Rješavanje kongruencija

Pejić, Ana Maria

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Ana Maria Pejić

Rješavanje kongruencija

Završni rad

Osijek, 2018.

Sveučilište J.J. Strossmayera u Osijeku
Odjel za matematiku
Sveučilišni preddiplomski studij matematike

Ana Maria Pejić

Rješavanje kongruencija

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2018.

Sažetak

U ovom završnom radu upoznat ćemo se s načinima i metodama rješavanja različitih tipova kongruencija. Na početku ćemo definirati sustave ostataka koji su nam vrlo bitni pri određivanju rješenja kongruencija. Nadalje, prikazat ćemo postupak rješavanja linearnih kongruencija, polinomijalnih kongruencija sa složenim modulima te polinomijalnih kongruencija s prostim potenciranim modulima. Navest ćemo te na primjerima primjenjivati Kineski teorem o ostatcima koji nam je koristan pri rješavanju sustava linearnih kongruencija. Također ćemo navesti i kroz primjere prikazati primjenu Fermatovog i Lagrangeovog teorema koji su nam korisni pri rješavanju kongruencija s prostim modulima.

Ključne riječi

Kongruencija, sustavi ostataka, prosti moduli

Solving congruences

Summary

In this final paper we will introduce ways and methods of solving different types of congruences. At the beginning we will define the residue systems, which are very important in obtaining solutions of congruences. Furthermore, the procedure of solving linear congruences, polynomial congruences with composite moduli and polynomial congruences with prime power moduli will be shown. We will cite The Chinese remainder theorem, which is very useful in solving simultaneous linear congruences, and apply it to examples. We will also cite and through examples present the applications of Fermat's and Lagrange's theorem, which are useful in solving congruences with prime moduli.

Key words

Congruence, residue systems, prime moduli

Sadržaj

Uvod

Gauss[1] nam je, u svome djelu *Disquisitiones arithmeticae*, predstavio zapis koji nam pojednostavljuje mnoge probleme vezane uz djeljivost cijelih brojeva, odnosno ***teoriju kongruencija***. U ovom radu bavit ćemo se rješavanjem kongruencija. Definirajmo kongruenciju te navedimo osnovna pravila:

Definicija 1. *Neka su a, b i m cijeli brojevi, $m > 0$. Kažemo da je a kongruentno b modulo m i pišemo*

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

ako m dijeli razliku $a - b$.

Drugim riječima, (1) je ekvivalentno $m \mid (a-b)$, odnosno m dijeli razliku $a-b$ ako i samo ako postoji cijeli broj h takav da je $a - b = m \cdot h$. Ako $m \nmid (a - b)$, onda a nije kongruentno b modulo m i pišemo $a \not\equiv b \,(\mathrm{mod}\, m)$.

Očigledno je $a \equiv 0 \,(\mathrm{mod}\, m)$ ako i samo ako $m \mid a$. Dodatno, $a \equiv b \,(\mathrm{mod}\, m)$ ako i samo ako $a - b \equiv 0 \,(\mathrm{mod}\, m)$.

Primjer 1.

1. $7 \equiv 4 \,(\mathrm{mod}\, 3)$, $11 \equiv 6 \,(\mathrm{mod}\, 5)$, $9 \equiv -3 \,(\mathrm{mod}\, 2)$
2. $4 \equiv 1 \,(\mathrm{mod}\, 3)$, $4 \equiv -2 \,(\mathrm{mod}\, 3)$.
3. $7 \equiv 1 \,(\mathrm{mod}\, 2)$, $7 \equiv 1 \,(\mathrm{mod}\, 3)$.
4. $a \equiv b \,(\mathrm{mod}\, 1)$, $\forall\, a$, b.

Napomena 1. *Iz Definicije 1 možemo lako iščitati sljedeća pravila za operacije s kongruencijama:*

a) *Ako je $a \equiv b \,(\mathrm{mod}\, m)$ i $b \equiv c \,(\mathrm{mod}\, m)$, tada je i $a \equiv c \,(\mathrm{mod}\, m)$.*
Naime, $a - b = h \cdot m$ i $b - c = h_1 \cdot m$ pa slijedi $a - c = (h + h_1) \cdot m$.

b) *Ako je $a \equiv b \,(\mathrm{mod}\, m)$ i $c \equiv d \,(\mathrm{mod}\, m)$, tada vrijedi $a \pm c \equiv b \pm d \,(\mathrm{mod}\, m)$.*
Jer je $a - b = h \cdot m$ i $c - d = h_1 \cdot m$, imamo $(a \pm c) - (b \pm d) = (h \pm h_1) \cdot m$.

c) *Ako je $a \equiv b \,(\mathrm{mod}\, m)$ i $c \equiv d \,(\mathrm{mod}\, m)$, tada je i $a \cdot c \equiv b \cdot d \,(\mathrm{mod}\, m)$.*
Kako je $a - b = h \cdot m$ i $c - d = h_1 \cdot m$, slijedi $a \cdot c - b \cdot d = (b \cdot h_1 + d \cdot h + h \cdot h_1 \cdot m) \cdot m$.

Uzmemo li c=d, imamo:

d) *Ako je $a \equiv b \,(\mathrm{mod}\, m)$, tada je i $a \cdot c \equiv b \cdot c \,(\mathrm{mod}\, m)$.*

Ponavljanjem pravila c), uz c=a i d=b, slijedi:

e) *Ako je $a \equiv b \,(\mathrm{mod}\, m)$, tada je $a^n \equiv b^n \,(\mathrm{mod}\, m), \forall\, n \in \mathbb{N}$.*

[1] Carl Friedrich Gauss (1777.-1855.), njemački matematičar i astronom.

Uzastopnom primjenom pravila e), d) i b) slijedi:

f) Ako je f(x) polinom s cjelobrojnim koeficijentima i ako je $a \equiv b \pmod{m}$*, tada je* $f(a) \equiv f(b) \pmod{m}$.

Prema pravilu d) iz Napomene 1, kongruencije možemo množiti proizvoljnim cijelim brojem, ali nije dozvoljeno dijeliti kongruencije svakim cijelim brojem čak i kada su kvocijenti cijeli brojevi. Na primjer, u kongruenciji

$$45 \equiv 9 \pmod{36}$$

brojevi 45 i 9 djeljivi su s 9, ali ako skratimo zajednički faktor 9 dobijemo netočan rezultat

$$5 \equiv 1 \pmod{36}.$$

Sljedeći teoremi reći će nam nešto o skraćivanju zajedničkih faktora članova kongruencija i dijeljenju kongruencija:

Teorem 1 (vidi [1, Chapter 5, Theorem 5.3.]). *Ako je* $c > 0$*, tada je*

$$a \equiv b \pmod{m} \text{ ako i samo ako } a \cdot c \equiv b \cdot c \pmod{m \cdot c}.$$

Dokaz: $m \mid (b-a)$ ako i samo ako $c \cdot m \mid c \cdot (b-a)$. □

Teorem 2 (vidi [1, Chapter 5, Theorem 5.4.]). *Ako je* $a \cdot c \equiv b \cdot c \pmod{m}$ *i ako je* $d = (m, c)$*, tada je*

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

Dokaz: Kako je $a \cdot c \equiv b \cdot c \pmod{m}$, imamo $m \mid c \cdot (a-b)$ pa slijedi $\frac{m}{d} \mid \frac{c}{d} \cdot (a-b)$. Dodatno, ako je $(\frac{m}{d}, \frac{c}{d}) = 1$, tj. $\frac{m}{d}$ i $\frac{c}{d}$ relativno prosti, tada $\frac{m}{d} \mid (a-b)$.

□

Budući da se u ovom radu bavimo rješavanjem kongruencija, napomenimo kako su sljedeći teoremi vrlo korisni pri rješavanju kongruencija:

Teorem 3 (vidi [1, Chapter 5, Theorem 5.5]). *Neka je* $a \equiv b \pmod{m}$*. Ako* $d \mid m$ *i* $d \mid a$*, tada* $d \mid b$.

Dokaz: Dovoljno je pretpostaviti da je $d > 0$. Ako $d \mid m$, tada $a \equiv b \pmod{m}$ implicira $a \equiv b \pmod{d}$. Ali ako $d \mid a$, tada je $a \equiv 0 \pmod{d}$ pa je $b \equiv 0 \pmod{d}$. □

Teorem 4 (vidi [1, Chapter 5, Theorem 5.6]). *Ako je* $a \equiv b \pmod{m}$*, tada je* $(a, m) = (b, m)$*. Drugim riječima, brojevi koji su kongruentni modulo m, s m imaju isti najveći zajednički djelitelj.*

Dokaz: Neka su $d = (a, m)$ i $e = (b, m)$. Tada $d \mid m$ i $d \mid a$ pa $d \mid b$; slijedi $d \mid e$. Analogno, $e \mid m, e \mid b$ pa $e \mid a$; slijedi $e \mid d$. Stoga je $d = e$. □

Teorem 5 (vidi [1, Chapter 5, Theorem 5.9]). *Ako je* $a \equiv b \pmod{m}$ *i* $a \equiv b \pmod{n}$ *uz* $(m, n) = 1$*, tada je* $a \equiv b \pmod{m \cdot n}$.

Dokaz: Budući da $m \mid (a-b)$ i $n \mid (a-b)$, onda i $m \cdot n \mid (a-b)$ jer je $(m, n) = 1$. □

1 Rješenja kongruencija i sustavi ostataka modulo m

Definicija 2. *Neka je $m > 0$. Označimo s $\hat{a}$ skup svih cijelih brojeva x takvih da vrijedi $x \equiv a \pmod{m}$. Tada $\hat{a}$ nazivamo klasa ostataka a modulo m.*

Takav $\hat{a}$ se sastoji od svih cijelih brojeva oblika $a + m \cdot q$, gdje je $q = 0, \pm 1, \pm 2, \ldots$.

Definicija 3. *Skup od m reprezentanata, po jednog iz svake klase ostataka $1, 2, \ldots, m$, naziva se potpun sustav ostataka modulo m.*

Teorem 6 (vidi [3, Chapter 3, Theorem 32])**.** *Ako su prirodni brojevi m i n relativno prosti te r cijeli broj, m brojeva*

$$r, n + r, 2n + r, \ldots, (m-1) \cdot n + r$$

čini potpun sustav ostataka modulo m.

Dokaz: Pokažimo da su $r, n + r, 2n + r, \ldots, (m-1) \cdot n + r$ nekongruentni modulo m. Ako pretpostavimo da $h \cdot n + r \equiv k \cdot n + r \pmod{m}$, $h \neq k$, tada je $(h - k) \cdot n \equiv 0 \pmod{m}$. Budući da je $(n, m) = 1$, slijedi $h \equiv k \pmod{m}$ što je u kontradikciji s pretpostavkom. □

Teorem 7 (vidi [1, Chapter 5, Theorem 5.11])**.** *Neka je $(k, m) = 1$. Ako je $a_1, \ldots, a_m$ potpun sustav ostataka modulo m, onda je i $ka_1, \ldots, ka_m$ također potpun sustav ostataka modulo m.*

Dokaz: Ako je $ka_i \equiv ka_j \pmod{m}$ tada je i $a_i \equiv a_j \pmod{m}$ jer je $(k, m) = 1$. Stoga ne postoje dva kongruentna elementa modulo m u skupu $ka_1, \ldots, ka_m$. Budući da je m elemenata u tom skupu, on tvori potpun sustav ostataka. □

Primjer 2. *Bilo koji skup od m cijelih brojeva, koji su nekongruentni modulo m, je potpun sustav ostataka modulo m. Na primjer, skupovi*

$$\{1, 2, \ldots, m\}; \qquad \{0, 1, 2, \ldots, m-1\};$$

$$\{1, m+2, 2m+3, 3m+4, \ldots, km+k+1\}$$

čine potpun sustav ostataka modulo m.

Neka je $f(x)$ polinom stupnja n s cjelobrojnim koeficijentima i neka je m dani modul. Svaki a za koji vrijedi $f(a) \equiv 0 \pmod{m}$ nazivamo rješenje kongruencije

$$f(x) \equiv 0 \pmod{m}. \tag{2}$$

Iz Napomene 1, pravilo f), slijedi da ako je a rješenje kongruencije (2), tada je svaki broj koji je kongruentan a modulo m također rješenje (2). Stoga možemo uzeti u obzir cijelu klasu takvih rješenja kao jedno rješenje kongruencije. To rješenje može biti reprezentirano bilo kojim brojem te klase. Svaki cijeli broj je kongruentan modulo m točno jednom broju niza

$$0, 1, 2, \ldots, m-1. \tag{3}$$

Da bismo riješili kongruenciju (2), ključno je odrediti koji broj iz niza (3) je rješenje te kongruencije. Dakle, vidimo da se (2) može riješiti u konačno mnogo pokušaja. To nam govori da, osim poteškoća tehničke prirode, kongruenciju (2) možemo ili riješiti ili pokazati da $f(x)$ nema rješenja. Broj rješenja kongruencija oblika (2), misleći na broj nekongruentnih rješenja, je broj iz skupa $1, 2, \ldots, m$ ili bilo kojeg drugog potpunog sustava ostataka modulo m. Dakle, svaka kongruencija oblika (2) ima najviše m mogućih rješenja.

Primjer 3. *Linearna kongruencija* $4x \equiv 7 \pmod 2$ *nema rješenja, budući da je* $4x - 7$ *uvijek neparan broj i takav nije djeljiv s 2.*

Primjer 4. *Linearna kongruencija* $4x \equiv 1 \pmod 3$ *ima točno jedno rješenje* $x \equiv 1 \pmod 3$.

Ako sustav ostataka modulo m sadrži broj koji je relativno prost s m, svi brojevi u skupu su relativno prosti s m. Za sustav ostataka s ovim svojstvom kažemo da je relativno prost s m. Definirajmo najprije Eulerovu φ-funkciju kako bismo mogli uvesti pojam reduciranog sustava ostataka modulo m.

Definicija 4. *Neka je m prirodan broj. S $\varphi(m)$ označavamo broj prirodnih brojeva manjih ili jednakih m koji su relativno prosti s m. Funkciju φ nazivamo Eulerova φ-funkcija.*

Sljedeće napomene navodimo bez dokaza, budući da navode pravila vezana uz Eulerovu φ-funkciju koja će nam biti korisna pri primjeni Eulerovog teorema kojeg ćemo navesti kasnije u tekstu.

Napomena 2 (vidi [1, Chapter 2, Theorem 2.5])**.**

a) $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1}$ *za p prost i $\alpha \geq 1$.*

b) $\varphi(mn) = \varphi(m)\varphi(n)(\frac{d}{\varphi(d)})$, *gdje je $d = (m, n)$.*

c) $\varphi(mn) = \varphi(m)\varphi(n)$ *ako je $(m, n) = 1$.*

d) $a \mid b$ *implicira* $\varphi(a) \mid \varphi(b)$.

e) $\varphi(n)$ *je paran za $n \geq 3$. Nadalje, ako n ima r neparnih prostih faktora, tada* $2^r \mid \varphi(n)$.

Dokaze nekih pravila iz prethodne napomene možete pronaći u [2, Chapter 6.1].

Napomena 3. *Ako je p prost tada je $\varphi(p) = p - 1$.*

Primjer 5. *Vrijedi:*

$$\varphi(3) = 2,\ \varphi(11) = 10.$$

Primjer 6. *Izračunajmo:*

a) $\varphi(21)$,

b) $\varphi(28)$.

Rješenje:

a) Kako je $21 = 7 \cdot 3$ te $(7, 3) = 1$, primjenom pravila c) iz Napomene 2 slijedi

$$\varphi(7 \cdot 3) = \varphi(7) \cdot \varphi(3).$$

Primjenimo li sada Napomenu 3, imamo $\varphi(7) = 6$ i $\varphi(3) = 2$, pa slijedi

$$\varphi(21) = 6 \cdot 2 = 12.$$

b) Kako je $28 = 4 \cdot 7 = 2^2 \cdot 7$ te $(7, 4) = 1$, primjenom pravila c) iz Napomene 2 slijedi

$$\varphi(4 \cdot 7) = \varphi(4) \cdot \varphi(7) = \varphi(2^2) \cdot \varphi(7).$$

Kada primjenimo pravilo a) iz Napomene 2 i Napomenu 3 slijedi

$$\varphi(28) = (4 - 2) \cdot 6 = 12.$$

Definicija 5. *Za reducirani sustav ostataka modulo m smatramo bilo koji skup od $\varphi(m)$ cijelih brojeva, koji su nekongruentni modulo m te svaki od njih relativno prost s m.*

Dakle, reducirani sustav ostataka modulo m je broj brojeva u nizu $1, 2, \ldots, m-1$ koji su relativno prosti s m.

Teorem 8 (vidi [1, Chapter 5, Theorem 5.17])**.** *Ako je $a_1, a_2, \ldots, a_{\varphi(m)}$ reducirani sustav ostataka modulo m i $(k, m) = 1$, onda je i $ka_1, ka_2, \ldots, ka_{\varphi(m)}$ također reducirani sustav ostataka modulo m.*

Dokaz: Ne postoje dva broja ka_i koja su nekongruentna modulo m. Također, kako je $(a_i, m) = (k, m) = 1$ imamo $(ka_i, m) = 1$ te je svaki ka_i relativno prost s m. □

Primjer 7. *Skup $\{1, 2, \ldots, 12\}$ je reducirani sustav ostataka modulo 13. Kako je $(2, 13) = 1$, slijedi da je i skup $\{2, 4, \ldots, 24\}$ reducirani sustav ostataka modulo 13.*

2 Linearne kongruencije

U ovom poglavlju opisat ćemo metodu rješavanja linearnih kongruencija pomoću Euklidovog algoritma. Navest ćemo i dokazati Kineski teorem o ostatcima te prikazati njegovu primjenu u rješavanju sustava linearnih kongruencija. Sljedećim teoremima je potpuno opisana teorija linearnih kongruencija koja će nam biti potrebna pri rješavanju primjera.

Teorem 9 (vidi [1, Chapter 5, Theorem 5.12])**.** *Neka je* $(a, m) = 1$*. Tada linearna kongruencija*

$$ax \equiv b \,(\mathrm{mod}\, m) \tag{4}$$

ima točno jedno rješenje.

Dokaz: Samo trebamo testirati brojeve $1, 2, \ldots, m$ budući da oni čine potpun sustav ostataka. Stoga formiramo produkte $a, 2a, \ldots, m \cdot a$. Budući da je $(a, m) = 1$ ti brojevi također čine potpun sustav ostataka. Dakle točno jedan od ovih produkata je kongruentan b modulo m. Što znači da točno jedan x zadovoljava (4). □

Primjer 8. *Pogledajmo kongruenciju* $8x \equiv 2 \,(\mathrm{mod}\, 5)$*. Kako je* $(8, 5) = 1$*, slijedi da dana kongruencija ima točno jedno rješenje i to* $x \equiv 4 \,(\mathrm{mod}\, 5)$*.*

Prethodni teorem nam govori da linearna kongruencija $ax \equiv b \,(\mathrm{mod}\, m)$ ima jedinstveno rješenje ako je $(a, m) = 1$, ali nam ne govori kako da odredimo to rješenje osim da redom testiramo brojeve potpunog sustava ostataka. Postoje mnogo brže metode za određivanje rješenja te ćemo ih obraditi u ovom radu.

Sljedeći teorem je poopćenje Teorema 9.

Teorem 10 (vidi [1, Chapter 5, Theorem 5.13])**.** *Neka je* $(a, m) = d$*. Tada linearna kongruencija*

$$ax \equiv b \,(\mathrm{mod}\, m) \tag{5}$$

ima rješenje ako i samo ako $d \mid b$*.*

Dokaz: Ako rješenje postoji, tada $d \mid b$ budući da $d \mid m$ i $d \mid a$. Suprotno, ako $d \mid b$ kongruencija

$$\frac{a}{d} \cdot x \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{m}{d} \right)$$

ima rješenje budući da je $\left(\frac{a}{d}, \frac{m}{d} \right) = 1$, te je to rješenje ujedno rješenje (5). □

Primjer 9. *Promotrimo kongruenciju* $3x \equiv 4 \,(\mathrm{mod}\, 6)$*. Budući da je* $(3, 6) = 3$ *te* $3 \nmid 4$*, slijedi da dana kongruencija nema rješenja.*

Primjer 10. *Pogledajmo sada kongruenciju* $14x \equiv 10 \,(\mathrm{mod}\, 4)$*. Kako je* $(14, 4) = 2$ *te* $2 \mid 10$*, slijedi da dana kongruencija ima rješenje i to su* $x \equiv 1 \,(\mathrm{mod}\, 4)$ *te* $x \equiv 3 \,(\mathrm{mod}\, 4)$*.*

Teorem 11 (vidi [1, Chapter 5, Theorem 5.14]). *Neka je $(a, m) = d$ i pretpostavimo da $d \mid b$. Tada linearna kongruencija*

$$ax \equiv b \,(\mathrm{mod}\, m) \tag{6}$$

ima točno d rješenja modulo m. Rješenja su dana s

$$t, t + \frac{m}{d}, t + 2\frac{m}{d}, \ldots, t + (d-1)\frac{m}{d}, \tag{7}$$

gdje je t rješenje jedinstveno modulo $\frac{m}{d}$ linearne kongruencije

$$\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{m}{d}\right). \tag{8}$$

Dokaz: Svako rješenje od (8) je ujedno i rješenje od (6). Suprotno, svako rješenje od (6) zadovoljava (8). Sada su d brojeva navedenih u (7) rješenja od (8), odnosno (6). Nikoja dva nisu kongruentna modulo m, budući da relacija

$$t + r\frac{m}{d} \equiv t + s\frac{m}{d} \,(\mathrm{mod}\, m), \;\; 0 \leq r < d, \, 0 \leq s < d$$

implicira

$$r\frac{m}{d} \equiv s\frac{m}{d} \,(\mathrm{mod}\, m),$$

stoga je $r \equiv s \,(\mathrm{mod}\, d)$. Ali je $0 \leq |r - s| < d$, pa je $r = s$. Preostaje nam pokazati da (6) nema drugih rješenja osim navedenih u (7). Ako je y rješenje od (6), tada je $ay \equiv at \,(\mathrm{mod}\, m)$ pa slijedi $y \equiv t \,(\mathrm{mod}\, \frac{m}{d})$. Stoga je $y = t + k\frac{m}{d}$, za neki k. Ali $k \equiv r \,(\mathrm{mod}\, d)$, za neki r koji zadovoljava $0 \leq r < d$. Stoga vrijedi

$$k\frac{m}{d} \equiv r\frac{m}{d} \,(\mathrm{mod}\, m), \;\; pa\, y \equiv t + r\frac{m}{d} \,(\mathrm{mod}\, m).$$

Dakle, y je kongruentno modulo m jednom od brojeva iz (7). □

Iako ćemo kasnije navesti detaljan postupak rješavanja linearnih kongruencija te primjeniti ga na primjerima, Teorem 11 ćemo ilustrirati na sljedećem primjeru:

Primjer 11. *Riješimo linearnu kongruenciju $32x \equiv 16 \,(\mathrm{mod}\, 20)$.*

Rješenje:
Znamo da je $(32, 20) = 4$. Kako $4 \mid 16$, prema Teoremu 11 slijedi da polazna kongruencija ima točno 4 rješenja modulo 20. Rješenja su $x \equiv 3, 3 + \frac{20}{4}, 3 + 2 \cdot \frac{20}{4}, 3 + 3 \cdot \frac{20}{4} \,(\mathrm{mod}\, 20)$, tj.

$$x \equiv 3, 8, 13, 18 \,(\mathrm{mod}\, 20),$$

gdje je 3 jedinstveno rješenje modulo 5 linearne kongruencije $8x \equiv 4 \,(\mathrm{mod}\, 5)$.

Teorem 12 (vidi [1, Chapter 5, Theorem 5.15]). *Ako je $(a, b) = d$, tada postoje cijeli brojevi x i y takvi da vrijedi*

$$ax + by = d. \tag{9}$$

Dokaz: Linearna kongruencija $ax \equiv d \,(\mathrm{mod}\, b)$ ima rješenje. Stoga postoji cijeli broj y takav da $d - ax = by$. Iz toga slijedi $ax + by = d$, što je bilo i potrebno dokazati. □

2.1 Rješavanje linearnih kongruencija

U ovom potpoglavlju prikazat ćemo postupak rješavanja linearnih kongruencija pomoću Teorema 6, 9 i 10 te primijeniti ga na nekoliko primjera. Bez dokaza navedimo *Euklidov algoritam*, budući nam je koristan pri rješavanju linearnih kongruencija:

Teorem 13 (Euklidov algoritam, [1, Chapter 1, Theorem 1.14])**.** *Neka su a i b pozitivni cijeli brojevi, gdje $b \nmid a$. Uzmimo $r_0 = a, r_1 = b$, i uzastopnim ponavljanjem Teorema o dijeljenju s ostatkom dobijemo skup ostataka $r_2, r_3, ..., r_n, r_{n+1}$ definiran redom relacijama*

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

Tada je r_n, posljednji nenul ostatak, jednak (a, b), tj. najvećem zajedničkom djelitelju brojeva a i b.

Neka je

$$ax \equiv b \,(\mathrm{mod}\, m) \tag{10}$$

i $d = (a, m)$. Primjenom određenih teorema možemo izvesti sljedeći postupak za rješavanje linearnih kongruencija.

- Postupak rješavanja:

  Izračunamo $d = (a, m)$.

  Ako $d \mid b$, prema Teoremu 11 slijedi da postoji d rješenja kongruencije (10) modulo m.

  Korak 1: Podijelimo kongruenciju (10) s d i imamo $\frac{a}{d}x \equiv \frac{b}{d} \left(\mathrm{mod}\, \frac{m}{d}\right)$.
  Uz nove oznake $a' = \frac{a}{d}$, $b' = \frac{b}{d}$ i $m' = \frac{m}{d}$ imamo

  $$a'x \equiv b' \,(\mathrm{mod}\, m'), \tag{11}$$

  pri čemu je $(a', m') = 1$.

  Korak 2: Vrijedi $(a', m') = 1$, pa prema Teoremu 12 postoje u i v takvi da je $a'u + m'v = 1$ te slijedi

  $$a'u \equiv 1 \,(\mathrm{mod}\, m').$$

  Primjenom *Euklidovog algoritma* odredimo u, v, pri čemu je u, prema Teoremu 9, jedinstveno rješenje kongruencije $a'u \equiv 1 \,(\mathrm{mod}\, m')$.

Korak 3: Prema Napomeni 1, pravilo d), vrijedi $a'(b'u) \equiv b' \pmod{m'}$. Tada su rješenja kongruencije (11) jednaka

$$x \equiv b'u \pmod{m'},$$

te uz oznaku $x_0 = b'u$, rješenja kongruencije (10) su

$$x \equiv x_0,\ x_0 + m', \ldots,\ x_0 + (d-1)m' \pmod{m}.$$

Pokažimo kako to funkcionira na sljedećim primjerima:

Primjer 12. *Riješimo linearnu kongruenciju* $60x \equiv 185 \pmod{455}$.

Rješenje:
Primjenom Euklidovog algoritma slijedi :

$$\begin{aligned} 455 &= 60 \cdot 7 + 35 \\ 60 &= 35 \cdot 1 + 25 \\ 35 &= 25 \cdot 1 + 10 \\ 25 &= 10 \cdot 2 + 5 \\ 10 &= 5 \cdot 2 \end{aligned}$$

Dakle, $(60, 455) = 5$ i $5 \mid 185$, pa slijedi da postoji 5 rješenja polazne kongruencije.
Podijelimo li polaznu kongruenciju s 5 dobivamo kongruenciju

$$12x \equiv 37 \pmod{91},$$

gdje je (12,91)=1. Prema Euklidovom algoritmu postoje u i v takvi da $12u + 91v = 1$, tj. $12u \equiv 1 \pmod{91}$.

$$\begin{aligned} 91 &= 12 \cdot 7 + 7 \\ 12 &= 7 \cdot 1 + 5 \\ 7 &= 5 \cdot 1 + 2 \\ 5 &= 2 \cdot 2 + 1 \\ 2 &= 1 \cdot 2 \end{aligned}$$

Primjenom rekurzivnih formula $u_{-1} = 0$, $u_0 = 1$, $u_i = u_{i-2} - u_{i-1} \cdot q_i$ slijedi nam tablica

i	-1	0	1	2	3	4
q_i	-	-	7	1	1	2
u_i	0	1	-7	8	-15	38

Dakle, $u \equiv 38 \pmod{91}$ je rješenje kongruencije $12u \equiv 1 \pmod{91}$.
Sada imamo $12(37u) \equiv 37 \pmod{91}$, pa je $37u$ rješenje kongruencije $12x \equiv 37 \pmod{91}$. Nadalje,

$$\begin{aligned} x_0 &\equiv 37u \pmod{91} \\ x_0 &\equiv 1406 \pmod{91} \\ x_0 &\equiv 41 \pmod{91} \end{aligned}$$

je jedno rješenje polazne kongruencije, pa su sva rješenja dana s

$$41,\ 41+91,\ 41+2\cdot 91,\ 41+3\cdot 91,\ 41+4\cdot 91 \pmod{455}.$$

Primjer 13. *Riješimo linearnu kongruenciju* $39x \equiv 6287 \pmod{826}$.

Rješenje:
Primjenom Euklidovog algoritma slijedi:

$$\begin{aligned} 826 &= 39\cdot 21 + 7 \\ 39 &= 7\cdot 5 + 4 \\ 7 &= 4\cdot 1 + 3 \\ 4 &= 3\cdot 1 + 1 \\ 3 &= 1\cdot 3 \end{aligned}$$

Dakle, $(39, 826) = 1$ i $1 \mid 6287$, pa slijedi da postoji 1 rješenje polazne kongruencije. Prema Euklidovom algoritmu postoje u i v takvi da $39u + 826v = 1$, tj. $39u \equiv 1 \pmod{826}$. Primjenom rekurzivnih formula $u_{-1} = 0$, $u_0 = 1$, $u_i = u_{i-2} - u_{i-1} \cdot q_i$ slijedi nam tablica

i	-1	0	1	2	3	4
q_i	-	-	21	5	1	1
u_i	0	1	-21	106	-127	233

Dakle, $u \equiv 233 \pmod{826}$ je rješenje kongruencije $39u \equiv 1 \pmod{826}$. Sada imamo $39(6287u) \equiv 6287 \pmod{826}$, pa je $6287u$ rješenje kongruencije $39x \equiv 6287 \pmod{826}$.
Dakle,

$$\begin{aligned} x &\equiv 6287u \pmod{826} \\ x &\equiv 1464871 \pmod{826} \\ x &\equiv 373 \pmod{826} \end{aligned}$$

je rješenje polazne kongruencije.

Još riješenih primjera linearnih kongruencija može se pronaći u [4].

2.2 Kineski teorem o ostatcima i sustavi kongruencija

Sustav dviju ili više linearnih kongruencija ne mora imati rješenje čak i ako svaka pojedina linearna kongruencija ima rješenje. Na primjer, ne postoji x koji zadovoljava

$$x \equiv 0 \,(\mathrm{mod}\, 6) \quad i \quad x \equiv 1 \,(\mathrm{mod}\, 3),$$

iako svaka od njih posebno ima rješenja. Moduli 3 i 6 nisu relativno prosti. Sljedećim teoremom pokazat ćemo da se svaki sustav dvaju ili više linearnih kongruencija, koje svaka odvojeno imaju jedinstveno rješenje, može riješiti ukoliko su moduli u parovima relativno prosti prirodni brojevi.

Teorem 14 (Kineski teorem o ostatcima, [1, Chapter 5, Theorem 5.26])**.** *Neka su $m_1, m_2, \ldots, m_r$ pozitivni cijeli brojevi, u parovima relativno prosti:*

$$(m_i, m_k) = 1, \quad za \quad i \neq k.$$

Neka su $b_1, b_2, \ldots, b_r$ proizvoljni cijeli brojevi. Tada sustav kongruencija

$$x \equiv b_1 \,(\mathrm{mod}\, m_1) \qquad x \equiv b_2 \,(\mathrm{mod}\, m_2) \qquad \ldots \qquad x \equiv b_r \,(\mathrm{mod}\, m_r) \tag{12}$$

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

Dokaz: Neka je $m = m_1 \cdot m_2 \cdots m_r$ i neka je $n_j = \frac{m}{m_j}$. Tada je $(m_j, n_j) = 1$, pa postoji cijeli broj x_j takav da je $n_j x_j \equiv b_j \,(\mathrm{mod}\, m_j)$. Promotrimo broj

$$x_0 = n_1 x_1 + \cdots + n_r x_r.$$

Za njega vrijedi: $x_0 \equiv 0 + \ldots 0 + n_j x_j + 0 + \cdots + 0 \equiv b_j \,(\mathrm{mod}\, m_j)$. Stoga je x_0 rješenje sustava kongruencija (12). Lako je pokazati da sustav kongruencija (12) ima samo jedno rješenje modulo m. Štoviše, ako su x i y dva rješenja sustava kongruencija (12), slijedi $x \equiv y \,(\mathrm{mod}\, m_j)$, za svaki j. Budući da su svi m_j u parovima relativno prosti, također slijedi $x \equiv y \,(\mathrm{mod}\, m)$. □

Sljedeći teorem je poopćenje Teorema 14.

Teorem 15 (vidi [1, Chapter 5, Theorem 5.27])**.** *Neka su $m_1, \ldots, m_r$ u parovima relativno prosti pozitivni cijeli brojevi, $b_1, \ldots, b_r$ proizvoljni cijeli brojevi te neka $a_1, \ldots, a_r$ zadovoljavaju*

$$(a_j, m_j) = 1, \; za \; j = 1, 2, \ldots, r.$$

Tada sustav linearnih kongruencija

$$a_1 x \equiv b_1 \,(\mathrm{mod}\, m_1) \qquad a_2 x \equiv b_2 \,(\mathrm{mod}\, m_2) \qquad \ldots \qquad a_r x \equiv b_r \,(\mathrm{mod}\, m_r)$$

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

Dokaz. Označimo s a_j' recipročnu vrijednost od a_j modulo m_j. On postoji jer je $(a_j, m_j) = 1$. Tada je kongruencija $a_j x \equiv b_j \,(\mathrm{mod}\, m_j)$ ekvivanelnta kongruenciji $x \equiv b_j a_j' \,(\mathrm{mod}\, m_j)$, pa jednostavno primjenimo Teorem 12. □

Pokažimo kako to funkcionira na primjeru:

Primjer 14. *Riješimo sustav kongruencija:*

$$x \equiv 5 \,(\mathrm{mod}\, 6), \qquad x \equiv 3 \,(\mathrm{mod}\, 10), \qquad x \equiv 8 \,(\mathrm{mod}\, 15).$$

Rješenje:
Budući da 6, 10, 15 nisu u parovima relativno prosti, ne možemo direktno primjeniti Kineski teorem o ostatcima. Naš sustav ekvivalentan je s

$$\begin{array}{lll} x \equiv 5 \,(\mathrm{mod}\, 2) & x \equiv 3 \,(\mathrm{mod}\, 2) & x \equiv 8 \,(\mathrm{mod}\, 3) \\ x \equiv 5 \,(\mathrm{mod}\, 3) & x \equiv 3 \,(\mathrm{mod}\, 5) & x \equiv 8 \,(\mathrm{mod}\, 5) \end{array}$$

Sada izdvojimo kongruencije čiji su moduli potencije istog prostog broja.

$$\begin{array}{rcl} x \equiv 5 \,(\mathrm{mod}\, 2) & \Leftrightarrow & x \equiv 1 \,(\mathrm{mod}\, 2) \\ x \equiv 3 \,(\mathrm{mod}\, 2) & \Leftrightarrow & x \equiv 1 \,(\mathrm{mod}\, 2) \end{array}$$

$$\begin{array}{rcl} x \equiv 5 \,(\mathrm{mod}\, 3) & \Leftrightarrow & x \equiv 2 \,(\mathrm{mod}\, 3) \\ x \equiv 8 \,(\mathrm{mod}\, 3) & \Leftrightarrow & x \equiv 2 \,(\mathrm{mod}\, 3) \end{array}$$

$$\begin{array}{rcl} x \equiv 3 \,(\mathrm{mod}\, 5) & & \\ x \equiv 8 \,(\mathrm{mod}\, 5) & \Leftrightarrow & x \equiv 3 \,(\mathrm{mod}\, 5) \end{array}$$

Sada imamo sustav kongruencija:

$$x \equiv 1 \,(\mathrm{mod}\, 2) \qquad x \equiv 2 \,(\mathrm{mod}\, 13) \qquad x \equiv 3 \,(mos\, 5)$$

gdje su 2, 3, 5 u parovima relativno prosti prirodni brojevi.

Uz oznake iz dokaza Teorema 14 slijedi $m = 2 \cdot 3 \cdot 5 = 30$ te $n_1 = 15$, $n_2 = 10$, $n_3 = 6$. Slijede nam linearne kongruencije s odgovarajućim rješenjima.

$$\begin{array}{ll} 15x_1 \equiv 1 \,(\mathrm{mod}\, 2) & x_1 \equiv 1 \,(\mathrm{mod}\, 2) \\ 10x_2 \equiv 2 \,(\mathrm{mod}\, 3) & x_2 \equiv 2 \,(\mathrm{mod}\, 3) \\ 6x_3 \equiv 3 \,(\mathrm{mod}\, 5) & x_3 \equiv 3 \,(\mathrm{mod}\, 5). \end{array}$$

Dakle, rješenje polaznog sustava kongruencija je

$$\begin{array}{rcl} x & \equiv & 15 \cdot 1 + 10 \cdot 2 + 6 \cdot 3 \,(\mathrm{mod}\, 30) \\ x & \equiv & 53 \,(\mathrm{mod}\, 30) \\ x & \equiv & 23 \,(\mathrm{mod}\, 30). \end{array}$$

3 Fermatov i Eulerov teorem

Fermatov teorem koji nam slijedi, poznat još kao *Mali Fermatov teorem*, bez dokaza je 1640. godine predstavio Pierre de Fermat[2]. Važna primjena Fermatovog teorema je u osnovnoj teoriji brojeva te kao test prostosti. Poseban je slučaj Eulerovog teorema, kojeg ćemo također iskazati u ovom poglavlju.

Teorem 16 (vidi [3, Chapter 3, Theorem 35.]). *Ako je p prost broj i a cijeli broj koji nije djeljiv s p, onda je razlika*

$$a^{p-1} - 1$$

djeljiva s p.

Drugim riječima, ako $p \nmid a$, onda vrijedi

$$a^{p-1} \equiv 1 \,(\mathrm{mod}\, p).$$

Specijelno za svaki cijeli broj a vrijedi

$$a^p \equiv a \,(\mathrm{mod}\, p).$$

Dokaz: Dovoljno je pokazati da je kongruencija

$$x^p \equiv x \,(\mathrm{mod}\, p)$$

rješiva za bilo koji cijeli broj x. Iz Napomene 1, pravilo f), slijedi da u obzir uzimamo samo vrijednosti $x = 0, 1, \ldots, p-1$. Provodimo matematičku indukciju. Kongruencija $x^p \equiv x \,(\mathrm{mod}\, p)$ vrijedi za $x = 0$. Pretpostavimo da vrijedi za $x = a$. Potrebno je pokazati da vrijedi i za $x = a + 1$. Binomni koeficijent

$$\binom{p}{k} = \frac{p(p-1)\cdots(p-\cdots-k+1)}{k!}$$

je očigledno djeljiv s p za $k = 1, 2, \ldots, p-1$. Stoga je

$$(a+1)^p = a^p + 1 + \sum_{k=1}^{p-1} \binom{p}{k} a^k \equiv a^p + 1 \equiv a + 1 \,(\mathrm{mod}\, p).$$

□

Prvi dokaz Teorema 16 je predstavio Euler[3] 1736. godine. On je kasnije postavio općenitiji rezultat:

Teorem 17 (Eulerov teorem,[3, Chapter 3, Theorem 36.]). *Ako je a prirodan broj te $(a, m) = 1$, tada vrijedi*

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

[2]Pierre de Fermat (1607.-1665), francuski matematičar i pravnik, jedan od najznačajnijih matematičara 17. stoljeća.

[3]Leonhard Euler (1707.-1783.), švicarski matematičar, fizičar i astronom.

Dokaz: Uzmimo da je $\varphi = \varphi(m)$. Neka je $a_a, a_2, \ldots, a_\varphi$ reducirani sustav ostataka modulo m. Tada su brojevi

$$a_1 a, \ldots, a_\varphi a$$

evidentno nekongruentni modulo m i relativno prosti s m. Stoga oni također formiraju reducirani sustav ostataka modulo m. Dakle, uzimajući produkt, imamo

$$a_1 a \cdot a_2 a \cdots a_\varphi a \equiv a_1 a_2 \cdots a_\varphi \,(\mathrm{mod}\, m)$$

te ako svaku stranu podijelimo produktom brojeva a_i možemo zaključiti da vrijedi

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

□

Primjer 15. *Dokažimo da*

$$27 \mid 49^{95} + 113^{41}.$$

Rješenje:
Označimo $49^{95} + 113^{41} = A$. Vrijedi li

$$A \equiv 0 \,(\mathrm{mod}\, 27)?$$

Lako dođemo do zaključka da je

$$49 \equiv 22 \,(\mathrm{mod}\, 27), \qquad (49, 27) = 1.$$

Sada primjenom pravila iz Napomene 2 slijedi

$$\begin{aligned} \varphi(27) &= \varphi(3^3) \\ &= 3^3 - 3^2 \\ &= 18. \end{aligned}$$

Primjenom *Eulerovog teorema* slijedi

$$49^{18} \equiv 1 \,(\mathrm{mod}\, 27).$$

Nadalje, uz pravilo e) iz Napomene 1 vrijedi:

$$\begin{aligned} 49^{95} &\equiv (49^{18})^5 \cdot 49^5 \,(\mathrm{mod}\, 27) \\ &\equiv 1^5 \cdot 49^5 \,(\mathrm{mod}\, 27) \\ &\equiv 22^5 \,(\mathrm{mod}\, 27) \\ &\equiv 7 \,(\mathrm{mod}\, 27). \end{aligned}$$

Sada imamo

$$113 \equiv 5 \,(\mathrm{mod}\, 49)$$

te primjenom *Eulerovog teorema* slijedi:

$$113^{18} \equiv 1 \,(\mathrm{mod}\, 49).$$

Analogno zaključujemo

$$\begin{aligned} 113^{41} &\equiv (113^{18})^2 \cdot 5^5 \,(\mathrm{mod}\, 27) \\ &\equiv 1^2 \cdot 5^5 \,(\mathrm{mod}\, 27) \\ &\equiv 20 \,(\mathrm{mod}\, 27). \end{aligned}$$

Stoga je $49^{95} + 113^{41} \equiv 7 + 20 \equiv 0 \,(\mathrm{mod}\, 27)$.

Primjer 16. *Odredimo ostatak pri dijeljenju broja* 3^{42} *brojem* 19.

Rješenje:
Problem ostataka pri dijeljenju jednog broja drugim rješavamo pomoću kongruencija. Primjenom
Fermatovog teorema imamo

$$3^{18} \equiv 1 \,(\mathrm{mod}\, 19).$$

Sada možemo pisati

$$\begin{aligned} 3^{42} &\equiv (3^{18})^2 \cdot 3^6 \,(\mathrm{mod}\, 19) \\ &\equiv 1^2 \cdot 729 \,(\mathrm{mod}\, 19) \\ &\equiv 7 \,(\mathrm{mod}\, 19). \end{aligned}$$

Dakle, ostatak pri dijeljenju 3^{19} brojem 19 iznosi 7.

Primjer 17. *Koristeći Eulerov teorem riješimo kongruenciju*

$$36x \equiv 5 \,(\mathrm{mod}\, 49).$$

Rješenje:
Kako je $(36, 49) = 1$, možemo primjeniti Eulerov teorem. Iz Napomene 2 slijedi

$$\begin{aligned} \varphi(49) &= \varphi(7^2) \\ &= 7^2 - 7 \\ &= 42. \end{aligned}$$

Eulerov teorem nam kaže da vrijedi

$$36^{42} \equiv 1 \,(\mathrm{mod}\, 49).$$

Pomnožimo li $36x \equiv 5 \,(\mathrm{mod}\, 49)$ s 36^{41} imamo

$$36^{42}x \equiv 36^{41} \cdot 5 \,(\mathrm{mod}\, 49).$$

Kako je $36^{42} \equiv 1 \pmod{49}$ vrijedi $x \equiv 36^{41} \cdot 5 \pmod{49}$. Sada je potrebno odrediti ostatak pri dijeljenju 36^{41} brojem 49. Primjenom pravila iz Napomena 2 i 3 slijedi

$$\begin{aligned} 36^{41} &\equiv (36^3)^{10} \cdot (36^3)^3 \cdot 36^2 \pmod{49} \\ &\equiv (8^5)^2 \cdot 8^3 \cdot 22 \pmod{49} \\ &\equiv 36^2 \cdot 22 \cdot 22 \pmod{49} \\ &\equiv 22 \cdot 22 \cdot 22 \pmod{49} \\ &\equiv 15 \pmod{49}. \end{aligned}$$

Prema tome,

$$x \equiv 15 \cdot 5 \equiv 26 \pmod{49}.$$

4 Lagrangeov teorem i polinomijalne kongruencije

Osnovni teorem algebre govori nam da svaki polinom f stupnja $n \geq 1$ s jednadžbom $f(x) = 0$ ima n nultočaka među kompleksnim brojevima. Ne postoji analogan teorem za kongruencije. Na primjer, vidjeli smo da neke linearne kongruencije nemaju rješenje, neke imaju jedinstveno rješenje a neke više od jednog rješenja. Iako se čini kako ne postoji poveznica između broja rješenja kongruencija i stupnja polinoma, ako imamo polinomijalnu kongruenciju modulo neki prost broj, sljedeći teorem nam može reći nešto o broju rješenja takve kongruencije.

Teorem 18 (Lagrangeov[4] teorem,[1, Chapter 5, Theorem 5.21])**.** *Neka je p prost i neka je*

$$f(x) = c_0 + c_1 x + \cdots + c_n x^n$$

polinom stupnja n s cjelobrojnim koeficijentima c_i takvima da je $c_n \not\equiv 0 \pmod p$. Tada kongruencija

$$f(x) \equiv 0 \pmod p \tag{13}$$

ima najviše n rješenja.

Napominjemo da ovaj zaključak ne vrijedi za složene module. Na primjer, kvadratna kongruencija $x^2 \equiv 1 \pmod 8$ ima 4 rješenja.

Dokaz: Dokaz slijedi indukcijom. Kada je $n = 1$ kongruencija je linearna:

$$c_1 x + c_0 \equiv 0 \pmod p.$$

Kako je $c_1 \not\equiv 0 \pmod p$, imamo $(c_1, p) = 1$ i postoji točno jedno rješenje. Pretpostavimo da je teorem valjan za polinom stupnja $n-1$. Pretpostavimo također da kongruencija (13) ima $n+1$ nekongruentno rješenje modulo p, npr.

$$x_0,\, x_1, \ldots,\, x_n,$$

gdje je $f(x_k) \equiv 0 \pmod p$, za svaki $k = 0,\, 1, \ldots,\, n$. Trebali bismo doći do kontradikcije. Imamo algebarski identitet

$$f(x) - f(x_0) = \sum_{r=1}^{n} c_r (x^r - x_0^r) = (x - x_0) g(x),$$

gdje je $g(x)$ polinom stupnja $n-1$ s cjelobrojnim koeficijentima i vodećim koeficijentom c_n. Stoga imamo

$$f(x_k) - f(x_0) = (x_k - x_0) g(x_k) \equiv 0 \pmod p,$$

budući da je $f(x_k) \equiv f(x_0) \equiv 0 \pmod p$. Ali $x_k - x_0 \not\equiv 0 \pmod p$ za $k \neq 0$ pa moramo imati $g(x_k) \equiv 0 \pmod p$, za svaki $k \neq 0$. To znači da kongruencija $g(x) \equiv 0 \pmod p$ ima n nekongruentnih rješenja modulo p, što je kontradiktorno našoj pretpostavci. Time smo dokazali teorem. □

[4] Joseph-Louis Lagrange (1736.-1813.), talijanski matematičar i astronom.

Primjer 18. *Riješimo kongruenciju*

$$2x^3 + x^2 + 5x - 1 \equiv 0 \,(\mathrm{mod}\, 7)$$

Rješenje:
Prema prethodnom teoremu dana kongruencija ima najviše 3 rješenja. Pronađimo rješenja:

$$\begin{aligned}
x = 0: &\quad 2x^3 + x^2 + 5x - 1 &\equiv& \;-1 \,(\mathrm{mod}\, 7)\\
x = 1: &\quad 2x^3 + x^2 + 5x - 1 &\equiv& \;0 \,(\mathrm{mod}\, 7)\\
x = 2: &\quad 2x^3 + x^2 + 5x - 1 &\equiv& \;1 \,(\mathrm{mod}\, 7)\\
x = 3: &\quad 2x^3 + x^2 + 5x - 1 &\equiv& \;0 \,(\mathrm{mod}\, 7)\\
x = 4: &\quad 2x^3 + x^2 + 5x - 1 &\equiv& \;2 \,(\mathrm{mod}\, 7)\\
x = 5: &\quad 2x^3 + x^2 + 5x - 1 &\equiv& \;5 \,(\mathrm{mod}\, 7)\\
x = 6: &\quad 2x^3 + x^2 + 5x - 1 &\equiv& \;0 \,(\mathrm{mod}\, 7).
\end{aligned}$$

Dakle, rješenja polazne kongruencije su $x \equiv 1,\, 3,\, 6 \,(\mathrm{mod}\, 7)$.

Primjer 19. *Riješimo kongruenciju*

$$5x^{99} + x^3 + 2x - 3 \equiv 0 \,(\mathrm{mod}\, 5).$$

Rješenje:
Kako je vodeći koeficijent djeljiv s 5, dana kongruencija je ekvivalentna s

$$x^3 + 2x - 3 \equiv 0 \,(\mathrm{mod}\, 5)$$

te ima najviše 3 rješenja. Pronađimo rješenje:

$$\begin{aligned}
x = 0: &\quad x^3 + 2x - 3 &\equiv& \;-3 \,(\mathrm{mod}\, 5)\\
x = 1: &\quad x^3 + 2x - 3 &\equiv& \;0 \,(\mathrm{mod}\, 5)\\
x = 2: &\quad x^3 + 2x - 3 &\equiv& \;4 \,(\mathrm{mod}\, 5)\\
x = 3: &\quad x^3 + 2x - 3 &\equiv& \;0 \,(\mathrm{mod}\, 5)\\
x = 4: &\quad x^3 + 2x - 3 &\equiv& \;4 \,(\mathrm{mod}\, 5).
\end{aligned}$$

Dakle, rješenja polazne kongruencije su $x \equiv 1,\, 3 \,(\mathrm{mod}\, 5)$.

Teorem 19 (vidi [1, Chapter 5, Theorem 5.22])**.** *Ako je $f(x) = c_0 + c_1 x + \cdots + c_n x^n$ polinom stupnja n s cjelobrojnim koeficijentima i ako kongruencija*

$$f(x) \equiv 0 \,(\mathrm{mod}\, p)$$

ima više od n rješenja a p je prost broj, tada je svaki koeficijent od f djeljiv s p.

Dokaz: Ako postoji koeficijent koji nije djeljiv s p, neka c_k bude takav s najvećim indexom. Tada je $k \leq n$ i kongruencija

$$c_0 + c_1 x + \cdots + c_k x^k \equiv 0 \,(\mathrm{mod}\, p)$$

ima više od k rješenja, pa prema Lagrangeovom teoremu, $p \mid c_k$, što je kontradikcija. □

Primjer 20. *Riješimo kongruenciju*

$$135x^2 - 51x + 237 \equiv 0 \,(\mathrm{mod}\, 0).$$

Rješenje:
Prema Teoremu 18 dana kongruencija ima najviše 2 rješenja. Pronađimo rješenja:

$$\begin{aligned} x = 0: \quad & 135x^2 - 51x + 237 \equiv 0 \,(\mathrm{mod}\, 3) \\ x = 1: \quad & 135x^2 - 51x + 237 \equiv 0 \,(\mathrm{mod}\, 3) \\ x = 2: \quad & 135x^2 - 51x + 237 \equiv 0 \,(\mathrm{mod}\, 3). \end{aligned}$$

Rješenja polazne kongruencije su $x \equiv 0,\ 1,\ 2 \,(\mathrm{mod}\, 5)$. Dakle, broj rješenja je veći od stupnja polinoma pa prema Teoremu 19 slijedi da $3 \mid 135$, $3 \mid (-51)$, $3 \mid 237$.

Teorem 20 (vidi [1, Chapter 5, Theorem 5.23])**.** *Za svaki prost p svi koeficijenti polinoma*

$$f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$$

djeljivi su s p.

Dokaz: Neka je $g(x) = (x-1)(x-2)\cdots(x-p+1)$. Nultočke polinoma g su $1,\ 2, \ldots,\ p-1$, stoga zadovoljavaju kongruenciju

$$g(x) \equiv 0 \,(\mathrm{mod}\, p).$$

Prema Eulerovom teoremu, ovi brojevi zadovoljavaju i kongruenciju $h(x) \equiv 0 \,(\mathrm{mod}\, p)$, gdje je

$$h(x) = x^{p-1} - 1.$$

Razlika polinoma $f(x) = g(x) - h(x)$ je polinom stupanja $p-2$ ali kongruencija $f(x) \equiv 0 \,(\mathrm{mod}\, p)$ ima $p-1$ rješenja, $1, \ldots,\ p-1$. Stoga, prema Teoremu 19, svaki koeficijent od $f(x)$ djeljiv je s p. □

Primjer 21. *Ilustrirajmo Teorem 20 na sljedećem primjeru:*

a) $f(x) = (x-1)(x-2)(x-3)(x-4) - x^4 + 1$,

b) $g(x) = (x-1)(x-2)(x-3)(x-4)(x-5)(x-6) - x^6 + 1$.

Rješenje:

a) Polinom f ekvivalentan je polinomu $F(x) = -10x^3 + 35x^2 - 50x + 25$. Vidljivo je da su svi koeficijenti polinoma djeljivi brojem 5.

b) Polinom g ekvivalentan je polinomu $G(x) = -21x^5 + 175x^4 - 735x3 + 1624x^2 - 1764x + 721$. Kao u prethodnim primjerima lako možemo provjeriti uvrštavanjem u polinom g da kongruencija $-21x^5 + 175x^4 - 735x3 + 1624x^2 - 1764x + 721 \equiv 0 \,(\mathrm{mod}\, 7)$ ima više od 5 rješenja. Prema Teoremu 19 svi koeficijenti polinoma G, odnosno g djeljivi su brojem 7.

4.1 Polinomijalne kongruencije sa složenim modulima

U sljedećem teoremu prikazat ćemo primjenu Kineskog teorema o ostatcima na polinomijalne kongruencije sa složenim modulima.

Teorem 21 (vidi [1, Chapter 5, Theorem 5.28])**.** *Neka je f polinom s cjelobrojnim koeficijentima i neka su $m_1, m_2, \ldots, m_r$ pozitivni, cijeli i u parovima relativno prosti brojevi te neka je $m = m_1 m_2 \cdots m_r$. Tada kongruencija*

$$f(x) \equiv 0 \,(\mathrm{mod}\, m) \tag{14}$$

ima rješenje ako i samo ako svaka od kongruencija

$$f(x) \equiv 0 \,(\mathrm{mod}\, m_i), \qquad i = 1, 2, \ldots, r \tag{15}$$

ima rješenje. Nadalje, ako $v(m)$ i $v(m_i)$ označavaju broj rješenja (14) i (15), tada vrijedi

$$v(m) = v(m_1)v(m_2)\cdots v(m_r).$$

Dokaz: Ako $f(a) \equiv 0 \,(\mathrm{mod}\, m)$ tada je $f(a) \equiv 0 \,(\mathrm{mod}\, m_i)$, za svaki i. Stoga je svako rješenje kongruencije (14) ujedno i rješenje od (15). Obrnuto, neka je a_i rješenje kongruencije (15). Tada prema Kineskom teoremu o ostatcima postoji cijeli broj a takav da je

$$a \equiv a_i \,(\mathrm{mod}\, m_i), \quad za \quad i = 1, 2, \ldots, r. \tag{16}$$

pa je

$$f(a) \equiv f(a_i) \equiv 0 \,(\mathrm{mod}\, m_i).$$

Kako su moduli u parovima relativno prosti, također imamo $f(a) \equiv 0 \,(\mathrm{mod}\, m)$. Stoga, ako svaka od kongruencija (15) ima rješenje, onda ima i kongruencija (14). Također, iz Kineskog teorema o ostatcima znamo da svaka $r-torka$ rješenja $(a_1, \ldots, a_r)$ kongruencija (15) dovodi do jedinstvenog cijelog broja a modulo m koji zadovoljava kongruencije (16). Kako svaki a_i prolazi kroz $v(m_i)$ rješenja kongruencija (15), broj cijelih brojeva koji zadovoljavaju kongruencije (16), stoga i kongruencije (15) je $v(m_1)\cdots v(m_r)$. □

Primjer 22. *Riješimo kongruenciju*

$$x^3 + 2x - 3 \equiv 0 \,(\mathrm{mod}\, 45).$$

Rješenje:
Kako je $(9, 5) = 1$, danu kongruenciju možemo rastaviti na

$$x^3 + 2x - 3 \equiv 0 \,(\mathrm{mod}\, 5),$$

$$x^3 + 2x - 3 \equiv 0 \,(\mathrm{mod}\, 9).$$

Kongruenciju $x^3 + 2x - 3 \equiv 0 \,(\mathrm{mod}\, 5)$ smo riješili u jednom od prethodnih primjera i njena rješenja su $x \equiv 1,\, 3 \,(\mathrm{mod} 5)$. Na analogan način preostaje nam riješiti kongruenciju $x^3 + 2x - 3 \equiv 0 \,(\mathrm{mod}\, 9)$. Imamo:

$$\begin{aligned}
x = 0: &\qquad x^3 + 2x - 3 &\equiv& \;\; -3 \,(\mathrm{mod}\, 9)\\
x = 1: &\qquad x^3 + 2x - 3 &\equiv& \;\; 0 \,(\mathrm{mod}\, 9)\\
x = 2: &\qquad x^3 + 2x - 3 &\equiv& \;\; 0 \,(\mathrm{mod}\, 9)\\
x = 3: &\qquad x^3 + 2x - 3 &\equiv& \;\; 3 \,(\mathrm{mod}\, 9)\\
x = 4: &\qquad x^3 + 2x - 3 &\equiv& \;\; 6 \,(\mathrm{mod}\, 9)\\
x = 5: &\qquad x^3 + 2x - 3 &\equiv& \;\; 6 \,(\mathrm{mod}\, 9)\\
x = 6: &\qquad x^3 + 2x - 3 &\equiv& \;\; 0 \,(\mathrm{mod}\, 9).
\end{aligned}$$

Dakle, rješenja su $x \equiv 1,\, 2,\, 6 \,(\mathrm{mod}\, 9)$.

Sada kombiniranjem prethodnih rješenja, imamo 6 sustava linearnih kongruencija koji se rješavaju primjenom Kineskog teorema o ostatcima na način koji smo prikazali na primjeru u Potpoglavlju 2.2.

1. $x \equiv 1 \,(\mathrm{mod}\, 5) \qquad x \equiv 1 \,(\mathrm{mod}\, 9) \quad \Rightarrow\; x \equiv 1 \,(\mathrm{mod}\, 45).$
2. $x \equiv 1 \,(\mathrm{mod}\, 5) \qquad x \equiv 2 \,(\mathrm{mod}\, 9) \quad \Rightarrow\; x \equiv 11 \,(\mathrm{mod}\, 45).$
3. $x \equiv 1 \,(\mathrm{mod}\, 5) \qquad x \equiv 6 \,(\mathrm{mod}\, 9) \quad \Rightarrow\; x \equiv 6 \,(\mathrm{mod}\, 45).$
4. $x \equiv 3 \,(\mathrm{mod}\, 5) \qquad x \equiv 1 \,(\mathrm{mod}\, 9) \quad \Rightarrow\; x \equiv 28 \,(\mathrm{mod}\, 45).$
5. $x \equiv 3 \,(\mathrm{mod}\, 5) \qquad x \equiv 2 \,(\mathrm{mod}\, 9) \quad \Rightarrow\; x \equiv 38 \,(\mathrm{mod}\, 45).$
6. $x \equiv 3 \,(\mathrm{mod}\, 5) \qquad x \equiv 6 \,(\mathrm{mod}\, 9) \quad \Rightarrow\; x \equiv 33 \,(\mathrm{mod}\, 45).$

Stoga su sva rješenja polazne kongruencije dana s $x \equiv 1,\, 6,\, 11,\, 28,\, 33,\, 38 \,(\mathrm{mod}\, 5)$.

4.2 Polinomijalne kongruencije s modulima koji su potencije prostog broja

Neka je f polinom s cjelobrojnim koeficijentima i pretpostavimo da za neki prosti broj p i za neki $\alpha \geq 2$ kongruencija

$$f(x) \equiv 0 \,(\mathrm{mod}\, p^{\alpha}) \tag{17}$$

ima rješenje, $x \equiv a \,(\mathrm{mod}\, p^{\alpha})$, gdje a biramo tako da se nalazi u intervalu

$$0 \leq a < p^{\alpha}.$$

Dakle, neka je $x = a$. To rješenje također zadovoljava kongruencije $f(x) \equiv 0 \,(\mathrm{mod}\, p^{\beta})$ za svaki $\beta < \alpha$. Posebno, a zadovoljava kongruenciju

$$f(x) \equiv 0 \,(\mathrm{mod}\, p^{\alpha-1}). \tag{18}$$

Sada podijelimo a s $p^{\alpha-1}$ i pišemo

$$a = qp^{\alpha-1} + r, \quad 0 \leq r < p^{\alpha-1}, \quad q \in \mathbb{Z}. \tag{19}$$

Za ostatak r definiran s (19) kažemo da je *generiran* s a. Kako je $r \equiv a \pmod{p^{\alpha-1}}$, broj r je također rješenje kongruencije (18). Drugim riječima, svako rješenje a kongruencije (17) u intervalu $0 \leq a < p^{\alpha}$ generira rješenje r kongruencije (18) u intervalu $0 \leq a < p^{\alpha-1}$. Počnimo s rješenjem kongruencije (18) na intervalu $0 \leq a < p^{\alpha-1}$ i sada se pitamo postoji li rješenje a kongruencije (17) u intervalu $0 \leq a < p^{\alpha}$ koje generira r. Ako postoji, kažemo da r možemo podići sa $p^{\alpha-1}$ na p^{α}. Sljedeći teorem pokazat će nam kako podizanje broja r ovisi o $f(r)$ modulo p^{α} i derivaciji $f'(r)$ modulo p.

Teorem 22 (vidi [1, Chapter 5, Theorem 5.30])**.** *Pretpostavimo da je $\alpha \geq 2$ i neka je $0 \leq r < p^{\alpha-1}$ rješenje kongruencije*

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}. \tag{20}$$

a) Pretpostavimo da je $f'(r) \not\equiv 0 \pmod{p}$. Tada r na jedinstven način možemo podići s $p^{\alpha-1}$ na $p^{\alpha-1}$. Dakle, postoji jedinstveni a u intervalu $0 \leq a < p^{\alpha}$ koji generira r i koji zadovoljava kongruenciju

$$f(x) \equiv 0 \pmod{p^{\alpha}}. \tag{21}$$

b) Pretpostavimo da je $f'(r) \equiv 0 \pmod{p}$. Tada imamo dvije mogućnosti:

b_1) Ako je $f(r) \equiv 0 \pmod{p^{\alpha}}$, r može biti podignut s $p^{\alpha-1}$ na p^{α} na p različitih načina.

b_2) Ako je $f(r) \not\equiv 0 \pmod{p^{\alpha}}$, r ne može biti podignut s $p^{\alpha-1}$ na p^{α}.

Dokaz: Ako je f stupnja n, imamo Taylorovu formulu

$$f(x+h) = f(x) + f'(x)h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^{(n)}(x)}{n!}h^n, \tag{22}$$

za svaki x i h. Naglasimo da svaki polinom $\frac{f^{(k)}(x)}{k!}$ ima cjelobrojne koeficijente. Uzmimo sada da je $x = r$ u (22), gdje je r rješenje od (20) u intervalu $0 \leq r < p^{\alpha-1}$ i neka je $h = qp^{\alpha-1}$, gdje je q cijeli broj. Kako je $\alpha \geq 2$ uvjeti u (22) uključuju h^2 i veće potencije od h su cjelobrojni višekratnici od p^{α}. Stoga iz (22) slijedi kongruencija

$$f(r + qp^{\alpha-1}) \equiv f(r) + f'(r)qp^{\alpha-1} \pmod{p^{\alpha}}.$$

Budući da r zadovoljava (20), možemo pisati $f(r) = kp^{\alpha-1}$, za neki cijeli broj k, te posljednja kongruencija postaje oblika

$$f(r + qp^{\alpha-1}) \equiv (qf'(r) + k)p^{\alpha-1} \pmod{p^{\alpha}}.$$

Neka je sada

$$a = r + qp^{\alpha-1}. \tag{23}$$

Tada a zadovoljava kongruenciju (21) ako i samo ako q zadovoljava linearnu kongruenciju

$$qf'(r) + k \equiv 0 \,(\mathrm{mod}\, p). \tag{24}$$

Ako je $f'(r) \not\equiv 0 \,(\mathrm{mod}\, p)$ prethodna kongruencija ima jedinstveno rješenje q mod p, te ako izaberemo q u intervalu $0 \leq q < p$ tada će broj a dan s (23) zadovoljavati kongruenciju (21) i nalazit će se u intervalu $0 \leq a < p^{\alpha}$. S druge strane, ako je $f'(r) \equiv 0 \,(\mathrm{mod}\, p)$, tada kongruencija (24) ima rješenje q ako i samo ako $p \mid k$, dakle ako i samo ako je $f(r) \equiv 0 \,(\mathrm{mod}\, p^{\alpha})$. Ako $p \nmid k$, ne postoji q kojeg možemo izabrati tako da a zadovoljava kongruenciju (21). Ali ako $p \mid k$, tada p vrijednosti $q = 0, 1, \ldots, p-1$ daju p rješenja a kongruencije (21) koji generiraju r i nalaze se u intervalu $0 \leq a < p^{\alpha}$. Time smo dokazali tvrdnju. □

Dokaz prethodnog teorema otkriva nam metodu za pronalaženje rješenja kongruencije (21) ako su nam poznata rješenja kongruencije (20). Uzastopnim ponavljanjem metode, problem svodimo na problem rješavanja kongruencije

$$f(x) \equiv 0 \,(\mathrm{mod}\, p).$$

Ako ta kongruencija nema rješenja, onda ni kongruencija (21) nema rješenja, a ako ima rješenja, izaberemo jedno rješenje koje se nalazi u intervalu $0 \leq r < p$ te ga nazovemo r. Ekvivalento rješenju r, bit će 0, 1 ili p rješenja kongruencije

$$f(x) \equiv 0 \,(\mathrm{mod}\, p^2), \tag{25}$$

što ovisi o brojevima $f'(r)$ i $k = \frac{f(r)}{p}$. Ako $p \nmid k$ i $p \mid f'(r)$, onda r ne može biti podignut do rješenja kongruencije (25). U tom slučaju počinjemo iznova s drugim rješenjem r. Ako ne postoji niti jedan takav r, kongruencija (25) nema rješenja. Ako $p \mid k$ za neki r, rješavamo linearnu kongruenciju

$$qf'(r) + k \equiv 0 \,(\mathrm{mod}\, p).$$

Ona ima 1 ili p rješenja q jer $p \nmid f'(r)$ ili $p \mid f'(r)$. Za svako rješenje q broj $a = r + qp$ daje nam rješenje kongruencije (25). Za svako rješenje kongruencije (25) možemo koristiti sličnu metodu pri pronalasku rješenja kongruencije

$$f(x) \equiv 0 \,(\mathrm{mod}\, p^3),$$

i tako dalje, dok ne dobijemo sva rješenja kongruencije (21).

Primjer 23 (vidi [4, Poglavlje 2, Zadatak 2.5.]). *Riješimo kongruenciju*

$$x^3 + x^2 - 5 \equiv 0 \,(\mathrm{mod}\, 7^3).$$

Rješenje:
Najprije riješimo kongruenciju

$$x^3 + x^2 - 5 \equiv 0 \,(\mathrm{mod}\, 7).$$

Već prikazanim postupkom dobijemo $x \equiv 2 \pmod 7$. Neka je $f(x) = x^3 + x^2 - 5$. Tada je $f'(x) = 3x^2 + 2x$ te slijedi $f'(2) = 16 \not\equiv 0 \pmod 7$. Sada možemo primjeniti prethodni teorem. Da bismo riješili kongruenciju $x^3 + x^2 - 5 \equiv 0 \pmod{7^2}$ trebamo riješiti

$$t \cdot f'(a) \equiv -\frac{f(a)}{7} \pmod 7, \quad 0 \leq t < 7, \quad za \quad a = 2.$$

Dobijemo kongruenciju $t \cdot 16 \equiv -1 \pmod 7$ i $t = 3$. Tada je $a + t \cdot 7 = 23$. Da bismo riješili polaznu kongruenciju trebamo riješiti kongruenciju

$$t \cdot f'(a) \equiv -\frac{f(a)}{49} \pmod 7, \quad 0 \leq t < 7, \quad za \quad a = 23.$$

Slijedi nam $t \cdot 16 \equiv -259 \pmod 7$ i $t = 0$. Stoga je $a + t \cdot 49 = 23$. Prema tome, rješenje polazne kongruencije je $x \equiv 23 \pmod{7^3}$.

Primjer 24. *Riješimo kongruenciju*

$$x^3 + x - 11 \equiv 0 \pmod{3^3}.$$

Rješenje:
Najprije riješimo kongruenciju

$$x^3 + x - 11 \equiv 0 \pmod 3.$$

Već prikazanim postupkom dobijemo $x \equiv 1 \pmod 3$. Neka je $f(x) = x^3 + x - 11$. Tada je $f'(x) = 3x^2 + 1$ te slijedi $f'(1) = 4 \not\equiv 0 \pmod 3$. Sada možemo primjeniti prethodni teorem. Da bismo riješili kongruenciju $x^3 + x - 11 \equiv 0 \pmod{3^2}$ trebamo riješiti

$$t \cdot f'(a) \equiv -\frac{f(a)}{3} \pmod 3, \quad 0 \leq t < 3, \quad za \quad a = 1.$$

Dobijemo kongruenciju $t \cdot 4 \equiv 3 \pmod 3$ i $t = 0$. Tada je $a + t \cdot 3 = 1$. Da bismo riješili polaznu kongruenciju trebamo riješiti kongruenciju

$$t \cdot f'(a) \equiv -\frac{f(a)}{9} \pmod 3, \quad 0 \leq t < 3, \quad za \quad a = 1.$$

Slijedi nam $t \cdot 4 \equiv 1 \pmod 3$ i $t = 1$. Stoga je $a + t \cdot 9 = 10$. Prema tome, rješenje polazne kongruencije je $x \equiv 10 \pmod{3^3}$.

Literatura

[1] T. M. Apostol, *Introduction to Analytic Number Theory*, Springer-Verlag, New York, 1976.

[2] W. Sierpinski, *Elementary Theory of Numbers*, North Holland, Amsterdam, 1988.

[3] T. Nagell, *Introduction to Number Theory*, John Wiley and sons, New York, 1950.

[4] A. Dujella, *Uvod u teoriju brojeva*, PMF - Matematički odjel, Sveučilište u Zagrebu, skripta.