Kvadratni ostatci

Lamot, Lorena

Sveučilište Josipa Jurja Strossmayera u Osijeku
Fakultet primijenjene matematike i informatike

Sveučilišni diplomski studij matematike
modul: financijska matematika i statistika

Kvadratni ostatci

Diplomski rad

Mentor:
izv. prof. dr. sc. Mirela Jukić Bokun

Student:
Lorena Lamot

Osijek, 2024.

Sadržaj

1 Uvod **1**

2 Kvadratni ostatci **3**
2.1 Definicija 3
2.2 Legendreov simbol 4
2.3 Svojstva Legendreovog simbola 6

3 Gaussov kvadratni zakon reciprociteta **13**
3.1 Iskaz i dokaz teorema 13
3.2 Pepinov test prostosti 15

4 Jacobijev simbol **17**
4.1 Definicija 17
4.2 Svojstva Jacobijevog simbola 18
4.3 Zakon kvadratnog reciprociteta za Jacobijev simbol 20
4.4 Algoritam za računanje Jacobijevog simbola 22
4.5 Eulerovi pseudoprosti brojevi 24

Literatura **29**

Sažetak **31**

Summary **33**

Životopis **35**

1 | Uvod

Kvadratni ostatci jedan su od temeljnih pojmova u teoriji brojeva i imaju široku primjenu, osobito u kriptografiji i testiranju prostosti brojeva. Cilj ovog rada je detaljno proučiti pojmove kvadratnih ostataka, Legendreovog i Jacobijevog simbola te njihove primjene.

U prvom poglavlju definirat ćemo kvadratne ostatke i Legendreov simbol. Nakon definicije, pokazat ćemo osnovna svojstva Legendreovog simbola te neke od njegovih primjena.

Drugo poglavlje posvećeno je jednom od najvažnijih rezultata u teoriji brojeva, Gaussovom zakonu kvadratnog reciprociteta. Nakon formalnog iskaza i dokaza teorema, primijenit ćemo ga na Pepinov test prostosti kojim možemo provjeriti je li neki Fermatov broj prost ili nije.

U trećem poglavlju uvodimo pojam Jacobijevog simbola, koji predstavlja generalizaciju Legendreovog simbola. U ovom dijelu navest ćemo osnovna svojstva Jacobijevog simbola te dokazati Zakon kvadratnog reciprociteta za Jacobijev simbol. Također, predstavit ćemo algoritam za efikasan izračun Jacobijevog simbola. Na kraju poglavlja, definirat ćemo Eulerove pseudoproste brojeve te iskazati i dokazati tvrdnje koje se koriste u testovima prostosti.

2 | Kvadratni ostatci

U ovom poglavlju definirat ćemo kvadratne ostatke koji će biti temelj svih daljnjih razmatranja. Zatim ćemo uvesti i pojam Legendreovog simbola te pokazati njegova svojstva i primjenu.

2.1 Definicija

Na početku navodimo definiciju kvadratnih ostataka.

Definicija 1. *Neka je a cijeli broj, m prirodan broj i $(a, m) = 1$. Ako kongruencija $x^2 \equiv a \pmod{m}$ ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U suprotnom kažemo da je a kvadratni neostatak modulo m.*

Ilustrirat ćemo ovu definiciju na sljedećem primjeru:

Primjer 1. *Odredimo sve kvadratne ostatke modulo 13.*

Rješenje: Kako bismo odredili kvadratne ostatke modulo 13, razmatramo kvadrate svih pozitivnih cijelih brojeva manjih od 13. Vrijedi sljedeće:

$$\begin{aligned}
1^2 &\equiv 1 \pmod{13},\\
2^2 &\equiv 4 \pmod{13},\\
3^2 &\equiv 9 \pmod{13},\\
4^2 &\equiv 16 \pmod{13} \equiv 3 \pmod{13},\\
5^2 &\equiv 25 \pmod{13} \equiv 12 \pmod{13},\\
6^2 &\equiv 36 \pmod{13} \equiv 10 \pmod{13},\\
7^2 &\equiv 49 \pmod{13} \equiv 10 \pmod{13},\\
8^2 &\equiv 64 \pmod{13} \equiv 12 \pmod{13},\\
9^2 &\equiv 81 \pmod{13} \equiv 3 \pmod{13},\\
10^2 &\equiv 100 \pmod{13} \equiv 9 \pmod{13},\\
11^2 &\equiv 121 \pmod{13} \equiv 4 \pmod{13},\\
12^2 &\equiv 144 \pmod{13} \equiv 1 \pmod{13}.
\end{aligned}$$

Dakle, 1,3,4,9,10,12 su kvadratni ostatci modulo 13, a 2,5,6,7,8,11 kvadratni neostatci modulo 13.

Iz prethodnog primjera uočavamo kako postoji 6 kvadratnih ostataka i 6 kvadratnih neostataka modulo 13. Kao što ćemo vidjeti u sljedećoj tvrdnji, analogno svojstvo vrijedi za sve proste brojeve p.

Teorem 1 (vidjeti [1, Teorem 4.1.]). *Ako je p neparan prost broj, reducirani sustav ostataka modulo p sadrži $\frac{p-1}{2}$ kvadratnih ostatka i $\frac{p-1}{2}$ kvadratnih neostataka.*

Dokaz: Skup $\left\{-\frac{p-1}{2}, \ldots, -2, -1, 1, 2, \ldots, \frac{p-1}{2}\right\}$ je reducirani sustav ostataka modulo p te je svaki kvadratni ostatak modulo p kongruentan kvadratu nekog od brojeva iz toga skupa, što znači da je kongruentan nekom od brojeva: $1^2, 2^2, \ldots, \left(\frac{p-1}{2}\right)^2$.
Potrebno je pokazati da su ovih $\frac{p-1}{2}$ brojeva međusobno nekongruentni modulo p.
Pretpostavimo suprotno, tj. da je $b^2 \equiv a^2 \pmod{p}$ za neke $1 \leq a < b \leq \frac{p-1}{2}$. Tada vrijedi: $b^2 - a^2 \equiv 0 \pmod{p}$, odnosno $(b-a)(b+a) \equiv 0 \pmod{p}$. S obzirom na to da je p prost broj, ovo implicira da p dijeli $b-a$ ili $b+a$. Međutim, budući da su $0 < b-a < p$ i $0 < b+a < p$, niti jedan od ovih slučajeva nije moguć te tako dolazimo do kontradikcije s pretpostavkom. Stoga su svi kvadrati međusobno nekongruentni modulo p i zaključujemo da postoji točno $\frac{p-1}{2}$ kvadratnih ostataka, dok su preostalih $\frac{p-1}{2}$ brojeva u reduciranom sustavu ostataka kvadratni neostatci.

□

Primjer 2. *Prost broj 23 ima 11 kvadratnih ostataka i 11 kvadratnih neostataka prema Teoremu 1. Kako bi pronašli sve kvadratne ostatke modulo 23 dovoljno je razmotriti $1^2, 2^2, \ldots, 11^2$.*

2.2 Legendreov simbol

Proučavanje kvadratnih ostataka i neostataka pojednostavljeno je Legendreovim simbolom koji je ime dobio po francuskom matematičaru Adrien-Marie Legendreu.

Definicija 2. *Neka je p neparan prost broj i a cijeli broj. Legendreov simbol $\left(\frac{a}{p}\right)$ definiran je kao:*

$$\left(\frac{a}{p}\right) = \begin{cases} 0\,, & \text{ako je } a \equiv 0 \pmod{p}, \\ 1\,, & \text{ako je } a \text{ kvadratni ostatak modulo } p, \\ -1\,, & \text{ako je } a \text{ kvadratni neostatak modulo } p. \end{cases}$$

Primjer 3. *Koristeći definiciju Legendreovog simbola i Primjer 1 vidimo da Legendreov simbol $\left(\frac{a}{13}\right)$, $a = 1, 2, ..., 12$ ima sljedeće vrijednosti:*

$$\left(\frac{1}{13}\right) = \left(\frac{3}{13}\right) = \left(\frac{4}{13}\right) = \left(\frac{9}{13}\right) = \left(\frac{10}{13}\right) = \left(\frac{12}{13}\right) = 1,$$
$$\left(\frac{2}{13}\right) = \left(\frac{5}{13}\right) = \left(\frac{6}{13}\right) = \left(\frac{7}{13}\right) = \left(\frac{8}{13}\right) = \left(\frac{11}{13}\right) = -1.$$

Sada navodimo kriterij za odlučivanje je li cijeli broj kvadratni ostatak nekog prostog broja koji će nam također biti koristan u dokazivanju svojstava Legendreovog simbola.

Teorem 2 (Eulerov kriterij, vidjeti [1, Teorem 4.2.]). *Neka je p neparan prost broj i neka je a cijeli broj. Tada vijedi:*

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

Dokaz. Kako bismo dokazali ovaj teorem, razmotrit ćemo 3 slučaja:

(i) Ako je $\left(\frac{a}{p}\right) = 0$, tada prema definiciji Legendreovog simbola p dijeli a, što znači da je tvrdnja očito ispunjena.

(ii) Ako je $\left(\frac{a}{p}\right) = 1$, tada kongruencija $x^2 \equiv a \pmod{p}$ ima rješenje. Neka je $x_0 \in \mathbb{Z}$ takav da vrijedi $x_0^2 \equiv a \pmod{p}$. Prema Malom Fermatovom teoremu (vidjeti [5, Theorem 2.7]), slijedi: $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv 1 \equiv \left(\frac{a}{p}\right) \pmod{p}$ te tvrdnja vrijedi i u ovom slučaju.

(iii) Ako je $\left(\frac{a}{p}\right) = -1$, tada za svaki $i \in \{1, \ldots, p-1\}$ možemo odabrati $j \in \{1, \ldots, p-1\}$ tako da vrijedi $i \cdot j \equiv a \pmod{p}$. Ovo je moguće zahvaljujući jedinstvenosti tog izbora (vidjeti [1, Teorem 3.5.]). Primijetimo da je $i \neq j$, budući da kongruencija $x^2 \equiv a \pmod{p}$ nema rješenja. Stoga se skup $\{1, \ldots, p-1\}$ može podijeliti na $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $i \cdot j \equiv a \pmod{p}$. Množenjem svih ovih $\frac{p-1}{2}$ kongruencija i koristeći Wilsonov teorem (vidjeti [5, Theorem 2.8]) koji nam govori da je $(p-1)! \equiv -1 \pmod{p}$, dobivamo: $a^{\frac{p-1}{2}} \equiv (p-1)! \equiv -1 \pmod{p}$. Time smo dokazali i posljednji slučaj.

□

Eulerov kriterij govori nam kako je a kvadratni ostatak modulo p onda i samo onda ako vrijedi sljedeće: $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Primjer 4. *Korištenjem Eulerovog kriterija odredimo je li 7 kvadratni ostatak modulo 11.*

Rješenje: Vrijedi sljedeće:

$$\left(\frac{7}{11}\right) \equiv 7^{\frac{11-1}{2}} \equiv 7^5 \pmod{11}$$

S obzirom da je $7^5 \equiv -1 \pmod{11}$, Eulerov kriterij nam govori da je $\left(\frac{7}{11}\right) = -1$. Stoga je 7 kvadratni neostatak modulo 11.

2.3 Svojstva Legendreovog simbola

Sada ćemo dokazati neka od osnovnih svojstava Legendreovog simbola.

Teorem 3 (vidjeti [6, Theorem 9.2.]). *Neka je p neparan prost broj te a i b cijeli brojevi koji nisu djeljivi s p. Tada vrijedi:*

(i) *ako je* $a \equiv b \pmod{p}$, *tada* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$,

(ii) $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$,

(iii) $\left(\frac{a^2}{p}\right) = 1$.

Dokaz. (i) Pretpostavimo da je $a \equiv b \pmod{p}$. Tada kongruencija $x^2 \equiv a \pmod{p}$ ima rješenje ako i samo ako kongruencija $x^2 \equiv b \pmod{p}$ ima rješenje. Iz toga slijedi da je $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

(ii) Prema Eulerovom kriteriju, znamo da vrijedi:

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

i

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

Sada imamo:

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

Budući da su jedine moguće vrijednosti Legendreovog simbola ± 1, zaključujemo da vrijedi: $\left(\frac{a}{p}\right)\left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

(iii) S obzirom da je $\left(\frac{a}{p}\right) = \pm 1$, iz dijela (ii) slijedi:

$$\left(\frac{a^2}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{p}\right) = 1.$$

□

Napomena 1. *Posljedica tvrdnje (ii) prethodnog teorema je ta da je umnožak dvaju kvadratnih ostataka ili dvaju kvadratnih neostataka nekog prostog broja kvadratni ostatak tog prostog broja, dok je umnožak kvadratnog ostatka i kvadratnog neostatka kvadratni neostatak.*

Sljedećom tvrdnjom pokazat ćemo kako možemo klasificirati one proste brojeve za koje je -1 kvadratni ostatak.

Teorem 4 (vidjeti [6, Theorem 9.3.]). *Neka je p neparan prost broj. Tada vrijedi:*

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

Dokaz. Prema Eulerovom kriteriju, znamo da vrijedi:

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

Ako je $p \equiv 1 \pmod 4$, tada je $p = 4l + 1$, za neki $l \in \mathbb{Z}$. Stoga imamo:

$$(-1)^{\frac{p-1}{2}} = (-1)^{2l} = 1,$$

što znači da je $\left(\frac{-1}{p}\right) = 1$.
Ako je $p \equiv 3 \pmod 4$, tada je $p = 4l + 3$, za neki $l \in \mathbb{Z}$. U tom slučaju imamo:

$$(-1)^{\frac{p-1}{2}} = (-1)^{2l+1} = -1,$$

što znači da je $\left(\frac{-1}{p}\right) = -1$. □

Ilustrirajmo sada svojstva Legendreovog simbola dokazana u prethoda dva teorema na konkretnom primjeru.

Primjer 5. *Izračunajmo vrijednost Legendreovog simbola $\left(\frac{-243}{23}\right)$.*

Rješenje: Vrijedi sljedeće:

$$\left(\frac{-243}{23}\right) = \left(\frac{-1}{23}\right) \cdot \left(\frac{3^2}{23}\right) \cdot \left(\frac{27}{23}\right) = \left(\frac{-1}{23}\right) \cdot \left(\frac{3^2}{23}\right) \cdot \left(\frac{2^2}{23}\right) = -1 \cdot 1 \cdot 1 = -1$$

Sljedeći rezultat, poznat kao Gaussova lema, daje nam još jedan kriterij za određivanje je li cijeli broj a, koji je relativno prost s prostim brojem p, kvadratni ostatak modulo p.

Teorem 5 (Gaussova lema, vidjeti [6]). *Neka je p neparan prost broj i a cijeli broj koji nije djeljiv s p. Neka je s broj najmanjih pozitivnih ostataka modulo p za brojeve $a, 2a, 3a, \ldots, \frac{p-1}{2}a$, koji su veći od $\frac{p}{2}$. Tada vrijedi:*

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

Dokaz. Neka $u_1, u_2, \ldots, u_s$ predstavljaju najmanje pozitivne ostatke brojeva $a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right)a$ modulo p koji su veći od $\frac{p}{2}$, a $v_1, v_2, \ldots, v_t$ predstavljaju najmanje pozitivne ostatke modulo p tih brojeva koji su manji od $\frac{p}{2}$. Budući da je $(ka, p) = 1$ za sve k za koje je $1 \leq k \leq \frac{p-1}{2}$, svi ti najmanji pozitivni ostaci modulo p pripadaju skupu $\{1, 2, \ldots, p-1\}$.
Pokazat ćemo da su brojevi $p - u_1, p - u_2, \ldots, p - u_s, v_1, v_2, \ldots, v_t$ upravo brojevi

$1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Da bismo to dokazali, dovoljno je pokazati da niti jedan od tih brojeva nije kongruentan modulo p, jer postoji točno $\frac{p-1}{2}$ brojeva u skupu, a svi su pozitivni i manji od $\frac{p-1}{2}$.
Jasno je da niti jedan u_i nije kongruentan ni s jednim drugim u_j modulo p, kao ni niti jedan v_i s bilo kojim drugim v_j. Ako bi vrijedila takva kongruencija, imali bismo $ma \equiv na \pmod{p}$, gde su m i n pozitivni cijeli brojevi manji ili jednaki $\frac{p-1}{2}$. Budući da p ne dijeli a, to implicira $m \equiv n \pmod{p}$, što je nemoguće.
Također, niti jedan od brojeva $p - u_i$ ne može biti kongruentan modulo p s nekim v_j, jer bi tada vrijedilo $ma \equiv p - na \pmod{p}$, što bi impliciralo $m \equiv -n \pmod{p}$ jer a nije djeljiv s p. To je nemoguće jer su i m i n elementi skupa $\{1, 2, \ldots, \frac{p-1}{2}\}$.
Sada kada znamo da brojevi $p - u_1, p - u_2, \ldots, p - u_s, v_1, v_2, \ldots, v_t$ zajedno čine cijeli niz brojeva $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku, zaključujemo da vrijedi:

$$(p - u_1)(p - u_2) \cdots (p - u_s)v_1v_2 \cdots v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p},$$

što implicira:

$$(-1)^s u_1u_2 \cdots u_sv_1v_2 \cdots v_t \equiv \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Budući da su u_i i v_i najmanji pozitivni ostatci brojeva $a, 2a, \ldots, \left(\frac{p-1}{2}\right)a$ modulo p, također znamo da vrijedi:

$$u_1u_2 \cdots u_sv_1v_2 \cdots v_t \equiv a \cdot 2a \cdots \left(\frac{p-1}{2}\right)a \equiv a^{\frac{p-1}{2}}\left(\frac{p-1}{2}\right)! \pmod{p}.$$

Stoga, iz prethodne dvije relacije slijedi:

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

S obzirom da je $\left(p, \left(\frac{p-1}{2}\right)!\right) = 1$, prethodna kongruencija implicira:

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

Pomnožimo li obje strane s $(-1)^s$ imamo:

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

Prema Eulerovom kriteriju, znamo da je $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$, pa iz toga slijedi:

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

što dokazuje teorem.

□

Primijenimo sada Gaussovu lemu na konkretnom primjeru.

Primjer 6. *Neka su $a = 3$ i $p = 13$. Da bismo primijenili Gaussovu lemu, izračunavamo najmanje pozitivne ostatke brojeva $3 \cdot 1, 3 \cdot 2, 3 \cdot 3, 3 \cdot 4, 3 \cdot 5$, i $3 \cdot 6$ modulo 13. Ti ostatci su redom 3, 6, 9, 12, 2 i 5. Budući da su točno dva od ovih ostataka veća od $\frac{13}{2}$, Gaussova lema nam daje da je $\left(\frac{3}{13}\right) = (-1)^2 = 1$.*

Značajnija primjena Gaussove leme je sljedeći teorem koji nam daje odgovor na pitanje o kvadratnim ostatcima broja 2 modulo p.

Teorem 6 (vidjeti [5, Theorem 4.6])**.** *Za svaki neparni prosti broj p vrijedi:*

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p^2-1}{8}} \pmod{p}.$$

Dokaz. Prema Gaussovoj lemi, potrebno je odrediti broj vrijednosti $2j$, za $j = 1, 2, \ldots, \frac{p-1}{2}$, koje su veće od $\frac{p}{2}$. Ako je $j \leq \frac{p}{4}$, tada je $2j < \frac{p}{2}$, pa postoji $\lfloor \frac{p}{4} \rfloor$ vrijednosti $2j$ koje su manje od $\frac{p}{2}$. Dakle, postoji $s = \frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor$ takvih vrijednosti koje su veće od $\frac{p}{2}$. Prema Gaussovoj lemi, to znači da:

$$\left(\frac{2}{p}\right) \equiv (-1)^{\frac{p-1}{2} - \lfloor \frac{p}{4} \rfloor} \pmod{p}.$$

Stoga, dovoljno je pokazati da:

$$s = \frac{p-1}{2} - \left\lfloor \frac{p}{4} \right\rfloor \equiv \frac{p^2-1}{8} \pmod{2}.$$

Rješenje se može podijeliti na slučajeve ovisno o kongruentnosti broja p modulo 8.
Ako je $p \equiv 1 \pmod{8}$, tada je $p = 8m + 1$ za neki cijeli broj m i imamo:

$$s = 4m - \left\lfloor \frac{8m+1}{4} \right\rfloor = 4m - 2m = 2m \equiv 0 \pmod{2}.$$

Ako je $p \equiv -1 \pmod{8}$, tada je $p = 8m - 1$ za neki cijeli broj m i imamo:

$$s = 4m - 1 - \left\lfloor \frac{8m-1}{4} \right\rfloor = 4m - 1 - (2m - 1) = 2m \equiv 0 \pmod{2}.$$

Ako je $p \equiv 3 \pmod{8}$, tada je $p = 8m + 3$ za neki cijeli broj m i imamo:

$$s = 4m + 1 - \left\lfloor \frac{8m+3}{4} \right\rfloor = 4m + 1 - 2m = 2m + 1 \equiv 1 \pmod{2}.$$

Ako je $p \equiv -3 \pmod{8}$, tada je $p = 8m - 3$ za neki cijeli broj m i imamo:

$$s = 4m - 2 - \left\lfloor \frac{8m-3}{4} \right\rfloor = 4m - 2 - (2m - 1) = 2m - 1 \equiv 1 \pmod{2}.$$

Dakle, ako $p \equiv \pm 1 \pmod 8$, tada je s paran, a ako $p \equiv \pm 3 \pmod 8$, tada je s neparan. Ostaje pokazati da isto vrijedi za $\frac{p^2-1}{8}$. Ako je $p = 8m \pm 1$, tada je:

$$\frac{p^2-1}{8} = \frac{64m^2 \pm 16m + 1 - 1}{8} = 8m^2 \pm 2m \equiv 0 \pmod 2,$$

a ako je $p = 8m \pm 3$, tada je:

$$\frac{p^2-1}{8} = \frac{64m^2 \pm 48m + 9 - 1}{8} = 8m^2 \pm 6m + 1 \equiv 1 \pmod 2,$$

i tvrdnja slijedi. □

Direktno iz prethodnog teorema slijedi sljedeća tvrdnja.

Korolar 1 (vidjeti [5, Corollary 4.2]). *Ako je p neparan prost broj, tada vrijedi:*

$$\left(\frac{2}{p}\right) = \begin{cases} 1, & \text{ako je } p \equiv \pm 1 \pmod 8, \\ -1, & \text{ako je } p \equiv \pm 3 \pmod 8. \end{cases}$$

Primjer 7. *Koristeći Teorem 6, izračunavamo Legendreove simbole za različite proste brojeve:*

$$\left(\frac{2}{19}\right) \equiv (-1)^{\frac{19^2-1}{8}} \equiv (-1)^{\frac{360}{8}} \equiv (-1)^{45} \equiv -1 \pmod{19},$$
$$\left(\frac{2}{23}\right) \equiv (-1)^{\frac{23^2-1}{8}} \equiv (-1)^{\frac{528}{8}} \equiv (-1)^{66} \equiv 1 \pmod{23},$$
$$\left(\frac{2}{31}\right) \equiv (-1)^{\frac{31^2-1}{8}} \equiv (-1)^{\frac{960}{8}} \equiv (-1)^{120} \equiv 1 \pmod{31},$$
$$\left(\frac{2}{41}\right) \equiv (-1)^{\frac{41^2-1}{8}} \equiv (-1)^{\frac{1680}{8}} \equiv (-1)^{210} \equiv -1 \pmod{41}.$$

Uz prethodne rezultate, za dokaz Gaussovog kvadratnog zakona reciprociteta kojim ćemo se baviti u sljedećem poglavlju potrebna će nam biti i sljedeća pomoćna tvrdnja.

Lema 1 (Einsteinova lema, vidjeti [5, Lemma 4.1]). *Neka je a cijeli, neparan broj, a $p > 2$ neparan prost broj takav da p ne dijeli a. Tada vrijedi:*

$$\left(\frac{a}{p}\right) = (-1)^M,$$

gdje je $M = \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor$.

Dokaz. Koristimo istu notaciju kao i u dokazu Gaussove leme. Neka $u_1, u_2, \ldots, u_s$ predstavljaju najmanje pozitivne ostatke brojeva $a, 2a, 3a, \ldots, \left(\frac{p-1}{2}\right) a$ modulo p koji su veći od $\frac{p}{2}$, a $v_1, v_2, \ldots, v_t$ predstavljaju najmanje pozitivne ostatke tih brojeva modulo p koji su manji od $\frac{p}{2}$.

Prema Teoremu o dijeljenju s ostatkom (vidjeti [1, Teorem 2.2]) znamo da za svaki $j = 1, 2, \ldots, \frac{p-1}{2}$, postoje cijeli brojevi q_j i t_j takvi da je

$$ja = q_j p + t_j, \quad \text{gdje je} \quad 1 \leq t_j < p.$$

Tada je $q_j = \left\lfloor \frac{ja}{p} \right\rfloor$ jer je $\frac{ja}{p} = q_j + \frac{t_j}{p} < q_j + 1$. Prema tome, za svaki takav j, vrijedi:

$$ja = \left\lfloor \frac{ja}{p} \right\rfloor p + t_j, \quad \text{gdje je} \quad 1 \leq t_j < p,$$

pri čemu je $t_j = u_j$, ako je $t_j > \frac{p}{2}$, i $t_j = v_j$, ako je $t_j < \frac{p}{2}$. Dakle, imamo

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{2.1}$$

Međutim, kao što je pokazano u dokazu Gaussove leme, vrijednosti $p - u_j$ za $j = 1, 2, \ldots, s$ i v_j za $j = 1, 2, \ldots, t$ samo su permutacija brojeva $1, 2, \ldots, \frac{p-1}{2}$. Stoga,

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{j=1}^{s} (p - u_j) + \sum_{j=1}^{t} v_j = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{2.2}$$

Oduzimanjem (2.2) od (2.1) dobivamo:

$$(a-1) \sum_{j=1}^{\frac{p-1}{2}} j = p \left(\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - s \right) + 2 \sum_{j=1}^{s} u_j. \tag{2.3}$$

Sada reduciramo jednakost (2.3) modulo 2 i s obzirom da su a i p neparni, tj. $a \equiv p \equiv 1 \pmod 2$, dobivamo:

$$0 \equiv \left(\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - s \right) \pmod 2,$$

iz čega slijedi da je $s \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor \pmod 2$.
Gaussova lema govori nam da vrijedi:

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

S obzirom da je $(-1)^s = (-1)^M$ zaključujemo da je:

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

□

Pogledajmo sada primjenu Einsteinove leme na primjeru.

Primjer 8. *Izračunat ćemo vrijednost Legendreovog simbola* $\left(\frac{5}{11}\right)$ *koristeći Einsteinovu lemu na sljedeći način:*

$$\sum_{j=1}^{\frac{11-1}{2}} \left\lfloor \frac{5j}{11} \right\rfloor = \left\lfloor \frac{5}{11} \right\rfloor + \left\lfloor \frac{10}{11} \right\rfloor + \left\lfloor \frac{15}{11} \right\rfloor + \left\lfloor \frac{20}{11} \right\rfloor + \left\lfloor \frac{25}{11} \right\rfloor = 0+0+1+1+2 = 4,$$

dakle,

$$\left(\frac{5}{11}\right) = (-1)^4 = 1.$$

3 | Gaussov kvadratni zakon reciprociteta

Neka su p i q neparni prosti brojevi. Pitanje koje se postavlja je: ako je p kvadratni ostatak modulo q, odnosno ako kongruencija $x^2 \equiv p \pmod{q}$ ima rješenja, možemo li zaključiti je li i q kvadratni ostatak modulo p, tj. ima li rješenja kongruencija $x^2 \equiv q \pmod{p}$, u kojoj su uloge brojeva p i q zamijenjene?

Sljedeći teorem, poznat kao Gaussov kvadratni zakon reciprociteta, pruža nam odgovor na ovo pitanje. Njega je prvi formulirao Legendre 1785. godine, ali nije uspio dati valjani dokaz. Tek je Gauss 1796. godine u svom djelu *Disquisitiones Arithmeticae* dao prvi ispravan dokaz ovog teorema. Gauss je smatrao ovaj teorem toliko značajnim da je dao čak osam različitih dokaza za njega, dok danas postoji preko 240 različitih dokaza.

3.1 Iskaz i dokaz teorema

Sada ćemo navesti iskaz i dokaz ovog važnog teorema koji povezuje dva Legendreova simbola $\left(\frac{p}{q}\right)$ i $\left(\frac{q}{p}\right)$.

Teorem 7 (Gaussov kvadratni zakon reciprociteta, vidjeti [5, Theorem 4.7])**.** *Neka su $p \neq q$ dva neparna prosta broja. Tada vrijedi:*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}. \tag{3.1}$$

Dokaz. Najprije ćemo dokazati da vrijedi sljedeće:

$$\frac{p-1}{2}\cdot\frac{q-1}{2} = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor. \tag{3.2}$$

Neka je

$$S = \{(jp, kq) : 1 \leq j \leq \frac{q-1}{2}, 1 \leq k \leq \frac{p-1}{2}\}.$$

Skup S ima $\frac{p-1}{2}\cdot\frac{q-1}{2}$ elemenata. Također, lako se vidi da je $jp \neq kq$ za bilo koje $1 \leq j \leq \frac{q-1}{2}$ ili $1 \leq k \leq \frac{p-1}{2}$.
Nadalje, rastavimo skup S na dva disjunktna skupa S_1 i S_2:

$$S = S_1 \cup S_2,$$

gdje su

$$S_1 = \{(jp, kq) \in S : jp < kq\},$$

i

$$S_2 = \{(jp, kq) \in S : jp > kq\}.$$

Ako je $(jp, kq) \in S_1$, tada je $j < \frac{kq}{p}$. Također, $\frac{kq}{p} \leq \frac{(p-1)q}{2p} < \frac{q}{2}$. Dakle,

$$\left\lfloor \frac{kq}{p} \right\rfloor < \frac{q}{2},$$

odakle slijedi

$$\left\lfloor \frac{kq}{p} \right\rfloor \leq \frac{q-1}{2}.$$

Stoga, kardinalitet skupa S_1 je $\sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$. Slično tome, kardinalitet skupa S_2 je $\sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$. Time je dokazano da vrijedi (3.2).

Sada označimo: $M = \sum_{k=1}^{\frac{p-1}{2}} \left\lfloor \frac{kq}{p} \right\rfloor$ i $N = \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{jp}{q} \right\rfloor$. Ako stavimo $q = a$ u Eisensteinovoj lemi, tada vrijedi:

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

Slično tome, iz Einsteinove leme slijedi i

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

Stoga imamo,

$$\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{M+N}.$$

Rezultat sada slijedi direktno iz (3.2). □

Napomena 2. *Lako se vidi da se formula* (3.1) *može zapisati i na sljedeći način:*

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

Sljedeća tvrdnja predstavlja ekvivalentnu formulaciju zakona reciprociteta.

Korolar 2 (vidjeti [5, Corollary 4.3])**.** *Neka su $p \neq q$ neparni prosti brojevi. Tada vrijedi:*

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

Primjer 9. *Izračunajmo Legendreov simbol $\left(\frac{3}{19}\right)$. Prema Gaussovom kvadratnom zakonu reciprociteta, vrijedi:*

$$\left(\frac{3}{19}\right) = (-1)^{\frac{3-1}{2}\cdot\frac{19-1}{2}} \left(\frac{19}{3}\right) = (-1)^{1\cdot 9} \left(\frac{1}{3}\right) = (-1)^9 \cdot 1 = -1.$$

Dakle, 3 nije kvadratni ostatak modulo 19.

Primjer 10 (vidjeti [3, Zadatak 2.7.]). *Dokažite da postoji beskonačno mnogo prostih brojeva oblika $6m+1$, gdje je m prirodan broj.*

Rješenje: Pretpostavimo suprotno, tj. da postoji samo konačno mnogo prostih brojeva oblika $6m+1$ te ih označimo s $p_1, p_2, \ldots, p_n$. Razmotrimo broj:

$$M = (2p_1p_2 \ldots p_n)^2 + 3.$$

Ako je p prosti djelitelj broja M, primjećujemo sljedeće:

- p ne može biti jednak 2, jer vrijedi $M \equiv 1 \pmod 2$,
- p ne može biti jednak 3, jer vrijedi $M \equiv 1 \pmod 3$,
- p ne može biti jednak nijednom od brojeva p_i, jer vrijedi $M \equiv 3 \pmod{p_i}$ za sve $p_i \geq 7$.

Dakle, prosti broj p mora biti oblika $6k+5$, gdje je k neki broj iz skupa prirodnih brojeva s nulom. Budući da p dijeli M, slijedi:

$$(2p_1p_2 \ldots p_n)^2 \equiv -3 \pmod p,$$

što znači da je -3 kvadratni ostatak modulo p. Koristeći Gaussov kvadratni zakon reciprociteta i svojstva Legendreova simbola, dobivamo:

$$\left(\frac{-3}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}\cdot\frac{3-1}{2}}\left(\frac{p}{3}\right) = (-1)^{p-1}\left(\frac{p}{3}\right).$$

Budući da je $p = 6k+5$, slijedi:

$$\left(\frac{-3}{p}\right) = \left(\frac{6k+5}{3}\right) = \left(\frac{2}{3}\right) = -1,$$

što znači da -3 nije kvadratni ostatak modulo p. Ovime dolazimo do kontradikcije i zaključujemo da ne može postojati konačno mnogo prostih brojeva oblika $6m+1$.

3.2 Pepinov test prostosti

Gaussov zakon kvadratnog reciprociteta ima mnogo primjena, a jedna od njih je dokazivanje valjanosti sljedećeg testa prostosti za Fermatove brojeve, odnosno brojeve oblika $F_n = 2^{2^n} + 1$, za $n \in \mathbb{N}$. Kako bi mogli dokazati sljedeći teorem najprije ćemo uvesti sljedeću definiciju.

Definicija 3. *Neka su a i p relativno prosti prirodni brojevi. Najmanji prirodni broj d za kojega vrijedi*

$$a^d \equiv 1 \pmod p$$

naziva se red od a modulo p.

Teorem 8 (Pepinov test, vidjeti [5, Theorem 4.8]). *Fermatov broj* $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$, *je prost broj ako i samo ako vrijedi:*

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n}. \tag{3.3}$$

Dokaz. Pretpostavimo najprije da vrijedi (3.3). Kvadriranjem obje strane u toj kongruenciji, dobivamo:

$$3^{F_n-1} \equiv 1 \pmod{F_n}.$$

Prema tome, ako je p prost broj koji dijeli F_n, onda vrijedi:

$$3^{F_n-1} \equiv 1 \pmod{p}.$$

Koristeći tvrdnju koja govori da d dijeli k ako i samo ako vrijedi $a^k \equiv 1 \pmod{p}$, gdje je d red od a modulo p (vidjeti [5, Propozicija 3.18]), zaključujemo da red od 3 modulo p, označimo ga s d, dijeli $F_n - 1 = 2^{2^n}$. Međutim, prema (3.3), d ne dijeli 2^{2^n-1}. Dakle, jedina mogućnost je da vrijedi $d = 2^{2^n} = F_n - 1$. Prema Malom Fermatovom teoremu (vidjeti [5, Theorem 2.7]), vrijedi $d = F_n - 1 \leq p - 1$, pa kako $p \mid F_n$, onda je $p = F_n$. Posljedično, p mora biti prost broj te je dovoljnost uvjeta (3.3) dokazana.

Pretpostavimo sada da je F_n prost, tada prema Gaussovom zakonu kvadratnog reciprociteta vrijedi:

$$\left(\frac{3}{F_n}\right) = \left(\frac{F_n}{3}\right) = \left(\frac{2}{3}\right) = -1, \tag{3.4}$$

gdje je prva jednakost točna jer $F_n \equiv 1 \pmod 4$ i $F_n \equiv 2 \pmod 3$, dok posljednja jednakost proizlazi iz Korolara 1. Prema Eulerovom kriteriju, imamo:

$$\left(\frac{3}{F_n}\right) \equiv 3^{\frac{F_n-1}{2}} \pmod{F_n}. \tag{3.5}$$

Kombiniranjem kongruencija (3.4) i (3.5) dobivamo:

$$3^{\frac{F_n-1}{2}} \equiv -1 \pmod{F_n},$$

što dokazuje nužnost uvjeta (3.3). □

Primjer 11. *Želimo uz pomoć Pepinovog testa zaključiti je li Fermatov broj F_4 prost. Za $F_4 = 2^{2^4} + 1 = 65537$, provjeravamo je li zadovoljen uvjet:*

$$3^{\frac{65537-1}{2}} \equiv 3^{32768} \pmod{65537}.$$

Računajući modulo 65537, *dobivamo:*

$$3^{32768} \equiv -1 \pmod{65537}.$$

Prema Pepinovom testu, Fermatov broj $F_4 = 65537$ je prost.

4 | Jacobijev simbol

U ovom poglavlju proučavat ćemo Jacobijev simbol koji predstavlja generalizaciju Legendreovog simbola. Jacobijevi simboli korisni su za izračunavanje vrijednosti Legendreovog simbola.

4.1 Definicija

Sada ćemo navesti definiciju Jacobijevog simbola te ju zatim demonstrirati na primjeru.

Definicija 4. *Neka je $n > 1$ neparan prirodni broj oblika $n = \prod_{j=1}^{k} p_j^{e_j}$, gdje su $e_j \in \mathbb{N}$ i p_j različiti prosti brojevi. Tada se Jacobijev simbol od a u odnosu na n definira kao*

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{k} \left(\frac{a}{p_j}\right)^{e_j},$$

za svaki $a \in \mathbb{Z}$, gdje su simboli na desnoj strani Legendreovi simboli.

Primjer 12. *Iz definicije Jacobijeva simbola slijedi:*

$$\left(\frac{2}{77}\right) = \left(\frac{2}{7}\right)\left(\frac{2}{11}\right).$$

Izračunajmo svaki Legendreov simbol zasebno pomoću Teorema 6:

$$\left(\frac{2}{7}\right) = (-1)^{\frac{7^2-1}{8}} = (-1)^6 = 1,$$

i

$$\left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1.$$

Stoga,

$$\left(\frac{2}{77}\right) = \left(\frac{2}{7}\right)\left(\frac{2}{11}\right) = 1 \cdot (-1) = -1.$$

Dakle, Jacobijev simbol $\left(\frac{2}{77}\right) = -1$.

Kada je n prost broj, Jacobijev simbol je isti kao i Legendreov simbol. Međutim, kada je n složen, vrijednost Jacobijevog simbola $\left(\frac{a}{n}\right)$ nam nužno ne govori ima li kongruencija $x^2 \equiv a \pmod{n}$ rješenja. Znamo da ako kongruencija $x^2 \equiv a \pmod{n}$ ima rješenja, tada vrijedi $\left(\frac{a}{n}\right) = 1$. Primijetimo da ako je p prost djelitelj od n i ako kongruencija $x^2 \equiv a \pmod{n}$ ima rješenja, tada i kongruencija $x^2 \equiv a \pmod{p}$ također ima rješenja te je tada $\left(\frac{a}{p}\right) = 1$. Stoga posljedično vrijedi:

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{k} \left(\frac{a}{p_j}\right)^{e_j} = 1.$$

Da bismo pokazali kako je moguće da je $\left(\frac{a}{n}\right) = 1$ čak i kada kongruencija $x^2 \equiv a \pmod{n}$ nema rješenja, pogledajmo sljedeći primjer.

Primjer 13. *Neka je $a = 2$ i $n = 55$. Prema definiciji Jacobijevog simbola vrijedi:*

$$\left(\frac{2}{55}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{11}\right).$$

Pomoću Teorema 6 računamo:

$$\left(\frac{2}{5}\right) = (-1)^{\frac{5^2-1}{8}} = (-1)^3 = -1 \quad i \quad \left(\frac{2}{11}\right) = (-1)^{\frac{11^2-1}{8}} = (-1)^{15} = -1.$$

Dakle, imamo:

$$\left(\frac{2}{55}\right) = (-1)\cdot(-1) = 1.$$

Iako vrijedi $\left(\frac{2}{55}\right) = 1$, kongruencija $x^2 \equiv 2 \pmod{55}$ nema rješenja jer kongruencije $x^2 \equiv 2 \pmod{5}$ i $x^2 \equiv 2 \pmod{11}$ također nemaju rješenja.

4.2 Svojstva Jacobijevog simbola

Sada ćemo navesti i dokazati osnovna svojstva Jacobijevog simbola.

Teorem 9 (vidjeti [5, Theorem 4.10])**.** *Neka je n neparan prirodan broj te neka su a i b cijeli brojevi. Tada vrijedi:*

(i) Ako je $a \equiv b \pmod{n}$, tada je $\left(\frac{a}{n}\right) = \left(\frac{b}{n}\right)$.

(ii) $\left(\frac{ab}{n}\right) = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right)$.

(iii) $\left(\frac{-1}{n}\right) = (-1)^{\frac{n-1}{2}}$.

(iv) $\left(\frac{2}{n}\right) = (-1)^{\frac{n^2-1}{8}}$.

Dokaz. U dokazima svih četiriju dijelova ovog teorema koristimo kanonsku faktorizaciju broja n na proste faktore: $n = \prod_{j=1}^{k} p_j^{a_j}$.

(i) Znamo da ako je p prost broj koji dijeli n, tada $a \equiv b \pmod{p}$. Iz Teorema 3 slijedi $\left(\frac{a}{p_j}\right) = \left(\frac{b}{p_j}\right)$ za sve $j = 1, 2, \ldots, k$. Stoga,

$$\left(\frac{a}{n}\right) = \prod_{j=1}^{k} \left(\frac{a}{p_j}\right)^{a_j} = \prod_{j=1}^{k} \left(\frac{b}{p_j}\right)^{a_j} = \left(\frac{b}{n}\right).$$

(ii) Iz Teorema 3 znamo da je $\left(\frac{ab}{p_j}\right) = \left(\frac{a}{p_j}\right)\left(\frac{b}{p_j}\right)$ za sve $j = 1, 2, \ldots, k$. Dakle,

$$\left(\frac{ab}{n}\right) = \prod_{j=1}^{k} \left(\frac{ab}{p_j}\right)^{a_j} = \prod_{j=1}^{k} \left(\frac{a}{p_j}\right)^{a_j} \left(\frac{b}{p_j}\right)^{a_j} = \left(\frac{a}{n}\right)\left(\frac{b}{n}\right).$$

(iii) Prema Teoremu 4 je $\left(\frac{-1}{p_j}\right) = (-1)^{\frac{p_j-1}{2}}$ za sve $j = 1, 2, \ldots, k$. Dakle,

$$\left(\frac{-1}{n}\right) = \prod_{j=1}^{k} \left(\frac{-1}{p_j}\right)^{a_j} = \prod_{j=1}^{k} (-1)^{a_j \frac{p_j-1}{2}} = (-1)^{\sum_{j=1}^{k} a_j \frac{p_j-1}{2}}. \tag{4.1}$$

Kako bismo dovršili dokaz ovog dijela, trebamo dokazati da vrijedi:

$$n \equiv 1 + \sum_{j=1}^{k} a_j(p_j - 1) \pmod{4}. \tag{4.2}$$

To ćemo dokazati metodom matematičke indukcije po k. Ako je $k = 1$, tada je

$$n = p_1^{a_1} = [1 + (p_1 - 1)]^{a_1},$$

a prema binomnom teoremu (vidjeti [5, Theorem 1.6]), ovo je jednako

$$1 + a_1(p_1 - 1) + \sum_{j=2}^{k} \binom{a_j}{j} (p_j - 1)^j \equiv 1 + a_1(p_1 - 1) \pmod{4},$$

budući da je $(p_1 - 1)^j \equiv 0 \pmod{4}$ za $j > 1$. Pretpostavimo da tvrdnja vrijedi za sve vrijednosti manje ili jednake $k = t \geq 2$. Tada je

$$\begin{aligned} n &= \prod_{j=1}^{t+1} p_j^{a_j} = \left(\prod_{j=1}^{t} p_j^{a_j}\right) p_{t+1}^{a_{t+1}} \\ &\equiv \left[1 + \sum_{j=1}^{t} a_j(p_j - 1)\right] \cdot [1 + a_{t+1}(p_{t+1} - 1)] \pmod{4}, \end{aligned}$$

prema indukcijskoj pretpostavci za $k = t$ i $k = 1$. Dakle, gornji izraz je kongruentan

$$1 + a_{t+1}(p_{t+1} - 1) + \sum_{j=1}^{t} a_j(p_j - 1) \equiv 1 + \sum_{j=1}^{t+1} a_j(p_j - 1) \pmod{4},$$

jer je za bilo koji j, $(p_j - 1)(p_{t+1} - 1) \equiv 0 \pmod 4$, što dokazuje tvrdnju (4.2). Koristeći tvrdnju (4.2) i oduzimajući 1, a zatim dijeleći s 2, dobivamo

$$\frac{n-1}{2} \equiv \sum_{j=1}^{k} \frac{a_j(p_j - 1)}{2} \pmod 2,$$

što je isti eksponent kao kod -1 u (4.1). Time je dokazan ovaj dio teorema.

(iv) Iz Teorema 6 znamo da vrijedi: $\left(\frac{2}{p_j}\right) = (-1)^{\frac{p_j^2-1}{8}}$ za sve $j = 1, 2, \ldots, k$. Dakle,

$$\left(\frac{2}{n}\right) = \prod_{j=1}^{k} \left(\frac{2}{p_j}\right)^{a_j} = \prod_{j=1}^{k} (-1)^{a_j \frac{p_j^2-1}{8}} = (-1)^{\sum_{j=1}^{k} a_j \frac{p_j^2-1}{8}}. \tag{4.3}$$

Koristeći binomni teorem kao u dokazu dijela (iii), dobivamo

$$(1 + p_j^2 - 1)^{a_j} \equiv 1 + a_j(p_j^2 - 1) \pmod{64},$$

budući da je $p_j^2 \equiv 1 \pmod 8$. Stoga, indukcijskom argumentacijom kao u dokazu dijela (iii), slijedi

$$n^2 \equiv 1 + \sum_{j=1}^{k} a_j(p_j^2 - 1) \pmod{64}.$$

Oduzimajući 1 i dijeleći s 8, dobivamo

$$\frac{n^2-1}{8} \equiv \sum_{j=1}^{k} \frac{a_j(p_j^2 - 1)}{8} \pmod 8,$$

što je eksponent od -1 u (4.3) te tvrdnja vrijedi.

□

Primjer 14. *Izračunajmo vrijednost Jacobijevog simbola:* $\left(\frac{238}{15}\right)$.

Rješenje: Vrijedi sljedeće:

$$\begin{aligned}\left(\frac{238}{15}\right) &= \left(\frac{14}{15}\right) \cdot \left(\frac{17}{15}\right) = \left(\frac{-1}{15}\right) \cdot \left(\frac{2}{15}\right) = (-1)^{\frac{15-1}{2}} \cdot (-1)^{\frac{15^2-1}{8}} \\ &= (-1)^7 \cdot (-1)^{28} = -1.\end{aligned}$$

4.3 Zakon kvadratnog reciprociteta za Jacobijev simbol

Sada ćemo pokazati da Gaussov zakon kvadratnog reciprociteta vrijedi i za Jacobijev simbol.

Teorem 10 (Zakon reciprociteta za Jacobijev simbol, vidjeti [5, Theorem 4.11]). *Ako su m i n neparni i relativno prosti prirodni brojevi > 1, tada vrijedi*

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

Dokaz. Neka je $m = \prod_{i=1}^{k} p_i^{a_i}$ i $n = \prod_{j=1}^{l} q_j^{b_j}$, gdje $p_i \neq q_j$ za sve i i j. Tada vrijedi:

$$\left(\frac{m}{n}\right) = \prod_{j=1}^{l}\left(\frac{m}{q_j}\right)^{b_j} = \prod_{j=1}^{l}\prod_{i=1}^{k}\left(\frac{p_i}{q_j}\right)^{a_i b_j}.$$

i

$$\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\left(\frac{n}{p_i}\right)^{a_i} = \prod_{i=1}^{k}\prod_{j=1}^{l}\left(\frac{q_j}{p_i}\right)^{a_i b_j}.$$

Iz toga slijedi:

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{j=1}^{l}\prod_{i=1}^{k}\left[\left(\frac{p_i}{q_j}\right)\left(\frac{q_j}{p_i}\right)\right]^{a_i b_j}.$$

Prema Gaussovom zakonu kvadratnog reciprociteta (Teorem 7) ovo je jednako

$$\left(\frac{m}{n}\right)\left(\frac{n}{m}\right) = \prod_{i=1}^{k}\prod_{j=1}^{l}(-1)^{a_i\left(\frac{p_i-1}{2}\right)b_j\left(\frac{q_j-1}{2}\right)} = (-1)^{T},$$

gdje je

$$T = \sum_{i=1}^{k}\sum_{j=1}^{l} a_i\left(\frac{p_i-1}{2}\right) b_j\left(\frac{q_j-1}{2}\right) = \sum_{i=1}^{k} a_i\left(\frac{p_i-1}{2}\right)\sum_{j=1}^{l} b_j\left(\frac{q_j-1}{2}\right).$$

Međutim, kao što je prikazano u dokazu Teorema 7, vrijedi:

$$\sum_{i=1}^{k} a_i\left(\frac{p_i-1}{2}\right) \equiv \frac{m-1}{2} \pmod 2,$$

i

$$\sum_{j=1}^{l} b_j\left(\frac{q_j-1}{2}\right) \equiv \frac{n-1}{2} \pmod 2,$$

Dakle,

$$\sum_{i=1}^{k} a_i\left(\frac{p_i-1}{2}\right)\sum_{j=1}^{l} b_j\left(\frac{q_j-1}{2}\right) = \frac{m-1}{2}\cdot\frac{n-1}{2} \pmod 2.$$

te iz toga slijedi tvrdnja teorema. □

Primjer 15. *Neka je $m = 13065 = 3\cdot 5\cdot 13\cdot 67$ i $n = 1309 = 7\cdot 11\cdot 17$. Tada je $(m,n) = 1$, i vrijedi:*

$$\left(\frac{13065}{1309}\right)\left(\frac{1309}{13065}\right) = (-1)^{\frac{13065-1}{2}\cdot\frac{1309-1}{2}} = (-1)^{6532\cdot 654} = 1.$$

Primjer 16 (vidjeti [3, Zadatak 4.30.]). *Izračunajte vrijednost Jacobijevog simbola* $\left(\frac{n^5}{n+2}\right)$ *u ovisnosti o neparnom prirodnom broju* n.

Rješenje: Koristeći Teorem 9 imamo:

$$\left(\frac{n^5}{n+2}\right) = \left(\frac{n}{n+2}\right)^5.$$

Primijenimo li sada Teoreme 9 i 10 na Jacobijev simbol $\left(\frac{n}{n+2}\right)$ dobivamo:

$$\begin{aligned}\left(\frac{n}{n+2}\right) &= (-1)^{\frac{n-1}{2}\cdot\frac{n+2-1}{2}} \cdot \left(\frac{n+2}{n}\right) = (-1)^{\frac{n^2-1}{4}} \cdot \left(\frac{2}{n}\right) \\ &= (-1)^{\frac{n^2-1}{4}} \cdot (-1)^{\frac{n^2-1}{8}} = (-1)^{3\cdot\frac{n^2-1}{8}}.\end{aligned}$$

Ako je $n \equiv 1 \pmod 8$, odnosno $n = 8k+1$, za neki cijeli broj k, vrijedi:

$$(-1)^{3\cdot\frac{n^2-1}{8}} = (-1)^{3\cdot\frac{(8k+1)^2-1}{8}} = (-1)^{3\cdot\frac{16k(4k+1)}{8}} = (-1)^{6k(4k+1)} = 1.$$

Ako je $n \equiv 3 \pmod 8$, odnosno $n = 8k+3$, za neki cijeli broj k, vrijedi:

$$(-1)^{3\cdot\frac{n^2-1}{8}} = (-1)^{3\cdot\frac{(8k+3)^2-1}{8}} = (-1)^{3\cdot\frac{8(8k^2+6k+1)}{8}} = (-1)^{24k^2+18k+3} = -1.$$

Ako je $n \equiv 5 \pmod 8$, odnosno $n = 8k+5$, za neki cijeli broj k, vrijedi:

$$(-1)^{3\cdot\frac{n^2-1}{8}} = (-1)^{3\cdot\frac{(8k+5)^2-1}{8}} = (-1)^{3\cdot\frac{8(8k^2+10k+3)}{8}} = (-1)^{24k^2+30k+9} = -1.$$

Ako je $n \equiv 7 \pmod 8$, odnosno $n = 8k+7$, za neki cijeli broj k, vrijedi:

$$(-1)^{3\cdot\frac{n^2-1}{8}} = (-1)^{3\cdot\frac{(8k+7)^2-1}{8}} = (-1)^{3\cdot\frac{8(8k^2+14k+6))}{8}} = (-1)^{24k^2+42k+18} = 1.$$

Dakle, $\left(\frac{n^5}{n+2}\right) = 1$, za $n \equiv 1,7 \pmod 8$ i $\left(\frac{n^5}{n+2}\right) = -1$, za $n \equiv 3,5 \pmod 8$.

4.4 Algoritam za računanje Jacobijevog simbola

Najprije ćemo definirati niz cijelih brojeva povezanih s vrijednostima Jacobijevog simbola koje želimo izračunati. Neka su $1 < n < m$ relativno prosti neparni brojevi te postavimo $R_0 = m$, $R_1 = n$. Tada ponovljenom primjenom Teorema o dijeljenju s ostatkom za $j = 0, 1, 2, \ldots, k-2$, dobivamo

$$R_j = R_{j+1}q_{j+1} + 2^{\alpha_{j+1}}R_{j+2},$$

gdje je $R_k = 1$. Sada ćemo iskazati teorem koji nam daje algoritam za računanje Jacobijevog simbola.

Teorem 11 (vidjeti [5, Theorem 4.12]). *Neka su $1 < n < m$ relativno prosti neparni brojevi. Tada vrijedi:*

$$\left(\frac{m}{n}\right) = (-1)^{U+V},$$

gdje su

$$U = \frac{1}{8}\sum_{j=1}^{k-1} \alpha_j (R_j^2 - 1),$$

i

$$V = \frac{1}{2}\sum_{j=1}^{k-2} (R_j - 1)(R_{j+1} - 1).$$

Dokaz. Prema Teoremu 9 znamo da vrijedi:

$$\left(\frac{m}{n}\right) = \left(\frac{R_0}{R_1}\right) = \left(\frac{2^{\alpha_1} R_2}{R_1}\right) = \left(\frac{2}{R_1}\right)^{\alpha_1} \left(\frac{R_2}{R_1}\right) = (-1)^{\alpha_1 \frac{R_1^2-1}{8}} \left(\frac{R_2}{R_1}\right).$$

Također, prema Teoremu 10 vrijedi:

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

Stoga je

$$\left(\frac{m}{n}\right) = (-1)^{\frac{R_1-1}{2}\cdot\frac{R_2-1}{2} + \alpha_1 \frac{R_1^2-1}{8}} \left(\frac{R_1}{R_2}\right).$$

Indukcijom se ovaj proces nastavlja, a za $j = 2, 3, \ldots, k-1$ vrijedi

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

Tako dobivamo traženi rezultat. □

Primjer 17. *Neka su $m = 623$ i $n = 111$. Izračunajmo Jacobijev simbol $\left(\frac{623}{111}\right)$ koristeći prethodno navedeni algoritam. Najprije postavimo: $R_0 = m = 623$ i $R_1 = n = 111$. Primjenom Teorema o dijeljenju s ostatkom imamo:*

$$\begin{aligned} R_0 &= 623 = R_1 q_1 + 2^{\alpha_1} R_2 = 111 \cdot 5 + 2^2 \cdot 17, \\ R_1 &= 111 = R_2 q_2 + 2^{\alpha_2} R_3 = 17 \cdot 6 + 2^0 \cdot 9, \\ R_2 &= 17 = R_3 q_3 + 2^{\alpha_3} R_4 = 9 \cdot 1 + 2^3 \cdot 1, \end{aligned}$$

pa je $k = 4$.

$$U = \frac{1}{8}\sum_{j=1}^{k-1} \alpha_j (R_j^2 - 1) = \frac{1}{8}[2 \cdot (111^2 - 1) + 0 \cdot (17^2 - 1) + 3 \cdot (9^2 - 1)] = 3110,$$

$$V = \frac{1}{2}\sum_{j=1}^{k-2} (R_j - 1)(R_{j+1} - 1) = \frac{1}{2}[(111 - 1)(17 - 1) + (17 - 1)(9 - 1)] = 944.$$

Stoga,

$$\left(\frac{623}{111}\right) = (-1)^{U+V} = (-1)^{3110+944} = (-1)^{4054} = 1.$$

4.5 Eulerovi pseudoprosti brojevi

Najprije navodimo definicije pseudoprostih i jakih pseudoprostih brojeva u bazi b kako bismo se nakon toga mogli upoznati s Eulerovim pseudoprostim brojevima.

Definicija 5. *Neka je m složeni broj i b cijeli broj. Kažemo da je broj m pseudoprost u bazi b ako vrijedi:*

$$b^m \equiv b \pmod{m}.$$

Definicija 6. *Neka je m neparan složeni broj te neka je $m-1 = 2^s \cdot t$, gdje je t neparan. Kažemo da je m jaki pseudoprost broj u bazi b ako za cijeli broj b vrijedi*

$$b^t \equiv 1 \pmod{m}$$

ili postoji r, $0 \leq r < s$, takav da je

$$b^{2^r \cdot t} \equiv -1 \pmod{m}.$$

Neka je p neparan prost broj. Prema Eulerovom kriteriju, znamo da vrijedi:

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

Stoga, ako želimo testirati je li pozitivan cijeli broj m prost možemo uzeti cijeli broj b, gdje je $(b, m) = 1$, i odrediti vrijedi li

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

gdje je $\left(\frac{b}{m}\right)$ Jacobijev simbol. Ako utvrdimo da ova kongruencija nema rješenja, tada je m složen broj. Na taj način možemo definirati vrstu pseudoprostih brojeva temeljenih na Eulerovom kriteriju.

Definicija 7. *Neka je m prirodan, neparan i složen broj koji zadovoljava kongruenciju*

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

gdje je b prirodan broj. Tada kažemo da je m Eulerov pseudoprost broj u bazi b.

Primjer 18. *Neka je $m = 561$ i $b = 2$. Računanjem dobivamo da vrijedi: $2^{280} \equiv 1 \pmod{561}$. Budući da je $561 \equiv 1 \pmod{8}$, koristeći Teorem 9. (iv) znamo da je $\left(\frac{2}{561}\right) = 1$. Stoga,*

$$2^{280} \equiv 1 \equiv \left(\frac{2}{561}\right) \pmod{561}.$$

Budući da je $561 = 3 \cdot 11 \cdot 17$ složen, neparan i pozitivan cijeli broj koji zadovoljava kongruenciju $b^{\frac{m-1}{2}} \equiv \left(\frac{b}{m}\right) \pmod{m}$, on je Eulerov pseudoprost broj u bazi 2.

Sljedeća tvrdnja pokazuje da je svaki Eulerov pseudoprost broj u bazi b također pseudoprost broj u toj bazi.

Propozicija 1 (vidjeti [6, Proposition 9.1.]). *Ako je m Eulerov pseudoprost broj u bazi b, tada je m pseudoprost broj u bazi b.*

Dokaz. Ako je m Eulerov pseudoprost broj u bazi b, tada vrijedi

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

Kvadriranjem obje strane ove kongruencije dobivamo

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

Budući da je $\left(\frac{b}{m}\right) = \pm 1$, vidimo da je $b^{m-1} \equiv 1 \pmod{m}$, što znači da je m pseudoprost broj u bazi b. □

Znamo da je svaki Eulerov pseudoprost broj i pseudoprost broj. Sada ćemo pokazati i da je svaki jaki pseudoprost broj Eulerov pseudoprost broj.

Teorem 12 (vidjeti [6, Theorem 9.8.]). *Ako je m jaki pseudoprost broj u bazi b, tada je m Eulerov pseudoprost broj u toj bazi.*

Dokaz. Neka je m jaki pseudoprosti broj u bazi b. Tada, ako je $m - 1 = 2^s \cdot t$, gdje je t neparan, vrijedi ili $b^t \equiv 1 \pmod{m}$ ili $b^{2^r \cdot t} \equiv -1 \pmod{m}$ za neki r s $0 \leq r \leq s-1$. Neka je $m = \prod_{i=1}^{k} p_i^{e_i}$ faktorizacija broja m na proste faktore.

Prvo razmotrimo slučaj kada je $b^t \equiv 1 \pmod{m}$. Neka je p prost djelitelj od m. Označimo s d red od b modulo p. Budući da $b^t \equiv 1 \pmod{p}$, znamo da d dijeli t. S obzirom da je t neparan, zaključujemo da je d također neparan. Prema tome, $d \mid \frac{p-1}{2}$, jer je d neparan djelitelj parnog broja $p-1$. Dakle,

$$b^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Prema Eulerovom kriteriju, zaključujemo da je $\left(\frac{b}{p}\right) \equiv 1$.

Za izračun Jacobijevog simbola $\left(\frac{b}{m}\right)$, uočavamo da za sve proste djelitelje p_i od m vrijedi $\left(\frac{b}{p_i}\right) = 1$. Dakle,

$$\left(\frac{b}{m}\right) = \left(\frac{b}{\prod_{i=1}^{k} {p_i}^{e_i}}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{e_i} = 1.$$

Budući da je $b^t \equiv 1 \pmod{m}$, slijedi da je $b^{m-1} = \left(b^t\right)^{2^s} \equiv 1 \pmod{m}$, što znači da je m Eulerov pseudoprost broj u bazi b.

Razmotrimo sada slučaj kada je $b^{2^r \cdot t} \equiv -1 \pmod{m}$ za neki r, gdje je $0 \leq r \leq s-1$. Ako je p prost djelitelj od m, tada je $b^{2^r \cdot t} \equiv -1 \pmod{p}$. Kvadriranjem obje strane te kongruencije dobivamo:

$$b^{2^{r+1} \cdot t} \equiv 1 \pmod{p}.$$

To implicira da $d \mid 2^{r+1} \cdot t$, ali i $d \nmid 2^r \cdot t$, gdje je d red od b modulo p. Dakle, $d = 2^{r+1} \cdot c$, gdje je c neparan broj. Budući da $d \mid p-1$ i $2^{r+1} \mid d$, slijedi da $2^{r+1} \mid p-1$. Tada je $p = 2^{r+1} \cdot l + 1$ za neki cijeli broj l. Budući da je $b^{\frac{d}{2}} \equiv -1 \pmod{p}$, imamo:

$$\left(\frac{b}{p}\right) \equiv b^{\frac{p-1}{2}} = b^{\frac{d}{2} \cdot \frac{p-1}{d}} \equiv (-1)^{\frac{p-1}{d}} = (-1)^{\frac{p-1}{2^{r+1}c}} \pmod{p}.$$

Kako je c neparan, znamo da je $(-1)^c = -1$. Stoga je:

$$\left(\frac{b}{p}\right) = (-1)^{\frac{p-1}{2^{r+1}}} = (-1)^l, \tag{4.4}$$

jer je $l = \frac{p-1}{2^{r+1}}$. Budući da svaki prost djelitelj p_i od m ima oblik $p_i = 2^{r+1}l_i + 1$, slijedi:

$$m = \prod_{i=1}^{k} p_i^{e_i} = \prod_{i=1}^{k} (2^{r+1}l_i + 1)^{e_i} \equiv \prod_{i=1}^{k} (1 + 2^{r+1}e_i l_i) \equiv 1 + 2^{r+1} \sum_{i=1}^{k} e_i l_i \pmod{2^{2r+2}}.$$

Dakle,

$$t \cdot 2^{s-1} = \frac{m-1}{2} \equiv 2^r \sum_{i=1}^{k} e_i l_i \pmod{2^{r+1}}.$$

Iz prethodne kongruencije slijedi:

$$t \cdot 2^{s-1-r} \equiv \sum_{i=1}^{k} e_i l_i \pmod{2}$$

i

$$b^{\frac{m-1}{2}} = (b^{2^r t})^{2^{s-1-r}} \equiv (-1)^{2^{s-1-r}} = (-1)^{\sum_{i=1}^{k} e_i l_i} \pmod{m}. \tag{4.5}$$

S druge strane, iz (4.4) imamo:

$$\left(\frac{b}{m}\right) = \prod_{i=1}^{k} \left(\frac{b}{p_i}\right)^{e_i} = \prod_{i=1}^{k} ((-1)^{l_i})^{e_i} = \prod_{i=1}^{k} (-1)^{e_i l_i} = (-1)^{\sum_{i=1}^{k} e_i l_i}.$$

Kombiniranjem prethodne jednakosti s (4.5) dobivamo:

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

iz čega zaključujemo da je m Eulerov pseudoprost broj u bazi b. □

Iako smo pokazali da je svaki jaki pseudoprost broj u bazi b Eulerov pseudoprost broj u toj bazi, obrat općenito ne vrijedi, odnosno svaki Eulerov pseudoprost broj u bazi b nije jaki pseudoprost broj u istoj bazi. To ćemo pokazati sljedećim primjerom.

Primjer 19. *U Primjeru 18 pokazali smo da je* 561 *Eulerov pseudoprost broj u bazi* 2*, ali sada ćemo pokazati da* 561 *nije jaki pseudoprost broj u istoj bazi. Da bismo to pokazali koristimo definiciju jakog pseudoprostog broja koja nam kaže da je broj m je jaki pseudoprost broj u bazi b ako je m neparan, složen broj te $m-1 = 2^s \cdot t$, gdje je t neparan, i zadovoljava jedan od sljedećih uvjeta:*

1. $b^t \equiv 1 \pmod{m}$, *ili*
2. *Postoji* r, $0 \leq r < s$, *takav da je* $b^{2^r \cdot t} \equiv -1 \pmod{m}$.

Za broj 561 *imamo:* $561 - 1 = 560 = 2^4 \cdot 35$, *dakle* $s = 4$ *i* $t = 35$. *Provjerimo sada uvjete iz definicije:*

1. *Vrijedi:* $2^{35} \not\equiv 1 \pmod{561}$. *Dakle, prvi uvjet iz definicije nije ispunjen.*
2. *Sada provjeravamo postoji li* r *takav da je* $0 \leq r < 4$ *i* $2^{2^r \cdot 35} \equiv -1 \pmod{561}$*:*
   - *Za* $r = 0$*:*
   $$2^{2^0 \cdot 35} \equiv 2^{35} \pmod{561} \not\equiv -1 \pmod{561}.$$
   - *Za* $r = 1$*:*
   $$2^{2^1 \cdot 35} \equiv 2^{70} \pmod{561} \not\equiv -1 \pmod{561}.$$
   - *Za* $r = 2$*:*
   $$2^{2^2 \cdot 35} \equiv 2^{140} \pmod{561} \not\equiv -1 \pmod{561}.$$
   - *Za* $r = 3$*:*
   $$2^{2^3 \cdot 35} \equiv 2^{280} \pmod{561} \not\equiv -1 \pmod{561}.$$

Budući da niti jedan od uvjeta nije ispunjen, broj 561 *nije jaki pseudoprost broj u bazi* 2.

Iako Eulerov pseudoprost broj u bazi b nije uvijek jaki pseudoprost broj u toj bazi, to će biti ako su ispunjeni dodatni uvjeti koje ćemo navesti u sljedeća dva teorema.

Teorem 13 (vidjeti [6, Theorem 9.9.])**.** *Ako je* $m \equiv 3 \pmod{4}$ *i* m *je Eulerov pseudoprost broj u bazi* b*, tada je* m *jaki pseudoprost broj u bazi* b*.*

Dokaz. Iz kongruencije $m \equiv 3 \pmod{4}$, znamo da je $m - 1 = 2^2 \cdot t$, gdje je $t = \frac{m-1}{2}$ neparan. Budući da je m Eulerov pseudoprost broj u bazi b, slijedi da:

$$b^t \equiv b^{\frac{m-1}{2}} = \left(\frac{b}{m}\right) \pmod{m}.$$

Ako je $\left(\frac{b}{m}\right) = \pm 1$, tada znamo da je $b^t \equiv 1 \pmod{m}$ ili $b^t \equiv -1 \pmod{m}$. Dakle, jedna od kongruencija u definiciji jakog pseudoprostog broja u bazi b mora biti zadovoljena. Stoga, m je jaki pseudoprost broj u bazi b. □

Teorem 14 (vidjeti [6, Theorem 9.10.])**.** *Ako je* m *Eulerov pseudoprost broj u bazi* b *i ako vrijedi* $\left(\frac{b}{m}\right) = -1$*, tada je* m *jaki pseudoprost broj u bazi* b*.*

Dokaz. Neka je $m-1 = 2^s \cdot t$, gdje je t neparan, a s je pozitivan cijeli broj. Budući da je m Eulerov pseudoprost broj u bazi b, imamo:

$$b^{2^{s-1}t} = b^{\frac{m-1}{2}} \equiv \left(\frac{b}{m}\right) \pmod{m}.$$

Ali s obzirom da vrijedi $\left(\frac{b}{m}\right) = -1$, vidimo da je:

$$b^{2^{s-1}t} \equiv -1 \pmod{m}.$$

Ovo je jedna od kongruencija u definiciji jakog pseudoprostog broja u bazi b. Budući da je m složen, on je jaki pseudoprost broj u bazi b. □

Prethodno navedene i dokazane tvrdnje imaju svoju primjenu u testovima prostosti. Jedan od njih je Solovay-Strassenov test koji identificira Eulerove pseudoproste brojeve.

Literatura

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

[2] G. A. Jones, J. M. Jones, *Elementary Number Theory*, Springer-Verlag, London, 2004.

[3] M. Jukić Bokun, I. Soldo, *Zbirka zadataka iz teorije brojeva*, Fakultet primijenjene matematike i informatike, Osijek, 2023.

[4] I. Matić, *Uvod u teoriju brojeva*, Odjel za matematiku, Sveučilište J. J. Strossmayera u Osijeku, Osijek, 2015.

[5] R. A. Mollin, *Fundamental Number Theory with Applications*, CRC Press, New York, 2008.

[6] K. H. Rosen, *Elementary Number Theory and Its Applications*, Addison-Wesley, Reading, 1993.

Sažetak

U ovom radu definirani su kvadratni ostatci i navedene neke korisne tvrdnje vezane uz njih. Uveden je pojam Legendreovog simbola te su pokazana njegova osnovna svojstva i primjene. Iskazan je i dokazan Gaussov kvadratni zakon reciprociteta te je pokazana njegova primjena u Pepinovom testu prostosti. Definiran je Jacobijev simbol i pokazana su njegova osnovna svojstva. Naveden je algoritam za izračunavanje Jacobijevog simbola te je dokazano da i za njega vrijedi Zakon kvadratnog reciprociteta. Na kraju su definirani Eulerovi pseudoprosti brojevi te su iskazani i dokazani rezultati koji se koriste u testovima prostosti.

Ključne riječi

kvadratni ostatci, Legendreov simbol, Jacobijev simbol, pseudoprosti brojevi, testovi prostosti

Quadratic Residues

Summary

In this paper, quadratic residues are defined and some useful statements related to them are presented. The concept of the Legendre symbol is introduced, along with its basic properties and applications. Gauss's quadratic reciprocity law is stated and its application in Pepin's primality test is demonstrated. The Jacobi symbol is defined and its basic properties are shown. An algorithm for calculating the Jacobi symbol is provided and it is proven that the Law of Quadratic Reciprocity also applies to it. Finally, Euler's pseudoprimes are defined and results used in primality tests are stated and proven.

Keywords

quadratic residues, Legendre symbol, Jacobi symbol, pseudoprimes, primality tests

Životopis

Rođena sam 7. kolovoza 1998. godine u Našicama. Pohađala sam Osnovnu školu kralja Tomislava u Našicama. Nakon završetka osnovne škole, upisala sam Srednju školu Isidora Kršnjavog u Našicama, smjer Opća gimnazija. Nakon završetka srednje škole, 2017. godine upisujem preddiplomski studij matematike na Odjelu za matematiku u Osijeku, odnosno današnjem Fakultetu primijenjene matematike i informatike. Preddiplomski studij završavam 2021. godine s temom završnog rada "Mjere zavisnosti - svojstva i zamke" pod mentorstvom izv. prof. dr. sc. Nenada Šuvak. Te godine upisujem i diplomski studij matematike, smjer Financijska matematika i statistika, na istom fakultetu. Tijekom zadnje godine studija odradila sam stručnu praksu u tvrtki Prvo plinarsko društvo d.o.o. u Vukovaru, gdje sam stekla i prvo radno iskustvo. Trenutno sam zaposlena na radnom mjestu učiteljice matematike i informatike u Osnovnoj školi Voćin.