanja sustava dviju kongruencija koristili smo se i metodom supstitucije. Tu metodu također možemo koristiti i u sustavima 3 ili više kongruencija. Pogledajmo na sljedećem primjeru.

Primjer 23. *Riješimo sljedeći sustav:*

$$\begin{aligned} x &\equiv 3 \pmod{5} \\ x &\equiv 5 \pmod{7} \\ x &\equiv 7 \pmod{9}. \end{aligned}$$

Rješenje: Kako su $5, 7, 9$ *u parovima relativno prosti, znamo da će sustav imati jedinstveno rješenje modulo* 315. *Krenemo li od zadnje kongruencije, kongruencije s najvećim modulom, imamo da je* $x = 7 + 9k, k \in \mathbb{Z}$. *Ubacimo sada tu supstituciju u drugu jednadžbu:*

$$\begin{aligned} x &\equiv 5 \pmod{7} \\ 7 + 9k &\equiv 5 \pmod{7} \\ 2 + 4k &\equiv 5 \pmod{7} \\ 4k &\equiv 3 \pmod{7} \\ k &\equiv 6 \pmod{7}. \end{aligned}$$

Tj.$k = 6 + 7l, l \in \mathbb{Z}$. *Ubacimo li to u* x *dobivamo:*

$$x = 7 + 9(6 + 7l) = 7 + 54 + 63l = 61 + 63l.$$

Ubacimo sada tu supstituciju u prvu jednadžbu:

$$\begin{aligned} x &\equiv 3 \pmod 5 \\ 61 + 63l &\equiv 3 \pmod 5 \\ 1 + 3l &\equiv 3 \pmod 5 \\ 3l &\equiv 2 \pmod 5 \\ l &\equiv 4 \pmod 5. \end{aligned}$$

Odnosno, $l = 4 + 5m, m \in \mathbb{Z}$. *Uvrstimo li to u* x *dobivamo:*

$$\begin{aligned} x &= 61 + 63l = 61 + 63(4 + 5m) = 313 + 315m \\ x &\equiv 313 \pmod{315}. \end{aligned}$$

4 Primjena sustava kongruencija

U ovom poglavlju spomenuti ćemo par primjena sustava kongruencija. U prvom djelu reći ćemo nešto o RSA kriptosustavu i kakvu ulogu imaju sustavi kongruencija u njemu. U drugom djelu ćemo definirati polinomijalne kongruencije te pokazati kakva je uloga sustava kongruencija u njima.

4.1 RSA kriptosustav

RSA kriptosustav najpoznatiji kriptosustav s javnim ključem čije djelovanje je najšire korišteno. Stvoren je 1977.godine. Njegovi tvorci su Ronald Rivest, Adi Shamir i Leonard Adleman. Siguran je baš zbog teške faktorizacije velikih prirodnih brojva. Paramatrizacija mu se sastoji od modula n, koji je umnožak dvaju prirodnih velikih brojeva p i q, te eksponenti e i d. Eksponenti voju korist pronalaze u šifriranju i dešifriranju.

Više o RSA kriptosustavu može se vidjeti u [1]

Primjenu sustava kongruencija u RSA kriptosustavu možemo vidjeti kod napada na RSA s malim javnim eksponentom.

U početku, često se uzimao mali enkripcijski eksponent e, najčešće $e = 3$. Tako se minimiziralo vrijeme potrebno za šifriranje. No izbor takvog enkripcijskog eksponenta nije bio dobar izbor. Pogledajmo situaciju u kojoj imamo tri korisnika s različitim vrijednostima javnog modula n_1, n_2, n_3. Pretpostavit ćemo da se svi troje koriste javnim eksponentom $e = 3$. Netko im želi poslati identičnu poruku m. Njihov protivnik saznaje šifrate:

$$\begin{aligned} c_1 &\equiv m^3 \pmod{n_1} \\ c_2 &\equiv m^3 \pmod{n_2} \\ c_3 &\equiv m^3 \pmod{n_3}. \end{aligned}$$

Sada, pomoću kineskog teorema o ostatcima, može pronaći rješenje danog sustava linearnih kongruencija:

$$\begin{aligned} x &\equiv c_1 \pmod{n_1} \\ x &\equiv c_2 \pmod{n_2} \\ x &\equiv c_3 \pmod{n_3}. \end{aligned}$$

Protivnik dobiva da je $x \equiv m^3 \pmod{n_1n_2n_3}$*, a kako je* $m^3 < n_1n_2n_3$ *slijedi da je* $x = m^3$*. Izračunavanjem trećeg korijena iz* x *protivnik saznaje poruku* m*. Ovakve napada možemo izbjeći tako da prije šifriranja porukama doda neki "random pad", tj.slučajni dodatak. Tako izbjegavamo slanje identičnih poruka različitim primateljima.*

4.2 Polinomijalne kongruencije čiji je modul složen broj

Polinomijalne kongruencije su kongruencije oblika $f(x) \equiv 0 \pmod{m}$*, gdje je* $f(x)$ *polinom sa cjelobrojnim koeficijentima. Sljedeći teorem će nam reći kako polinomijalnu kongruenciju čiji je modul složen broj možemo rastaviti na sustav kongruencija čiji su moduli prosti brojevi, čiji umnožak čini dani složen broj.*

Teorem 12 (vidjeti [4, Theorem 5.28.])**.** *Neka je* f *polinom s cjelobrojnim koeficijentima, neka su* $m_1, m_2, ..., m_r \in \mathbb{N}$ *u parovima relativno prosti, te neka je* $m = m_1m_2 \cdots m_r$*. Tada kongruencija*

$$f(x) \equiv 0 \pmod{m} \tag{4.1}$$

ima rješenje akko svaka od kongruencija

$$f(x) \equiv 0 \pmod{m_i}, i = 1, 2, ..., r \tag{4.2}$$

ima rješenje. Štoviše, ako s $v(m)$ *označimo broj rješenja kongruencije* (4.1)*, a s* $v(m_i)$ *broj rješenja kongruencije* (4.2)*, tada je*

$$v(m) = v(m_1)v(m_2) \cdots v(m_r) \tag{4.3}$$

Dokaz. Dokaz se može naći u [4, Theorem 5.28.] □

Literatura

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

[2] *H.L. Keng, Introduction to Number Theory, Berlin Heidelberg, New York, 1982.*

[3] *W.Stein An Explicit Approach to Elementary Number Theory, Harvard University, Cambridge, 2001.*

[4] *T.M.Apostol, Introduction to Analytic Number Theory, Berlin Heidelberg, New York, 1982.*