Jacobijev simbol

Boljfetić, Magdalena

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:025267

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-09-12**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

Jacobijev simbol

Boljfetić, Magdalena

Master's thesis / Diplomski rad

2021

Degree Grantor / Ustanova koja je dodijelila akademski / stručni stupanj: **University of Zagreb, Faculty of Science / Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet**

Permanent link / Trajna poveznica: https://urn.nsk.hr/urn:nbn:hr:217:025267

Rights / Prava: In copyright / Zaštićeno autorskim pravom.

Download date / Datum preuzimanja: **2024-06-20**

Repository / Repozitorij:

Repository of the Faculty of Science - University of Zagreb

SVEUČILIŠTE U ZAGREBU
PRIRODOSLOVNO–MATEMATIČKI FAKULTET
MATEMATIČKI ODSJEK

Magdalena Boljfetić

JACOBIJEV SIMBOL

Diplomski rad

Voditelj rada:
izv. prof. dr. sc. Zrinka Franušić

Zagreb, 2021.

Ovaj diplomski rad obranjen je dana _____ pred ispitnim povjerenstvom u sastavu:

1. _____, predsjednik
2. _____, član
3. _____, član

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

Diplomski rad posvećujem svojoj obitelji koja me podržavala tijekom cijelog mojeg obrazovanja.
Zahvaljujem mentorici, izv. prof. dr. sc. Zrinki Franušić, na ukazanom povjerenju, uloženom trudu, podršci i motivaciji tijekom cijelog studija.

Diplomski rad napravljen je u sklopu aktivnosti Projekta KK.01.1.1.01.0004 - Znanstveni centar izvrsnosti za kvantne i kompleksne sustave te reprezentacije Liejevih algebri.

Sadržaj

Uvod

"Matematika je kraljica znanosti, a teorija brojeva je kraljica matematike."

Carl Friedrich Gauss

Teorija brojeva jedna je od grana matematike koja se bavi proučavanjem svojstava prirodnih, cijelih i racionalnih brojeva. Razvoj teorije brojeva seže još od starogrčkih matematičara Diofanta i Euklida, a ocem moderne teorije brojeva smatra se Carl Friedrich Gauss. Teorija brojeva se kroz povijest većinu vremena odvajala od ostalih područja matematike smatrajući se "najčišćom" granom matematike, odnosno granom matematike koja nema konkretne primjene. Međutim, od sredine 70-ih godina 20. stoljeća teorija brojeva smatra se najvažnijom granom matematike za primjenu u kriptografiji.

Tema ovog diplomskog rada jest Jacobijev simbol, njegova svojstva i neke njegove primjene. Do pojma Jacobijevog simbola dolazi se postepeno. Najprije je potrebno definirati kvadratni ostatak modulo m, odnosno cijeli broj a za koji je kongruencija $x^2 \equiv a \pmod{m}$ rješiva. Zatim se uvodi pojam Legendreovog simbola $\left(\frac{a}{p}\right)$ koji je svojevrsni indikator kvadratnog ostatka modulo p, pri čemu je p neparan prost broj. Legendreov simbol $\left(\frac{a}{p}\right)$ poprima vrijednost 1 ako je a kvadratni ostatak modulo p, vrijednost -1 ako a nije kvadratni ostatak (tj. ako je a kvadratni neostatak) modulo p, te 0 ako p dijeli a. Glavna svojstva Legendreovog simbola proizlaze direktno iz tzv. *Eulerovog kriterija* koji kaže da je $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$. *Gaussov kvadratni zakon reciprociteta* jedan je od važnijih teorema teorije brojeva. On povezuje Legendreove simbole $\left(\frac{p}{q}\right)$ i $\left(\frac{q}{p}\right)$ za različite neparne proste brojeve p i q. Jednakost navedenih simbola vrijedi ako p ili q daju ostatak 1 pri dijeljenju s 4, a u suprotnom (tj. ako su oba broja kongruenta 3 modulo 4) simboli poprimaju suprotne vrijednosti. Za cijeli broj a i neparan prirodni broj Q definira se Jacobijev simbol $\left(\frac{a}{Q}\right)$ kao poopćenje Legendrevog simbola:

$$\left(\frac{a}{Q}\right) = \left(\frac{a}{q_1}\right)\left(\frac{a}{q_2}\right)\cdots\left(\frac{a}{q_n}\right),$$

gdje je $Q = q_1 q_2 \cdots q_n$, a $q_1, q_2, \ldots q_n$ su neparni prosti brojevi. Pokazuje se da Jacobijev simbol zadovoljava ista svojstva kao i Legendreov simbol, uključujući i Gaussov kvadratni zakon reciprociteta, no više nije indikator kvadratnog ostatka modulo Q.

Jacobijev simbol ima primjenu u testiranju prostosti, odnosno složenosti danog broja, a test se bazira na Eulerovom kriteriju. Naime, ako za neki neparan prirodan broj n ne vrijedi kongruencija

$$\left(\frac{b}{n}\right) \equiv b^{(n-1)/2} \pmod{n},$$

onda je n složen. Ovo predstavlja osnovnu ideju za tzv. *Solovay-Strassenov test prostosti*. U suprotnom, ako kongruencija vrijedi, onda n može biti ili prost ili složen. Složeni neparni brojevi za koje vrijedi navedena kongruencija nazivaju se *Eulerovi pseudoprosti brojevi u bazi b*.

Rad sadrži niz riješenih primjera iz ovog područja, a u zadnjem poglavlju navedeni su kratki životopisi matematičara koji su značajno doprinijeli razvoju ovog dijela teorije brojeva.

Poglavlje 1

Legendreov simbol

1.1 Kvadratni ostatci

Definicija 1.1.1. *Neka su a i m cijeli brojevi takvi da je $m > 1$ i $\text{nzd}(a, m) = 1$. Ako kongruencija $x^2 \equiv a \pmod{m}$ ima rješenja, onda kažemo da je a **kvadratni ostatak modulo** m. U protivnom kažemo da je a **kvadratni neostatak modulo** m.*

Kao što možemo primijetiti u definiciji, kvadratni ostatci i neostatci definirani su samo kada je najveći zajednički dijelitelj od a i m jednak 1, to jest kada su brojevi a i m relativno prosti. U sljedećem primjeru odredimo kvadratne ostatke i neostatke modulo neki zadani broj koristeći Definiciju 1.1.1.

Primjer 1.1.2. *Odredite sve kvadratne ostatke i neostatke modulo*

(a) $m = 7$*;*

(b) $m = 9$.

Rješenje. (a) Trebamo odrediti sve cijele brojeve a koji su relativno prosti s brojem 7 tako da postoji rješenje kongruencije $x^2 \equiv a \pmod{7}$. Skup svih nenegativnih reduciranih ostataka modulo 7 je $\{1, 2, 3, 4, 5, 6\}$. Budući da je

$$1^2 = 1, 2^2 = 4, 3^2 \equiv 2 \pmod{7}, 4^2 \equiv 2 \pmod{7}, 5^2 \equiv 4 \pmod{7}, 6^2 \equiv 1 \pmod{7},$$

zaključujemo da rješenje kongruencije postoji za sve cijele brojeve a takve da je $a \equiv 1, 2, 4 \pmod{7}$.

Uočimo, da smo to brže mogli zaključiti da smo odabrali skup reduciranih ostataka modulo 7 najmanjih po apsolutnoj vrijednosti $\{1, -1, 2, -2, 3, -3\}$ jer je $1^2 = (-1)^2 = 1$, $2^2 = (-2)^2 = 4$ i $3^2 = (-3)^2 = 9 \equiv 2 \pmod{7}$.

Dakle, svi kvadratni ostatci modulo 7 su $a \equiv 1, 2, 4 \pmod 7$ a neostatci su $a \equiv 3, 5, 6 \pmod 7$.

(b) Skup svih nenegativnih reduciranih ostataka modulo 9 je $\{1, 2, 4, 5, 7, 8\}$ a za kvadrate elementa tog skupa vrijedi:

$$1^2 = 1, 2^2 = 4, 4^2 \equiv 7 \pmod 9, 5^2 \equiv 7 \pmod 9, 7^2 \equiv 4 \pmod 9, 8^2 \equiv 1 \pmod 9.$$

Kongruencija $x^2 \equiv a \pmod 9$ ima rješenja za $a \equiv 1, 4, 7 \pmod 9$ pa ti brojevi predstavljaju kvadratne ostatke modulo 9. (I ovdje smo to mogli brže zaključiti da smo za reducirani sustav ostataka odabrali skup $\{1, -1, 2, -2, 4, -4\}$). Kvadratni neostatci modulo 9 su $a \equiv 2, 5, 8 \pmod 9$.

□

Teorem 1.1.3. *Neka je p neparan prosti broj. Reducirani sustav ostataka modulo p sastoji se od $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ kvadratnih neostataka.*

Dokaz. Budući da je skup $\{1, -1, 2, -2, \ldots, \frac{p-1}{2}, -\frac{p-1}{2}\}$ reducirani sustav ostataka modulo p, zaključujemo da je svaki kvadratni ostatak modulo p kongruentan nekom od brojeva $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.

Sada ćemo pokazati da su svi elementi skupa $\{1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2\}$ međusobno nekongruentni modulo p. Pretpostavimo da nisu, to jest da postoje k i l takvi da je $\leq k < l \leq \frac{p-1}{2}$ i $k^2 \equiv l^2 \pmod p$. To znači da $p \mid l^2 - k^2 = (l-k) \cdot (l+k)$. Kako je p prost broj, slijedi da $p \mid l - k$ ili $p \mid l + k$. No, to nije moguće jer $1 \leq l - k, l + k < p$. Stoga u reduciranom sustavu ostataka modulo p ima točno $\frac{p-1}{2}$ kvadratnih ostataka i isto toliko neostataka. □

1.2 Definicija Legendreovog simbola

Definicija 1.2.1. *Neka je p neparan prost broj i a cijeli broj.* ***Legendreov simbol****, u oznaci $\left(\frac{a}{p}\right)$, definira se kao*

$$\left(\frac{a}{p}\right) = \begin{cases} -1, & \textit{ako } a \textit{ nije kvadratni ostatak modulo } p, \\ 1, & \textit{ako je } a \textit{ kvadratni ostatak modulo } p, \\ 0, & \textit{ako } p \mid a. \end{cases}$$

Iz prethodne definicije je jasno da Legendreov simbol možemo shvatiti kao *indikator* kvadratnog ostatka modulo p.

Primjer 1.2.2. *Odredite Legendreove simbole $\left(\frac{121}{7}\right)$, $\left(\frac{14}{7}\right)$, $\left(\frac{10}{7}\right)$.*

Rješenje. Budući da je $121 = 11^2$ slijedi da je $\left(\frac{121}{7}\right) = 1$, zatim $7 \mid 14$ pa je $\left(\frac{14}{7}\right) = 0$. Prema Primjeru 2.1.2(a) slijedi da je $\left(\frac{10}{7}\right) = -1$ jer je $10 \equiv 3 \pmod 7$. □

Propozicija 1.2.3. *Neka je a cijeli broj i p neparan prost. Broj rješenja kongruencije $x^2 \equiv a \pmod p$ jednak je $1 + \left(\frac{a}{p}\right)$.*

Napominjemo da pod pojmom *broj rješenja kongruencije* mislimo na broj međusobno nekongruentnih (modulo p) rješenja.

Dokaz.

- Ako $p \mid a$, onda su sva rješenja kongruencije $x^2 \equiv a \pmod p$ dana s $x \equiv 0 \pmod p$. Dakle, broj rješenja kongruencije je 1 što je jednako izrazu $1 + \left(\frac{a}{p}\right)$.

- Ako je a kvadratni ostatak modulo p, onda prema Definiciji 1.1.1 postoji $x_1 \in \mathbb{Z}$ takav da je $x_1^2 \equiv a \pmod p$. No, tada je i $(-x_1)^2 \equiv a \pmod p$. Uočimo da su x_1 i $-x_1$ međusobno nekongruentni modulo p jer bi suprotnom vrijedilo da $p \mid 2x_1$ što nije moguće. Dakle, kongruencija $x^2 \equiv a \pmod p$ ima barem 2 rješenja. Još trebamo ustanoviti da nema drugih rješenja. Ako bi postojao $x_2 \in \mathbb{Z}$ takav da $x_2 \not\equiv \pm x_1 \pmod p$, onda bi vrijedilo $x_1^2 - x_2^2 = (x_1 - x_2)(x_1 + x_2) \equiv 0 \pmod p$ što očito ne vrijedi (jer $p \nmid x_1 - x_2, x_1 + x_2$). Stoga kongruencija $x^2 \equiv a \pmod p$ ima točno $2 = 1 + \left(\frac{a}{p}\right)$ rješenja.

- Ako je a kvadratni neostatak modulo p, onda prema Definiciji 1.1.1 kongruencija $x^2 \equiv a \pmod p$ nema rješenja pa ponovo vrijedi $0 = 1 + \left(\frac{a}{p}\right)$.

□

1.3 Eulerov kriterij

U prethodnom poglavlju pokazali smo kako Legendreov simbol $\left(\frac{a}{p}\right)$ računamo direktno iz definicije kvadratnog ostatka modulo p. Za to smo trebali odrediti sve kvadrate elemenata skupa $\{1, 2, \ldots, \frac{p-1}{2}\}$ što je za veći p uistinu velik posao. *Eulerov*[2] *kriterij* je naziv za tvrdnju koja nam daje *formulu* za računanje Legendreovog simbola. Štoviše, pomoću te formule moći ćemo izvesti još neka svojstva Legenderovog simbola koja uvelike olakšavaju njegovo određivanje.

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

Teorem 1.3.1 (Eulerov kriterij)**.** *Za svaki cijeli broj a i neparni prosti broj p vrijedi*

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}. \tag{1.1}$$

Da bismo dokazali Eulerov kriterij potrebne su nam dvije važne tvrdnje iz Elemetarne teorije brojeva. To su *Mali Fermatov teorem* i *Wilsonov teorem*. Wilsonov teorem važan je zato što daje nužan i dovoljan uvijet da bi broj bio prost.

Teorem 1.3.2 (Mali Fermatov teorem)**.** *Neka je p prost broj i $a \in \mathbb{N}$ takav da $p \nmid a$. Tada*

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

Teorem 1.3.3 (Wilsonov teorem)**.** *Broj p prost ako i samo ako je $(p-1)! \equiv -1 \pmod{p}$.*

Dokaz Eulerovog kriterija. Razlikujemo tri slučaja: 1. $p \mid a$, 2. a je kvadratni ostatak modulo p i 3. a je kvadratni neostatak modulo p.

1. Kako je $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$, relacija (1.2) vrijedi.

2. Postoji $x_0 \in \mathbb{Z}$ takav da je $x_0^2 \equiv a \pmod{p}$. Iz Malog Fermatovog teorema 1.3.2 slijedi
$$a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 = \left(\frac{a}{p}\right) \pmod{p}.$$

3. Neka je $\left(\frac{a}{p}\right) = -1$. Vrijedi tvrdnja:

   Za svaki $i \in \{1, \ldots, p-1\}$ postoji jedinstven $j \in \{1, \ldots, p-1\} \setminus \{i\}$ takav da vrijedi $i \cdot j \equiv a \pmod{p}$.

   Za $i \in \{1, \ldots, p-1\}$ kongruencija $ix \equiv a \pmod{p}$ ima jedinstveno rješenje $x = i \in \{1, \ldots, p-1\}$. Još trebamo ustanoviti da je $i \neq j$. U suprotnom bi vrijedilo da $i^2 \equiv a \pmod{p}$ što znači da bi a bio kvadratni ostatak, što nije. Time smo dokazali istaknutu tvrdnju prema kojoj se $\{1, ..., p-1\}$ "raspada" na $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $i \cdot j \equiv a \pmod{p}$. Ako pomnožimo svih tih $\frac{p-1}{2}$ kongruencija i primijenimoWilsonov teorem 1.3.3 dobit ćemo $a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}$.

□

Primjer 1.3.4. *Izračunajte vrijednost Legendreovog simbola $\left(\frac{50}{71}\right)$ pomoću Eulerov kriterija.*

Rješenje. Vrijedi

$$\left(\frac{50}{71}\right) \equiv 50^{35} = 2^{35}5^{70} \pmod{71}.$$

Prema Malom Fermatovom teoremu 1.3.2 je $5^{70} \equiv 1 \pmod{71}$. Nadalje, je $2^{35} \equiv 1 \pmod{71}$ pa je $\left(\frac{50}{71}\right) = 1$. □

Teorem 1.3.5 (Svojstva Legendreovog simbola)**.** *Neka su $a, b \in \mathbb{Z}$ i p neparan prost broj. Tada vrijedi:*

1. *ako je $a \equiv b \pmod{p}$, onda je $\left(\frac{a}{p}\right) \equiv \left(\frac{b}{p}\right)$;*
2. $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$;
3. *ako $p \nmid a$, onda* $\left(\frac{a^2}{p}\right) = 1$.

Dokaz. Tvrdnje 1 i 2 trivijalno vrijede ako $p \mid a$ ili $p \mid b$. Pretpostavimo da $p \nmid a, b$.

1. Ako je $a \equiv b \pmod{p}$, onda kongruencija $x^2 \equiv a \pmod{p}$ ima rješenja ako i samo ako rješenja ima kongruencija $x^2 \equiv b \pmod{p}$.

2. Koristeći Eulerov kriterij dobivamo

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}, \quad \left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p},$$

   pa slijedi

$$\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) \equiv a^{\frac{p-1}{2}} b^{\frac{p-1}{2}} \equiv (ab)^{\frac{p-1}{2}} \equiv \left(\frac{ab}{p}\right) \pmod{p}.$$

3. Kongruencija $x^2 \equiv a^2 \pmod{p}$ ima rješenja pa je $\left(\frac{a^2}{p}\right) = 1$ jer $p \nmid a$.

□

Primjer 1.3.6. *Za sve $n \in \mathbb{Z}$ i neparne proste brojeve p vrijedi*

$$\sum_{i=1}^{p-1} \left(\frac{i \cdot n}{p}\right) = 0$$

Rješenje. Prema svojstvu (2) Teorema 1.3.5 vrijedi

$$\sum_{i=1}^{p-1}\left(\frac{i\cdot n}{p}\right)=\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)\left(\frac{n}{p}\right)=)\left(\frac{n}{p}\right)\sum_{i=1}^{p-1}\left(\frac{i}{p}\right).$$

U skupu $\{1,2,\ldots,p-1\}$ ima točno $(p-1)/2$ kvadratnih ostatak i $(p-1)/2$ kvadratnih neostataka (Teorem 1.1.3) pa je

$$\sum_{i=1}^{p-1}\left(\frac{i}{p}\right)=0.$$

□

Teorem 1.3.7. *Ako je p neparan prost broj, tada*

$$\left(\frac{-1}{p}\right)=\begin{cases}1, & \text{ako je } p\equiv 1 \pmod 4\\ -1, & \text{ako je } p\equiv -1 \pmod 4.\end{cases}$$

Dokaz. Iz Eulerovog kriterija znamo da je

$$\left(\frac{-1}{p}\right)\equiv(-1)^{\frac{p-1}{2}} \pmod p.$$

Ako je $p\equiv 1 \pmod 4$), onda $p=4k+1$, za neki prirodan broj k, pa je

$$(-1)^{\frac{p-1}{2}}=(-1)^{2k}=1.$$

Ako je $p\equiv -1 \pmod 4$, onda $p=4k-1$, za neki prirodan broj k, pa

$$(-1)^{\frac{p-1}{2}}=(-1)^{2k-1}=-1.$$

□

Korolar 1.3.8. *Ako je p neparan prost broj, tada je* $\left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Primjer 1.3.9. *Izračunajte Legendreov simbol* $\left(\frac{55}{67}\right)$.

Rješenje. Koristimo svojstva iz Teorema 1.3.5:

$$\left(\frac{55}{67}\right)=\left(\frac{5}{67}\right)\cdot\left(\frac{11}{67}\right)=\left(\frac{-62}{67}\right)\cdot\left(\frac{-56}{67}\right)=\left(\frac{-1}{67}\right)\cdot\left(\frac{2}{67}\right)\cdot\left(\frac{31}{67}\right)\cdot\left(\frac{-1}{67}\right)\cdot\left(\frac{8}{67}\right)\cdot\left(\frac{7}{67}\right).$$

Kako je

$$\left(\frac{-1}{67}\right)^2=1,\ \left(\frac{2}{67}\right)\cdot\left(\frac{8}{67}\right)=\left(\frac{16}{67}\right)=1,$$

te $7\cdot 31\equiv 16=4^2 \pmod{67}$ slijedi da je $\left(\frac{55}{67}\right)=1$. □

1.4 Kvadratni zakon reciprociteta

Kvadratni zakon reciprociteta se često naziva i *Gaussov* kvadratni zakon reciprociteta. Naime, Euler i Legendre su pretpostavili njegovu tvrdnju, no dokaz je prvi dao Gauss te ga je obavio u djelu *Disquisitiones Arithmeticae* godine 1801. Tvdnja kvadratnog zakona reciprociteta omogućava još elegantnije i brže računanje Legendreovog simbola.

Teorem 1.4.1 (Gaussova kvadratni zakon reciprociteta)**.** *Neka su p i q dva različita neparna prosta broja. Tada*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = \begin{cases} -1, & \text{ako } p \equiv q \equiv 3 \pmod 4, \\ 1, & \text{ako } p \equiv 1 \pmod 4 \text{ ili } q \equiv 1 \pmod 4. \end{cases}$$

Gauss, ne samo da je prvi pronašao dokaz prethodne tvrdnje, već je dao čak osam različitih dokaza. Trenutno postoji više od 150 dokaza kvadratnog zakona reciprociteta. Mi ćemo ovdje izložiti jedan za koji nam je potrebna tzv. *Gaussova lema* i jedna tehnička lema.

Prema *Teoremu o dijeljenju s ostatkom* za svaki $a \in \mathbb{Z}$ i $b \in \mathbb{N}$ postoje jedinstveni $q \in \mathbb{Z}$ i $0 \leq r < b$ takvi da je $a = bq + r$. Broj r, odnosno najmanji nenegativni ostatak pri dijeljenju broja a brojem b označavat ćemo s $r = a \mod b$.

Teorem 1.4.2 (Gaussova lema)**.** *Neka su $a \in \mathbb{Z}$, p neparni prost broj i* $\operatorname{nzd}(a,p) = 1$. *Ako je*

$$n := \sharp^{1}\left(\{a \mod p, 2a \mod p, 3a \mod p, \ldots, \frac{p-1}{2}\cdot a \mod p\} \cap \langle \frac{p}{2}, p-1]\right),$$

tada je $\left(\frac{a}{p}\right) = (-1)^n$.

Dokaz. Označimo s $r_1, \ldots, r_n$ ostatke koji su veći od $\frac{p}{2}$, a sa $s_1, \ldots, s_k$ ostatke manje od $\frac{p}{2}$. Za navedene ostatke vrijedi:

- $r_i \neq r_j$ za $i \neq j$. Zaista, ako $r_i = r_j$, onda $\alpha p \equiv \beta p \pmod p$ za neke $1 \leq \alpha, \beta \leq \frac{p-1}{2}$ i $\alpha \neq \beta$. No, tada $p \mid \alpha - \beta$ što nije moguće.
- $s_i \neq s_j$ za $i \neq j$.

Iz pretodnog i očite činjenice da je $r_i \neq s_j$ za $i = 1, \ldots n$, $j = 1, \ldots, k$, vrijedi da je $n + k = \frac{p-1}{2}$.

Sada ustanovimo sljedeća svojstva:

[1] broj elemenata skupa

- $p - r_i \neq p - r_j$ za sve $i \neq j$.
- $0 < p - r_i < \frac{p}{2}$, za $i = 1, \ldots, n$,
- $p - r_i \neq s_j$, za sve $i = 1, \ldots n$, $j = 1, \ldots, k$. Ako bi vrijedila jednakost $p - r_i = s_j$ tada bi imali $-\alpha p \equiv \beta p \pmod{p}$ za neke $1 \leq \alpha, \beta \leq \frac{p-1}{2}$ i $\alpha \neq \beta$. To znači da $p \mid a(\alpha + \beta)$. No, takvo što moguće jer $\text{nzd}(a, p) = 1$ i $2 \leq \alpha + \beta \leq p - 1$.

Iz prethodnih tvrdnji zaključujemo da su svi elementi skupa $\{p-r_1, \ldots, p-r_n, s_1, \ldots, s_k\}$ međusobno različiti, veći od 0, manji ili jednaki $\frac{p-1}{2}$ elementi te da je kardinalni broj tog skupa upravo $\frac{p-1}{2}$. Stoga je

$$\{p - r_1, \ldots, p - r_n, s_1, \ldots, s_k\} = \{1, \ldots, \frac{p-1}{2}\},$$

odnosno

$$(p - r_1) \cdots (p - r_n) s_1 \cdots s_k = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right).$$

Sada dobivamo

$$\begin{aligned}
\left(\frac{p-1}{2}\right)! &\equiv (-r_1) \cdots (-r_n) s_1 \cdots s_k \\
&\equiv (-1)^n r_1 \cdots r_n s_1 \cdots s_k \\
&\equiv (-1)^n a \cdot 2a \cdot 3a \cdots \left(\frac{p-1}{2}\right) a \\
&= (-1)^n a^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.
\end{aligned}$$

Skraćivanjem kongruencije s $\left(\frac{p-1}{2}\right)!$ dobivamo

$$(-1)^n a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Prema Eulerovom kriteriju 1.3.1 je $\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}$ pa smo dokazali traženu tvrdnju, $\left(\frac{a}{p}\right) \equiv (-1)^n \pmod{p}$. □

Primjer 1.4.3. *Koristeći Gaussovu lemu odredite vrijednost Legendreovog simbola* $\left(\frac{7}{11}\right)$.

Rješenje. Zadano je $a = 7$, $p = 11$. Odredimo najmanje nenegativne ostatke pri dijeljenju broja $7k$ brojem 11, za sve $k = 1, \ldots, 5$,

$$\begin{aligned} 1 \cdot 7 &\equiv 7 \pmod{11}, \\ 2 \cdot 7 &\equiv 3 \pmod{11}, \\ 3 \cdot 7 &\equiv 10 \pmod{11}, \\ 4 \cdot 7 &\equiv 6 \pmod{11}, \\ 5 \cdot 7 &\equiv 2 \pmod{11}. \end{aligned}$$

Točno 3 ostatka su veća od $\frac{p-1}{2} = 5$ pa je $\left(\frac{7}{11}\right) = (-1)^3 = -1$. □

Primjenom Gaussove leme 1.4.2 može se dokazati sljedeće lema čiji ćemo dokaz preskočiti.

Lema 1.4.4. *Neka je a neparni cijeli broj i p neparni prost broj. Tada je*

$$\left(\frac{a}{p}\right) = (-1)^t, \ \textit{za } t = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor^{2}.$$

Također vrijedi

$$\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}} = \begin{cases} -1, & \textit{ako } p \equiv 3 \textit{ ili } 5 \pmod 8, \\ 1, & \textit{ako } p \equiv 1 \textit{ ili } 7 \pmod 8. \end{cases}$$

Ideja dokaza. Pokazuje se da su brojevi n (definiran u Lemi 1.4.2) i t, odnosno $(p^2 - 1)/8$ (u slučaju $a = 2$) iste parnosti. Dokaz se može naći u [3]. □

Dokaz teorem 1.4.1. Neka je

$$S = \left\{ (x, y) \in \mathbb{Z}^2 \, : \, 1 \leq x \leq \frac{p-1}{2}, \ 1 \leq y \leq \frac{q-1}{2} \right\}.$$

Skup S koji ima $\frac{p-1}{2} \cdot \frac{q-1}{2}$ članova, tj. $|S| = \frac{p-1}{2} \cdot \frac{q-1}{2}$, prikazat ćemo ako uniju dva disjunktna podskupa S_1 i S_2 s obzirom na to je li $qx > py$ ili $qx < py$. Uočimo da je $px \neq qy$ za $(x, y) \in S$. Dakle, neka su

$$S_1 = \{(x, y) \in S \, : \, py < qx\} = \{(x, y) \in \mathbb{Z}^2 \, : \, 1 \leq x \leq \frac{p-1}{2}, \ 1 \leq y < \frac{qx}{p}\},$$

[2] $\lfloor x \rfloor$ je najveće cijelo broja $x \in \mathbb{R}$

$$S_2 = \{(x,y) \in S \,:\, qx < py\} = \{(x,y) \in \mathbb{Z}^2 \,:\, 1 \leq y \leq \frac{q-1}{2},\ 1 \leq x < \frac{py}{q}\}.$$

"Prebrojimo" elemente skupova S_1 i S_2:

$$|S_1| = \sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor,\ |S_2| = \sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor.$$

Kako je

$$S = S_1 \cup S_2,\ S_1 \cap S_2 = \emptyset,$$

vrijedi $|S| = |S_1| + |S_2|$, pa je

$$(-1)^{|S|} = (-1)^{|S_1|+|S_2|} = (-1)^{|S_1|}(-1)^{|S_2|}.$$

Prema Lemi 1.4.4 je

$$(-1)^{|S_1|} = \left(\frac{p}{q}\right),\ (-1)^{|S_2|} = \left(\frac{q}{p}\right),$$

čime smo dokazali tvrdnju

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

□

Primjer 1.4.5. *Koristeći Gaussov kvadratni zakon reciprociteta odredite vrijednost Legendreovog simbola* $\left(\frac{-14}{61}\right)$.

Rješenje. Vrijedi

$$\left(\frac{-14}{61}\right) = \left(\frac{-1}{61}\right)\cdot\left(\frac{2}{61}\right)\cdot\left(\frac{7}{61}\right).$$

Kako je $61 \equiv 1 \pmod 4$, prema Teoremu 1.3.7 je

$$\left(\frac{-1}{61}\right) = 1.$$

Nadalje, prema Lemi 1.4.4 jer je $61 \equiv 5 \pmod 8$ imamo

$$\left(\frac{2}{61}\right) = -1.$$

Primjenom Gaussova kvadratnog zakona reciprociteta 1.4.1 dobivamo

$$\left(\frac{7}{61}\right) = \left(\frac{61}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{7}{5}\right) = \left(\frac{2}{5}\right) = -1,$$

pa je $\left(\frac{-14}{61}\right) = 1$. □

Primjer 1.4.6. *Pokažite da postoji beskonačno mnogo prostih brojeva oblika* $5k+4$.

Rješenje. Prvo ćemo odrediti sve proste brojeve p za koje je $\left(\frac{5}{p}\right) = 1$. Kako je $5 \equiv 1 \pmod 4$, prema Gaussovom kvadratnom zakonu reciprociteta 1.4.1 vrijedi da je

$$\left(\frac{5}{p}\right) = \left(\frac{p}{5}\right).$$

Kvadratni ostatci modulo 5 su svi cijeli brojevi kongruentni 1 ili 4. Stoga je $\left(\frac{5}{p}\right) = 1$ ako i samo ako je $p \equiv \pm 1 \pmod 5$.

Pretpostavimo da su $p_1, \ldots, p_n$ svi prosti brojevi oblika $5k+4$, odnosno pretpostavljamo da prostih brojeva oblika $5k+4$ ima konačno mnogo. Tada je broj

$$N = 5p_1^2 \cdots p_n^2 - 1$$

također oblika $5k+4$. Neka je q neki prosti djelitelj od N. Očito je $q \neq p_i$ za sve $i = 1, \ldots, n$. Nadalje, vrijedi

$$5(p_1 \cdots p_n)^2 \equiv 1 \pmod p,$$

pa množenjem s 5 dobivamo

$$(5p_1 \cdots p_n)^2 \equiv 5 \pmod p.$$

Iz zadnje kongruencije zaključujemo da je 5 kvadratni ostatak modulo p. Stoga je $p \equiv \pm 1 \pmod 5$. Ako bi svi prosti djelitelji od N bili oblika $5k+1$ (tj. kongruentni 1 modulo 5), onda bi i n bio tog oblika. Dakle, N mora imati prostog djelitelja oblika $5k+4$ i budući da je taj djelitelj različit od p_i, za sve $i = 1, \ldots, n$, zaključujemo da je pretpostavka da postoji konačno mnogo prostih brojeva oblika $5k+4$ kriva.

□

1.5 Kvadratni korijen modulo n

Neka je $n = p \cdot q$ za neke p, q neparne proste brojeve, te $a \in \mathbb{N}$ i $a < n$. Pretpostavit ćemo da kongruencija

$$x^2 \equiv a \pmod{n}, \tag{1.2}$$

ima rješenje $x_0 \in \mathbb{Z}$. Svako rješenje kongruencije (1.2) naziva se *kvadratni korijen modulo n*. Pokazat ćemo da postoje točno četiri, međusobno nekongruentna modulo n, kvadratna korijena modulo n.

Očito je da kongruencija (1.2) ekvivalenta sustavu kongruencija

$$x^2 \equiv a \pmod{p},\ x^2 \equiv a \pmod{q}. \tag{1.3}$$

Budući da smo pretpostavili da je kongruencija (1.2) rješiva, slijedi da je a kvadratni ostatak modulo p i kvadratni ostatak modulo q. U tom slučaju svaka od kongruencija iz (1.4) ima točno dva rješenja (Propozicija 1.2.3). Dakle, postoje $x_1, x_2 \in \mathbb{N}$ i $x_1 < p$, $x_2 < q$ takvi da je

$$x \equiv x_1 \pmod{p},\ x \equiv p - x_1 \pmod{p}$$

te

$$x \equiv x_2 \pmod{q},\ x \equiv q - x_2 \pmod{q}.$$

Stoga je početna kvadratna kongruencija (1.2) ekvivalentna četiri sustava od po dvije linearne kongruencije:

(i) $x \equiv x_1 \pmod{p}$, $x \equiv x_2 \pmod{q}$;

(ii) $x \equiv x_1 \pmod{p}$, $x \equiv q - x_2 \pmod{q}$;

(iii) $x \equiv p - x_1 \pmod{p}$, $x \equiv x_2 \pmod{q}$;

(iv) $x \equiv p - x_1 \pmod{p}$, $x \equiv q - x_2 \pmod{q}$.

O rješenjima sustava linearnih kongruencija govori tvrdnja Kineskog teorema o ostatcima.

Teorem 1.5.1 (Kineski teorem o ostatcima)**.** *Neka su $m_1, \ldots, m_r$ u parovima relativno prosti prirodni brojevi, te neka su $a_1, \ldots, a_r$ cijeli brojevi. Tada sustav kongruencija*

$$\begin{aligned} x &\equiv a_1 \pmod{m_1} \\ x &\equiv a_2 \pmod{m_2}, \\ &\vdots \\ x &\equiv a_r \pmod{m_r} \end{aligned}$$

ima rješenja. Ako je x_0 jedno rješenje, onda su sva rješenja tog sustava dana s

$$x \equiv x_0 \pmod{m_1 m_2 \cdots m_r}.$$

Skica rješenja. Rješenje sustava kongruencija iz teorema dano je s

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

gdje je $n_i = m_1 m_2 \cdots \hat{m}_i \cdots m_r = (m_1 m_2 \cdots m_r)/m_i$ i $n_i x_i \equiv a_i \pmod{m_i}$ za $i = 1, \ldots, r$.

Pokazuje se da su svaka dva rješenja sustava kongruencija kongruentna modulo $m_1 m_2 \cdots m_r$. □

Budući da su p i q različiti prosti brojevi, sustavi (i)-(iv) zadovoljavaju uvjete prethodnog teorema i slijedi da svaki od sustava (i)-(iv) ima točno jedno rješenje modulo $pq = n$. Lako se vidi da su rješenja svakog od sustava međusobno nekongruentna modulo n pa smo pokazali da ako kongruencija (1.2) ima rješenja, onda ih ima točno četiri. Nadalje, ako su y_1 i y_2 redom rješenja sustava (i) i (ii), onda su rješenja od (iii) i (iv) dana s $n - y_2$ i $n - y_1$.

Za neke oblike prostih brojeva, kao što ćemo vidjeti u sljedećim propozicijama, možemo eksplicitno odrediti rješenja kongruencije $x^2 \equiv a \pmod{p}$.

Propozicija 1.5.2. *Neka je a kvadratni ostatak modulo p. Ako je broj p oblika $4k+3$, onda su rješenja kongruencije $x^2 \equiv a \pmod{p}$ dana s*

$$x_{1,2} = \pm a^{\frac{p+1}{4}}.$$

Dokaz. Koristeći činjenicu da je a kvadratni ostatak modulo p i iz Eulerovog kriterija 1.3.1 imamo:

$$x_{1,2}^2 \equiv a^{\frac{p+1}{2}} \equiv a \cdot a^{\frac{p-1}{2}} \equiv a \pmod{p}.$$

Rješenja x_1 i x_2 su očito nekongruentna modulo p. □

Pretpostavimo da su $p \equiv q \equiv 3 \pmod 4$. Tada prema prethodnoj propoziciji slijedi da kongruencija (1.2) ekvivalentna sljedeća četiri sustava kongruencija:

$$x \equiv \pm a^{\frac{p+1}{4}} \pmod{p}, \; x \equiv \pm a^{\frac{q+1}{4}} \pmod{q}.$$

(Svaki od sustava se dobije različitom kombinacijom predznaka).

Primjer 1.5.3. *Odredite, ako postoje, kvadratne korijene broja* 560 *modulo* 2369.

Rješenje. Trebamo riješiti kongruenciju $x^2 \equiv 560 \pmod{2369}$. Kako je $2369 = 103 \cdot 23$ i $103, 23$ su prosti brojevi koji daju ostatak 3 pri dijeljenju s 4, prema Propoziciji 1.5.2 slijedi da je navedena kvadratna kongruencija ekvivalentana sljedećim sustavima linearnih kongruencija:

(i) $x \equiv 560^{26} \equiv 56 \pmod{103},\ x \equiv 560^6 \equiv 3 \pmod{23}$,

(ii) $x \equiv 560^{26} \equiv 26 \pmod{103},\ x \equiv -560^6 \equiv -3 \pmod{23}$,

(iii) $x \equiv -560^{26} \equiv -56 \pmod{103},\ x \equiv 560^6 \equiv 3 \pmod{23}$,

(iv) $x \equiv -560^{26} \equiv -56 \pmod{103},\ x \equiv -560^6 \equiv -3 \pmod{23}$.

Rješavamo redom svaki od sustava. Kako je

$$23 \cdot (\pm 92) \equiv \pm 56 \pmod{103},\ 103 \cdot (\pm 17) \equiv \pm 3 \pmod{23},$$

rješenja sustava (i)-(iv) su:

$$x \equiv 23 \cdot 92 + 103 \cdot 17 = 3867 \equiv 1498 \pmod{2369},$$

$$x \equiv 23 \cdot 92 + 103 \cdot (-17) = 365 \pmod{2369},$$

$$x \equiv 23 \cdot (-92) + 103 \cdot 17 = -365 \equiv 2004 \pmod{2369},$$

$$x \equiv 23 \cdot (-92) + 103 \cdot (-17) = -3867 \equiv 871 \pmod{2369}.$$

Kao što smo napomenuli, nismo morali računati rješenja sustava (iii) i (iv) jer za njih vrijedi da su jednaka $-y_0, -x_0$ (odnosno $n - y_0$, $n - x_0$) ako su x_0, y_0 rješenja sustava (i) i (ii).

Svi korijeni od 560 modulo 2369 su:

$$x \equiv 365, 871, 1498, 2004 \pmod{2369}.$$

□

Za proste brojeve oblika $4k + 1$ općenito ne možemo eksplicitno naći rješenje kongruencije $x^2 \equiv a \pmod{p}$, ako ono postoji, no za proste brojeve podoblika $8k + 5$ ipak možemo prilično dobro "suziti" izbor mogućih rješenja.

Propozicija 1.5.4. *Neka je a kvadratni ostatak modulo p. Ako je broj p oblika $8k+5$, onda je rješenje kongruencije $x^2 \equiv a \pmod{p}$ jedan od brojeva*

$$a^{\frac{p+3}{8}},\ 2^{\frac{p-1}{4}} a^{\frac{p+3}{8}}.$$

Dokaz. Ako je $p = 8k + 5$, onda je $a^{(p-1)/2} = a^{4k+2} \equiv 1 \pmod{p}$ (Eulerov kriterij 1.3.1). Iz toga slijedi da je $a^{2k+1} \equiv \pm 1 \pmod{p}$, odnosno

$$a^{2k+2} \equiv \pm a \pmod{p}. \tag{1.4}$$

S obzirom na predznak u relaciji (1.4) razlikujemo:

- Ako je $a^{2k+2} \equiv a \pmod{p}$, onda je $(a^{k+1})^2 \equiv a \pmod{p}$ pa je rješenje kvadratne kongruencije $x^2 \equiv a \pmod{p}$ dano s $x \equiv a^{\frac{p+3}{8}} \pmod{p}$.
- Ako $a^{2k+2} \equiv -a \pmod{p}$, onda ćemo iskoristiti činjenicu da je broj 2 kvadratni neostatak modulo p, tj. $2^{(p-1)/2} = 2^{4k+2} \equiv -1 \pmod{p}$. Kako je

  $$2^{4k+2}a^{2k+2} \equiv (-1)(-a) = a \pmod{p}$$

  slijedi da je $x \equiv 2^{2k+1}a^{k+1} = 2^{\frac{p-1}{4}}a^{\frac{p+3}{8}} \pmod{p}$ rješenje kvadratne kongruencije $x^2 \equiv a \pmod{p}$.

□

Poglavlje 2

Jacobijev simbol

2.1 Jacobijev simbol

Jacobijev simbol uvodi se kao generalizacija Legendreovog simbola opisanog u prvom poglavlju. Dakle, definirat ćemo simbol $\left(\frac{a}{Q}\right)$ gdje je Q općenito neparan broj, a ne nužno neparan prost broj kao u slučaju Legendreovog simbola.

Definicija 2.1.1. *Neka je Q neparni prirodni broj oblika $Q = q_1^{t_1} \cdots q_s^{t_s}$, gdje su q_i različiti neparni prosti brojevi i $t_i \in \mathbb{N}$ za sve $i = 1, \ldots, s$. Za $a \in \mathbb{Z}$ definiramo* ***Jacobijev simbol****, u oznaci $\left(\frac{a}{Q}\right)$, kao*

$$\left(\frac{a}{Q}\right) = \left(\frac{a}{q_1^{t_1} q_2^{t_2} \cdots q_s^{t_s}}\right) = \left(\frac{a}{q_1}\right)^{t_1} \left(\frac{a}{q_2}\right)^{t_2} \cdots \left(\frac{a}{q_s}\right)^{t_s},$$

gdje su $\left(\frac{a}{q_j}\right)$, $j = 1, \ldots, s$, Legendreovi simboli.

Uočimo da je $Q = q_1^{t_1} \cdots q_s^{t_s}$, gdje su q_i različiti neparni prosti brojevi i $t_i \in \mathbb{N}$ za sve $i = 1, \ldots, s$, upravo kanonski rastav broja Q na proste faktore. No, i za $Q = p_1 p_2 \cdots p_k$, gdje su $p_1, p_2, \ldots, p_k$ neparni prosti brojevi i ne nužno različiti vrijedi:

$$\left(\frac{a}{Q}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right) \cdots \left(\frac{a}{p_k}\right).$$

Primjer 2.1.2. *Odredite vrijednost Jacobijevog simbola* $\left(\frac{5935}{18837}\right)$.

Rješenje. Broj 18837 neparan je složeni broj čija je faktorizacija

$$18837 = 7 \cdot 3^2 \cdot 13 \cdot 23.$$

Prema Definiciji 2.1.1, imamo

$$\left(\frac{5935}{18837}\right) = \left(\frac{5935}{7}\right) \cdot \left(\frac{5935}{3}\right)^2 \cdot \left(\frac{5935}{13}\right) \cdot \left(\frac{5935}{23}\right)$$

Iskoristimo li prvo svojstvo Legendreovog simbola iz Teorema 1.3.5 dobivamo

$$\left(\frac{5935}{18837}\right) = \left(\frac{6}{7}\right) \cdot \left(\frac{1}{3}\right)^2 \cdot \left(\frac{7}{13}\right) \cdot \left(\frac{1}{23}\right). \tag{2.1}$$

Kako je

$$\left(\frac{6}{7}\right) = -1, \ \left(\frac{1}{3}\right) = 1, \ \left(\frac{7}{13}\right) = -1, \ \left(\frac{1}{23}\right) = 1,$$

uvrštavanjem u relaciju (2.1) imamo

$$\left(\frac{5935}{18837}\right) = (-1) \cdot 1^2 \cdot (-1) \cdot 1 = 1.$$

□

Kao što možemo primjetiti iz definicija 1.2.1 i 2.1.1, Jacobijev i Legendreov simbol se podudaraju ako je Q prosti broj. Također, ako je $\text{nzd}(a, Q) > 1$, onda je $\left(\frac{a}{Q}\right) = 0$, a inače je $\left(\frac{a}{Q}\right) \in \{-1, 1\}$.

Sljedeće što možemo primjetiti jest da vrijednost Jacobijevog simbola $\left(\frac{a}{Q}\right)$ ne govori ništa o rješenju kongruencije $x^2 \equiv a \pmod{Q}$. Naime, Legendreov simbol je *indikator* kvadratnog ostatka. Dakle, kongruencija $x^2 \equiv a \pmod{p}$ (pri čemu je p prost broj) ima rješenje ako i samo ako je vrijednost Legendreovog simbola jednaka 1. Ako kongruencija $x^2 \equiv a \pmod{Q}$, $Q = q_1^{t_1} \cdots q_s^{t_s}$, ima rješenja onda i kongruencije $x^2 \equiv a \pmod{q_i}$ imaju rješenje za sve $i = 1, \ldots, s$ (pri čemu smo pretpostavili da je $Q = q_1^{t_1} \cdots q_s^{t_s}$, i q_i neparni prosti brojevi) pa je stoga i $\left(\frac{a}{Q}\right) = 1$. Obrat ne mora vrijediti, odnosno iz $\left(\frac{a}{Q}\right) = 1$ ne možemo zaključiti da je a kvadratni ostatak modulo Q, odnosno da je kongruencija $x^2 \equiv a \pmod{Q}$ rješiva.

Primjer 2.1.3. *Broj* 3 *nije kvadratni ostatak ni modulo* 5*, ni modulo* 7*, odnosno*

$$\left(\frac{3}{5}\right) = -1, \left(\frac{3}{57}\right) = -1.$$

Zbog toga 3 *nije kvadratni ostatak modulo* 35*, no očito je vrijednost Jacobijevog simbola* $\left(\frac{3}{35}\right) = 1$.

Propozicija 2.1.4. *Neka je* $Q = q_1^{t_1} \cdots q_s^{t_s}$*, gdje su* q_i *različiti neparni prosti brojevi, te* $t_i \in \mathbb{N}$*. Ako je* a *kvadratni ostatak modulo* q_i *za sve* $i = 1, \ldots, s$*, onda kongruencija* $x^2 \equiv a \pmod{Q}$ *ima rješenja.*

Za dokaz tvrdnje potrebna nam je tzv. Henselova lema:

Teorem 2.1.5 (Henselova lema)**.** *Neka je* f *polinom s cjelobrojnim koeficijentima. Ako je* $f(a) \equiv 0 \pmod{p^j}$ *i* $f'(a) \not\equiv 0 \pmod{p}$*, onda postoji jedinstven broj* $t \in \{0, 1, 2, \ldots, p-1\}$ *takav da je* $f(a + tp^j) \equiv 0 \pmod{p)^{j+1}}$.

Dokaz Propozije 2.1.4. Prema pretpostavci kongruencija $x^2 \equiv a \pmod{q_i}$ ima rješenja, za $i = 1, \ldots, s$. Ako je $t_i > 1$, onda uzastopnom primjenom Henselove leme 2.1.5 za polinom $f(x) = x^2 - a$ dobivamo da i kongruencija $x^2 \equiv a \pmod{q_i^{t_i}}$ ima rješenja. Neka je ${a_i}^2 \equiv a \pmod{q_i^{t_i}}$, za $i = 1, \ldots, s$. Budući da su moduli $q_1^{t_1}, \ldots, q_s^{t_s}$ u parovima relativno prosti, prema Kineskom teoremu o ostatcima 1.5.1 slijedi da sustav

$$x \equiv a_1 \pmod{q_1^{t_1}}, \ldots, x \equiv a_s \pmod{q_s^{t_s}} \tag{2.2}$$

ima jedinstveno rješenje b modulo $Q = q_1^{t_1} \cdots q_s^{t_s}$, tj.

$$b \equiv a_1 \pmod{q_1^{t_1}}, \ldots, b \equiv a_s \pmod{q_s^{t_s}}.$$

Kvadriranjem prethodnih relacija dobivamo

$$b^2 \equiv a \pmod{q_1^{t_1}}, \ldots, b^2 \equiv a_s \pmod{q_s^{t_s}}.$$

Kako su $q_1^{t_1}, \ldots, q_s^{t_s}$ su u parovima relativno prosti, slijedi da je

$$b^2 \equiv a \pmod{Q},$$

tj. kongruencija $x^2 \equiv a \pmod{Q}$ ima rješenje. □

2.2 Svojstva Jacobijevog simbola

U sljedećim teoremima nabrojat ćemo svojstva Jacobijevog simbola, a nakon toga primjenjujući te teoreme odrediti vrijednosti Jacobijevog simbola.

Teorem 2.2.1. *Neka je $Q > 1$ neparni prirodan broj i a, b cijeli brojevi takvi da je* $\text{nzd}(a, Q) = 1$ *i* $\text{nzd}(b, Q) = 1$. *Tada vrijedi:*

1. *ako je* $a \equiv b \pmod{Q}$, *onda je* $\left(\frac{a}{Q}\right) \equiv \left(\frac{b}{Q}\right)$;
2. $\left(\frac{ab}{Q}\right) = \left(\frac{a}{Q}\right)\left(\frac{b}{Q}\right)$;
3. $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$;
4. $\left(\frac{2}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$.

Dokaz. Pretpostavimo da je $Q = q_1^{t_1} \cdots q_s^{t_s}$ gdje su $q_1, \ldots, q_s$ različiti neparni prosti brojevi, a $t_1, \ldots, t_s \in \mathbb{N}$.

1. Kako je $a \equiv b \pmod{Q}$ slijedi da je $a \equiv b \pmod{q_j}$, $j = 1, \ldots, s$. Prema Teoremu 1.3.5(1) dobivamo:

$$\left(\frac{a}{Q}\right) = \left(\frac{a}{q_1}\right)^{t_1}\left(\frac{a}{q_2}\right)^{t_2}\cdots\left(\frac{a}{q_s}\right)^{t_s} = \left(\frac{b}{q_1}\right)^{t_1}\left(\frac{b}{q_2}\right)^{t_2}\cdots\left(\frac{b}{q_s}\right)^{t_s} = \left(\frac{b}{Q}\right).$$

2. Primjenom Teoremu 1.3.5(2) imamo:

$$\begin{aligned}\left(\frac{ab}{Q}\right) &= \left(\frac{ab}{q_1}\right)^{t_1}\left(\frac{ab}{q_2}\right)^{t_2}\cdots\left(\frac{ab}{q_s}\right)^{t_s}\\ &= \left(\frac{a}{q_1}\right)^{t_1}\left(\frac{b}{q_1}\right)^{t_1}\left(\frac{a}{q_2}\right)^{t_2}\left(\frac{b}{q_2}\right)^{t_2}\cdots\left(\frac{a}{q_s}\right)^{t_s}\left(\frac{b}{q_s}\right)^{t_s}\\ &= \left(\frac{a}{Q}\right)\left(\frac{b}{Q}\right).\end{aligned}$$

3. Korolar 1.3.8 povlači da je $\left(\frac{-1}{q}\right) = (-1)^{\frac{q-1}{2}}$ za neparan prost broj q. Otuda je

$$\begin{aligned}\left(\frac{-1}{Q}\right) &= \left(\frac{-1}{q_1}\right)^{t_1}\left(\frac{-1}{q_2}\right)^{t_2}\cdots\left(\frac{-1}{q_s}\right)^{t_s}\\ &= (-1)^{\frac{q_1-1}{2}t_1}(-1)^{\frac{q_2-1}{2}t_2}\cdots(-1)^{\frac{q_s-1}{2}t_s}\\ &= (-1)^{\sum_{j=1}^{s}\frac{q_j-1}{2}\cdot t_j}\end{aligned}$$

Budući da je

$$Q = (1+(q_1-1))^{t_1}(1+(q_2-1))^{t_2}\cdots(1+(q_s-1))^{t_s}$$

te

$$(1+(q_j-1))^{t_j} \equiv 1 + t_j(q_j-1) \pmod 4,$$

jer je $q_j - 1$ paran, slijedi da je

$$Q \equiv 1 + t_1(q_1-1) + t_2(q_2-1) + \cdots + t_s(q_s-1) \pmod 4.$$

Iz toga zaključujemo da je

$$\frac{Q-1}{2} \equiv t_1\cdot\frac{q_1-1}{2} + t_2\cdot\frac{q_2-1}{2} + \cdots + t_s\cdot\frac{q_s-1}{2} \pmod 2,$$

pa je $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q-1}{2}}$.

4. Iz Leme 1.4.4 imamo $\left(\frac{2}{q}\right) = (-1)^{\frac{q^2-1}{8}}$ za neparan prost broj q. Dalje slično kao dokaz prethodne tvrdnje. Vrijedi

$$\begin{aligned}\left(\frac{2}{Q}\right) &= \left(\frac{2}{q_1}\right)^{t_1}\left(\frac{2}{q_2}\right)^{t_2}\cdots\left(\frac{2}{q_s}\right)^{t_s}\\ &= (-1)^{\sum_{j=1}^{s}\frac{q_j{}^2-1}{2}\cdot t_j},\end{aligned}$$

to jest

$$Q^2 = (1+(q_1^2-1))^{t_1}(1+(q_2^2-1))^{t_2}\cdots(1+(q_s^2-1))^{t_s}.$$

Iz $q_j^2 - 1 \equiv 0 \pmod 8$ dobivamo

$$(1+(q_j^2-1))^{t_j} \equiv 1 + t_j(q_j^2-1) \pmod 8,$$

odnosno

$$Q^2 \equiv 1 + t_1(q_1^2-1) + t_2(q_2^2-1) + \cdots + t_s(q_2^2-1) \pmod{64}.$$

Iz toga slijedi

$$\frac{Q^2-1}{8} \equiv t_1 \cdot \frac{q_1^2-1}{8} + t_2 \cdot \frac{q_2^2-1}{8} + \cdots + t_s \cdot \frac{q_s^2-1}{8} \pmod 8,$$

pa je $\left(\frac{-1}{Q}\right) = (-1)^{\frac{Q^2-1}{8}}$. □

Legendreov simbol najbrže možemo odrediti primjenom Gaussovog kvadratnog zakona reciprociteta 1.4.1 jer omogućava zamjenu $\left(\frac{p}{q}\right)$ s $\left(\frac{q}{p}\right)$. U sljedećem teoremu pokazat ćemo kako ta tvrdnja vrijedi i za Jacobijev simbol.

Teorem 2.2.2. *Ako su brojevi Q, P neparni relativno prosti prirodni brojevi, onda je*

$$\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

Dokaz. Neka su

$$P = p_1^{m_1} \cdots p_r^{m_r},\ Q = q_1^{t_1} \cdots q_s^{t_s}$$

kanonski rastavi brojeva P i Q na proste faktore. Prema tome je

$$\left(\frac{P}{Q}\right) = \left(\frac{P}{q_1}\right)^{t_1}\left(\frac{P}{q_2}\right)^{t_2}\cdots\left(\frac{P}{q_s}\right)^{t_s} = \prod_{i=1}^{s}\left[\left(\frac{P}{q_i}\right)\right]^{t_i} = \prod_{i=1}^{s}\prod_{j=1}^{r}\left[\left(\frac{p_i}{q_j}\right)\right]^{m_i t_j}$$

i

$$\left(\frac{Q}{P}\right) = \left(\frac{Q}{P_1}\right)^{m_1}\left(\frac{Q}{P_2}\right)^{m_2}\cdots\left(\frac{Q}{p_r}\right)^{m_r} = \prod_{j=1}^{r}\left[\left(\frac{Q}{p_j}\right)\right]^{m_j} = \prod_{j=1}^{r}\prod_{i=1}^{s}\left[\left(\frac{q_i}{p_j}\right)\right]^{m_j t_i}.$$

Primjenom Gaussovog kvadratnog zakona reciprociteta 1.4.1 i svojstva Jacobijevog simbola 2.2.1(3) imamo:

$$\begin{aligned}
\left(\frac{Q}{P}\right)\left(\frac{P}{Q}\right) &= \prod_{i=1}^{r}\prod_{j=1}^{s}\left[\left(\frac{p_j}{q_i}\right)\left(\frac{q_i}{p_j}\right)\right]^{m_j r_i} \\
&= \prod_{i=1}^{r}\prod_{j=1}^{s}(-1)^{m_j\left(\frac{p_j-1}{2}\right)r_i\left(\frac{q_i-1}{2}\right)} \\
&= (-1)^{\sum_{i=1}^{r}\sum_{j=1}^{s}\left(\frac{p_j-1}{2}\right)\left(\frac{q_i-1}{2}\right)m_j r_i} \\
&= (-1)^{\sum_{j=1}^{s} m_j\left(\frac{p_j-1}{2}\right)\sum_{i=1}^{r} r_i\left(\frac{q_i-1}{2}\right)}
\end{aligned}$$

Budući da su brojevi $\sum_{j=1}^{s} m_j \left(\frac{p_j-1}{2}\right)$ i $\frac{P-1}{2}$, te $\sum_{i=1}^{r} r_i \left(\frac{q_i-1}{2}\right)$ i $\frac{Q-1}{2}$ iste parnosti (što je pokazano u dokazu Teorema 2.2.1(3)), slijedi

$$(-1)^{\sum_{j=1}^{s} m_j \left(\frac{p_j-1}{2}\right) \sum_{i=1}^{r} r_i \left(\frac{q_i-1}{2}\right)} = (-1)^{\frac{P-1}{2}\cdot\frac{Q-1}{2}}.$$

□

Teorem 2.2.2 kraće zapisujemo kao

$$\left(\frac{P}{Q}\right) = \begin{cases} -\left(\frac{Q}{P}\right), & \text{ako } P \equiv Q \equiv 3 \pmod 4, \\ \left(\frac{Q}{P}\right), & \text{inače.} \end{cases}$$

Primjer 2.2.3. *Koristeći svojstva Jacobijevog simbola odredite vrijednost od* $\left(\frac{18728}{11781}\right)$.

Rješenje. Simbol ćemo izračunati na način da iz gornjeg broja izlučujemo najveću potenciju broja 2 i primjenjujemo Gaussov zakon reciprociteta:

$$\begin{aligned}
\left(\frac{18728}{11781}\right) &= \left(\frac{2}{11781}\right)^3 \left(\frac{2341}{11781}\right) && \textit{svojstvo 2.2.1(2)} \\
&= (-1)^3 \left(\frac{11781}{2341}\right) && \textit{svojstvo 2.2.2} \\
&= -\left(\frac{76}{2341}\right) && \textit{svojstvo 2.2.1(1)} \\
&= -\left(\frac{2}{2341}\right)^2 \cdot \left(\frac{19}{11781}\right) && \textit{svojstvo 2.2.1(2)} \\
&= -\left(\frac{4}{19}\right) && \textit{svojstvo 2.2.1(1)} \\
&= -\left(\frac{2}{19}\right)^2 = -(-1)^2 = -1.
\end{aligned}$$

□

2.3 Algoritam za računanje Jacobijevog simbol

Opisat ćemo algoritam za računanje Jacobijevog simbola koji se bazira na specijalnom algoritmu za dijeljenje ostatkom. Najprije se prisjetimo standardnog algoritma za dijeljenje s ostatkom, odnosno *Euklidovog algoritma* koji se zasniva na *Teoremu o djeljenju s ostatkom.*

Teorem 2.3.1 (Teorem o dijeljenju s ostatkom)**.** *Neka su $a, b \in \mathbb{Z}$ takvi da je $a > 0$. Tada postoje jedinstveni cijeli brojevi q i r, za koje vrijedi*

$$b = q \cdot a + r,$$

gdje je $0 \leq r < a$.

Uzastopnom primjenom Teorema 2.3.1 dobiva se *Euklidov algoritam*:

$$\begin{aligned} b &= q_1 a + r_1, 0 < r_1 < a, \\ a &= q_2 r_1 + r_2, 0 < r_2 < r_1, \\ r_1 &= q_3 r_2 + r_3, 0 < r_3 < r_2, \\ &\vdots \\ r_{n-2} &= q_n r_{n-1} + r_n, 0 < r_n < r_{n-1}, \\ r_{n-1} &= q_{n+1} r_n + 0. \end{aligned}$$

Budući da algoritam generira niz padajućih prirodnih brojeva (r_i), jasno je da će algoritam u konačno mnogo koraka završiti ($r_{n+1} = 0$). Vrijedi da je $\text{nzd}(a, b) = r_n$.

Primjer 2.3.2. *Pomoću Euklidovog algoritam odredite* $\text{nzd}(775, 117)$.

Rješenje.

$$\begin{aligned} 775 &= 6 \cdot 117 + 73, \\ 117 &= 1 \cdot 73 + 44, \\ 73 &= 1 \cdot 44 + 29, \\ 44 &= 1 \cdot 29 + 15, \\ 29 &= 1 \cdot 15 + 14, \\ 15 &= 1 \cdot 14 + 1, \\ 14 &= 14 \cdot 10 + 0. \end{aligned}$$

Dakle, $\text{nzd}(775, 117) = 1$. □

Neka su a i b pozitivni cijeli brojevi takvi da je $a < b$ i $\text{nzd}(a, b) = 1$. Uz $R_0 = a$, $R_1 = b$, modifikacijom Euklidovog algoritma dobivamo:

$$\begin{aligned} R_0 &= R_1 q_1 + 2^{s_1} R_2, \\ R_1 &= R_2 q_2 + 2^{s_2} R_3, \\ R_2 &= R_3 q_3 + 2^{s_3} R_4, \\ &\vdots \\ R_{n-3} &= R_{n-2} q_{n-2} + 2^{s_{n-2}} R_{n-1}, \\ R_{n-2} &= R_{n-1} q_{n-1} + 2^{s_{n-1}} \cdot 1, \end{aligned} \tag{2.3}$$

gdje su $s_j \in \mathbb{N}_0$ i R_j neparni prirodni brojevi manji od R_{j-1} za $j = 1, 2, 3, \ldots, n-1$, a $R_n = 1$.

Primjer 2.3.3. *Provedite algoritam* (2.3) *za* $a = 117$ *i* $b = 775$.

Rješenje.

$$\begin{aligned} 117 &= 0 \cdot 775 + 117, \\ 775 &= 6 \cdot 117 + 73, \\ 117 &= 1 \cdot 73 + 2^2 \cdot 11, \\ 73 &= 6 \cdot 11 + 7, \\ 11 &= 1 \cdot 7 + 2^2 \cdot 1. \end{aligned}$$

□

Algoritam (2.3) iskoristit ćemo za računanje Jacobijevog simbola.

Teorem 2.3.4. *Neka su* $a, b \in \mathbb{Z}$ *takvi da je* $a < b$ *i* $\text{nzd}(a, b) = 1$, *te neka su* R_j *neparni prirodni brojevi i* s_j *nenegativni cijeli brojevi,* $j = 1, 2, \ldots, n-1$, *dobiveni algoritmom* (2.3). *Tada je*

$$\left(\frac{a}{b}\right) = (-1)^N,$$

gdje je

$$N = s_1 \frac{R_1^2 - 1}{8} + \cdots + s_{n-1} \frac{R_{n-1}^2 - 1}{8} + \frac{R_1 - 1}{2} \cdot \frac{R_2 - 1}{2} + \cdots + \frac{R_{n-2} - 1}{2} \cdot \frac{R_{n-1} - 1}{2}.$$

Dokaz. Koristeći svojstvo 1), 2) i 4) iz Teorema 2.2.1 imamo:

$$\left(\frac{a}{b}\right) = \left(\frac{R_0}{R_1}\right) = \left(\frac{2^{s_1} R_2}{R_1}\right) = \left(\frac{2}{R_1}\right)^{s_1} \left(\frac{R_2}{R_1}\right) = (-1)^{s_1 \frac{{R_1}^2 - 1}{8}} \left(\frac{R_2}{R_1}\right).$$

Iz Teorema 2.2.2 slijedi da je

$$\left(\frac{R_2}{R_1}\right) = (-1)^{\frac{R_1 - 1}{2} \cdot \frac{R_2 - 1}{2}} \left(\frac{R_1}{R_2}\right),$$

pa imamo

$$\left(\frac{a}{b}\right) = (-1)^{\frac{R_1 - 1}{2} \cdot \frac{R_2 - 1}{2} + s_1 \frac{R_1^2 - 1}{8}} \left(\frac{R_1}{R_2}\right).$$

Općenito za $j = 2, 3, \ldots, n-1$ vrijedi:

$$\left(\frac{R_{j-1}}{R_j}\right) = (-1)^{\frac{R_j - 1}{2} \cdot \frac{R_{j+1} - 1}{2} + s_j \frac{R_j^2 - 1}{8}} \left(\frac{R_j}{R_{j+1}}\right).$$

Specijalno u zadnjem koraku ($j = n-1$) zbog $R_n = 1$ imamo

$$\left(\frac{R_{n-2}}{R_{n-1}}\right) = (-1)^{\frac{R_{n-1}-1}{2}\cdot\frac{R_{n-1}}{2}+s_{n-1}\frac{R_{n-1}^2-1}{8}} \cdot 1 = (-1)^{s_{n-1}\frac{R_{n-1}^2-1}{8}}.$$

Stoga je $\left(\frac{a}{b}\right) = (-1)^N$ za

$$N = \frac{R_1-1}{2}\cdot\frac{R_2-1}{2}+s_1\frac{R_1^2-1}{8}+\cdots+\frac{R_{n-2}-1}{2}\cdot\frac{R_{n-1}-1}{2}+s_{n-2}\frac{R_{n-2}^2-1}{8}+s_{n-1}\frac{R_{n-1}^2-1}{8},$$

što je i trebalo pokazati. □

Primjer 2.3.5. *Primjenom Teorema 2.3.4 odredite vrijednost Jacobijevog simbola* $\left(\frac{117}{775}\right)$.

Rješenje. Iz Primjera 2.3.3 imamo da je:

$$(R_0, R_1, R_2, R_3, R_4, R_5) = (117, 775, 117, 73, 11, 7),$$

te

$$(s_1, s_2, s_3, s_4, s_5) = (0, 0, 2, 0, 2).$$

Prema Teoremu 2.3.4:

$$N = s_3\frac{R_3^2-1}{8} + s_5\frac{R_5^2-1}{8} + \sum_{i=1}^{4}\frac{(R_i-1)(R_{i+1}-1)}{4} = 26073,$$

što daje

$$\left(\frac{117}{775}\right) = -1.$$

□

Jasno je da ne moramo računati broj N iz Teoremu 2.3.4 već parnost izraza

$$\frac{R_j-1}{2}\cdot\frac{R_{j+1}-1}{2} + s_j\frac{R_j^2-1}{8}$$

koji se dobije u svakom koraku algoritma (2.3). Dakle, algoritam za računanje Jacobijevog simbola glasio bi:

$S = 1$;
`Za` $j = 1, \ldots, n-1$,

$$\texttt{ako je } \tfrac{R_j-1}{2}\cdot\tfrac{R_{j+1}-1}{2}+s_j\tfrac{R_j^2-1}{8} \mod 2 = 1\texttt{, onda } S := S\cdot(-1).$$

Konkretno za $\left(\frac{117}{775}\right)$ (iz primjera 2.3.3 i 2.3.5) primjenom algoritma dobili bismo: $S = 1$

$j = 1$: $117 = 0\cdot 775 + 117 \Rightarrow \frac{775-1}{2}\cdot\frac{117-1}{2} + 0 \equiv 0 \pmod 2 \Rightarrow S = 1$

$j = 2$: $775 = 6\cdot 117 + 73 \Rightarrow \frac{117-1}{2}\cdot\frac{73-1}{2} + 0 \equiv 0 \pmod 2 \Rightarrow S = 1$

$j = 3$: $117 = 1\cdot 73 + 2^2\cdot 11 \Rightarrow \frac{73-1}{2}\cdot\frac{11-1}{2} + 2\cdot\frac{73^2-1}{8} \equiv 0 \pmod 2 \Rightarrow S = 1$

$j = 4$: $73 = 6\cdot 11 + 7 \Rightarrow \frac{11-1}{2}\cdot\frac{7-1}{2} + 0 \equiv 1 \pmod 2 \Rightarrow S = -1$

$j = 5$: $11 = 1\cdot 7 + 2^2\cdot 1 \Rightarrow 0 + 2\cdot\frac{7^2-1}{8} \equiv 0 \pmod 2 \Rightarrow S = -1 \Rightarrow \left(\frac{117}{775}\right) = -1$

2.4 Eulerovi pseudoprosti brojevi

U ovom dijelu rada bavimo se problemom je li neki proizvoljan prirodan broj n prost ili složen. Jedan od razloga za ispitivanjem prostosti velih brojeva leži u tome što neki kriptosustavi javnog ključa (npr. RSA) koriste velike proste brojeve. Ispitivati redom sve djelitelje (ili sve proste djelitelje) manje ili jednake od $\sqrt{n}$ je za velike brojeve n vrlo dugotrajan postupak. Eratostenovo sito učinkovito daje sve proste brojeve manje od neke zadane gornje ograde, no i ta procedura nije dovoljno brza za jako velike brojeve. Zato se ispitivanje složenosti broja n čini pomoću tzv. *testova prostosti*. Ako broj n ne zadovolji neki od kriterija testa prostosti, onda je sigurno složen, a ako zadovolji sve kriterije, onda je možda prost, odnosno *vjerojatno* prost. Naime, testovi prostosti uglavnom spadaju u probabilističke testove i obično je vjerojatnost da je broj n prost veća ako je n zadovoljio više testova (ili kriterija).

Početnu ideju za testove prostosti, odnosno testova složenosti daje Mali Fermatov teorem 1.3.2 koji kaže da je

$$a^{p-1} \equiv 1 \pmod p,$$

za svaki prosti broj p i svaki prirodan broj a koji nije djeljiv s p. Njegov obrat može se iskoristiti za testiranje složenosti nekog broja. Naime, ako su a i n relativno prosti brojevi i vrijedi da

$$a^{n-1} \not\equiv 1 \pmod n,$$

onda je n složen broj. No, važno je naglasiti da ako vrijedi relacija

$$a^{n-1} \equiv 1 \pmod n, \tag{2.4}$$

iz toga se ne može zaključiti da je n prost kao što možemo vidjeti u sljedećem primjeru.

Primjer 2.4.1. *Za složene brojeve* $341 = 11 \cdot 31$, $91 = 7 \cdot 13$, $561 = 3 \cdot 11 \cdot 17$ *vrijedi:*

- $2^{340} \equiv 1 \pmod{341}$,
- $3^{90} \equiv 1 \pmod{91}$,
- $2^{560} \equiv 1 \pmod{561}$, $5^{560} \equiv 1 \pmod{561}$.

Dakle, brojevi $91, 341, 561$ *prolaze test* (2.4) *zasnovan na Malom Fermatovom teoremu, ali nisu prosti već složeni. Uočimo da promjenom baze* a *u testu* (2.4) *dobivamo sljedeće rezultate:*

- $3^{340} \equiv 56 \not\equiv 1 \pmod{341}$,
- $2^{90} \equiv 64 \not\equiv 1 \pmod{91}$,

iz kojih zaključujemo da su 91 *i* 341 *složeni brojevi. No, broj* 561 *prolazi test* (2.4) *za svaku bazu. Naime, vrijedi*

$$a^{560} \equiv 1 \pmod{561},$$

za sve a *koji su relatvno prosti s* 561.

Definicija 2.4.2. *Neka je neparan složen broj* n *i* a *cijeli broj koji je relativno prost s* n. *Kažemo da je* n ***pseudoprost u bazi*** a *ako je*

$$a^{n-1} \equiv 1 \pmod{n}.$$

Kratko pišemo da je n $\mathrm{psp}(a)$.

Složen broj n *koji je pseudoprost u bazi* a, *za svaki cijeli broj* a *koji je relativno prost s* n, *zove se* ***Carmichaelov broj***.

Iz Primjera 2.4.1 vidimo da je 341 psp(2), 91 psp(3), a 561 je Carmichaelov broj. Ako za k odabranih baza a vrijedi test (2.4) za neki broj n, onda je vjerojatnost da je n složen manja ili jednaka 0.5^k. No, nedostatak ovog testa su Carmichaelovi brojevi koji su složeni i prolaze ga u svakoj bazi, a može se pokazati da ih postoji beskonačno mnogo. Iz toga razloga koriste se i drugi testovi koji nemaju takav nedostatak.

Test koji se zasniva na Eulerovom kriteriju naziva se *Solovay-Strassenovov test prostosti*. Prema Teoremu 1.3.1 (Eulerov kriterij) za svaki cijeli broj a i neparni prosti broj p vrijedi

$$\left(\frac{a}{p}\right) \equiv a^{\frac{p-1}{2}} \pmod{p}.$$

Želimo li ispitati je li prirodan broj n prost ili složen možemo testirati relaciju

$$\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} \pmod{n}, \tag{2.5}$$

za neki cijeli broj a takav da je $\text{nzd}(a, n) = 1$. Ako kongruencija ne vrijedi, tj. ako

$$\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} \pmod{n},$$

onda je n sigurno složen. Ako kongruencija (2.5) vrijedi, onda broj n može biti ili prost ili složen.

Primjer 2.4.3. *Za složene brojeve* $561 = 3 \cdot 11 \cdot 17$, $703 = 19 \cdot 37$ *vrijedi:*

- $2^{280} \equiv 1 \equiv \left(\frac{2}{280}\right) \pmod{561}$, $5^{280} \equiv 67 \not\equiv \left(\frac{5}{280}\right) \pmod{561}$,
- $2^{351} \equiv 265 \not\equiv \left(\frac{2}{280}\right) \pmod{703}$, $3^{351} \equiv -1 \equiv \left(\frac{5}{280}\right) \pmod{703}$.

Test (2.5) *je za oba broja, samo u različitim bazama, pokazao da su složeni.*

Definicija 2.4.4. *Neka je neparan složen broj n i a cijeli broj koji je relativno prost s n. Kažemo da je n* ***Eulerov pseudoprost u bazi*** *a ako je*

$$a^{\frac{n-1}{2}} \equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Kratko pišemo da je n $\text{epsp}(a)$.

U Primjeru 2.4.3 se pokazalo da je 561 epsp(2), ali nije epsp(5), te da je 703 epsp(3), ali nije epsp(2). Pokazuje se da je biti Eulerov pseudoprost u bazi a *jače* svojstvo nego biti pseudoprost u bazi a.

Propozicija 2.4.5. *Neka je n Eulerov pseudoprost broj u bazi a. Tada je n pseudoprost u bazi a.*

Dokaz. Budući da je n $\text{epsp}(b)$, vrijedi kongruencija (2.5) iz koje kvadriranjem slijedi

$$a^{n-1} \equiv \left(\frac{a}{n}\right)^2 = 1 \pmod{n},$$

što znači da n $\text{psp}(a)$. □

Obrat prethodne prepozicije ne vrijedi. Na primjer, 561 je psp(5) ali nije epsp(5).

Prednost testa pomoću relacije (2.5) jest u tome da ne postoje analogoni Carmichaelovih brojeva, već za svaki složen broj n test nije zadovoljen za barem pola mogućih baza.

Lema 2.4.6. *Ako je n neparan prirodan broj koji nije potpuni kvadrat, tada postoji prirodan broj a, $1 < a < n$, koji je relativno prost s n i za koji je* $\left(\frac{a}{n}\right) = -1$.

Dokaz. Ako je n prost broj, onda se prema Teoremu 1.1.3 skup $\{1, 2, \ldots, n\}$ sastoji od $(n-1)/2$ kvadratnih ostataka i isto toliko neostataka pa tvrdnja leme u tom slučaju vrijedi.

Neka je n neparan složen broj. Budući da nije potpuni kvadrat, možemo ga zapisati kao

$$n = p^e s,$$

gdje je p neparan prost broj, e i s neparni brojevi, te $\text{nzd}(p, s) = 1$. Neka je $t < p$ kvadratni neostatak od p (koji postoji prema Teoremu 1.1.3). Prema Kineskom teoremu o ostatcima 1.5.1 sustav kongruencija

$$x \equiv t \pmod{p^e}, \; x \equiv 1 \pmod{s},$$

ima jedinstveno rješenje a modulo $n = p^e s$ takvo da je $1 < a < n$. Dakle, vrijedi $a \equiv t \pmod{p)^e}$, $a \equiv 1 \pmod{s}$, te

$$\left(\frac{a}{n}\right) = \left(\frac{a}{p^e}\right)\left(\frac{a}{s}\right) = \left(\frac{a}{p}\right)^e \left(\frac{a}{s}\right) = (-1)^e \cdot 1 = -1.$$

□

Lema 2.4.7. *Ako je n neparan prirodan broj koji nije potpun kvadrat, tada postoji prirodan broj a, $1 < a < n$, koji je relativno prost s n i za koji*

$$a^{(n-1)/2} \not\equiv \left(\frac{a}{n}\right) \pmod{n}.$$

Dokaz. Pretpostavimo suprotno, tj. neka za sve $1 < a < n$ koji su relativno prost s n vrijedi

$$a^{(n-1)/2} \equiv \left(\frac{a}{n}\right) \pmod{n}. \tag{2.6}$$

Kvadriranjem prethodne relacije slijedi da je

$$a^{n-1} \equiv 1 \pmod{n}.$$

Dakle, n je pseudoprost u svakoj bazi pa slijedi da je n Carmichaelov broj. Može se pokazati da je tada n oblika

$$n = q_1 q_2 \cdots q_r,$$

gdje su $q_1, q_2 \ldots, q_r$ međusobno različiti prosti brojevi.

Želimo pokazati da mora vrijediti kongruencija $a^{(n-1)/2} \equiv 1 \pmod{n}$, za sve a. Pretpostavimo da postoji a, $1 < a < n$, $\text{nzd}(a, n) = 1$, za kojeg kongruencija ne vrijedi, tj.

$$a^{(n-1)/2} \equiv -1 \pmod{n}.$$

Neka je b, $1 < b < n$, rješenje sustava kongruencija

$$x \equiv a \pmod{q_1}, \; x \equiv 1 \pmod{q_2 \cdots q_r},$$

koje je jedinstveno modulo n prema Kineskom teoremu o ostatcima. Otuda je

$$b^{(n-1)/2} \equiv a^{(n-1)/2} \equiv -1 \pmod{q_1}, \; b^{(n-1)/2} \equiv 1 \pmod{q_2 \cdots q_r},$$

pa je

$$b^{(n-1)/2} \not\equiv \pm 1 \pmod{n},$$

što je u suprotnosti s početnom pretpostavkom (2.6). Dakle, za sve a, $1 < a < n$, $\text{nzd}(a, n) = 1$, mora vrijediti

$$a^{(n-1)/2} \equiv 1 \pmod{n}.$$

Stoga prema (2.6) dobivamo da

$$\left(\frac{a}{n}\right) \equiv 1 \pmod{n}$$

vrijedi za sve a ($1 < a < n$, $\text{nzd}(a, n) = 1$), no to nije moguće prema Lemi 2.4.6 i stoga postoji barem jedan a za kojeg (2.6) ne vrijedi. □

Koristeći prethodne dvije leme može se pokazati sljedeći važan teorem koji je osnova za vjerojatnosni test zasnovan na Eulerovom kriteriju.

Teorem 2.4.8. *Neka je n neparan složen broj. Tada je broj baza a, $1 < a < n$, takvih da je broj n Eulerov pseudoprost u bazi a manji $\varphi(n)/2$.*

Dokaz. Prema Lemi 2.4.7 postoji b, $1 < b < n$, koji je relativno prost s n i za koji je

$$b^{(n-1)/2} \not\equiv \left(\frac{b}{n}\right) \pmod{n}. \tag{2.7}$$

Označimo s a_j, $j = 1, \ldots, m$, pozitivne cijele brojeve manje od n koji su relativni prosti s n i

$$a_j^{\frac{n-1}{2}} \equiv \left(\frac{a_j}{n}\right) \pmod{n}.$$

Nadalje, označimo s r_j, $j = 1, \ldots, m$ najmanji pozitivne brojeve za koje je $ba_j \equiv r_j \pmod{n}$. Uočimo da mora vrijediti

$$r_j^{\frac{n-1}{2}} \not\equiv \left(\frac{r_j}{n}\right) \pmod{n},$$

za sve $j = 1, ..., m$ jer bi u suprotnom imali kontradikciju s (2.7). S obzirom na to da svaki od elemenata iz skupa $\{a_1, \ldots, a_m\}$ i $\{r_1, \ldots, r_m\}$ zadovoljava različite kongruencije, nužno je

$$a_i \neq r_j, \ \forall i, j \in \{1, \ldots, m\}.$$

Kako su a_i, r_i za sve $1 = 1, \ldots, m$ relativno prosti s n i manji od n slijedi da je $\{a_1, \ldots, a_m\} \cup \{r_1, \ldots, r_m\}$ podskup reduciranog sustava najmanjih pozitivnih ostatka čiji je kardinalitet $\varphi(n)$. Stoga je $m \leq \varphi(n)/2$. □

Ovim teoremom pokazali smo da ako je n neparan cijeli broj vjerojatnost da je n Eulerov pseudoprost broj u bazi a za $1 < a < n$ i $\text{nzd}(a, n) = 1$ manja je od $\frac{1}{2}$. Opišimo sada postupak određivanja prostosti pomoću Solovay-Strassenovog testa za dani broj n:

1. korak: Na slučajan način odabiremo k brojeva a_i, $0 < a_i < n$.

2. korak: Računamo

$$p = a_i^{\frac{n-1}{2}} - \left(\frac{a_i}{n}\right) \mod n,$$

sve dok je $i \leq k$ i $p = 0$.

3. korak: Ako je $i < k$, onda je n složen (jer je u tom slučaju nastupio slučaj $p \neq 0$).

Ako je $i = k$ i $p = 0$, n je *vjerojatno prost* (jer je prošao test za svaku bazu a_i).

Vjerojatnost da je broj n složen manja je ili jednaka $\left(\frac{1}{2}\right)^k$. U praksi se uzima $k = 50$ ili $k = 100$, što znači da je vjerojatnost da je n složen manja od 10^{-15} ili 10^{-30}.

Poglavlje 3

Životopisi matematičara

3.1 Pierre de Fermat

Francuski matematičar i pravnik rođen 17. kolovoza 1601. u gradu blizu Toulousea naziva se Pierre de Fermat. Rođen je u bogatoj trgovačkoj obitelji te je imao brata i dvije sestre. Smatra se kako se školovao u franjevačkom samostanu iako za to nema dokaza. Studij je započeo u Toulouseu, nastavio u Bordeauxu, a završio u Orleansu. Nakon što je diplomirao građansko pravo 1631. godine, dobio je titulu *de* u imenu i postao članom parlamenta u Toulouseu, gdje je većinu svojeg života i živio. Umro je u epidemiji kuge 12. siječnja 1665. godine.

Fermat se još za vrijeme studija bavio matematičkim problemima i dao prve rezultate o minimumima i maksimumima funkcija. Veliki značaj u matematici vidljiv je u teoriji brojeva, otkrivanju analitičke geometrije te postavljanju temelja za teoriju vjerojatnosti. Jedna od zanimljivosti je u tome da Fermat svoje teoreme nije objavljivao nego ih je zapisivao na marginama knjiga i u pismima prijateljima. Tako je jedna od najpoznatijih njegovih bilješki na marginama *Veliki Fermatov teorem* za čiji je dokaz trebalo 350 godina. Također, zanimljivo je to što je Fermat ispod zapisa teorema napisao kako nema mjesta za njegov dokaz makar zna kako glasi. Po njemu se naziva i *Mali Fermatov teorem* koji daje velike značajke u teoriji brojeva. Fermat je poznat i po svojem karakterističnom stilu pisanja u kojem poziva druge da pokažu rezultate koje je on već dobio. Upravo zbog toga, sukobio se s Descartesom nazivajući njegov zakon loma *pipanje u mraku*. Fermatov značaj u matematici je i otkriće diferencijalnog računa kao vezu između ekstrema funkcije i tangenti. Osim toga, izračunao je površine odsječaka parabola i hiperbola, težište rotacionog paraboloida i time dobio rezultate koji su uvod u integriranje.

3.2 Leonhard Euler

Jedan od najpoznatijih matematičara 18. stoljeća rođen u Baselu u Švicarskoj naziva se Leonhard Euler. Kako je škola koju je pohađao bila siromašna, elementarnoj matematici podučavao ga je njegov otac, Paul Euler. Svoje prvo opće obrazovanje započeo je 1720. godine na Sveučilištu u Baselu gdje je magistrirao filozofiju 1723. godine. Zbog očeve želje upisao je teologiju, ali nakon što ga je ohrabrio Johann Bernoulli prekinuo je studij teologije i upisao studij matematike. Tijekom cijelog studija proučavao je matematičke radove i djela Newtona, Galilea, Jacoba Bernoullija i mnogih drugih značajnih matematičara. Godine 1727. objavio je članak o rasporedu jarbola na brodu. Nakon završetka studija otišao je u Sankt Peterburg gdje je podučavao primjenu matematike i mehanike u fiziologiji na Sanktpeterbuškoj akademiji znanosti. Jedna od zanimljivosti iz njegovog života je spoznaja da je bio slijep na desno oko i imao trinaestero djece od kojih je samo petero preživjelo rano djetinjstvo. Umro je 1783. godine od izljeva krvi u mozak.

Njegov prvi značajni rezultat u matematici je tzv. *baselski problem*. Tim problemom bavili su se i drugi matematičari poput Jacoba Bernoullija, Johanna Bernoullija, Leibniza, de Moivrea, a problem je bio u pronalasku zatvorenog oblika beskonačnog reda. Euler je rješenje problema dao 1735. godine i to se smatra prvim dokazom baselskog problema. Eulerov veliki značaj možemo vidjeti i u začecima teorije funkcija kompleksne varijable. Naime, definirao je eksponencijalnu funkciju e^x i povezao ju s trigonometrijskim funkcijama sinusa i kosinusa. Danas tu poveznicu nazivamo *Eulerova formula*. U teoriji brojeva, svoj značaj ostavio je dokazujući 1736. godine *Mali Fermatov teorem* i generalizirajući ga 1760. godine koristeći funkciju $\varphi(n)$. Danas tu funkciju nazivamo *Eulerova funkcija*. Njegovo djelo u četiri sveska, *Opera Omnia*, obuhvaća razna geometrijska istraživanja. Neka od istraživanja su dokaza Heronove formule za površinu, proučavanja odnosa između ortocentra, težišta i središta opisane kružnice, kružnica devet točaka, Eulerova formula za poliedre i mnoga druga. U teoriji grafova ostavio je svoj doprinos razmatrajući problem *Köenigsberških mostova* pokušavajući otkriti postoji li šetnja preko svih sedam mostova pruskog grada na način da se svaki most prijeđe samo jednom. Osim doprinosa u matematici ostavio je i doprinose u mehanici, astronomiji, kartografiji i brodogradnji.

3.3 Carl Friedrich Gauss

Njemački matematičar rođen 30. travnja 1777. godine naziva se Carl Friedrich Gauss. Živio je u siromašnoj obitelji, a njegova majka bila je nepismena. Kao dječak otkrio je zbroj prvih 100 prirodnih brojeva i dobio naziv *čudo od djeteta*. Sa jedanaest godina započeo je svoje školovanje u gimnaziji gdje je učio njemački i latinski jezik. Studij

matematike započeo je 1792. godine na Brunswick Collegiom Carolinum gdje je otkrio Bodeov zakon, binomni poučak i kvadratni zakon reciprociteta. Godine 1795. studij je nastavio na Göttingenskom sveučilištu kojeg je napustio 1798. godine. Iako je napustio studij u to je vrijeme došao do jednog od svojih prvih otkrića, konstrukcije pravilnog sedamnaesterokuta s ravnalom i šestarom. Nakon nekog vremena vratio se na studij, magistrirao i napisao doktorski rad na temu osnovnog teorema algebre. Umro je 23. veljače 1855. godine u Göttingenu od srčanog udara.

Svoje prvo djelo *Disquisitiones Arithmeticae*, koje je definiralo teoriju brojeva kao zasebnu cjelinu, napisao je 1798. godine, a objavio 1801. Osim toga, dao je 8 dokaza zakona kvadratnog reciprociteta od kojih su šest objavljenja za vrijeme njegova života te dva nakon smrti. Svoju drugu knjigu *Theoria motus corporum coelestium in sectionibus conicis Solem ambientium* objavio je 1809. godine. U prvom djelu knjige opisao je diferencijalne jednadžbe, presjeke stošca i eliptičke putanje. Drugi dio knjige posvećen je određivanju putanja planeta. Osim teorije brojeva i teorijske astronomije ostavio je značaj i u matematičkoj statistici objasnivši metodu najmanjih kvadrata.

3.4 Adrien-Marie Legendre

Adrien-Marie Legendre, francuski je matematičar i astronom rođen u bogatoj obitelji 18. rujna 1752. godine. Svoje obrazovanje stekao je na tri francuska sveučilišta na kojima se bavio matematikom i fizikom. Za svojeg života dobio je brojne nagrade Berlinske akademije i na taj način postao članom Kraljevskog društva. Bio je članom odjela za matematiku na Nacionalnom institutu znanosti i umjetnosti od 1795. godine. Umro je 9. siječnja 1833. godine u Parizu, a njegovo ime ugravirano je na Eifellovom tornju.

Njegovu matematičku zaslugu vidimo u teoriji brojeva postavljajući kvadratni zakon reciprociteta. Također, po njemu naziv dobiva i simbol koji možemo shvatiti kao indikator kvadratnog ostatka, Legendreov simbol. Bavio se i problemima vezanima uz proste brojeve i o primjeni analize na teoriju brojeva. U svojem djelu, *Traité des fonctions elliptiques*, sveo je eliptične integrale na tri standardna oblika, sastavio je tablice vrijednosti eliptičnih integrala i ta znanja povezao sa problemima u mehanici. Važno je spomenuti kako je dokazao da je broj π iracionalan broj. Njegova važnost može se primijetiti i u geometriji i njegovom djelu *Élacuteements de géométrie* u kojem preuređuje i pojednostavljuje metodu euklidske geometrije.

3.5 Carl Gustav Jacobi

Carl Gustav Jacobi njemački je matematičar važan za teoriju brojeva te diferencijalni i integralni račun. Rođen je 1804. godine u Potsdamu, gdje je i umro 1851. godine. Bio je drugo od četvero djece bankara Simona Jacobija. Imao je brata Moritza von Jacobi koji je također poznat kao inženjer i fizičar. Kao dijete školovao se kod kuće. Sa samo dvanaest godina upisao je gimnaziju, a nakon svega pola godine zbog njegove izvrsnosti u svim predmetima premješten je u više razrede. Iako je pokazivao izvanredne sposobnosti i zanimanje za sve predmete, Sveučilište u Berlinu nije ga primilo sve do šesnaeste godine te je tijekom toga vremena imao svoje prve pokušaje istraživanja pokušavajući riješiti jednadžbe u radikalima.

Njegov najznačajniji doprinos u teoriji brojeva je primjena eliptičnih funkcija dokazujući Fermatov teorem o dva kvadrata i Lagrangeov teorem o četiri kvadrata. Uz primjenu eliptičnih funkcija njegov doprinos u teoriji brojeva je nastavak Gaussova rada, tj. novi dokazi kvadratnog zakona reciprociteta, teorema o modularnoj aritmetici. Time je dao uvjete za rješivost kvadratnih jednadžbi i Jacobijev simbol, generalizaciju Legendreovog simbola. Njegova najznačajnija djela nazivaju se *Novi temelji teorije eliptičkih funkcija* i *O strukturi i svojstvima determinanata*.

Bibliografija

[1] F. M. Brückler, *Povijest matematike*, bilješke s predavanja, ak. god. 2020/21.

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

[3] A Dujella, M. Maretić, *Kriptografija*, Element, Zagreb, 2007.

[4] N. Elezović, *Prosti brojevi i kriptografija*, dio nastavnog materijala za predmet Diskontna matematika, FER, Sveučilište u Zagrebu, https://www.fer.unizg.hr/_download/repository/diskont1-13.pdf,

[5] A. Jurasić, M. Rukavina, *Pseudoprosti brojevi*, Matematičko fizički list (1332-1552) 62 (2011), 1; 20-25

[6] I. Matić, *Uvod u teoriju brojeva*, skripta, Odjel za matematiku Sveučilišta J. J. Strossmayera u Osijeku, https://www.mathos.unios.hr/images/homepages/mirela/UUTB/uvod_u_teoriju_brojeva.pdf

[7] K. H. Rosen, *Elementary Number Theory and lts Applications*, Addison Wesley, 1993.

Sažetak

Jacobijev simbol generalizacija je Legendreovog simbola $\left(\frac{a}{p}\right)$, gdje je a cijeli broj i p neparan prost broj, kojeg definiramo kao 1, -1 ili 0 ovisno o tome je li kvadratni ostatak modulo p, kvadratni neostatak modulo p ili p dijeli a. U ovom diplomskom radu predstavljena su i dokazana brojna svojstva Jacobijevog simbola. Zajedno s kvadratnim zakonom reciprociteta ta se svojstva mogu koristiti za vrlo učinkovito računavanje vrijednosti Jacobijevog simbola. Također, Jacobijev simbol koristi se u testovima prostosti i u definiciji pseudoprostih brojeva.

Summary

The Jacobi symbol is a generalization of the Legendre symbol $\left(\frac{a}{p}\right)$, where a is an integer and p is an odd prime, which is defined to be equal to 1, -1 or 0 depending on whether a is a quadratic residue modulo p, a quadratic nonresidue modulo p or p divides a. In this master's thesis a number of useful properties of the Jacobi symbol are presented and proved. Together with the law of quadratic reciprocity, they can be used to compute the Jacobi symbol very efficiently. Also, Jacobi symbols are used in primality testing and in the definition of a type of pseudoprime.

Životopis

Rođena sam 8. veljače 1996. u Zagrebu. Živim u Zlataru, gdje 2002. godine upisujem prvi razred u Osnovnoj školi Ante Kovačić. Uz redovno osnovnoškolsko obrazovanje 2005. godine upisujem i Glazbenu školu Bonar u Zlataru. Završetkom trećeg razreda osnovne glazbene škole Bonar, nastavljam osnovnoškolsko obrazovanje u Glazbenoj školi u Varaždinu, flautistički smjer koji završavam 2011. godine. Svoje obavezno osnovnoškolsko obrazovanje završavam 2010. godine, a nakon toga upisujem opću gimnaziju u Srednjoj školi Zlatar. Zahvaljujući svojem najvećem uzoru u matematici, profesorici Boženi Palanović, otkrila sam veliki interes za matematiku pa 2014. godine upisujem Preddiplomski sveučilišni studij Matematike na Prirodoslovno- matematičkom fakultetu u Zagrebu. Odabrala sam nastavnički smjer kojeg sam završila 2018. godine. Nakon završetka Preddiplomskog studija, upisala sam Diplomski sveučilišni studij Matematike, također nastavnički smjer. Trenutno radim kao nastavnica matematike u Srednjoj školi Konjščina i veselim se budućem radu s djecom.