Kongruencije

Rajkovača, Monika

Master's thesis / Diplomski rad

2022

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **Josip Juraj Strossmayer University of Osijek, Department of Mathematics / Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:126:223303

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij Financijska matematika i statistika

Monika Rajkovača

Kongruencije

Diplomski rad

Osijek, 2022.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku
Diplomski studij Financijska matematika i statistika

Monika Rajkovača

Kongruencije

Diplomski rad

Mentor: prof. dr. sc. Ivan Matić

Osijek, 2022.

Sadržaj

Uvod

Uz kongruencije vežemo ime jednog velikog matematičkog genija – Johanna Carla Friedricha Gaussa (1777.-1855.). Gauss je tijekom studija matematike napisao djelo *Istraživanja u aritmetici (lat. Disquisitiones arithmeticae).* Djelo je završeno 1798. godine, a objavljeno 1801. Upravo tim djelom Gauss je postavio temelje suvremenoj teoriji brojeva. Nazvan je i *Princem matematike* zbog svojih doprinosa istoj.
Prije nego su *Istraživanja* bila objavljena, teoriju brojeva činio je niz teorema i pretpostavki koji nisu bili povezani ni u kakvu cjelinu. On je spojio i sistematizirao rad svojih prethodnika te dodao mnoštvo svojih zaključaka. Ovo je prvo djelo koje je dobilo logičan slijed i strukturu te su to kasnije koristili i drugi. Na prvoj stranici spomenutog djela, predstavio je teoriju kongruencija. Uveo je definiciju te zapis kongruencije kakav koristimo i danas. Time je pridonio pojednostavljenju mnogih problema koji se tiču djeljivosti cijelih brojeva.
U prvom poglavlju navest ćemo definiciju kongruencije koju nam je dao Gauss u svom djelu još početkom devetnaestog stoljeća. Dokazat ćemo svojstva te uvidjeti zašto je ovaj *Princ* uveo baš ovakvu oznaku za kongruenciju. Kroz drugo poglavlje upoznat ćemo se s pojmom klase ostataka te potpunim sustavom ostataka. Nakon toga, u trećem poglavlju promatrat ćemo najjednostavnije polinomijalne kongruencije - linearne kongruencije te egzistenciju i broj njihovih rješenja. Osim Gaussa, još je nekoliko vrsnih matematičara čija su otkrića navedena u *Istraživanjima u aritmetici* – Fermat, Euler, Lagrange. U četvrtom poglavlju uvest ćemo pojam reduciranog sustava ostataka te iskazati i dokazati Euler-Fermatov teorem. U petom poglavlju objasnit ćemo Lagrangeov teorem, a u šestom prikazati njegove primjene. U sedmom poglavlju bavit ćemo se sustavima linearnih kongruencija te Kineskim teoremom o ostatcima čije ćemo primjene navesti u poglavlju broj 8. U devetom poglavlju pokazat ćemo kako možemo reducirati problem rješavanja polinomijalnih kongruencija. Kroz posljednja dva poglavlja iskazat ćemo i dokazati teorem o prebrojavanju skupova koji se naziva Princip unakrsne klasifikacije te pokazati kako se pomoću tog principa može napraviti dekompozicija reduciranih sustava ostataka.

1. Definicija i osnovna svojstva

Za početak, uvest ćemo pojam i oznaku kongruencije te osnovna svojstva.
Cijeli brojevi (pozitivni, negativni ili nula) bit će označeni malim latiničnim slovima i malim slovima grčke abecede.

Definicija 1.1. *Neka su dani cijeli brojevi a i b te prirodan broj m. Kažemo da je a kongruentan b modulo m u oznaci*

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

ako m dijeli razliku brojeva a i b. Broj m naziva se modul kongruencije.

Drugim riječima, kongruencija (1) ekvivalentna je relaciji djeljivosti

$$m \mid (a - b).$$

Posebno, $a \equiv 0 \pmod{m}$ ako i samo ako m dijeli cijeli broj a. Stoga, $a \equiv b \pmod{m}$ ako i samo ako $a - b \equiv 0 \pmod{m}$.
Ako broj m ne dijeli razliku brojeva a i b kažemo da su a i b nekongruentni modulo m i pišemo $a \not\equiv b \pmod{m}$.

Primjer 1.1. *(a)* $5 \equiv 2 \pmod{3}$

(b) $22 \equiv 10 \pmod{12}$

(c) $1 \equiv -1 \pmod{2}$

(d) $3^2 \equiv -1 \pmod{5}$

(e) n je paran ako i samo ako je $n \equiv 0 \pmod{2}$

(f) n je neparan ako i samo ako je $n \equiv 1 \pmod{2}$

(g) $a \equiv b \pmod{1}$*, za sve a i b*

(h) Ako je $a \equiv b \pmod{m}$*, onda je* $a \equiv b \pmod{d}$ *kada* $d \mid m$*, pri čemu je* $d > 0$.

Oznaku za kongruenciju $\equiv$ također je uveo Gauss kako bi sugerirao na analogiju s oznakom za jednakost $=$. U sljedeća dva teorema pokazat ćemo da kongruencije uistinu posjeduju mnoga svojstva nalik svojstvima jednakosti.

Teorem 1.1. ([1, Teorem 5.1]) *Kongruencija je relacija ekvivalencije. To jest, vrijedi:*

- *refleksivnost:* $a \equiv a \pmod{m}$
- *simetričnost:* $a \equiv b \pmod{m}$ *implicira* $b \equiv a \pmod{m}$
- *tranzitivnost:* $a \equiv b \pmod{m}$ *i* $b \equiv c \pmod{m}$ *implicira* $a \equiv c \pmod{m}$.

Dokaz. Dokaz je trivijalan, a slijedi direktno iz svojstava djeljivosti:

- refleksivnost: $m \mid 0$.
- simetričnost: ako m dijeli razliku brojeva a i b $(a - b)$, onda m dijeli i razliku brojeva b i a $(b - a)$.
- tranzitivnost: ako m dijeli razliku brojeva a i b $(a - b)$ i ako dijeli razliku brojeva b i c $(b-c)$, onda dijeli i njihovu linearnu kombinaciju, odnosno $m \mid ((a-b)+(b-c)) = (a-c)$.

□

Teorem 1.2. ([1, Teorem 5.2]) *Neka je* $a \equiv b \pmod{m}$ *i* $\alpha \equiv \beta \pmod{m}$. *Tada vrijedi:*
(a) $ax + \alpha y \equiv bx + \beta y \pmod{m}$, *za sve* $x, y \in \mathbb{Z}$,
(b) $a\alpha \equiv b\beta \pmod{m}$,
(c) $a^n \equiv b^n \pmod{m}$, *za svaki* $n \in \mathbb{N}$,
(d) $f(a) \equiv f(b) \pmod{m}$, *za svaki polinom* f *s cjelobrojnim koeficijentima.*

Dokaz. (a) Budući da $m \mid (a-b)$ i $m \mid (\alpha - \beta)$ imamo

$$m \mid x(a-b) + y(\alpha - \beta) = (ax + \alpha y) - (bx + \beta y).$$

(b) $a\alpha - b\beta = \alpha(a-b) + b(\alpha - \beta) \equiv 0 \, (mod\ m)$ prema dijelu (a).
(c) Tvrdnja slijedi matematičkom indukcijom uvrštavanjem $\alpha = a$ i $\beta = b$ u dio (b).
(d) Tvrdnja slijedi matematičkom indukcijom do stupnja polinoma f koristeći se dijelom (c). □

Teorem 1.2 govori nam da se dvije kongruencije promatrane modulo isti broj mogu zbrajati, oduzimati ili množiti, član po član, na isti način kao što to možemo raditi s jednadžbama. Ista svojstva vrijede i za bilo koji konačan broj kongruencija s istim modulom.
Razmotrimo sada jedan primjer kojim ćemo ilustrirati korisnost tih svojstava.

Primjer 1.2. ([1, Primjer 1, str. 108]) ***Kriterij djeljivosti brojem 9.*** *Prirodan broj* n *djeljiv je brojem* 9 *ako i samo ako je zbroj znamenki tog broja djeljiv brojem 9. Ovo svojstvo se lako dokaže koristeći kongruencije. Ako su znamenke broja* n *u decimalnom zapisu* $a_0, a_1, ..., a_k$, *tada* n *možemo zapisati u obliku*

$$n = a_0 + 10a_1 + 10^2 a_2 + \cdots + 10^k a_k.$$

Koristeći Teorem 1.2 imamo:

$$\begin{aligned} 10 &\equiv 1 \pmod{9}, \\ 10^2 &\equiv 1 \pmod{9}, \\ &\vdots \\ 10^k &\equiv 1 \pmod{9} \end{aligned}$$

iz čega slijedi

$$n \equiv a_0 + a_1 + \cdots + a_k \pmod{9}.$$

Primijetimo da sve ove kongruencije također sadrže i modulo 3. Pa prema tome, broj je djeljiv brojem 3 ako i samo ako je zbroj njegovih znamenki djeljiv brojem 3.
Sada ćemo nastaviti s daljnjim razvijanjem svojstava kongruencija. Zajednički ne-nul faktori ne mogu uvijek biti izlučeni iz obaju članova kongruencije kao što mogu u jednadžbama. Pogledajmo na primjeru.

Primjer 1.3. *U kongruenciji* $48 \equiv 18 \pmod{10}$ *oba člana su djeljiva brojem 6, ali ukoliko bismo izlučili zajednički faktor 6, dobili bismo* $8 \equiv 3 \pmod{10}$, *što nije točno.*

U teoremu koji slijedi pokazat ćemo da zajednički faktor može biti izlučen ukoliko je modul također djeljiv tim faktorom.

Teorem 1.3. ([1, Teorem 5.3]) *Ako je* c *prirodan broj, onda vrijedi* $a \equiv b \pmod{m}$ *ako i samo ako je* $ac \equiv bc \pmod{mc}$.

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

Sljedeći teorem opisuje zakon izlučivanja koji se može koristiti u slučaju kada modul nije djeljiv zajedničkim faktorom.

Teorem 1.4. ([1, Teorem 5.4]) ***Zakon izlučivanja.*** *Ako je* $ac \equiv bc \pmod{m}$ *i* $d = (m, c)$, *tada*

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

Drugim riječima, zajednički faktor c *može se izlučiti pod uvjetom da je modul djeljiv najvećim zajedničkim djeliteljem brojeva* m *i* c. *Posebno, zajednički faktor koji je relativno prost s modulom uvijek se može izlučiti.*

Dokaz. Zbog $ac \equiv bc \pmod{m}$ vrijedi

$$m \mid c(a-b)$$

pa

$$\frac{m}{d} \;\Big|\; \frac{c}{d}(a-b).$$

Ali $(\frac{m}{d}, \frac{c}{d}) = 1$ pa $\frac{m}{d} \mid (a-b)$. □

Teorem 1.5. ([1, Teorem 5.5]) *Pretpostavimo da je* $a \equiv b \pmod{m}$. *Ako* d *dijeli* m *i* d *dijeli* a, *onda* d *dijeli i* b.

Dokaz. Možemo uzeti da je $d > 0$. Ako $d \mid m$ onda $a \equiv b \pmod{m}$ implicira da vrijedi $a \equiv b \pmod{d}$. Ali ako $d \mid a$ onda je $a \equiv 0 \pmod{d}$ pa je i $b \equiv 0 \pmod{d}$, odnosno d dijeli b. □

Teorem 1.6. ([1, Teorem 5.6]) *Ako je* $a \equiv b \pmod{m}$, *onda vrijedi* $(a, m) = (b, m)$. *Odnosno, brojevi kongruentni modulo* m *imaju jednake najveće zajedničke djelitelje s* m.

Dokaz. Označimo s d najveći zajednički djelitelj brojeva a i m, a s e najveći zajednički djelitelj brojeva b i m. Tada d dijeli m i d dijeli a pa prema prethodnom teoremu d dijeli i b; dakle, vrijedi i $d \mid e$. Na isti način dolazimo do toga da vrijedi i obratno. Stoga, $d = e$. □

Teorem 1.7. ([1, Teorem 5.7]) *Ako je* $a \equiv b \pmod{m}$ *i* $0 \leq |b-a| < m$, *tada je* $a = b$.

Dokaz. Iz $m \mid (a-b)$ proizlazi da je $m \leq |a-b|$ osim ako je $a - b = 0$. □

Teorem 1.8. ([4, Teorem 1.4]) *Vrijedi* $a \equiv b \pmod{m}$ *ako i samo ako* a *i* b *daju isti ostatak pri dijeljenju s* m.

Dokaz. Zapišimo a i b u obliku $a = mq + r$, $b = mQ + R$, pri čemu su $0 \leq r < m$ i $0 \leq R < m$. Zatim, $a - b = mq + r - mQ - R \equiv r - R \pmod{m}$ i $0 \leq |r - R| < m$. Sada primijenimo Teorem 1.7 i dolazimo do tvrdnje. □

Teorem 1.9. ([1, Teorem 5.9]) *Ako je* $a \equiv b \pmod{m}$ *i* $a \equiv b \pmod{n}$ *pri čemu je* $(m, n) = 1$, *tada vrijedi* $a \equiv b \pmod{mn}$.

Dokaz. Obzirom da i m i n dijele razliku $a - b$, onda i njihov produkt dijeli tu razliku zbog toga što su relativno prosti. □

2. Klase ostataka i potpuni sustavi ostataka

U ovom poglavlju, definirat ćemo klasu ostataka modulo m, navesti odgovarajuća svojstva te definirati potpuni sustav ostataka modulo m.

Definicija 2.1. *Neka je $m > 0$ fiksni modul. S $\hat{a}$ označavamo skup svih $x \in Z$ za koje vrijedi $x \equiv a \pmod{m}$ te $\hat{a}$ nazivamo klasom ostataka a modulo m.*

Prema tome, $\hat{a}$ je skup svih cijelih brojeva oblika $a + mq$, gdje je $q = 0, \pm 1, \pm 2, \ldots$ Sljedeća svojstva klasa ostataka su posljedice ove definicije.

Teorem 2.1. ([1, Teorem 5.10]) *Za dani modul m imamo:*
(a) $\hat{a} = \hat{b}$ ako i samo ako $a \equiv b \pmod{m}$.
(b) Dva cijela broja x i y su u istoj klasi ostataka ako i samo ako $x \equiv y \pmod{m}$.
(c) Klase ostataka $\hat{1}, \hat{2}, \ldots, \hat{m}$ međusobno su disjunktne i njihova unija je čitav skup $\mathbb{Z}$.

Dokaz. Dijelovi (a) i (b) slijede direktno iz definicije.
Da bismo dokazali dio (c), primijetimo da su brojevi $0, 1, 2, \ldots, m-1$ nekongruentni modulo m (prema Teoremu 1.7). Dakle, prema (b) dijelu ovog teorema klase ostataka

$$\hat{0}, \hat{1}, \hat{2}, \ldots, \widehat{m-1}$$

su disjunktne. Ali svaki $x \in Z$ mora biti točno u jednoj od ovih klasa zbog $x = qm + r$ gdje je $0 \leq r < m$ pa je $x \equiv r \pmod{m}$ i $x \in \hat{r}$. Budući da je $\hat{0} = \hat{m}$, tvrdnja (c) je dokazana. □

Definicija 2.2. *Skup koji se sastoji od m predstavnika, svaki od kojih pripada drugoj klasi ostataka $\hat{1}, \hat{2}, \ldots, \hat{m}$ nazivamo potpuni sustav ostataka modulo m.*

Svaki skup koji se sastoji od m cijelih brojeva, nikoja dva od kojih nisu međusobno kongruentni modulo m, je potpuni sustav ostataka modulo m. Primjer koji slijedi prikazuje potpune sustave ostataka modulo m.

Primjer 2.1. *(a)* $\{1, 2, \ldots, m\}$

(b) $\{0, 1, 2, \ldots, m-1\}$

(c) $\{1, 2, 3, 4, 5\}$

(d) $\{0, 1, 2, 3, 4\}$

Teorem 2.2. ([3, Lema 2.1.7.]) *Pretpostavimo da $(k, m) = 1$. Ako je $\{a_1, \ldots, a_m\}$ potpuni sustav ostataka modulo m, onda je i $\{ka_1, \ldots, ka_m\}$ potpuni sustav ostataka modulo m.*

Dokaz. Ako vrijedi $ka_i \equiv ka_j \pmod{m}$, onda vrijedi i $a_i \equiv a_j \pmod{m}$ obzirom na to da su brojevi k i m relativno prosti. Prema tome, nikoja dva elementa u skupu $\{ka_1, \ldots, ka_m\}$ nisu međusobno kongruentna modulo m. Budući da se u ovom skupu nalazi m elemenata, oni tvore potpuni sustav ostataka. □

3. Linearne kongruencije

Polinomijalne kongruencije u teoriji kongruencija mogu se proučavati na gotovo isti način kao što se algebarske jednadžbe mogu proučavati u algebri. U ovom poglavlju bavit ćemo se polinomima $f(x)$ s cjelobrojnim koeficijentima. Vrijednosti ovakvih polinoma bit će cijeli brojevi kada je x cijeli broj.
Cijeli broj x koji zadovoljava polinomijalnu kongruenciju

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

naziva se rješenje kongruencije.
Naravno, ako vrijedi $x \equiv y \pmod{m}$, tada vrijedi i $f(x) \equiv f(y) \pmod{m}$ pa svaka kongruencija koja ima jedno rješenje, ima ih beskonačno mnogo. Zbog toga je dogovoreno da se rješenja koja pripadaju istim klasama ostataka neće brojati kao različita. Dakle, kada budemo govorili o broju rješenja kongruencije poput (2), podrazumijevat ćemo broj nekongruentnih rješenja. Odnosno, broj rješenja sadržan u skupu $\{1, 2, \ldots, m\}$ ili bilo kojem drugom potpunom sustavu ostataka modulo m.
Zbog navedenog, svaka polinomijalna kongruencija modulo m ima najviše m rješenja.
Broj rješenja polinomijalnih kongruencija ilustrirat ćemo sljedećim primjerima.

Primjer 3.1. ([1, Primjer 1, str. 111]) *Pogledajmo linearnu kongruenciju* $2x \equiv 3 \pmod{4}$. *Za bilo koji* x, $2x - 3$ *je neparan broj pa prema tome ne može biti djeljiv brojem* 4. *Dakle, ova linearna kongruencija nema rješenja.*

Primjer 3.2. ([1, Primjer 2, str. 111]) *Pogledajmo kvadratnu kongruenciju* $x^2 \equiv 1 \pmod{8}$. *Ova kongruencija ima točno četiri rješenja dana s* $x \equiv 1, 3, 5, 7 \pmod{8}$.

Teorija linearnih kongruencija je u potpunosti opisana kroz tri teorema koja slijede.

Teorem 3.1. ([1, Teorem 5.12]) *Pretpostavimo da su brojevi* a *i* m *relativno prosti. Tada linearna kongruencija*

$$ax \equiv b \pmod{m} \tag{3}$$

ima jedinstveno rješenje.

Dokaz. Obzirom da brojevi $1, 2, 3, \ldots, m$ tvore potpuni sustav ostataka, trebamo ispitati samo njih. Zbog toga, formiramo produkte $a, 2a, 3a, \ldots, ma$. Obzirom na činjenicu da su a i m relativno prosti iz pretpostavke teorema, navedeni brojevi isto čine potpuni sustav ostataka. Prema tome je točno jedan od njih kongruentan b modulo m. Odnosno, postoji točno jedan x koji je rješenje kongruencije $ax \equiv b \pmod{m}$. □

Ako su a i m relativno prosti, jedinstveno rješenje kongruencije $ax \equiv 1 \pmod{m}$ naziva se inverz od a modulo m. Ako s a' označimo inverz od a, tada je ba' rješenje kongruencije (3).

Iako prema Teoremu 3.1 linearna kongruencija (3) ima jedinstveno rješenje ako su a i m relativno prosti, taj teorem ne otkriva način na koji možemo doći do tog rješenja osim da redom ispitujemo brojeve u potpunom sustavu ostataka. Za određivanje tog rješenja, postoje ekspeditivnije metode od kojih ćemo neke razraditi u sljedećim poglavljima.

Sada ćemo nastaviti s drugim teoremom koji opisuje teoriju linearnih kongruencija.

Teorem 3.2. ([1, Teorem 5.13]) *Označimo s d najveći zajednički djelitelj brojeva a i m. Linearna kongruencija*

$$ax \equiv b \pmod{m} \tag{4}$$

ima rješenja ako i samo ako d dijeli b.

Dokaz. Ako rješenje postoji, onda $d \mid b$ jer je $d = (a, m)$. Obratno, ako $d \mid b$ kongruencija

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

ima rješenje obzirom da je $(\frac{a}{d}, \frac{m}{d}) = 1$. Rješenje navedene kongruencije je rješenje i kongruencije (4). □

Teorem 3.3. ([1, Teorem 5.14]) *Označimo s d najveći zajednički djelitelj brojeva a i m te neka d dijeli b. Linearna kongruencija*

$$ax \equiv b \pmod{m} \tag{5}$$

ima točno d rješenja modulo m koja su dana s

$$u,\ u + \frac{m}{d},\ u + 2\frac{m}{d}, \ldots,\ u + (d-1)\frac{m}{d}, \tag{6}$$

pri čemu je u rješenje jedinstveno modulo $\frac{m}{d}$ linearne kongruencije

$$\frac{a}{d}\, x \equiv \frac{b}{d} \pmod{\frac{m}{d}}. \tag{7}$$

Dokaz. Svako rješenje kongruencije (7) je također i rješenje kongruencije (5). Obratno, svako rješenje kongruencije (5) zadovoljava kongruenciju (7).
Brojevi $u, u + \frac{m}{d}, u + 2\frac{m}{d}, \ldots, u + (d-1)\frac{m}{d}$ su rješenja kongruencije (7) zbog (5). Nikoja dva od navedenih rješenja nisu kongruentna modulo m obzirom da relacija

$$u + r\frac{m}{d} \equiv u + s\frac{m}{d} \pmod{m},\ \text{gdje je } 0 \le r < d,\ 0 \le s < d$$

implicira

$$r\frac{m}{d} \equiv s\frac{m}{d} \pmod{m},\ \text{i zbog toga je } r \equiv s \pmod{d}.$$

Vrijedi da je $0 \le |r - s| < d$ pa je onda $r = s$.
Sada još preostaje pokazati kako kongruencija (5) nema drugih rješenja osim onih danih u (6). Pretpostavimo da je y rješenje kongruencije (5). Tada vrijedi $ay \equiv au \pmod{m}$ pa je $y \equiv u \pmod{\frac{m}{d}}$. Stoga je $y = u + k\frac{m}{d}$ za neki k. Ali $k \equiv r \pmod{d}$ za neki r takav da je $r \in [0, d\rangle$. Prema tome,

$$k\frac{m}{d} \equiv r\frac{m}{d} \pmod{m} \ \text{ te je } \ y \equiv u + r\frac{m}{d} \pmod{m}.$$

Znači, y je kongruentan modulo m nekom od brojeva

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

čime je dokazana tvrdnja da su ovo jedina rješenja kongruencije (5). □

Sada ćemo pokazati da je najveći zajednički djelitelj dvaju brojeva, a i b, linearna kombinacija tih brojeva s cjelobrojnim koeficijentima.

Teorem 3.4. ([1, Teorem 1.2]) *Neka su a i b cijeli brojevi. Postoji zajednički djelitelj d ovih brojeva oblika $d = ax + by$, pri čemu su x i y cijeli brojevi. Štoviše, svaki zajednički djelitelj brojeva a i b dijeli d.*

Dokaz. Prvo pretpostavimo da su $a, b \geq 0$. Tvrdnju ćemo dokazati koristeći matematičku indukciju do n, pri čemu je $n = a + b$.
Ako je $n = 0$, tada je i $a = b = 0$ i uzmemo $d = 0$ s $x = y = 0$.
Zatim pretpostavimo da je teorem dokazan za $0, 1, 2, \ldots, n-1$. Zbog simetrije možemo pretpostaviti da je $a \geq b$. Ako je $b = 0$, uzmimo da je $d = a$, $x = 1$ i $y = 0$. Ako je $b \geq 1$, primijenimo teorem na $a - b$ i b. Budući da je $(a - b) + b = a = n - b \leq n - 1$, pretpostavka indukcije je primjenjiva te postoji zajednički djelitelj d razlike $a - b$ i broja b oblika $d = (a-b)x+by$. Ovaj d također dijeli i $(a+b)-b = a$ pa je prema tome d zajednički djelitelj brojeva a i b pa imamo da je $d = ax + (y - x)b$, linearna kombinacija brojeva a i b.
Da bismo upotpunili dokaz još preostaje pokazati da svaki zajednički djelitelj dijeli d. Zajednički djelitelj dijeli a i b pa zbog linearnosti dijeli i d.
U slučaju da je $a < 0$ ili $b < 0$ (ili oboje), možemo primijeniti upravo dokazani rezultat na $|a|$ i $|b|$. Tada postoji zajednički djelitelj d brojeva $|a|$ i $|b|$ oblika $d = |a|x + |b|y$. Ako je $a < 0$, tada je $|a|x = -ax = a(-x)$. Analogno vrijedi i za $b < 0$. Dakle d je ponovno linearna kombinacija brojeva a i b. □

Isti rezultat slijedi i kao posljedica Teorema 3.3.

Teorem 3.5. ([1, Teorem 5.15]) *Ako je d najveći zajednički djelitelj brojeva a i b, onda postoje x i $y \in Z$ za koje je*

$$ax + by = d. \tag{8}$$

Dokaz. Kako je $(a, b) = d$, postoji $x \in \mathbb{Z}$ za koji je $ax \equiv d \pmod{b}$. Kako b dijeli $d - ax$, postoji $y \in \mathbb{Z}$ takav da je $d - ax = by$. Shodno tome, dolazimo da izraza $ax + by = d$, što se i tražilo. □

Primijetimo, geometrijski gledano, parovi (x, y) koji zadovoljavaju jednadžbu $ax + by = d$ su točke s cjelobrojnim koordinatama koje leže na pravcu. Rješenje kongruencije $ax \equiv d \pmod{b}$ je $x-$koordinata svake od ovih točaka.

4. Reducirani sustavi ostataka i Euler-Fermatov teorem

U ovom poglavlju za početak ćemo definirati Eulerovu funkciju te navesti njezina svojstva. Pomoću te funkcije uvest ćemo pojam reduciranog sustava ostataka te iskazati i dokazati Euler-Fermatov teorem.

Definicija 4.1. *Ako je $n \geq 1$, Eulerova funkcija $\varphi(n)$ definirana je kao ukupan broj prirodnih brojeva relativno prostih broju n koji su ujedno i manji (ili jednaki) od njega.*
Dakle,

$$\varphi(n) = \sum_{k=1}^{n}{}' 1,$$

pri čemu $'$ ukazuje na to da se suma odnosi na one k koji su relativno prosti s n.

U sljedećoj napomeni navodimo tvrdnju o Eulerovoj funkciji koju ćemo više puta koristiti.

Napomena 4.1. ([1, Teorem 2.4]) *Za prirodan broj n vrijedi*

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right). \tag{9}$$

Teorem 4.1. ([1, Teorem 2.5]) *Eulerova funkcija ima sljedeća svojstva:*

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

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

(c) $\varphi(mn) = \varphi(m)\varphi(n)$, *za m i n relativno proste,*

(d) $a|b \Rightarrow \varphi(a)|\varphi(b)$,

(e) $\varphi(n)$ *je paran za $n \geq 3$. Štoviše, ukoliko n ima r različitih neparnih prostih faktora, onda vrijedi $2^r|\varphi(n)$.*

Dokaz. (a) Tvrdnja slijedi uvrštavanjem p^α umjesto n u (9).
(b) Da bismo dokazali ovo svojstvo, zapišimo (9) u obliku $\frac{\varphi(n)}{n} = \prod_{p|n}\left(1 - \frac{1}{p}\right)$. Zatim primijetimo kako je svaki prosti djelitelj produkta mn ili prosti djelitelj broja m ili prosti djelitelj broja n te da oni prosti brojevi koji dijele i m i n, također dijele i najvećeg zajedničkog djelitelja tih brojeva. Stoga vrijedi

$$\frac{\varphi(mn)}{mn} = \prod_{p|mn}\left(1 - \frac{1}{p}\right) = \frac{\prod_{p|m}\left(1 - \frac{1}{p}\right)\prod_{p|n}\left(1 - \frac{1}{p}\right)}{\prod_{p|(m,n)}\left(1 - \frac{1}{p}\right)} = \frac{\frac{\varphi(m)}{m}\frac{\varphi(n)}{n}}{\frac{\varphi(d)}{d}},$$

iz čega proizlazi tvrdnja (b).
(c) Tvrdnja (c) poseban je slučaj tvrdnje (b) pa i dokaz proizlazi iz dokaza tvrdnje pod (b).
(d) Tvrdnju (d) dokazat ćemo pomoću tvrdnje (b). Budući da $a \mid b$ vrijedi da je $b = ac$ pri čemu je $1 \leq c \leq b$. Ukoliko je $c = b$, onda je $a = 1$ pa je tvrdnja (d) trivijalno zadovoljena. Stoga pretpostavimo da vrijedi $c < b$. Koristeći tvrdnju (b) vrijedi:

$$\varphi(b) = \varphi(ac) = \varphi(a)\varphi(c)\frac{d}{\varphi(d)} = d\varphi(a)\frac{\varphi(c)}{\varphi(d)}, \tag{10}$$

pri čemu je $d = (a, c)$. Dokaz slijedi matematičkom indukcijom po b. Za $b = 1$, tvrdnja je trivijalna. Zatim pretpostavimo da tvrdnja vrijedi za sve cijele brojeve manje od b. Tada vrijedi za c pa $\varphi(d) \mid \varphi(c)$ budući da $d \mid c$. Desni član jednakosti (10) je višekratnik od $\varphi(a)$ pa slijedi da $\varphi(a) \mid \varphi(b)$. Time je tvrdnja (d) dokazana.
(e) Ako je $n = 2^\alpha$, $\alpha \geq 2$, tvrdnja (a) pokazuje nam da je $\varphi(n)$ paran. Ukoliko n ima barem jedan neparan prosti faktor, pišemo

$$\varphi(n) = n \prod_{p|n} \frac{p-1}{p} = \frac{n}{\prod_{p|n} p} \prod_{p|n} (p-1) = c(n) \prod_{p|n} (p-1),$$

pri čemu je $c(n)$ cijeli broj. Produkt koji množi $c(n)$ je paran pa je i $\varphi(n)$ paran. Štoviše, svaki neparni prosti broj p daje faktor 2 ovom produktu, pa $2^r \mid \varphi(n)$ ukoliko n ima r različitih neparnih prostih faktora.

□

Definicija 4.2. *Reducirani sustav ostataka modulo m je skup koji se sastoji od $\varphi(m)$ cijelih brojeva međusobno nekongruentnih modulo m svaki od kojih je relativno prost s m.*

Teorem 4.2. ([1, Teorem 5.16]) *Neka je $\{a_1, a_2, \ldots a_{\varphi(m)}\}$ reducirani sustav ostataka modulo m te neka su brojevi k i m relativno prosti. Tada je i $\{ka_1, ka_2, \ldots ka_{\varphi(m)}\}$ reducirani sustav ostataka modulo m.*

Dokaz. Nikoja dva broja ka_i i ka_j, $i \neq j$, nisu međusobno kongruentna modulo m. Također, budući da vrijedi $(a_i, m) = (k, m) = 1$, onda vrijedi i $(ka_i, m) = 1$ pa je ka_i relativno prost s m. □

Teorem 4.3. ([1, Teorem 5.17]) ***Euler-Fermatov teorem.*** *Pretpostavimo da su brojevi a i m relativno prosti. Tada vrijedi*

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

Dokaz. Neka je $\{b_1, b_2, \ldots, b_{\varphi(m)}\}$ reducirani sustav ostataka modulo m. Tada je $\{ab_1, ab_2, \ldots, ab_{\varphi(m)}\}$ također reducirani sustav ostataka modulo m pa je produkt svih cijelih brojeva u prvom skupu kongruentan produktu onih u drugom skupu. Stoga

$$b_1 \cdots b_{\varphi(m)} \equiv a^{\varphi(m)} b_1 \cdots b_{\varphi(m)} \pmod{m}.$$

Svaki b_i je relativno prost s m pa možemo skratiti svaki b_i da bismo dobili tvrdnju teorema.

□

Teorem 4.4. ([1, Teorem 5.18]) *Neka je p prost broj. Ako p ne dijeli a, onda vrijedi*

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

Dokaz. Tvrdnja slijedi direktno iz Euler-Fermatovog teorema jer je za prost broj p vrijednost Eulerove funkcije jednaka $p - 1$, to jest $\varphi(p) = p - 1$. □

Teorem 4.5. ([3, Korolar 2.2.3.]) ***Mali Fermatov teorem.*** *Za bilo koji cijeli broj a i bilo koji prost broj p vrijedi*

$$a^p \equiv a \pmod{p}.$$

Dokaz. Ukoliko p ne dijeli a, tvrdnja je ista kao tvrdnja Teorema 4.4. Ukoliko p dijeli a, onda su i a^p i a kongruentni $0 \mod p$. □

Napomena 4.2. *Obrat Malog Fermatovog teorema ne vrijedi.*

Euler-Fermatov teorem može se koristiti pri računanju rješenja linearnih kongruencija na način iskazan u sljedećem teoremu.

Teorem 4.6. ([1, Teorem 5.20]) *Ako su brojevi a i m relativno prosti, onda je rješenje (jedinstveno modulo m) linearne kongruencije*

$$ax \equiv b \pmod{m} \tag{11}$$

dano s

$$x \equiv ba^{\varphi(m)-1} \pmod{m}. \tag{12}$$

Dokaz. Zbog Euler-Fermatovog teorema broj $x \equiv ba^{\varphi(m)-1} \pmod{m}$ zadovoljava kongruenciju $ax \equiv b \pmod{m}$. Rješenje je jedinstveno modulo m jer su a i m relativno prosti. □

Nakon iskazanog načina za dobivanje rješenja linearnih kongruencija pomoću Euler-Fermatovog teorema, ilustrirajmo to sljedećim primjerom.

Primjer 4.1. *Odredimo sva rješenja linearne kongruencije* $16x \equiv 27 \pmod{29}$.
Budući da je $(16, 29) = 1$, *postoji jedinstveno rješenje modulo* 29 *ove kongruencije. Koristeći (12), dobivamo:*

$$x \equiv 27 \cdot 16^{\varphi(29)-1} \pmod{29}.$$

Kako je 29 *prost broj, vrijedi da je* $\varphi(29) = 29 - 1 = 28$.
Dakle sada imamo:

$$x \equiv 27 \cdot 16^{27} \pmod{29}.$$

Modulo 29 *vrijedi* $16^2 \equiv 24$, $16^3 \equiv 7$, $16^4 \equiv 25$, $16^8 \equiv 16$.
16^{27} *možemo zapisati kao produkt* $16^8 \cdot 16^8 \cdot 16^8 \cdot 16^3$ *te dolazimo do rješenja* $x \equiv 27 \cdot 20 \pmod{29} \equiv 18 \pmod{29}$.

5. Polinomijalne kongruencije modulo p. Lagrangeov teorem

Fundamentalni teorem algebre kaže kako za svaki polinom f stupnja većeg ili jednakog 1 jednadžba oblika $f(x) = 0$ ima n rješenja u skupu kompleksnih brojeva. Ne postoji tvrdnja koja je direktan analogon ovom teoremu za polinomijalne kongruencije. Primjerice, u prethodnim poglavljima mogli smo uočiti kako neke linearne kongruencije nemaju rješenja, neke imaju točno jedno, a neke pak imaju više od jednog rješenja. Prema tome, čini se da ne postoji jednostavna veza između broja rješenja i stupnja polinomijalne kongruencije. Međutim, u slučaju kada kongruenciju promatramo modulo prost broj vrijedi Lagrangeov teorem koji govori upravo o poveznici broja rješenja i stupnja kongruencije. Taj teorem sada ćemo iskazati i dokazati.

Teorem 5.1. ([1, Teorem 5.21]) ***Lagrangeov teorem.*** *Neka je p prost broj te neka je*

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

polinom stupnja n s cjelobrojnim koeficijentima pri čemu za vodeći koeficijent c_n vrijedi $c_n \not\equiv 0 \pmod{p}$.
Tada polinomijalna kongruencija

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

ima najviše n rješenja.

Dokaz. Tvrdnju ćemo dokazati matematičkom indukcijom po stupnju n polinoma f. U slučaju kada je $n = 1$, imamo linearnu kongruenciju:

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

Kako je $c_1 \not\equiv 0 \pmod{p}$, onda vrijedi da je $(c_1, p) = 1$ te postoji jedinstveno rješenje.
Zatim pretpostavimo da je tvrdnja teorema istinita za polinome stupnja $n - 1$.
Također, pretpostavimo kako kongruencija $f(x) \equiv 0 \pmod{p}$ ima $n + 1$ međusobno nekongruentnih rješenja modulo p te ih označimo s

$$x_0, x_1, x_2, \ldots, x_n,$$

pri čemu je $f(x_k) \equiv 0 \pmod{p}$ za sve $k = 0, 1, 2, \ldots, n$. Trebamo doći do kontradikcije.
Vrijedi sljedeći algebarski identitet

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

pri čemu je $g(x)$ polinom stupnja $n-1$ s cjelobrojnim koeficijentima i vodećim koeficijentom c_n. Prema tome, vrijedi

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

obzirom da je $f(x_k) \equiv f(x_0) \equiv 0 \pmod{p}$. Međutim, $x_k - x_0 \not\equiv 0 \pmod{p}$ za $k \neq 0$ pa zbog toga mora vrijediti $g(x_k) \equiv 0 \pmod{p}$ za sve $k \neq 0$. Prema navedenom, dolazimo do toga da kongruencija $g(x) \equiv 0 \pmod{p}$ ima n međusobno nekongruentnih rješenja modulo p. To je u kontradikciji s pretpostavkom indukcije čime je dokaz završen. □

6. Primjene Lagrangeovog teorema

Ovo poglavlje rada posvetit ćemo primjenama prethodno dokazanog Lagrangeovog teorema.

Teorem 6.1. ([1, Teorem 5.22]) *Neka je f polinom stupnja n s cjelobrojnim koeficijentima dan s $f(x) = c_0 + c_1x + \cdots + c_nx^n$ i neka je p prost broj. Ukoliko kongruencija $f(x) \equiv 0 \pmod{p}$ ima više od n rješenja, onda je svaki koeficijent tog polinoma f djeljiv brojem p.*

Dokaz. Ukoliko postoji koeficijent koji nije djeljiv brojem p, uzmimo da je c_k takav koeficijent s najvećim indeksom. Tada je $k \leq n$ te kongruencija

$$c_0 + c_1x + \cdots + c_kx^k \equiv 0 \pmod{p}$$

broji više od k rješenja te prema Lagrangeovu teoremu p dijeli c_k što je kontradikcija. □

Sada ćemo primijeniti Teorem 6.1 na specifičan polinom.

Teorem 6.2. ([1, Teorem 5.23]) *Neka je p prost broj. Svi koeficijenti polinoma f danog s*

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

djeljivi su brojem p.

Dokaz. Uzmimo da je $g(x) = (x-1)(x-2)\cdots(x-p+1)$. Nultočke polinoma g su brojevi $1, 2, \ldots, p-1$, stoga su oni rješenja kongruencije

$$g(x) \equiv 0 \pmod{p}.$$

Prema Euler-Fermatovom teoremu, ovi brojevi su i rješenja kongruencije $h(x) \equiv 0 \pmod{p}$, pri čemu je $h(x) = x^{p-1} - 1$. Polinom $f(x)$ koji je razlika polinoma $g(x)$ i $h(x)$ je polinom stupnja $p-2$, a kongruencija $f(x) \equiv 0 \pmod{p}$ ima $p-1$ rješenja, $1, 2, \ldots, p-1$, pa je prema Teoremu 6.1 svaki koeficijent polinoma $f(x)$ djeljiv s p. □

Sljedeća dva teorema dobivamo razmatranjem dva specifična koeficijenta polinoma $f(x) = (x-1)(x-2)\cdots(x-p+1) - x^{p-1} + 1$.

Teorem 6.3. ([1, Teorem 5.24]) ***Wilsonov teorem.*** *Za prost broj p vrijedi*

$$(p-1)! \equiv -1 \pmod{p}.$$

Dokaz. Konstantni član polinoma $f(x)$ u Teoremu 6.2 je $(p-1)! + 1$. □

Napomena 6.1. ([3, Propozicija 2.3.2.]) *Vrijedi i obrat Wilsonovog teorema. Odnosno, ako je $n > 1$ rješenje kongruencije $(n-1)! \equiv -1 \pmod{n}$, onda je n prost broj.*

Ilustrirajmo obrat Wilsonovog teorema na primjeru.

Primjer 6.1. ([3, Primjer 16.]) *Uzmimo broj* 100! *koji je* 158*−znamenkasti broj. Koristeći obrat Wilsonovog teorema slijedi* $100! \equiv -1 \pmod{101}$, *odnosno* 101 *dijeli broj* $100! + 1$.

Teorem 6.4. ([1, Teorem 5.25]) ***Wolstenholmeov teorem.*** *Za prost broj $p \geq 5$ vrijedi*

$$\sum_{k=1}^{p-1} \frac{(p-1)!}{k} \equiv 0 \pmod{p^2}. \tag{14}$$

Dokaz. Suma s lijeve strane kongruencije (14) je suma svih mogućih produkata od po $p-2$ različitih elemenata skupa $\{1, 2, \ldots, p-1\}$. Ta suma također je jednaka koeficijentu uz $-x$ polinoma

$$g(x) = (x-1)(x-2)\cdots(x-p+1).$$

Zapravo, $g(x)$ možemo zapisati u obliku

$$g(x) = x^{p-1} - S_1 x^{p-2} + S_2 x^{p-3} - \cdots + S_{p-3}x^2 - S_{p-2}x + (p-1)!,$$

pri čemu je S_k suma svih produkata od po k elemenata skupa $\{1, 2, \ldots, p-1\}$. Prema Teoremu 6.2 svaki od brojeva $S_1, S_2, \ldots, S_{p-2}$ djeljiv je s p, a mi želimo pokazati da je S_{p-2} djeljiv s p^2. Vrijedi $g(p) = (p-1)!$ pa

$$(p-1)! = p^{p-1} - S_1 p^{p-2} + \cdots + S_{p-3}p^2 - S_{p-2}p + (p-1)!.$$

Kako je $p \geq 5$, izlučivanjem $(p-1)!$ i reducirajući jednadžbu $\bmod p^3$ dobivamo:

$$pS_{p-2} \equiv 0 \pmod{p^3},$$

te dolazimo do kongruencije

$$S_{p-2} \equiv 0 \pmod{p^2},$$

što se i tražilo. □

Wolstenholmeov teorem ilustrirat ćemo sljedećim primjerom.

Primjer 6.2. *Za $p = 7$ imamo:*

$$\sum_{k=1}^{6} \frac{6!}{k} = \frac{6!}{1} + \frac{6!}{2} + \frac{6!}{3} + \frac{6!}{4} + \frac{6!}{5} + \frac{6!}{6} = 6! \cdot \left(1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6}\right) = 6! \cdot \frac{49}{20} = 720 \cdot \frac{49}{20} = 1764.$$

$p^2 = 49$, a $\frac{1764}{49} = 36$, odnosno ostatak pri dijeljenju broja 1764 s 49 je 0.

7. Sustavi linearnih kongruencija. Kineski teorem o ostatcima

Primijetimo da sustav dviju ili više linearnih kongruencija ne mora imati rješenje, čak i ako svaka kongruencija zasebno ima rješenje. Pogledajmo primjerice linearne kongruencije $x \equiv 1 \pmod 2$ i $x \equiv 0 \pmod 4$. Gledajući zasebno, svaka od njih ima rješenje, ali ne postoji x koji istovremeno zadovoljava i jednu i drugu kongruenciju. U ovom slučaju, moduli kongruencija 2 i 4 nisu relativno prosti. Želimo pokazati kako sustav dviju ili više linearnih kongruencija svaka od kojih ima jedinstveno rješenje, također ima rješenje u slučaju kada su moduli kongruencija u parovima relativno prosti.

Teorem 7.1. ([1, Teorem 5.26]) ***Kineski teorem o ostatcima.*** *Pretpostavimo da su $m_1, \ldots, m_r \in \mathbb{N}$, u parovima relativno prosti:*

$$(m_j, m_k) = 1 \text{ za } j \neq k.$$

Za proizvoljne cijele brojeve $b_1, \ldots, b_r$ sustav kongruencija

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

ima jedinstveno rješenje modulo produkt $m_1 \cdots m_r$.

Dokaz. Neka je $M = m_1 \cdots m_r$ i neka je $M_k = \frac{M}{m_k}$. Tada su M_k i m_k relativno prosti pa svaki M_k ima jedinstveni inverz M_k' modulo m_k. Označimo

$$x = b_1 M_1 M_1' + b_2 M_2 M_2' + \cdots + b_r M_r M_r'.$$

Promotrimo sada svaki član ove sume modulo m_k. Budući da je $M_j \equiv 0 \pmod{m_k}$ za $j \neq k$ vrijedi:

$$x \equiv b_k M_k M_k' \equiv b_k \pmod{m_k}.$$

Stoga x zadovoljava svaku kongruenciju u sustavu. Pokažimo još da sustav ima jedinstveno rješenje $\bmod M$. Ukoliko bi x i y bila dva rješenja ovog sustava vrijedilo bi $x \equiv y \pmod{m_k}$ za sve k, a obzirom na činjenicu da su m_k i m_j u parovima relativno prosti za $k \neq j$, također vrijedi $x \equiv y \pmod M$ čime je dokaz završen. □

Sada ćemo lako izvesti generalizaciju Kineskog teorema o ostatcima.

Teorem 7.2. ([1, Teorem 5.27]) *Pretpostavimo da su $m_1, \ldots, m_r \in \mathbb{N}$, u parovima relativno prosti. Neka su $a_1, \ldots, a_r$ takvi da vrijedi*

$$(a_k, m_k) = 1 \text{ za } k = 1,\ 2, \ldots,\ r.$$

Tada za proizvoljne cijele brojeve $b_1, \ldots, b_r$ sustav linearnih 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 jedinstveno rješenje modulo produkt $m_1 \cdots m_r$.

Dokaz. S a_k' označimo inverz od a_k modulo m_k. Taj inverz postoji jer su a_k i m_k relativno prosti. Tada je kongruencija $a_k x \equiv b_k \pmod{m_k}$ ekvivalentna kongruenciji $x \equiv b_k a_k' \pmod{m_k}$ te primjenom Teorema 7.1 dolazimo do traženog rezultata. □

8. Primjene Kineskog teorema o ostatcima

U ovom poglavlju obradit ćemo dvije primjene Kineskog teorema o ostatcima.
Prva primjena bavi se polinomijalnim kongruencijama promatranim modulo složen broj.

Teorem 8.1. ([1, Teorem 5.28]) *Neka je f polinom s cjelobrojnim koeficijentima te neka su $m_1, m_2 \ldots, m_r \in \mathbb{N}$ u parovima relativno prosti. Produkt $m_1 m_2 \cdots m_r$ označimo s m. Tada kongruencija*

$$f(x) \equiv 0 \pmod{m} \tag{15}$$

ima rješenje ako i samo ako svaka od kongruencija

$$f(x) \equiv 0 \pmod{m_i} \text{ za } i = 1,\ 2,\ \ldots,\ r \tag{16}$$

ima rješenje. Štoviše, ako s $v(m)$ označimo broj rješenja kongruencije (15), a s $v(m_i)$ broj rješenja kongruencije (16), tada vrijedi

$$v(m) = v(m_1)v(m_2)\cdots v(m_r). \tag{17}$$

Dokaz. Ukoliko je $f(a) \equiv 0 \pmod{m}$, onda je i $f(a) \equiv 0 \pmod{m_i}$, za sve i. Zbog toga je svako rješenje kongruencije (15) ujedno i rješenje kongruencije (16).
Obratno, označimo s a_i rješenje kongruencije (16). Prema Kineskom teoremu o ostatcima postoji $a \in \mathbb{Z}$ za koji vrijedi

$$a \equiv a_i \pmod{m_i} \text{ za } i = 1,\ 2,\ \ldots,\ r, \tag{18}$$

pa je

$$f(a) \equiv f(a_i) \equiv 0 \pmod{m_i}. \tag{19}$$

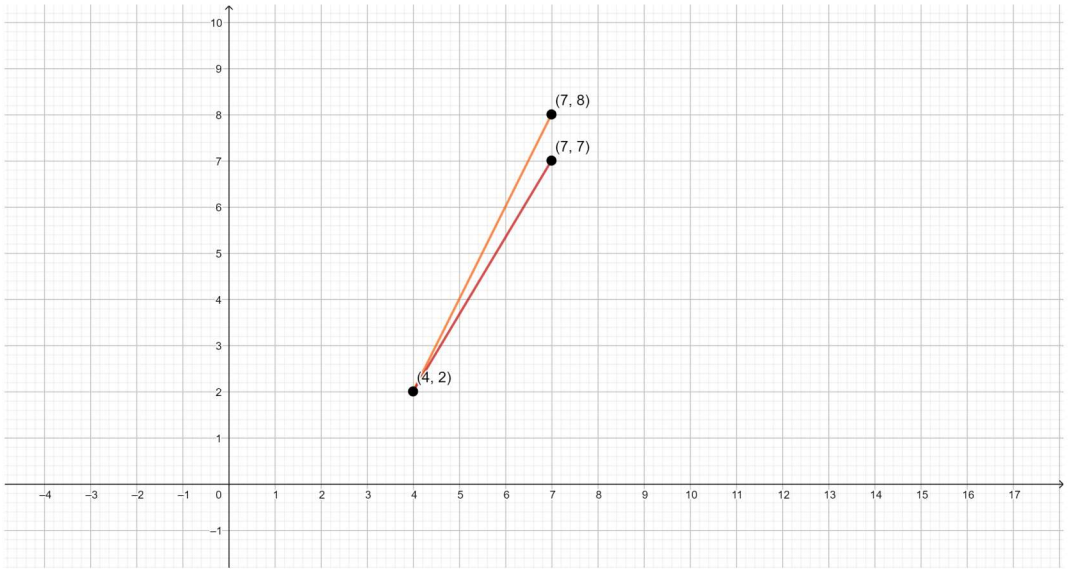
Budući da su $m_1, \ldots, m_r$ u parovima relativno prosti, vrijedi i $f(a) \equiv 0 \pmod{m}$. Zbog navedenog, ukoliko svaka od kongruencija u (16) ima rješenje, rješenje ima i kongruencija (15).
Prema Teoremu 7.1 znamo da svaka uređena r-torka rješenja $(a_1, \ldots, a_r)$ kongruencija u (16) daje jedinstveno, modulo m, rješenje a od (18). Kako postoji $v(m_i)$ rješenja a_i kongruencije (16), broj cijelih brojeva a koji zadovoljavaju (18) pa i (16) je produkt $v(m_1)\cdots v(m_r)$ čime je dokazana jednakost (17). □

Druga primjena Kineskog teorema o ostatcima bavi se skupom točaka cjelobrojne rešetke vidljivih iz ishodišta. Prvo ćemo iskazati kada su dvije točke rešetke uzajamno vidljive, a potom ćemo iskazati i dokazati teorem koji je primjena Teorema 7.1.

Definicija 8.1. *Za dvije točke rešetke, P i Q, kažemo da su uzajamno vidljive ukoliko dužina koja ih povezuje ne sadrži druge točke rešetke osim krajnjih točaka, P i Q.*

Primjer 8.1. *Pogledajmo Sliku 1, točke $(4, 2)$ i $(7, 7)$ su uzajamo vidljive, a točke $(4, 2)$ i $(7, 8)$ nisu.*

Napomena 8.1. ([1, Teorem 3.8]) *Dvije točke rešetke (a, b) i (k, l) uzajamno su vidljive ako i samo ako vrijedi $(a - k, b - l) = 1$.*



Slika 1: Točke rešetke

Teorem 8.2. ([1, Teorem 5.29]) *Skup točaka rešetke u ravnini vidljivih iz ishodišta sadrži proizvoljno velike kvadratne razmake. To jest, za dani $k \in \mathbb{N}$ postoji točka rešetke (a, b) takva da niti jedna točka rešetke oblika*

$$(a + r, b + s),\ 0 < r \leq k,\ 0 < s \leq k,$$

nije vidljiva iz ishodišta.

Dokaz. Neka je $p_1,\ p_2,\ \ldots$ niz prostih brojeva. Za dani $k > 0$ promotrimo matricu dimenzija $k \times k$ čiji prvi redak čini prvih k prostih brojeva, zatim drugi redak čini sljedećih k prostih brojeva, i tako dalje. Neka je m_i produkt prostih brojeva u $i-$tom retku i neka je M_i produkt prostih brojeva u $i-$tom stupcu. Tada su brojevi m_j i m_k, za $j \neq k$, u parovima relativno prosti, a isto vrijedi i za brojeve M_j i M_k, $j \neq k$.
Sada promotrimo sustav kongruencija

$$\begin{aligned} x &\equiv -1 \pmod{m_1} \\ x &\equiv -2 \pmod{m_2} \\ &\vdots \\ x &\equiv -k \pmod{m_k}. \end{aligned}$$

Ovaj sustav ima rješenje a koje je jedinstveno modulo produkt $m_1 \cdots m_k$. Analogno, sustav kongruencija

$$\begin{aligned} y &\equiv -1 \pmod{M_1} \\ y &\equiv -2 \pmod{M_2} \\ &\vdots \\ y &\equiv -k \pmod{M_k} \end{aligned}$$

ima rješenje b koje je jedinstveno modulo produkt $M_1 \cdots M_k = m_1 \cdots m_k$.
Sada zamislimo kvadrat čiji su nasuprotni vrhovi točke (a, b) i $(a + k, b + k)$.
Svaka točka rešetke unutar ovog kvadrata je oblika

$$(a + r, b + s),\ \text{pri čemu vrijedi } 0 < r < k,\ 0 < s < k,$$

a one za koje vrijedi $r = k$ ili $s = k$ leže na rubovima tog kvadrata.
Sada još preostaje pokazati da niti jedna takva točka nije vidljiva iz ishodišta. Vrijedi

$$a \equiv -r \pmod{m_r} \quad \text{i} \quad b \equiv -s \pmod{M_s}$$

pa prema tome prost broj koji se nalazi na presjeku retka r i stupca s dijeli i zbroj $a + r$ i zbroj $b + s$. Stoga $a + r$ i $b + s$ nisu relativno prosti pa prema tome točka rešetke $(a + r, b + s)$ nije vidljiva iz ishodišta. □

9. Polinomijalne kongruencije promatrane modulo potencija prostog broja

Teorem 8.1 pokazuje da se problem rješavanja polinomijalne kongruencije

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

može svesti na problem rješavanja sustava kongruencija oblika

$$f(x) \equiv 0 \pmod{p_i^{\alpha_i}} \quad \text{za} \quad i = 1, 2, \ldots, r,$$

pri čemu je $m = p_1^{\alpha_1} \cdots p_r^{\alpha_r}$.
U ovom poglavlju pokazat ćemo da problem možemo dodatno reducirati na kongruencije promatrane modulo prost broj plus skup linearnih kongruencija.
Neka je f polinom s cjelobrojnim koeficijentima i pretpostavimo da za prost broj p i $\alpha \geq 2$ kongruencija

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

ima rješenje, recimo $x = a$, pri čemu za a vrijedi $0 \leq a < p^{\alpha}$.
To rješenje je također i rješenje svake od kongruencija $f(x) \equiv 0 \pmod{p^{\beta}}$ za $\beta < \alpha$, odnosno, a je rješenje kongruencije

$$f(x) \equiv 0 \pmod{p^{\alpha-1}}. \tag{21}$$

Sada podijelimo a s $p^{\alpha-1}$ i zapišimo ga u obliku

$$a = qp^{\alpha-1} + r, \text{ pri čemu je } 0 \leq r < p^{\alpha-1}. \tag{22}$$

Za ostatak r u zapisu (22) kažemo da je generiran s a. Budući da je $r \equiv a \pmod{p^{\alpha-1}}$, broj r također je i rješenje kongruencije (21). Drugim riječima, iz svakog rješenja a kongruencije (20) u intervalu $0 \leq a < p^{\alpha}$ dobivamo rješenje r kongruencije (21) u intervalu $0 \leq r < p^{\alpha-1}$.
Sada pretpostavimo da počinjemo s rješenjem r kongruencije (21) u intervalu $0 \leq r < p^{\alpha-1}$ i pitamo se postoji li rješenje a kongruencije (20) u intervalu $0 \leq a < p^{\alpha}$ iz kojeg dobivamo rješenje r. Ukoliko postoji, kažemo da r može biti uzdignut s $p^{\alpha-1}$ na p^{α}. Sljedeći teorem pokazuje da mogućnost uzdizanja r ovisi o $f(r) \mod p^{\alpha}$ i o derivaciji $f'(r) \mod p$.

Teorem 9.1. ([1, Teorem 5.30]) *Neka je $\alpha \geq 2$ te neka je r rješenje kongruencije*

$$f(x) \equiv 0 \pmod{p^{\alpha-1}} \tag{23}$$

unutar intervala $[0, p^{\alpha-1}\rangle$.

(a) Pretpostavimo da vrijedi $f'(r) \not\equiv 0 \pmod{p}$. Tada r na jedinstven način može biti uzdignut s $p^{\alpha-1}$ na p^{α}. To jest, postoji jedinstveni $a \in [0, p^{\alpha}\rangle$ iz kojeg dobivamo r te koji je rješenje kongruencije (20).

(b) Pretpostavimo da vrijedi $f'(r) \equiv 0 \pmod{p}$. U ovom slučaju, dvije su moguće opcije:

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

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

Dokaz. Ukoliko je f polinom stupnja n, onda za sve x i sve h vrijedi identitet poznat kao Taylorova formula

$$f(x+h) = f(x) + \frac{f'(x)}{1!}h + \frac{f''(x)}{2!}h^2 + \cdots + \frac{f^{(n)}(x)}{n!}h^n. \tag{24}$$

Svaki polinom $\frac{f^{(k)}(x)}{k!}$ ima cjelobrojne koeficijente. Sada uzmimo $x = r$ u (24), pri čemu je r rješenje od (23) u intervalu $[0, p^{\alpha-1}\rangle$, i neka je $h = qp^{\alpha-1}$ pri čemu je $q \in \mathbb{Z}$. Budući da je $\alpha \geq 2$, članovi s desne strane jednakosti (24) oblika $m \cdot h^t, t > 1$, su cjelobrojni višekratnici od p^α. Stoga iz (24) proizlazi kongruencija

$$f(r + qp^{\alpha-1}) \equiv f(r) + f'(r)qp^{\alpha-1} \pmod{p^\alpha}. \tag{25}$$

Kako je r rješenje kongruencije (23), možemo pisati $f(r) = kp^{\alpha-1}$ za $k \in \mathbb{Z}$ pa kongruencija (25) postaje

$$f(r + qp^{\alpha-1}) \equiv (qf'(r) + k)p^{\alpha-1} \pmod{p^\alpha}. \tag{26}$$

Neka je sada

$$a = r + qp^{\alpha-1}. \tag{27}$$

Tada je a rješenje kongruencije (20) ako i samo ako vrijedi

$$qf'(r) + k \equiv 0 \pmod{p}. \tag{28}$$

Za slučaj kada je $f'(r) \not\equiv 0 \pmod{p}$ ova kongruencija ima jedinstveno rješenje $q \mod p$ te ukoliko izaberemo q iz intervala $[0, p\rangle$, broj a dan s (27) bit će rješenje kongruencije (20) unutar intervala $[0, p^\alpha\rangle$.
S druge strane, u slučaju $f'(r) \equiv 0 \pmod{p}$, kongruencija (28) ima rješenje q ako i samo ako p dijeli k, odnosno, ako i samo ako vrijedi $f(r) \equiv 0 \pmod{p^\alpha}$. Kada p ne dijeli k, ne postoji takav q za koji bi a zadovoljio (20). Međutim, ako p dijeli k, onda p vrijednosti $q = 0, 1, \ldots, p-1$ daje p rješenja $a \in [0, p^\alpha\rangle$ kongruencije (20), svako do kojih daje traženo rješenje r kongruencije (21) čime je dokaz završen. □

Dokaz Teorema 9.1 opisuje metodu za rješavanje kongruencija oblika (20) ukoliko su poznata rješenja kongruencije (23). Primjenjujući metodu uzastopno, problem je naposljetku reduciran na problem rješavanja kongruencije oblika

$$f(x) \equiv 0 \pmod{p}. \tag{29}$$

Ukoliko kongruencija (29) nema rješenja, neće ga imati niti kongruencija (20). Ukoliko kongruencija (29) ima rješenja, odaberimo jedno rješenje $r \in [0, p\rangle$. Obzirom na r, postojat će 0, 1, ili p rješenja kongruencije

$$f(x) \equiv 0 \pmod{p^2} \tag{30}$$

ovisno o brojevima $f'(r)$ i $k = \frac{f(r)}{p}$. Ukoliko p ne dijeli k i p dijeli $f'(r)$, onda r ne može biti uzdignut do rješenja kongruencije (30). U ovom slučaju, počinjemo proces iznova izabravši drugi r. Ukoliko niti jedan r ne može biti uzdignut, onda (30) nema rješenje.
Ako p dijeli k za neki r, ispitujemo linearnu kongruenciju

$$qf'(r) + k \equiv 0 \pmod{p}. \tag{31}$$

Ova kongruencija ima ili p rješenja ili jedno rješenje q ovisno o tome dijeli li p derivaciju $f'(r)$ ili ne. Za svako rješenje q, broj $a = r + qp$ daje rješenje kongruencije (30). Za svako rješenje kongruencije (30) slična procedura može se koristiti kako bi se pronašla sva rješenja kongruencije

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

i tako dalje sve dok sva rješenja kongruencije

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

nisu dobivena.

10. Princip unakrsne klasifikacije

Pri rješavanju nekih problema teorije brojeva može nam pomoći opći teorem o prebrojavanju skupova, koji često nazivamo princip unakrsne klasifikacije, a čija je inačica i formula uključivanja-isključivanja. Radi se o formuli kojom brojimo broj elemenata konačnog skupa S koji ne pripadaju unaprijed određenim podskupovima $S_1, \ldots, S_n$.

Napomena 10.1. *Neka je S skup s konačnim brojem elemenata. Ukoliko je T podskup skupa S, s $N(T)$ označavamo broj elemenata skupa T. Skup onih elemenata skupa S koji ne pripadaju podskupu T označavamo sa $S - T$. Shodno tome,*

$$S - \bigcup_{i=1}^{n} S_i$$

sastoji se od svih onih elemenata unutar S koji se ne nalaze niti u jednom od podskupova $S_1, \ldots, S_n$.
Da bismo pojednostavili zapis, za presjek $S_i \cap S_j$ pisat ćemo S_iS_j, za presjek $S_i \cap S_j \cap S_k$ pisat ćemo $S_iS_jS_k$, i tako dalje.

Teorem 10.1. ([1, Teorem 5.31]) ***Princip unakrsne klasifikacije.*** *Neka je S skup s konačnim brojem elemenata i neka su $S_1, S_2, \ldots, S_n$ podskupovi toga skupa. Tada vrijedi:*

$$\begin{aligned} N\left(S - \bigcup_{i=1}^{n} S_i\right) = \quad & N(S) - \sum_{1\le i\le n} N(S_i) + \sum_{1\le i<j\le n} N(S_iS_j) \\ & - \sum_{1\le i<j<k\le n} N(S_iS_jS_k) + \cdots + (-1)^n N(S_1S_2\cdots S_n). \end{aligned}$$

Dokaz. Ukoliko je $T \subseteq S$, s $N_r(T)$ označit ćemo broj elemenata podskupa T koji se ne nalaze niti u jednom od prvih r podskupova $S_1, S_2, \ldots S_r$, pri čemu je $N_0(T)$ isto što i $N(T)$.
Elemente nabrojane iz $N_{r-1}(T)$ dijelimo u dva disjunktna skupa, na one koji se ne nalaze u podskupu S_r i na one koji se nalaze. Stoga vrijedi

$$N_{r-1}(T) = N_r(T) + N_{r-1}(TS_r).$$

Dakle, prethodnu jednakost možemo zapisati u obliku

$$N_r(T) = N_{r-1}(T) - N_{r-1}(TS_r). \tag{32}$$

Uzmimo sada da je $T = S$ te koristeći jednakost (32) izrazimo svaki član s desne strane pomoću N_{r-2}. Tada dobivamo

$$\begin{aligned} N_r(S) &= \big(N_{r-2}(S) - N_{r-2}(SS_{r-1})\big) - \big(N_{r-2}(S_r) - N_{r-2}(S_rS_{r-1})\big) \\ &= N_{r-2}(S) - N_{r-2}(S_{r-1}) - N_{r-2}(S_r) + N_{r-2}(S_rS_{r-1}). \end{aligned}$$

Primjenjujući (32) uzastopno, u konačnici dobivamo

$$N_r(S) = N_0(S) - \sum_{i=1}^{r} N_0(S_i) + \sum_{1\le i<j\le r} N_0(S_iS_j) - \cdots + (-1)^r N_0(S_1S_2\cdots S_r).$$

Za $r = n$ dobivamo traženu formulu. □

Za daljnje potrebe ovog poglavlja, uvest ćemo pojam Möbiusove funkcije te predstaviti vezu između Möbiusove i Eulerove funkcije.

Definicija 10.1. *Möbiusovu funkciju μ definiramo na sljedeći način:*

$$\mu(1) = 1;$$

Ako je $n > 1$, zapišimo ga u obliku $n = {p_1}^{a_1} \dots {p_k}^{a_k}$. Tada

$$\mu(n) = (-1)^k \text{ ako } a_1 = a_2 = \cdots = a_k = 1,$$
$$\mu(n) = 0, \text{ inače.}$$

Napomena 10.2. ([1, Teorem 2.3]) *Eulerova funkcija povezana je s Möbiusovom sljedećom formulom:*

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}.$$

Primjer 10.1. ([1, Primjer, str. 124]) *Formula za produkt Eulerove funkcije može se izvesti iz pricnipa unakrsne klasifikacije. S $p_1, \dots, p_r$ označimo različite proste djelitelje broja n. Neka je $S = \{1, 2, \dots, n\}$ te neka je S_k podskup skupa S unutar kojeg se nalaze oni cijeli brojevi koji su djeljivi brojem p_k. Brojevi u skupu S relativno prosti s n su oni koji se ne nalaze niti u jednom od skupova $S_1, S_2, \dots S_r$ pa je prema tome*

$$\varphi(n) = N\left(S - \bigcup_{k=1}^{r} S_k\right).$$

U slučaju kada d dijeli n postoji $\frac{n}{d}$ višekratnika broja d u skupu S. Stoga je

$$N(S_i) = \frac{n}{p_i}, N(S_iS_j) = \frac{n}{p_ip_j}, \dots, N(S_1 \cdots S_r) = \frac{n}{p_1 \cdots p_r},$$

pa prema principu unakrsne klasifikacije vrijedi

$$\begin{aligned}
\varphi(n) &= n - \sum_{i=1}^{n} \frac{n}{p_i} + \sum_{1 \le i < j \le r} \frac{n}{p_ip_j} - \cdots + (-1)^r \frac{n}{p_1 \cdots p_r} \\
&= n \sum_{d|n} \frac{\mu(d)}{d} \\
&= n \prod_{p|n} \left(1 - \frac{1}{p}\right).
\end{aligned}$$

Sada ćemo pokazati još jednu primjenu principa unakrsne klasifikacije, a koja se tiče reduciranog sustava ostataka modulo k. Prebrojat ćemo elemente reduciranog sustava ostataka modulo k koji istovremeno pripadaju danoj klasi ostatka r modulo d, pri čemu d dijeli k i r i d su relativno prosti.

Teorem 10.2. ([1, Teorem 5.32]) *Neka su dani prirodni brojevi d i k te cijeli broj r za koje vrijedi $d \mid k$ i $(r, d) = 1$. Tada je broj elemenata skupa $S = \{r + td : t = 1, 2, \dots, \frac{k}{d}\}$ koji su relativno prosti s k jednak kvocijentu $\frac{\varphi(k)}{\varphi(d)}$.*

Dokaz. Ukoliko prost broj p dijeli k i sumu $r + td$, onda p ne dijeli d, inače bi vrijedilo da p dijeli r što je u kontradikciji s pretpostavkom teorema da su r i d relativno prosti. Stoga su prosti brojevi koji dijele k i elemente skupa S upravo oni koji dijele k, ali ne dijele d. Označimo ih s $p_1, \ldots, p_m$ te neka je

$$k' = p_1 p_2 \cdots p_m.$$

Tada su elementi skupa S koji su relativno prosti s k oni koji nisu djeljivi niti jednim od ovih prostih brojeva. Označimo sa S_i skup $\{x : x \in S \text{ i } p_i \mid x\}$ za $i = 1, 2, \ldots, m$.
Ako je $x \in S_i$ i $x = r + td$, tada je $r + td \equiv 0 \pmod{p_i}$. Budući da p_i ne dijeli d, postoji jedinstveni $t \mod p_i$ s navedenim svojstvom, dakle, točno jedan t u svakom od intervala $[1, p_i]$, $[p_i + 1, 2p_i]$, $\ldots$, $[(q-1)p_i + 1, qp_i]$, pri čemu je $qp_i = \frac{k}{d}$.
Dakle,

$$N(S_i) = \frac{\frac{k}{d}}{p_i}.$$

Slično dobivamo i

$$N(S_i S_j) = \frac{\frac{k}{d}}{p_i p_j}, \ldots, N(S_1 \cdots S_m) = \frac{\frac{k}{d}}{p_1 \cdots p_m}.$$

Prema principu unakrsne klasifikacije broj cijelih brojeva unutar skupa S koji su relativno prosti s k je

$$N\left(S - \bigcup_{i=1}^{m} S_i\right) = \frac{k}{d} \sum_{\delta \mid k'} \frac{\mu(\delta)}{\delta} = \frac{k}{d} \prod_{p \mid k'} \left(1 - \frac{1}{p}\right) = \frac{k \prod_{p \mid k} \left(1 - \frac{1}{p}\right)}{d \prod_{p \mid d} \left(1 - \frac{1}{p}\right)} = \frac{\varphi(k)}{\varphi(d)}.$$

□

11. Svojstvo dekompozicije reduciranih sustava ostataka

Kao primjenu Teorema 10.2, u ovom poglavlju raspravljat ćemo o svojstvu dekompozicije reduciranih sustava ostataka. Započet ćemo numeričkim primjerom.

Primjer 11.1. *Neka je S reducirani sustav ostataka modulo 15, recimo*

$$S = \{1, 2, 4, 7, 8, 11, 13, 14\}.$$

Osam elemenata skupa S prikazat ćemo u matrici dimenzija 4×2 kako slijedi:

$$\begin{bmatrix} 1 & 2 \\ 4 & 8 \\ 7 & 11 \\ 13 & 14 \end{bmatrix}.$$

Primijetimo da svaki redak matrice sadrži reducirani sustav ostataka modulo 3, a brojevi u svakom stupcu međusobno su kongruentni modulo 3.

Ovim primjerom ilustrirali smo općenito svojstvo reduciranih sustava ostataka koje ćemo iskazati i dokazati u sljedećem teoremu.

Teorem 11.1. ([1, Teorem 5.33]) *Neka je S reducirani sustav ostataka modulo k te neka je $d > 0$ djelitelj broja k. Tada vrijedi sljedeća dekompozicija skupa S:*

(a) S je unija $\frac{\varphi(k)}{\varphi(d)}$ disjunktnih skupova, svaki od kojih je reducirani sustav ostataka modulo d.

(b) S je unija $\varphi(d)$ disjunktnih skupova, svaki od kojih se sastoji od $\frac{\varphi(k)}{\varphi(d)}$ međusobno kongruentnih brojeva modulo d.

Dokaz. Da bismo dokazali ovaj teorem, prvo ćemo pokazati da su dijelovi (a) i (b) ekvivalentni, a potom ćemo dokazati dio (b).
Ukoliko (b) vrijedi, $\varphi(k)$ elemenata skupa S možemo prikazati u obliku matrice koristeći $\varphi(d)$ disjunktnih skupova iz (b) kao stupce. Takva matrica ima $\frac{\varphi(k)}{\varphi(d)}$ redaka. Svaki redak sadrži reducirani sustav ostataka modulo d te su to traženi disjunktni skupovi za dio (a). Na isti način dolazimo do toga da tvrdnja pod (a) implicira tvrdnju pod (b).
Sada ćemo dokazati da vijedi dio (b). Da bismo to učinili, sa S_d ćemo označiti dani reducirani sustav ostataka modulo d i pretpostavit ćemo da $r \in S_d$. Pokazat ćemo da je u skupu S najmanje $\frac{\varphi(k)}{\varphi(d)}$ cijelih brojeva n, međusobno nekongruentnih modulo k za koje vrijedi $n \equiv r \pmod{d}$. Budući da postoji $\varphi(d)$ vrijednosti od r u skupu S_d i $\varphi(k)$ cijelih brojeva u skupu S, ne može postojati više od $\frac{\varphi(k)}{\varphi(d)}$ takvih brojeva n pa je time dokazan dio (b).
Traženi brojevi n bit će odabrani iz klase ostataka modulo k koju predstavlja sljedećih $\frac{k}{d}$ cijelih brojeva:

$$r, r + d, r + 2d, \ldots, r + \frac{k}{d}d.$$

Ovi su brojevi međusobno kongruentni modulo d, a međusobno nekongruentni modulo k. Budući da su r i d relativno prosti, Teorem 10.2 pokazuje da je $\frac{\varphi(k)}{\varphi(d)}$ njih relativno prosto s brojem k pa je ovime dokaz završen. □

Nakon iskazanog teorema, možemo primijetiti da je u Primjeru 11.1 k jednak 15, a d jednak 3. Redci matrice predstavljaju disjunktne skupove iz dijela (a) u iskazu teorema, a stupci predstavljaju disjunktne skupove iz dijela (b). Ukoliko Teorem 11.1 primijenimo na djelitelj jednak 5 dobivamo dekompoziciju danu sljedećom matricom

$$\begin{bmatrix} 1 & 2 & 4 & 8 \\ 11 & 7 & 14 & 13 \end{bmatrix}.$$

Svaki je redak reducirani sustav ostataka modulo 5 i svaki se stupac sastoji od međusobno kongruentnih brojeva modulo 5.

Literatura

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

[2] A. Dujella, *Teorija brojeva*, Školska knjiga, Zagreb, 2019.

[3] I. Matić, *Uvod u teoriju brojeva*, Osijek, 2013.

[4] S. Paripović, *Primjena kongruencija*, Diplomski rad, Sveučilište J. J. Strossmayera u Osijeku, Odjel za matematiku, Osijek, 2018.

Sažetak

Kroz ovaj diplomski rad bavit ćemo se kongruencijama. Teorija kongruencija pripada teoriji brojeva, a za njezin razvoj posebno su značajni matematičari Johann Carl Friedrich Gauss, Leonhard Euler, Pierre de Fermat te Joseph-Louis Lagrange. Prvo ćemo se upoznati s pojmom kongruencije te proći kroz osnovna svojstva. Nadalje, definirat ćemo klasu ostataka modulo m, navesti odgovarajuća svojstva i definirati potpuni sustav ostataka modulo m. Proučavat ćemo polinomijalne kongruencije, odnosno navest ćemo te dokazati uvjete postojanosti rješenja takvih kongruencija te broj rješenja istih. U radu ćemo definirati Eulerovu funkciju te navesti njezina svojstva. Pomoću te funkcije uvest ćemo pojam reduciranog sustava ostataka te iskazati i dokazati Euler-Fermatov teorem. Nakon toga slijedi iskaz i dokaz Lagrangeovog teorema koji govori o poveznici broja rješenja polinomijalne kongruencije te njezina stupnja. Nastavno na to, prikazat ćemo neke primjene Lagrangeovog teorema. Također ćemo promatrati sustave linearnih kongruencija, odnosno pokazat ćemo kako sustav dviju ili više linearnih kongruencija svaka od kojih ima jedinstveno rješenje, takoder ima rješenje u slučaju kada su moduli kongruencija u parovima relativno prosti. O tome nam govori Kineski teorem o ostatcima i njegova generalizacija. Navest ćemo i neke od primjena Kineskog teorema, od kojih jedna prikazuje kako se može reducirati problem rješavanja polinomijalnih kongruencija. Iskazat ćemo i dokazati teorem o prebrojavanju skupova koji se naziva Princip unakrsne klasifikacije te kroz primjer prikazati izvod za produkt Eulerove funkcije pomoću tog principa. Na kraju ćemo pokazati kako se pomoću Principa unakrsne klasifikacije može napraviti dekompozicija reduciranih sustava ostataka modulo m. Sve navedeno potkrijepit ćemo primjerima.

Ključne riječi:
kongruencija, klasa ostataka modulo m, potpuni sustav ostataka modulo m, linearna kongruencija, polinomijalna kongruencija, Eulerova funkcija, reducirani sustav ostataka modulo m, Euler-Fermatov teorem, Lagrangeov teorem, sustav linearnih kongruencija, Kineski teorem o ostatcima, Princip unakrsne klasifikacije, dekompozicija

Congruences

Summary

Through this thesis we will deal with congruences. The theory of congruences is part of theory of numbers, and the mathematicians Johann Carl Friedrich Gauss, Leonhard Euler, Pierre de Fermat and Joseph-Louis Lagrange are especially important for its development. First, we will get acquainted with the concept of congruence and go through the basic properties. Furthermore, we will define the residue class modulo m, list the corresponding properties and define a complete residue system modulo m. We will study polynomial congruences, that is, we will state and prove conditions of existence of solutions of such congruences and the number of solutions. In this paper, we will define the Euler totient function and state its properties. Using this function, we will introduce the notion of a reduced residue system and state and prove the Euler-Fermat theorem. This is followed by the statement and proof of Lagrange's theorem, which speaks of relationship of the number of solutions of polynomial congruence and of her degree. Next, we will present some applications of Lagrange's theorem. We will also look at simultaneous linear congruences, i.e we will show how a system of two or more linear congruences each of which has a unique solution, also has a solution in the case where modules of congruences are relatively prime in pairs. This is dealt with by the Chinese remainder theorem and the generalization of that theorem. We will also list some of the applications of the Chinese theorem, one of which shows how the problem of solving polynomial congruences can be reduced. We will state and prove a set counting theorem called the Principle of cross-classification and through an example show the derivative for the product of the Euler totient function using this principle. Finally, we will show how decomposition of reduced residue systems modulo m can be done using the Principle of cross-classification. We will support all of the above with examples.

Keywords:
congruence, residue class modulo m, complete residue system modulo m, linear congruence, polynomial congruence, Euler totient function, reduced residue system modulo m, Euler-Fermat theorem, Lagrange theorem, simultaneous linear congruences, Chinese remainder theorem, the principle of cross-classification, decomposition

Životopis

Monika Rajkovača rođena 20.8.1997. u Slavonskom Brodu. Nakon završene osnovne škole "Ivan Goran Kovačić", upisujem Gimnaziju "Matija Mesić" u Slavonskom Brodu koju završavam 2016. godine. Iste godine upisujem preddiplomski studij matematike na Odjelu za matematiku u Osijeku i 2019. godine stječem naziv sveučilišne prvostupnice matematike uz završni rad s temom *Kongruentni brojevi* pod vodstvom izv. prof. dr. sc. Mirele Jukić Bokun. Odmah po završetku preddiplomskog studija, upisujem diplomski studij, smjer Financijska matematika i statistika, također na Odjelu za matematiku. Za vrijeme diplomskog studija odradila sam stručnu praksu u tvrtki Žito d.o.o. Osijek u Odjelu za maloprodaju i kooperaciju. Tijekom završne godine studija, završila sam PPDM izobrazbu na Filozofskom fakultetu u Osijeku te radila kao nastavnica matematike u Srednjoj medicinskoj školi u Slavonskom Brodu.