Kvadratni zakon reciprociteta

Mink, Katarina

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Katarina Mink

Kvadratni zakon reciprociteta

Završni rad

Osijek, 2021.

Sveučilište J. J. Strossmayera u Osijeku
Odjel za matematiku

Katarina Mink

Kvadratni zakon reciprociteta

Završni rad

Voditelj: doc. dr. sc. Mirela Jukić Bokun

Osijek, 2021.

Sažetak: U ovom radu proučavamo kvadratni zakon reciprociteta. Prvo se upoznajemo s pojmovima koji će nam trebati, kao što su kongruencije, kvadratni ostatci i Legendreov simbol. Zatim iskazujemo kvadratni zakon reciprociteta i dokazujemo ga na dva načina, pomoću Gaussove leme i na temelju množenja elemenata koji imaju određena svojstva. Na kraju proučavamo primjene kvadratnog zakona reciprociteta u dokazivanju tvrdnji o prostim brojevima i u Fermatovom teoremu o sumi dva kvadrata.

Ključne riječi: kongruencije, kvadratni ostatci, kvadratni zakon reciprociteta, Fermatov teorem o sumi dva kvadrata

Quadratic reciprocity law

Abstract: In this paper we study quadratic reciprocity law. First we introduce terms we will need, such as congruences, square residues and the Legendre symbol. Then we express the quadratic reciprocity law and prove it in two ways, using the Gaussian lemma and using the multiplication of elements with specific properties. Finally, we study the applications of the quadratic reciprocity law in proving claims about prime numbers and in Fermat's two square theorem.

Key words: congruence, quadratic residues, quadratic reciprocity law, Fermmat's two square theorem

Sadržaj

Uvod

Teorija brojeva je grana matematike koja se bavi pročavanjem svojstava skupa prirodnih brojeva i jedna je od najstarijih grana matematike. Njemački matematičar Carl Friedrich Gauss rekao je: "Matematika je kraljica svih znanosti, a teorija brojeva je kraljica matematike".
Jedan od najvažnijih rezultata teorije brojeva je kvadratni zakon reciprociteta. Do prvih zaključaka o ovom teoremu došli su Euler i Legendre, ali prvi koji je iskazao i dokazao kvadratni zakon reciprociteta je Gauss u svom djelu "Disquisitiones Arithmeticae", 1801. godine. Gauss ga je nazivao još i "zlatnim teoremom". Objavio je šest dokaza kvadratnog zakona reciprociteta, a još dva dokaza su poslije njegove smrti pronađena među njegovim radovima. Do sada je objavljeno preko 240 dokaza ovog teorema. Poopćenje kvadratnog zakona reciprociteta bilo je ključno za razvoj moderne algebre, moderne teorije brojeva i još mnogih grana matematike.

U prvom poglavlju ovog rada uvest ćemo neke osnovne tvrdnje kao što su kongruencije, kvadratni ostatci i Legendreov simbol, te ćemo iskazati teoreme koji će nam bit važni za razumijevanje kvadratnog zakona reciprociteta. U drugom poglavlju iskazat ćemo i objasniti kvadratni zakon reciprociteta te izvesti dva dokaza. U trećem poglavlju vidjet ćemo neke od primjena kvadratnog zakona reciprociteta. Mi ćemo ga koristiti pri dokazivanju nekih rezultata o prostim brojevima i o sumi dva kvadrata.

1. Osnovne tvrdnje

Uvedimo pojmove koji su nam potrebni za razumijevanje kvadratnog zakona reciprociteta.

1.1. Kongruencije

Prvo ćemo se prisjetiti definicije kongruencije, nekih svojstava kongruencija te ostalih tvrdnji koje će nam biti korisne u nastavku. Dokazi ovih tvrdnji mogu se naći u [2].

Definicija 1.1. *Neka je $n \in \mathbb{N}$ i neka su $a, b \in \mathbb{Z}$. Ako n dijeli razliku $a - b$ tada kažemo da je a kongruentno b modulo n (a i b su kongruentni modulo n) te pišemo $a \equiv b \pmod{n}$.*

Primijetimo da je a djeljivo s n ako i samo ako vrijedi $a \equiv 0 \pmod{n}$. Isto tako, ako je $c \in \mathbb{N}$ i $a \equiv b \pmod{n}$, tada je i $ac \equiv bc \pmod{nc}$.

Primjer 1.1. *Lako se vidi da vrijedi* $13 \equiv 5 \pmod{8}$ *i* $5 \equiv 5 \pmod{8}$,
$10 \equiv 2 \pmod{8}$ *i* $20 \equiv 4 \pmod{16}$, *a* $16 \equiv 0 \pmod{8}$.

Pogledajmo sada tvrdnje vezane uz potpune i reducirane sustave ostataka, pri čemu ćemo uvesti i pojam Eulerove funkcije.

Definicija 1.2. *Skup $S = \{a_1, a_2, \ldots, a_n\}$ naziva se potpuni sustav ostataka modulo n ako za svaki $b \in \mathbb{Z}$ postoji točno jedan $a_i \in S$, $i = 1, \ldots, n$ za koji vrijedi $b \equiv a_i \pmod{n}$.*

Zbog ilustracije, navedimo nekoliko primjera potpunih sustava ostataka modulo 4: $\{0, 1, 2, 3\}$, $\{1, 2, 3, 4\}$, $\{-1, 0, 1, 2\}$, itd.
Vidimo da ih postoji beskonačno mnogo, a to nam govori i idući teorem.

Teorem 1.1. *Neka je $\{a_1, a_2, \ldots, a_n\}$ potpuni sustav ostataka modulo n, te neka je $(b, n) = 1$, $b \in \mathbb{Z}$. Tada je i $S = \{ba_1, ba_2, \ldots, ba_n\}$ potpuni sustav ostataka modulo n.*

Definicija 1.3. *Skup $S = \{a_1, a_2, \ldots, a_n\}$ naziva se reducirani sustav ostataka modulo n ako za svaki $b \in \mathbb{Z}$, $(b, n) = 1$ postoji točno jedan $a_i \in S$, $i = 1, \ldots, n$ za koji vrijedi $b \equiv a_i \pmod{n}$.*

Definicija 1.4. *Neka je $n \in \mathbb{N}$. Broj prirodnih brojeva u nizu $1, 2, 3, \ldots, n$ koji su relativno prosti s n označavamo s $\varphi(n)$. Time je definirana funckija $\varphi : \mathbb{N} \to \mathbb{N}$ koja se naziva Eulerova funkcija. Primijetimo da je $\varphi(n)$ ujedno i broj elemenata reduciranog sustava ostataka modulo n.*

Teorem 1.2. *Neka je $\{a_1, a_2, \ldots, a_{\varphi(n)}\}$ reducirani sustav ostataka modulo n, te neka je $(b, n) = 1$, $b \in \mathbb{Z}$. Tada je i $S = \{ba_1, ba_2, \ldots, ba_{\varphi(n)}\}$ reducirani sustav ostataka modulo n.*

Teorem 1.3 (Mali Fermatov teorem)**.** *Neka je p prost broj i a cijeli broj. Tada je $a^p \equiv a \pmod{p}$. Ako p ne dijeli a vrijedi i $a^{p-1} \equiv 1 \pmod{p}$.*

Teorem 1.4 (Wilsonov teorem)**.** *Ako je p prost broj, onda je $(p-1)! \equiv -1 \pmod{p}$.*

1.2. Kvadratni ostatci i Legendreov simbol

Sada pogledajmo posjeduje li cijeli broj a kvadratni korijen modulo n i pogledajmo što je Legendreov simbol.

Definicija 1.5. *Neka su $a \in \mathbb{Z}$ i $n \in \mathbb{N}$, $(a,n) = 1$. Ako kongruencija $x^2 \equiv a \pmod{n}$ ima rješenja, tada kažemo da je a kvadratni ostatak modulo n. U suprotnom, kažemo da je a kvadratni neostatak modulo n.*

Primjer 1.2. *Prirodni brojevi 1, 2 i 4 su kvadratni ostatci modulo 7, a prirodni brojevi 3, 5 i 6 su kvadratni neostatci modulo 7.*

Teorem 1.5. *Neka je p neparan prost broj. Reducirani sustav ostataka modulo p sastoji se od $\frac{p-1}{2}$ kvadratnih ostataka i $\frac{p-1}{2}$ kvadratnih neostataka.*

Dokaz: Vidi [2].

□

Definicija 1.6. *Neka je p neparan prost broj i a cijeli broj. Legendreov simbol $\left(\frac{a}{p}\right)$ definiran je s*

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

Dakle, broj rješenja kongruencije $x^2 \equiv a \pmod{p}$ je jednak $1 + \left(\frac{a}{p}\right)$.

Primjer 1.3. *Uzmimo iste brojeve kao u prethodnom primjeru i primijetimo:*

$$\begin{aligned} \left(\frac{1}{7}\right) &= \left(\frac{2}{7}\right) = 1, \\ \left(\frac{3}{7}\right) &= \left(\frac{6}{7}\right) = -1, \\ \left(\frac{14}{7}\right) &= 0. \end{aligned}$$

Pogledajmo sada neke tvrdnje i svojstva Legendreova simbola.

Teorem 1.6 (Eulerov kriterij)**.** *Neka je p neparan prost broj. Tada vrijedi*

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

Prema tome, a je kvadratni ostatak modulo p ako i samo ako je $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Dokaz: Ako je $\left(\frac{a}{p}\right) = 0$ onda po definiciji Legendreova simbola $p \mid a$, pa je tvrdnja očito zadovoljena.
Ako je $\left(\frac{a}{p}\right) = 1$ onda po definiciji Legendreova simbola i kvadratnog ostatka postoji $b \in \mathbb{Z}$ takav da je $b^2 \equiv a \pmod{p}$. Sada iz Malog Fermatovog teorema (Teorem 1.3) slijedi

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

Preostaje još pogledati slučaj kada je $\left(\frac{a}{p}\right) = -1$. Za svaki $i \in \{1, \ldots, p-1\}$ odaberimo $j \in \{1, \ldots, p-1\}$ tako da vrijedi $ij \equiv a \pmod{p}$. To je moguće po Teoremu 1.2. Primijetimo da je $i \neq j$ jer kongruencija $x^2 \equiv a \pmod{p}$ nema rješenja. Dakle, skup $\{1, \ldots, p-1\}$ se sastoji od $\frac{p-1}{2}$ parova (i, j) za koje vrijedi $ij \equiv a \pmod{p}$. Množenjem ovih $\frac{p-1}{2}$ kongruencija te koristeći Wilsonov teorem (Teorem 1.4) dobivamo

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

□

Iduća svojstva većinom proizlaze iz Eulerova kriterija.

Propozicija 1.1. *Neka je p neparan broj i $a, b \in \mathbb{Z}$. Tada vrijedi:*
1) Ako je $a \equiv b \pmod{p}$, onda je $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.
2) $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3) Ako je $(a, p) = 1$, onda je $\left(\frac{a^2}{p}\right) = 1$.
4) $\left(\frac{1}{p}\right) = 1, \qquad \left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$.

Dokaz: 1) Ako je $a \equiv b \pmod{p}$, onda je $a^{\frac{p-1}{2}} \equiv b^{\frac{p-1}{2}} \pmod{p}$ pa je prema Eulerovom kriteriju $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$
2) Iz

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

slijedi $\left(\frac{ab}{p}\right) = \left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3) Kongruencija $x^2 \equiv a^2 \pmod{p}$ očito ima rješenje $x = a$.
4) Prva tvrdnja je specijalni slučaj od 3), dok druga slijedi uvrštavanjem $a = -1$ u Eulerov kriterij.

□

Korolar 1.1. *Za neparan prost broj p vrijedi*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \text{ako je } p \equiv 1 \pmod{4}, \\ -1, & \text{ako je } p \equiv 3 \pmod{4} \end{cases}$$

Dokaz: Tvrdnja slijedi primjenom Propozicije 1.1 (4).
Ako je $p = 4k + 1$, za neki $k \in \mathbb{Z}$, tada

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{4k+1-1}{2}} = (-1)^{2k} = 1$$

Ako je $p = 4k + 3$, za neki $k \in \mathbb{Z}$, tada

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{4k+3-1}{2}} = (-1)^{2k+1} = -1$$

□

2. Kvadratni zakon reciprociteta

Kvadratni zakon reciprociteta može se smatrati ključnim teoremom u teoriji brojeva, slično kao što Pitagorin teorem možemo smatrati temeljnim rezultatom u geometriji. Zbog toga je do danas konstruirano mnogo različitih dokaza, a mi ćemo ovdje izvesti dva. Prije nego što krenemo s dokazima, iskazat ćemo teorem na nekoliko načina.

2.1. Iskaz

Teorem 2.1 (Kvadratni zakon reciprociteta)**.** *Neka su p i q različiti neparni prosti brojevi. Tada vrijedi*

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

Drugim riječima, ako su p i q oblika $4k+3$, onda jedna od kongruencija $x^2 \equiv p \pmod{q}$, $x^2 \equiv q \pmod{p}$ ima rješenja, a druga nema. Ako barem jedan od brojeva p i q ima oblik $4k+1$, onda ili obje ove kongruencije imaju rješenja ili obje nemaju rješenja.

U nekoj literaturi kvadratni zakon reciprociteta iskazan je na sljedeći način:
Neka su p i q različiti neparni prosti brojevi. Tada vrijedi

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

Iz ovakvog zapisa bolje se uočava veza između kvadratnog ostataka modulo p i kvadratnog ostataka modulo q koja se čini čudesna:
$\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$, osim u slučaju kada $p \equiv q \equiv 3 \pmod{4}$, a tada vrijedi $\left(\frac{q}{p}\right) = -\left(\frac{p}{q}\right)$.

Ne postoji očiti razlog zašto bi činjenica da je p kvadratni ostatak modulo q utjecala na to je li q kvadratni ostatak modulo p, ali zapravo jedno određuje drugo. Zbog toga što ne postoji očiti razlog ove relacije, ne postoji ni jednostavan direktan dokaz.

2.2. Prvi dokaz

Iskažimo i dokažimo prvo neke tvrdnje koje ćemo koristiti u prvom dokazu.

Lema 2.1 (Gaussova lema)**.** *Neka je p neparan prost broj i $(a,p) = 1$. Pogledajmo brojeve $a, 2a, 3a, \ldots, \frac{p-1}{2}a$, te njihove najmanje nenegativne ostatke pri dijeljenju s p. Označimo s n broj ostataka koji su veći od $\frac{p}{2}$. Tada je $\left(\frac{a}{p}\right) = (-1)^n$.*

Dokaz: Neka su $r_1, r_2, \ldots, r_n$ ostatci koji su veći od $\frac{p}{2}$, a $s_1, s_2, \ldots, s_k$, $k \in \mathbb{N}$ preostali ostatci. Po Teoremu 1.1 brojevi $r_1, r_2, \ldots, r_n, s_1, s_2, \ldots, s_k$ su međusobno različiti i niti jedan od njih nije jednak nuli. Nadalje, $n + k = \frac{p-1}{2}$.
Brojevi $p - r_i$, $i = 1, \ldots, n$ su međusobno različiti i $0 < p - r_i < \frac{p}{2}$.
Sada pretpostavimo da je $p - r_i = s_j$, $j = 1, \ldots, k$. Tada je $r_i \equiv \alpha a \pmod{p}$ i $s_j \equiv \beta a \pmod{p}$ za neke $1 \leq \alpha, \beta \leq \frac{p-1}{2}$, pa iz $a(\alpha + \beta) \equiv 0 \pmod{p}$ i $(a,p) = 1$ slijedi da je $\alpha + \beta \equiv 0 \pmod{p}$. To je nemoguće jer je $2 \leq \alpha + \beta \leq p - 1$. Došli smo do kontradikcije pa

slijedi da niti jedan $p - r_i$ nije jednak nekom s_j.
Prema tome, brojevi $p - r_1, p - r_2, \ldots, p - r_n, s_1, s_2, \ldots, s_k$ su svi međusobno različiti, ima ih $\frac{p-1}{2}$ i elementi su skupa $\{1, 2, \ldots, \frac{p-1}{2}\}$. Stoga su to upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Množeći ih dobivamo

$$(p - r_1)(p - r_2) \cdots (p - r_n)s_1 s_2 \cdots s_k = 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right).$$

Odavde je

$$\begin{aligned} 1 \cdot 2 \cdots \left(\frac{p-1}{2}\right) &\equiv (-r_1)(-r_2) \cdots (-r_n)s_1 s_2 \cdots s_k \\ &\equiv (-1)^n r_1 r_2 \cdots r_n s_1 s_2 \cdots s_k \\ &\equiv (-1)^n a \cdot 2a \cdots \left(\frac{p-1}{2}\right) a \pmod{p}. \end{aligned}$$

Skratimo ovu kongruenciju s $\left(\frac{p-1}{2}\right)!$ i dobivamo $1 \equiv (-1)^n a^{\frac{p-1}{2}} \pmod{p}$, pa je po Eulerovom kriteriju (Teorem 1.6)

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

□

Teorem 2.2. *Neka je p neparan prost broj i $(a, 2p) = 1$. Tada je $\left(\frac{a}{p}\right) = (-1)^t$, gdje je*

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

Također vrijedi $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, tj. broj 2 je kvadratni ostatak modulo p ako i samo ako je p oblika $8k \pm 1$.

Dokaz: Koristit ćemo iste oznake kao u dokazu prošlog teorema. Neka su opet r_i i s_i ostatci pri dijeljenju brojeva ja s $p, j = 1, 2, \ldots, \frac{p-1}{2}$. Kvocijenti pri tom dijeljenju su brojevi $\left\lfloor \frac{ja}{p} \right\rfloor$. Ako je sada $(a, p) = 1$, onda imamo

$$\sum_{j=1}^{\frac{p-1}{2}} ja = \sum_{j=1}^{\frac{p-1}{2}} p \left\lfloor \frac{ja}{p} \right\rfloor + \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i,$$

te

$$\sum_{j=1}^{\frac{p-1}{2}} j = \sum_{i=1}^{n} (p - r_i) + \sum_{i=1}^{k} s_i = np - \sum_{i=1}^{n} r_i + \sum_{i=1}^{k} s_i.$$

Oduzimanjem ova dva izraza dobivamo

$$(a-1) \sum_{j=1}^{\frac{p-1}{2}} j = p \left(\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n \right) + 2 \sum_{i=1}^{n} r_i.$$

Nadalje je

$$\sum_{j=1}^{\frac{p-1}{2}} j = \frac{\frac{p-1}{2}\frac{p+1}{2}}{2} = \frac{p^2-1}{8},$$

pa je

$$(a-1)\frac{p^2-1}{8} \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor - n \pmod 2.$$

Ako je a neparan, tj. $(a, 2p) = 1$, onda odavde dobivamo

$$n \equiv \sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{ja}{p} \right\rfloor \pmod 2.$$

Ako je $a = 2$, onda dobivamo

$$n \equiv \frac{p^2-1}{8} \pmod 2,$$

jer je $\left\lfloor \frac{2j}{p} \right\rfloor = 0$ za $j = 1, 2, \ldots, \frac{p-1}{2}$. Sada tvrdnja našeg teorema slijedi iz Gaussove leme.

□

Dokaz kvadratnog zakona reciprociteta: Neka su p, q različiti neparni prosti brojevi i $S = \{(x, y) : x, y \in \mathbb{Z}, 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\}$. Primjetimo da S ima $\frac{p-1}{2}\frac{q-1}{2}$ članova i da je uvijek $qx \neq py$.
Podijelimo sada skup S na njegova dva disjunktna podskupa S_1 i S_2 na temelju toga je li $qx > py$ ili $qx < py$.
Neka je S_1 skup svih parova (x, y) takvih da je $1 \leq x \leq \frac{p-1}{2}$ i $1 \leq y \leq \frac{qx}{p}$. Takvih parova će biti

$$\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor.$$

Analogno, neka je S_2 skup svih parova (x, y) takvih da je $1 \leq x \leq \frac{py}{q}$ i $1 \leq y \leq \frac{q-1}{2}$, a takvih parova će biti

$$\sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor.$$

Primjetimo da je tada

$$\sum_{j=1}^{\frac{p-1}{2}} \left\lfloor \frac{qj}{p} \right\rfloor + \sum_{j=1}^{\frac{q-1}{2}} \left\lfloor \frac{pj}{q} \right\rfloor = \frac{p-1}{2}\frac{q-1}{2}.$$

Tada po Teoremu 2.2 vrijedi

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

□

2.3. Drugi dokaz

Izvedimo još jedan dokaz kvadratnog zakona reciprociteta. Ovaj dokaz temelji se na množenju elemenata koji imaju multiplikativni inverz modulo produkt dva različita prosta broja. Opet ćemo prvo iskazati i dokazati tvrdnje koje ćemo korisititi u ovom dokazu.

Lema 2.2. *Neka su p i q međusobno različiti prosti brojevi. Tada je*

$$\prod_{\substack{1\leq x\leq \frac{pq-1}{2},\\ x\ invertibilam\ modulo\ pq}} x \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p},$$

$$\prod_{\substack{1\leq x\leq \frac{pq-1}{2},\\ x\ invertibilam\ modulo\ pq}} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}.$$

Dokaz: Pogledajmo invertibilne elemente modulo pq, a to su oni elementi koji nisu djeljivi niti s p niti s q. Skup invertibilnih elemenata x koji se nalaze u $\{1, 2, \ldots, \frac{pq-1}{2}\}$, promatran modulo p, sastoji se od $\frac{q-1}{2}$ nizova $1, 2, \ldots, p-1$ i niza $1, 2, \ldots, \frac{p-1}{2}$. Još samo trebamo isključiti niz koji se sastoji od višekratnika broja q, $2q, 3q, \ldots, \frac{p-1}{2}q$.
Uočimo sada da smo dobili

$$\prod_{\substack{1\leq x\leq \frac{pq-1}{2},\\ x\ \text{invertibilam modulo pq}}} x \equiv (p-1)!^{\frac{q-1}{2}} \left(\frac{p-1}{2}\right)! \Big/ q^{\frac{p-1}{2}} \left(\frac{p-1}{2}\right)! \pmod{p}.$$

Pokratimo $\left(\frac{p-1}{2}\right)!$, prema Wilsonovom teoremu znamo $(p-1)! \equiv -1 \pmod{p}$ i prema Eulerovom kriteriju $q^{\frac{p-1}{2}} \equiv \left(\frac{q}{p}\right) \pmod{p}$ te dobijemo:

$$\prod_{\substack{1\leq x\leq \frac{pq-1}{2},\\ x\ \text{invertibilam modulo pq}}} x \equiv (-1)^{\frac{q-1}{2}} \left(\frac{q}{p}\right) \pmod{p}.$$

Analogno dobijemo i

$$\prod_{\substack{1\leq x\leq \frac{pq-1}{2},\\ x\ \text{invertibilam modulo pq}}} x \equiv (-1)^{\frac{p-1}{2}} \left(\frac{p}{q}\right) \pmod{q}.$$

□

Dokaz kvadratnog zakona reciprociteta: Prikažimo prvo produkte

$$\prod_{\substack{1\leq x\leq \frac{pq-1}{2},\\ x\ \text{invertibilam modulo pq}}} x \pmod{p} \qquad \text{i} \qquad \prod_{\substack{1\leq x\leq \frac{pq-1}{2},\\ x\ \text{invertibilam modulo pq}}} x \pmod{q}$$

iz Leme 2.2 isključivo pomoću potencija od -1.
Uočimo da se za svaki $x \in \{1, 2, \ldots, pq-1\}$ točno jedan element skupa $\{x, -x\} \pmod{pq}$ pojavljuje u nizu $1, 2, \ldots, \frac{pq-1}{2}$. Sada uočimo da se među odgovarajućim uređenim parovima ostataka $(a, b) = (x \bmod p, x \bmod q)$ pojavljuje točno jedan od parova $(a, b), (-a, -b)$. Točno po jedan od svakog mogućeg para ostataka $(\bmod p, \bmod q)$ dobivamo uzimajući $1 \leq a \leq p-1$

i $1 \leq b \leq \frac{q-1}{2}$.
Svaki $a \in \{1, 2, \ldots, p-1\}$ se pojavljuje u točno $\frac{q-1}{2}$ parova, dok se svaki $b \in \{1, 2, \ldots, \frac{q-1}{2}\}$ pojavljuje u točno $p-1$ parova. Dobivamo

$$\prod_{\substack{1 \leq x \leq \frac{pq-1}{2}, \\ x \text{ invertibilam modulo pq}}} (x, x) \equiv \pm \left((p-1)!^{\frac{q-1}{2}}, \left(\frac{q-1}{2} \right)!^{p-1} \right) (\mathrm{mod}\, p, \mathrm{mod}\, q).$$

Sada prikažimo potecije ovih faktorijela kao potencije od -1. To ćemo napraviti pomoću Wilsonova teorema.
Za prvu komponentu imamo: $(p-1)! \equiv -1 \pmod{p}$ pa je

$$(p-1)!^{\frac{q-1}{2}} \equiv (-1)^{\frac{q-1}{2}} \pmod{p}.$$

Kako bi i drugu komponentu prikazali kao potenciju od -1 prvo primjetimo da vrijedi:

$$\begin{aligned} -1 &\equiv (q-1)! \pmod{q} \\ &\equiv 1 \cdot 2 \cdot \ldots \frac{q-1}{2} \cdot \left(-\frac{q-1}{2} \right) \ldots (-2) \cdot (-1) \pmod{q} \\ &\equiv \left(\frac{q-1}{2} \right)!^2 (-1)^{\frac{q-1}{2}} \pmod{q}. \end{aligned}$$

Prema tome je $\left(\frac{q-1}{2}\right)!^2 \equiv (-1)(-1)^{\frac{q-1}{2}} \pmod{q}$.
Potenciranjem dobivamo

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

Kada smo obje komponente prikazali kao potencije od -1 to izgleda ovako:

$$\prod_{\substack{1 \leq x \leq \frac{pq-1}{2}, \\ x \text{ invertibilam modulo pq}}} (x, x) \equiv \pm \left((-1)^{\frac{q-1}{2}}, (-1)^{\frac{p-1}{2}} (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \right) (\mathrm{mod}\, p, \mathrm{mod}\, q).$$

Izjednačavanjem dobivene kongruencije s rezultatom iz Leme 2.2 dolazimo do toga da vrijedi jedno od sljedećeg:

$$\left(\frac{q}{p} \right) = 1 \quad \text{i} \quad \left(\frac{p}{q} \right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}}$$

ili

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

Iz ovoga slijedi

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

□

3. Primjene kvadratnog zakona reciprociteta

Promotrimo zašto je kvadratni zakon reciprociteta tako bitan i gdje se primjenjuje. Osim što nam olakšava računanje Legendreovih simbola i vrlo je koristan u kriptografiji, primjenjujemo ga i u mnogim dokazima.

3.1. Beskonačnost prostih brojeva određenog oblika

Mi ćemo koristiti kvadratni zakon reciprociteta da bi dokazali postojanje beskonačno mnogo prostih brojeva oblika $5k+4$, $8k+3$ i $12k+11$. Naši dokazi će biti slični Euklidovom dokazu o postojanju beskonačno mnogo prostih brojeva pa ćemo prvo pokazati njega i lemu koju ćemo koristiti, a zatim ćemo dokazivati naše tvrdnje.

Teorem 3.1 (Euklidov teorem)**.** *Postoji beskonačno mnogo prostih brojeva.*

Dokaz: Pretpostavimo suprotno, tj. pretpostavimo da prostih brojeva ima konačno mnogo. Označimo ih s $p_1, p_2, \ldots, p_n$, $n \in \mathbb{N}$ i promotrimo broj

$$N = p_1 p_2 \ldots p_n + 1.$$

Broj N je očito veći od 1 pa mora imati prostog djelitelja kojeg ćemo označiti s p. Jer su $p_1, p_2, \ldots, p_n$ svi prosti brojevi, p mora biti $p = p_i$, za neki $i = 1, \ldots, n$. Zato $p \mid p_1 p_2 \ldots p_n$. Iz $p \mid N$ i $p \mid p_1 p_2 \ldots p_n$ slijedi da $p \mid 1$, a to je nemoguće jer niti jedan prost broj ne dijeli 1 i došli smo do kontradikcije pa zaključujemo da prostih brojeva ima beskonačno mnogo.

□

Lema 3.1. *Neka je p prost broj i $(p, 5) = 1$. Tada $\left(\frac{5}{p}\right) = 1$ ako i samo ako $p \equiv 1$ ili $4 \pmod 5$.*

Dokaz: Iz kvadratnog zakona reciprociteta imamo

$$\left(\frac{5}{p}\right) = (-1)^{\frac{p-1}{2}\frac{5-1}{2}} \left(\frac{p}{5}\right) = (-1)^{p-1} \left(\frac{p}{5}\right).$$

Također znamo

$$\left(\frac{p}{5}\right) = \begin{cases} 1, & \text{ako je } p \equiv 1 \text{ ili } 4 \pmod 5, \\ -1, & \text{ako je } p \equiv 2 \text{ ili } 3 \pmod 5. \end{cases}$$

Iz toga slijedi $\left(\frac{5}{p}\right) = 1$ ako i samo ako $p \equiv 1$ ili $4 \pmod 5$.

□

Teorem 3.2. *Postoji beskonačno mnogo prostih brojeva kongruentnih $4 \pmod 5$.*

Dokaz: Pretpostavimo suprotno, tj. pretpostavimo da postoji konačno mnogo prostih brojeva kongruentnih $4 \pmod 5$. Označimo ih s $p_1, p_2, \ldots, p_n$, $n \in \mathbb{N}$ i promotrimo broj

$$N = (2p_1 p_2 \ldots p_n)^2 - 5.$$

Pokažimo prvo da su svi prosti djelitelji broja N kongruentni 1 ili $4 \pmod 5$.
Neka je p bilo koji prost djelitelj broja N. Tada $p \mid (2p_1 p_2 \ldots p_n)^2 - 5$, tj. $(2p_1 p_2 \ldots p_n)^2 \equiv 5$

(mod p). Slijedi da je 5 kvadratni ostatak modulo p. Iz Leme 3.1 slijedi $p \equiv 1$ ili $4 \pmod 5$. Sada pokažimo da N ima prostog djelitelja koji je kongruentan $4 \pmod 5$.
Ako su svi prosti djelitelji od N kongruentni $1 \pmod 5$, tada

$$N \equiv 1 \pmod 5.$$

Također, znamo da $p_i \equiv 4 \pmod 5$ za sve $i = 1, \ldots, n$, pa $p_i^2 \equiv 16 \equiv 1 \pmod 5$. Iz toga slijedi da je $N \equiv 4 \pmod 5$, a to je u kontradikciji s $N \equiv 1 \pmod 5$. Zaključujemo da postoji barem jedan neparan prost broj p koji dijeli N koji je kongruentan $4 \pmod 5$.
Po početnoj pretpostavci, $p_1, p_2, \ldots, p_n$ su svi prosti brojevi kongruentni $4 \pmod 5$. Slijedi da je $p = p_i$, za neki $i = 1, \ldots, n$. Imamo da $p \mid N$ i $p \mid (2p_1p_2 \ldots p_n)^2$ pa slijedi da $p \mid 5$ i došli smo do kontradikcije pa zaključujemo da je prostih brojeva $p \equiv 4 \pmod 5$ beskonačno mnogo.

□

Lema 3.2. *Neka je p neparan prost broj. Tada je -2 kvadratni ostatak modulo p ako i samo ako $p \equiv 1$ ili $3 \pmod 8$.*

Dokaz: Iz svojstava Legendreova simbola i Teorema 2.2 imamo

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

Također znamo

$$(-1)^{\frac{p-1}{2}} = \begin{cases} 1, & \text{ako je } p \equiv 1 \pmod 4, \\ -1, & \text{ako je } p \equiv 3 \pmod 4, \end{cases}$$

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

Slijedi da je $\left(\frac{-2}{p}\right) = 1$ ako i samo ako je $p \equiv 1$ ili $3 \pmod 8$.

□

Teorem 3.3. *Postoji beskonačno mnogo prostih brojeva kongruentnih $3 \pmod 8$.*

Dokaz: Pretpostavimo suprotno, tj. pretpostavimo da postoji konačno mnogo prostih brojeva kongruentnih $3 \pmod 8$. Označimo ih s $p_1, p_2, \ldots, p_n$, $n \in \mathbb{N}$ i promotrimo broj

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

Pokažimo prvo da su svi prosti djelitelji broja N kongruentni 1 ili $3 \pmod 8$.
Neka je p bilo koji prost djelitelj broja N. Tada $p \mid (p_1p_2 \ldots p_n)^2 + 2$, tj. $(p_1p_2 \ldots p_n)^2 \equiv -2 \pmod p$. Slijedi da je -2 kvadratni ostatak modulo p. Iz Leme 3.2 slijedi $p \equiv 1$ ili $3 \pmod 8$.
Sada pokažimo da N ima prostog djelitelja koji je kongruentan $3 \pmod 8$.
Ako su svi prosti djelitelji od N kongruentni $1 \pmod 8$, tada

$$N \equiv 1 \pmod 8.$$

Također, znamo da $p_i \equiv 3 \pmod 8$ za sve $i = 1, \ldots, n$, pa $p_i^2 \equiv 9 \equiv 1 \pmod 8$. Iz toga slijedi da je $N \equiv 3 \pmod 8$, a to je u kontradikciji s $N \equiv 1 \pmod 8$. Zaključujemo da postoji barem jedan neparan prost broj p koji dijeli N i kongruentan je $3 \pmod 8$.
Po početnoj pretpostavci, $p_1, p_2, \ldots, p_n$ su svi prosti brojevi kongruentni $3 \pmod 8$. Slijedi da je $p = p_i$, za neki $i = 1, \ldots, n$. Imamo da $p \mid N$ i $p \mid (p_1p_2 \ldots p_n)^2$ pa slijedi da $p \mid 2$, a to je u kontradikciji s $p \equiv 3 \pmod 8$. Zaključujemo da je prostih brojeva $p \equiv 3 \pmod 8$ beskonačno mnogo.

□

Lema 3.3. *Neka je p neparan prost broj i $(p,3)=1$. Tada $\left(\frac{3}{p}\right)=1$ ako i samo ako $p \equiv 1$ ili 11 (mod 12).*

Dokaz: Iz kvadratnog zakona reciprociteta imamo

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

Također znamo

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

Iz toga slijedi $\left(\frac{3}{p}\right)=1$ ako i samo ako $p \equiv 1$ ili 11 (mod 12).

□

Teorem 3.4. *Postoji beskonačno mnogo prostih brojeva kongruentnih 11 (mod 12).*

Dokaz: Pretpostavimo suprotno, tj. pretpostavimo da postoji konačno mnogo prostih brojeva kongruentnih 11 (mod 12). Označimo ih s $p_1, p_2, \ldots, p_n$, $n \in \mathbb{N}$ i promotrimo broj

$$N = 3(p_1 p_2 \ldots p_n)^2 - 4.$$

Prvo želimo pokazati da su svi prosti djelitelji broja N kongruentni 1 ili 11 (mod 12).
Neka je p bilo koji prost djelitelj broja N. Tada $p \mid 3(p_1p_2\ldots p_n)^2-4$, tj. $3(p_1p_2\ldots p_n)^2 \equiv 4 \pmod p$. Slijedi da je 3 kvadratni ostatak modulo p. Iz Leme 3.3 slijedi $p \equiv 1$ ili 11 (mod 12).
Sada želimo pokazati da N ima prostog djelitelja koji je kongruentan 11 (mod 12).
Ako su svi prosti djelitelji od N kongruentni 1 (mod 12), tada

$$N \equiv 1 \pmod{12}.$$

Također, znamo da $p_i \equiv 11 \pmod{12}$ za sve $i = 1, \ldots, n$, pa $p_i^2 \equiv 1 \pmod{12}$. Iz toga slijedi da je $N \equiv -1 \pmod{12}$, a to je u kontradikciji s $N \equiv 1 \pmod{12}$. Zaključujemo da postoji barem jedan neparan prost broj p koji dijeli N i kongruentan je 11 (mod 12).
Po početnoj pretpostavci, $p_1, p_2, \ldots, p_n$ su svi prosti brojevi kongruentni 11 (mod 12). Slijedi da je $p = p_i$, za neki $i = 1, \ldots, n$. Imamo da $p \mid N$ i $p \mid 3(p_1p_2\ldots p_n)^2$ pa slijedi da $p \mid 4$, a to je u kontradikciji s $p \equiv 11 \pmod{12}$. Zaključujemo da je prostih brojeva $p \equiv 11 \pmod{12}$ beskonačno mnogo.

□

3.2. Fermatov teorem o sumi dva kvadrata

Sada ćemo koristiti kvadratni zakon reciprociteta da bi pokazali neke rezultate o prostim brojevima oblika a^2+2b^2, $a, b \in \mathbb{Z}$. Ovdje nam je posebno zanimljiv Fermatov teorem o sumi dva kvadrata. Fermat je teorem iskazao, ali ga nije uspio dokazati. Euler je prvi matematičar koji je dokazao taj Fermatov teorem, a usput je došao do zaključaka o kvadratnom zakonu reciprociteta kojeg će Gauss kasnije i dokazati. Prvo ćemo iskazati Fermatov teorem i lemu koja će nam biti potrebna u dokazivanju naše tvrdnje.

Lema 3.4. *Za bilo koje $a, b, c, d \in \mathbb{Z}$ vrijedi*

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2 + (ad-bc)^2.$$

Dokaz: Vrijedi sljedeće:

$$\begin{aligned}(ac+bd)^2 + (ad-bc)^2 &= ((ac)^2 + 2(ac)(bd) + (bd)^2) + ((ad)^2 - 2(ad)(bc) + (bc)^2) \\ &= a^2c^2 + 2abcd + b^2d^2 + a^2d^2 - 2abcd + b^2c^2 \\ &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (a^2+b^2)(c^2+d^2).\end{aligned}$$

□

Analogno se pokazuje da vrijedi sljedeća lema koju ćemo koristiti u dokazima.

Lema 3.5. *Za bilo koje $a, b, c, d, n \in \mathbb{Z}$*

$$(a^2+nb^2)(c^2+nd^2) = (ac+nbd)^2 + n(ad-bc)^2.$$

Teorem 3.5 (Fermatov teorem)**.** *Ako je p neparan prost broj i $p \equiv 1 \pmod 4$, tada postoje $a, b \in \mathbb{Z}$ takvi da je $p = a^2+b^2$.*

Dokaz: Prvo nađimo cijele brojeve a, b i pozitivan cijeli broj $k < p$ takav da

$$a^2 + b^2 = kp.$$

Ako je $k = 1$ gotovi smo.
Ako je $k > 1$, tada tražimo cijele brojeve a_1 i b_1 takve da vrijedi

$$a_1^2 + b_1^2 = k_1 p,$$

za neki cijeli broj k_1, $1 \leq k_1 < k$. Ovaj proces mora stati i $p = a_n^2 + b_n^2$ za neke cijele brojeve a_n, b_n.
Dokažimo da postoje brojevi a, b, k koji zadovoljavaju $a^2 + b^2 = kp$.
Iz Korolara 1.1 slijedi da je -1 kvadratni ostatak $\bmod p$. Zato za neki u, $0 \leq u \leq p-1$ imamo

$$p \mid u^2 + 1 \Rightarrow u^2 + 1 = kp,$$

za neki cijeli broj k i $a^2+b^2 = kp$ je zadovoljeno sa $a = u, b = 1$. Jer je $0 \leq u \leq p-1$, slijedi $1 \leq k \leq p-1$.
Ako je $k = 1$ gotovi smo.
Za $k > 1$ pokažimo kako konstruirati a_1, b_1 i k_1 koji zadovoljavaju $a_1^2 + b_1^2 = k_1 p$. Označimo s r i s brojeve

$$a \equiv r \pmod k, \qquad b \equiv s \pmod k, \qquad |r|, |s| \leq \frac{k}{2}.$$

Tada

$$r^2 + s^2 \equiv a^2 + b^2 \equiv 0 \pmod{k}.$$

Dakle, $r^2 + s^2 = k_1 k$ za neki $k_1 \geq 0$. Mi tvrdimo da je tada $k_1 > 0$. Ako nije, tada $r = s = 0$ i $a \equiv b \equiv 0 \pmod{k}$. Jer je $a^2 + b^2 = kp$, to povlači da $k^2 \mid kp$ i $k \mid p$. Ovo je u kontradikciji s $1 \leq k < p$ pa zaključujemo da je $k_1 > 0$.
Iz Leme 3.4 slijedi

$$(r^2 + s^2)(a^2 + b^2) = (ra + sb)^2 + (rb - sa)^2.$$

Kada uvrstimo $r^2 + s^2 = k_1 k$ i $a^2 + b^2 = kp$ slijedi

$$(ra + sb)^2 + (rb - sa)^2 = k_1 k^2 p.$$

Jer je $ra + sb \equiv r^2 + s^2 \equiv 0 \pmod{k}$, $rb - sa \equiv rs - sr \equiv 0 \pmod{k}$, slijedi $k^2 \mid (ra + sb)^2$ i $k^2 \mid (rb - sa)^2$. Dijeljenjem $(ra + sb)^2 + (rb - sa)^2 = k_1 k^2 p$ s k_2 dobijemo

$$\left(\frac{ra + sb}{k}\right)^2 + \left(\frac{rb - sa}{k}\right)^2 = k_1 p.$$

Također,

$$k_1 k = r^2 + s^2 \leq \left(\frac{k}{2}\right)^2 + \left(\frac{k}{2}\right)^2 = \frac{k^2}{2}.$$

Iz toga slijedi $0 < k_1 \leq \frac{k}{2} < k$, a to smo htjeli pokazati.

□

Teorem 3.6. *Neka je p neparan prost broj, $p \equiv 1$ ili $3 \pmod{8}$. Tada postoje $a, b \in \mathbb{Z}$ takvi da je $p = a^2 + 2b^2$.*

Dokaz: Dokaz je sličan dokazu prošlog teorema. Prvo ćemo naći cijele brojeve a, b i pozitivan cijeli broj $k < p$ takav da vrijedi

$$a^2 + 2b^2 = kp.$$

Ako je $k = 1$ gotovi smo.
Ako je $k > 1$, tada tražimo cijele brojeve a_1 i b_1 takve da vrijedi

$$a_1^2 + 2b_1^2 = k_1 p,$$

za neki cijeli broj k_1, $1 \leq k_1 < k$.
Dokažimo da postoje brojevi a, b, k koji zadovoljavaju $a^2 + 2b^2 = kp$.
Po Lemi 3.2 slijedi da je -2 kvadratni ostatak $\pmod{p}$. Zato za neki u, $0 \leq u \leq p - 1$ imamo

$$p \mid u^2 + 2 \Rightarrow u^2 + 2 = kp,$$

za neki cijeli broj k i $a^2 + 2b^2 = kp$ je zadovoljeno sa $a = u, b = 1$. Jer je $0 \leq u \leq p - 1$, slijedi $kp \leq (p-1)^2 + 2 = p^2 - 2p + 3 < p^2$. Imamo $1 \leq k \leq p$.
Ako je $k = 1$ gotovi smo.
Za $k > 1$ pokažimo kako konstruirati a_1, b_1 i k_1 koji zadovoljavaju $a_1^2 + 2b_1^2 = k_1 p$. Označimo s r i s brojeve

$$a \equiv r \pmod{k}, \qquad b \equiv s \pmod{k}, \qquad |r|, |s| \leq \frac{k}{2}.$$

Tada

$$r^2 + 2s^2 \equiv a^2 + 2b^2 \equiv 0 \pmod{k}$$

Dakle, $r^2+2s^2 = k_1 k$ za neki $k_1 \geq 0$. Mi tvrdimo da je tada $k_1 > 0$. Ako nije, tada $r = s = 0$ i $a \equiv b \equiv 0 \pmod{k}$. Jer je $a^2+2b^2 = kp$, to povlači da $k^2 \mid kp$ i $k \mid p$. Ovo je u kontradikciji s $1 \leq k < p$ pa zaključujemo da je $k_1 > 0$.
Iz Leme 3.5 slijedi

$$(r^2 + 2s^2)(a^2 + 2b^2) = (ra + 2sb)^2 + 2(rb - sa)^2.$$

Kada uvrstimo $r^2 + 2s^2 = k_1 k$ i $a^2 + 2b^2 = kp$ slijedi

$$(ra + 2sb)^2 + 2(rb - sa)^2 = k_1 k^2 p.$$

Jer je $ra+2sb \equiv r^2+2s^2 \equiv 0 \pmod{k}$, $rb-sa \equiv rs-sr \equiv 0 \pmod{k}$, slijedi $k^2 \mid (ra+2sb)^2$ i $k^2 \mid (rb - sa)^2$. Dijeljenjem $(ra + 2sb)^2 + 2(rb - sa)^2 = k_1 k^2 p$ s k_2 dobijemo

$$\left(\frac{ra + 2sb}{k}\right)^2 + 2\left(\frac{rb - sa}{k}\right)^2 = k_1 p.$$

Također,

$$k_1 k = r^2 + 2s^2 \leq \left(\frac{k}{2}\right)^2 + 2\left(\frac{k}{2}\right)^2 = \frac{3k^2}{4}.$$

Iz toga slijedi $0 < k_1 < k$, a to smo htjeli pokazati.

□

Literatura

[1] A. Almuteri, *Quadratic reciprocity: Proofs and Applications*, University os Mississippi, Diplomski rad, 2019.
URL: https://egrove.olemiss.edu/cgi/viewcontent.cgi?article=2539&context=etd

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

[3] K. Martin, *An (algebraic) introduction to Number Theory*
URL: http://www2.math.ou.edu/~kmartin/intro-nt/nt.pdf

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

[5] URL: https://mathworld.wolfram.com/QuadraticReciprocityTheorem.html