Kvadratni ostatci i primjene

Rezo, Ana

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

Ana Rezo

Kvadratni ostatci i primjene

Završni rad

Osijek, 2020.

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

Ana Rezo

Kvadratni ostatci i primjene

Završni rad

Mentor: doc. dr. sc. Ivan Soldo

Osijek, 2020.

Sažetak

U ovom završnom radu upoznat ćemo se s kvadratnim ostatcima i nekim njihovim primjenama. U uvodu ćemo definirati kvadratne ostatke i navest ćemo neke primjere. U prvom poglavlju definirat ćemo Legendreov simbol i navest ćemo osnovna svojstva Legendreova simbola koja ćemo primijeniti na primjeru. Upoznat ćemo se i s Eulerovim teoremom. U drugom poglavlju iskazat ćemo i dokazati Gaussovu lemu i kvadratni zakon reciprociteta te ćemo vidjeti primjenu kvadratnog zakona reciprociteta. U trećem poglavlju definirat ćemo Jacobijev simbol te ćemo se susresti sa svojstvima Jacobijeva simbola koja ćemo iskoristiti u primjeru. U posljednjem poglavlju iskazat ćemo i dokazati nekoliko primjena kvadratnih ostataka na rješavanje diofantskih jednadžbi.

Ključne riječi

Kvadratni ostatci, Legendreov simbol, Eulerov teorem, Gaussov (kvadratni) zakon reciprociteta, Jacobijev simbol

Quadratic residues and its applications

Summary

In this final paper we are going to introduce ourselves to quadratic residues and some of its applications. At the beginning, we will define quadratic residues and give some examples. In the first chapter, we will define Legendre's symbol, enlist the basic properties of Legendre's symbol and use those properties on an example. We will be, as well, introduced to Euler's theorem. In the second chapter, we are going to express and prove Gauss's lemma, quadratic law of reciprocity and we will show the usage of quadratic law of reciprocity. In the third chapter, we will define and introduce ourselves to the properties of Jacobi symbol and we'll show the usage of the properties on an example. In the last chapter, we are going to express and prove some of applications of quadratic residues on Diophantine equations.

Key words

Quadratic residues, the Legendre symbol, Euler's theorem, Gauss'(quadratic) reciprocity law, the Jacobi symbol

Sadržaj

Uvod

Za početak definirajmo što su to kvadratni ostatci:

Definicija 1. *Neka je* $(a, n) = 1$. *Ako kongruencija*

$$x^2 \equiv a \pmod{n},\ a \in \mathbb{Z}$$

ima rješenja, onda kažemo da je a kvadratni ostatak modulo n. U suprotnom za a kažemo da je kvadratni neostatak modulo n.

U Definiciji 1 nužan je uvjet $(a, n) = 1$, odnosno samo su u tom slučaju definirani kvadratni ostatci i neostatci. Primjerice, konvergencija $x^2 \equiv 0 \pmod{n}$ uvijek ima rješenja, ali 0 nije niti kvadratni ostatak niti kvadratni neostatak modulo n.

Primjer 1. *Odredimo kvadratne ostatke modulo 11.*

Rješenje:
Imamo:

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

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

Primjetimo kako u Primjeru 1 imamo 5 kvadratnih ostataka i 5 kvadratnih neostataka. To nas dovodi do prvoga teorema:

Teorem 1 (vidjeti [2, Teorem 4.1.])**.** *Neka je p neparni prost broj. Reducirani sustav ostataka modulo p sastoji se od* $\frac{p-1}{2}$ *kvadratnih ostataka i* $\frac{p-1}{2}$ *kvadratnih neostataka.*

Dokaz. Reducirani sustav ostataka modulo p može biti i skup $\{-\frac{p-1}{2}, \ldots, -3, -2, -1, 1, 2, 3, \ldots, \frac{p-1}{2}\}$. Svaki kvadratni ostatak modulo p kongruentan je kvadratu nekog od tih brojeva, odnosno svaki kvadratni ostatak modulo p kongruentan je nekom od brojeva $\{1^2, 2^2, 3^2, \ldots, (\frac{p-1}{2})^2\}$.

Potrebno je još pokazati da su brojevi $\{1, 2, 3, ..., \frac{p-1}{2}\}$ međusobno različiti, odnosno da su ti brojevi međusobno nekongruentni modulo p.
Pretpostavimo da je $m^2 \equiv n^2 \pmod{p}$, za $m, n \in \{1, 2, ..., \frac{p-1}{2}\}$. Tada imamo: $p \mid m^2 - n^2$, tj. $p \mid (m-n)(m+n)$. Tada je $(m-n)(m+n) \equiv 0 \pmod{p}$, pa je $(m-n) \equiv 0 \pmod{p}$ ili $(m+n) \equiv 0 \pmod{p}$, a to je u suprotnosti s pretpostavkama za m i n jer je $0 < m - n < p$ i $0 < m + n < p$. Dakle, $m - n = 0$, tj. $m = n$, što je i trebalo pokazati. □

Primjer 2. *Koristeći Teorem 1, vidimo da prost broj 5 ima 2 kvadratna ostatka i 2 kvadratna neostatka. Kvadratni ostatci modulo 5 su 1 i 4, a kvadratni neostatci modulo 5 su 2 i 3.*

Primjer 3. *Prema Teoremu 1, prost broj 29 ima 14 kvadratnih ostataka i 14 kvadratnih neostataka. Dovoljno je pogledati* $1^2, 2^2, \cdots, \left(\frac{29-1}{2}\right)^2$ *i tako ćemo dobiti sve kvadratne ostatke modulo 29.*

1 Legendreov simbol

U ovom poglavlju definiramo i analiziramo Legendreov simbol. Ime je dobio po francuskom matematičaru Adrien-Marie Legendreu. Zadan nam je neparan prost broj p i cijeli broj a. Dakle:

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

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

Primjer 4. *Neka je $p = 7$. Kvadratni ostatci modulo 7 su 1, 2, 3. Kvadratni neostatci modulo 7 su 3, 5, 6. Prema Definiciji 2 imamo sljedeće:*

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1,$$
$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1,$$
$$\left(\frac{7k}{7}\right) = 0, \ \forall k \in \mathbb{Z}.$$

Iskažimo sada i dokažimo Eulerov teorem:

Teorem 2 (Eulerov teorem, vidjeti [2, Teorem 4.2.])**.** *Za svaki cijeli broj a i neparni prosti broj p vrijedi*

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

Dokaz. Promatrat ćemo 3 slučaja: $\left(\frac{a}{p}\right) = 0$, $\left(\frac{a}{p}\right) = 1$, $\left(\frac{a}{p}\right) = -1$.

- Ako uzmemo prvi slučaj, odnosno $\left(\frac{a}{p}\right) = 0$, onda prema Definiciji 2 imamo da je a djeljiv s p, pa je $a^{\frac{p-1}{2}} \equiv 0 \pmod{p}$ pa je polazna tvrdnja zadovoljena.

- Promatramo drugi slučaj, tj. neka vrijedi $\left(\frac{a}{p}\right) = 1$. Tada postoji $x_0 \in \mathbb{Z}$ sa svojstvom da je $x_0^2 \equiv a \pmod{p}$. Iz Malog Fermatova teorema (vidjeti [5, Theorem 5]) imamo: $a^{\frac{p-1}{2}} \equiv x_0^{p-1} \equiv \left(\frac{a}{p}\right) \pmod{p}$, čime je dokazan i drugi slučaj.

- Neka je sada $\left(\frac{a}{p}\right) = -1$. Tada kongruencija $x^2 \equiv a \pmod{p}$ nema rješenja. Za svaki $i \in \{1, ..., p-1\}$ uzmimo $j \in \{1, ..., p-1\}$ tako da je $i \cdot j \equiv a \pmod{p}$ (to možemo napraviti na jedinstven način koristeći (vidjeti [2, Teorem 3.5]). Primijetimo da je $i \neq j$ jer kongruencija $x^2 \equiv a \pmod{p}$ nema rješenja. Skup $\{1, \ldots, p-1\}$ raspada se na $\frac{p-1}{2}$ parova (i, j). Za te parove (i, j) vrijedi $i \cdot j \equiv a \pmod{p}$. Tada imamo $\frac{p-1}{2}$

kongruencija. Množeći sve te kongruencije te koristeći Wilsonov teorem (vidjeti [5, Theorem 3]), dobivamo:

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

čime smo dokazali i treći slučaj.

□

Dakle, Eulerov teorem kaže da je a kvadratni ostatak modulo p ako i samo ako vrijedi da je $a^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Primjer 5. *Koristeći Eulerov teorem provjerimo je li* 3 *kvadrati ostatak modulo* 17.

Rješenje:

$$\left(\frac{3}{17}\right) \equiv 3^{\frac{17-1}{2}} \equiv 3^8 \pmod{17},$$

$$3^8 \equiv (3^2)^4 \equiv (-8)^4 \equiv 8^2 \cdot 8^2 \equiv (-4)(-4) \equiv 16 \equiv -1 \pmod{17}.$$

Dakle, 3 je kvadratni neostatak modulo 17, tj. kongruencija $x^2 \equiv 3 \pmod{17}$ nema rješenja.

Navedimo sada neka bitna svojstva Legendreova simbola:

Propozicija 1 (vidjeti [2, Propozicija 4.3.])**.** *Za neparan prost broj p i za svaka dva cijela broja a, b, vrijedi sljedeće:*

1) *Ako je* $a \equiv b \pmod{p}$, *onda je* $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.

2) $\left(\frac{a}{p}\right) \cdot \left(\frac{b}{p}\right) = \left(\frac{ab}{p}\right)$.

3) *Ako je* $(a,p) = 1$, *onda je* $\left(\frac{a^2}{p}\right) = 1$.

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

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

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

2) Korištenjem Eulerova kriterija iz Teorema 2 imamo sljedeće:

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

pa, budući da je Legendreov simbol jednak 1, -1 ili 0, slijedi jednakost.

3) Kongruencija $x^2 \equiv a^2 \pmod{p}$ očito ima rješenje $x = a$.

4) $\left(\frac{1}{p}\right) = 1$ je specijalni slučaj svojstva 3).
Dokažimo da je $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$. Koristeći Eulerov kriterij, dobivamo da je $\left(\frac{-1}{p}\right) \equiv (-1)^{\frac{p-1}{2}} \pmod{p}$.
Ako je $p \equiv 1 \pmod 4$, onda je $\frac{p-1}{2}$ paran broj pa je $\left(\frac{-1}{p}\right) = 1$.
Ako je $p \equiv 3 \pmod 4$, onda je $\frac{p-1}{2}$ neparan broj pa je $\left(\frac{-1}{p}\right) = -1$.

5) Koristeći Eulerov kriterij vrijedi da je $\left(\frac{2}{p}\right) \equiv 2^{\frac{p-1}{2}} \pmod{p}$. Prvo ćemo si olakšati dokazivanje ove tvrdnje te ćemo dokazati sljedeće kongruencije:

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

Ako vrijedi $p = 4n+1$, odnosno $p \equiv 1 \pmod 4$, onda imamo:

$$\begin{aligned}
(4n)! &\equiv (1 \cdot 3 \cdots (4n-1))(2 \cdot 4 \cdots 4n) \pmod{p} \\
&\equiv (1 \cdot 3 \cdots (4n-1))(1 \cdot 2 \cdots 2n)2^{2n} \\
&\equiv (1 \cdot 3 \cdots (2n-1))((2n+1)(2n+3) \cdots (4n-1))(1 \cdot 2 \cdots 2n)2^{2n} \\
&\equiv ((-1)(-3) \cdots (-2n+1))(-1)^n((2n+1)(2n+3) \cdots (4n-1))(1 \cdot 2 \cdots 2n)2^{2n} \\
&\equiv (4n(4n-2) \cdots (2n+2))(-1)^n((2n+1)(2n+3) \cdots (4n-1))(1 \cdot 2 \cdots 2n)2^{2n} \\
&\equiv (-1)^n \cdot 2^{2n} \cdot (4n)! \pmod{p}.
\end{aligned}$$

Kako je $p > 4n$, slijedi da je $(p, (4n)!) = 1$. Iz prethodnoga izraza dobivamo:

$$1 \equiv (-1)^n \cdot 2^{2n} \equiv (-1)^{\frac{p-1}{4}} \cdot 2^{\frac{p-1}{2}} \pmod{p}.$$

Odatle je $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod{p}$, za $p \equiv 1 \pmod 4$.
Analogno se dobije i da je $2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p-1}{4}} \pmod{p}$, za $p \equiv 3 \pmod 4$.
Sada treba razmotriti sve mogućnosti:

$p \equiv 1 \pmod 8$: imamo da je $p \equiv 1 \pmod 4$ i $\frac{p-1}{4}$ je paran broj te je $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$;

$p \equiv 3 \pmod 8$: sada imamo $p \equiv 3 \pmod 4$ i $\frac{p+1}{4}$ je neparan broja pa je $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$;

$p \equiv 5 \pmod 8$: u ovom je slučaju $p \equiv 1 \pmod 4$ i $\frac{p-1}{4}$ je neparan broj te je $2^{\frac{p-1}{2}} \equiv -1 \pmod{p}$;

$p \equiv 7 \pmod 8$: ovdje je $p \equiv 3 \pmod 4$ i $\frac{p+1}{4}$ je paran broj pa je $2^{\frac{p-1}{2}} \equiv 1 \pmod{p}$.

Sada iz prethodnih slučajeva direktno slijedi tvrdnja.

□

Primjer 6. *Koristeći svojstva iz Propozicije 1, izračunajmo sljedeće Legendreove simbole:*

a)

$$\begin{aligned}\left(\frac{-18}{5}\right) &= \left(\frac{-1}{5}\right)\left(\frac{18}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right)\left(\frac{9}{5}\right) = \left(\frac{-1}{5}\right)\left(\frac{2}{5}\right)\left(\frac{3^2}{5}\right) \\ &= (-1)^{\frac{5-1}{2}} \cdot (-1)^{\frac{5^2-1}{8}} \cdot 1 = (-1)^2 \cdot (-1)^3 \cdot 1 = -1.\end{aligned}$$

b)

$$\left(\frac{153}{17}\right) = \left(\frac{3^2}{17}\right)\left(\frac{17}{17}\right) = 1 \cdot 0 = 0.$$

c)

$$\left(\frac{486}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{3^2}{23}\right)\left(\frac{27}{23}\right) = \left(\frac{2}{23}\right)\left(\frac{3^2}{23}\right)\left(\frac{2^2}{23}\right) = (-1)^{\frac{23^2-1}{8}} \cdot 1 \cdot 1 = 1.$$

2 Gaussov zakon reciprociteta i primjene

Neka su p i q prosti brojevi. Ako kongruencija $x^2 \equiv p \pmod{q}$ ima rješenja, odnosno ako je p kvadratni ostatak modulo q, onda ne možemo jasno vidjeti je li q kvadratni ostatak modulo p, odnosno da kongruencija $x^2 \equiv q \pmod{p}$ ima rješenja. Rješenje ovoga problema daje nam Gaussov (kvadratni) zakon reciprociteta koji ćemo proučavati u ovom poglavlju. Tvrdnju toga teorema prvi su naslutili Legendre i Euler, no Gauss ga je prvi dokazao. Kako Pitagorin teorem možemo smatrati najvažnijim rezultatom u geometriji, tako i Gaussov zakon reciprociteta možemo smatrati ključnim rezulatatom u teoriji brojeva koji se pojavljuje pri proučavanju kvadratne diofantske jednadžbe. Budući da je to ključan teorem, danas je poznato više od 240 različitih dokaza.

Kako bismo uspješno dokazali Gaussov zakon reciprociteta, potrebna su nam sljedeća dva pomoćna rezultata koja potkrijepljujemo i odgovarajućim dokazima i primjerima.

Teorem 3 (Gaussova lema, vidjeti [2, Teorem 4.4.]). *Neka je p neparan prost broj i neka je $(n,p)=1$. Promotrimo brojeve $n, 2n, 3n, \ldots, \frac{p-1}{2}\cdot n$, te njihove najmanje nenegativne ostatke pri dijeljenju s p. Ako sa m označimo broj ostataka koji su veći od $\frac{p}{2}$, tada je $\left(\frac{n}{p}\right) \equiv (-1)^m \pmod{p}$.*

Dokaz. Označimo s $r_1, \ldots, r_m$ ostatke koji su veći od $\frac{p}{2}$ te sa $s_1, \ldots, s_k$ preostale ostatke. Ti ostatci su međusobno različiti i niti jedan od njih nije jednak nuli. Neka je $m + k = \frac{p-1}{2}$. Brojevi $p - r_i$ međusobno su različiti i vrijedi $0 < p - r_i < \frac{p}{2}$, za $i = 1, \ldots, m$. Također vrijedi da niti jedan $p - r_i$ nije jednak nekom s_j. Kada bi bilo da je $p - r_i = s_j$, onda je $r_i \equiv \alpha n \pmod{p}$, $s_j \equiv \beta n \pmod{p}$, za $1 \leq \alpha, \beta \leq \frac{p-1}{2}$, pa bi iz $n(\alpha+\beta) \equiv 0 \pmod{p}$ i $(n,p)=1$ slijedilo da je $\alpha + \beta \equiv 0 \pmod{p}$, a to je nemoguće jer je $2 \leq \alpha + \beta \leq p-1$. Zato su svi brojevi $p - r_1, \ldots, p - r_m, s_1, \ldots, s_k$ međusobno različiti. Tih brojeva ima $\frac{p-1}{2}$ i oni su elementi skupa $\{1, 2, \ldots, \frac{p-1}{2}\}$. To su upravo brojevi $1, 2, \ldots, \frac{p-1}{2}$ u nekom poretku. Sada množeći dobivamo:

$$(p - r_1) \cdot \ldots \cdot (p - r_m) \cdot s_1 \cdot \ldots \cdot s_k = 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}.$$

Iz prethodnoga je

$$\begin{aligned} 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} &\equiv (-r_1) \cdot \ldots \cdot (-r_m) s_1 \cdot \ldots \cdot s_k \pmod{p} \\ &\equiv (-1)^m r_1 \cdot \ldots \cdot r_m \cdot s_1 \cdot \ldots \cdot s_k \pmod{p} \\ &\equiv (-1)^m n \cdot 2n \cdot 3n \cdot \ldots \cdot \left(\frac{p-1}{2}\right) n \pmod{p} \\ &\equiv (-1)^m \cdot n^{\frac{p-1}{2}} \cdot 1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2} \pmod{p}. \end{aligned}$$

Skraćivanjem kongruencije s $1 \cdot 2 \cdot \ldots \cdot \frac{p-1}{2}$, dobivamo

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

Koristeći sada Eulerov teorem slijedi da je

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

čime je Gaussova lema dokazana. □

Pogledajmo kako Gaussova lema funkcionira na primjeru:

Primjer 7. *Uzmimo* $p = 13$ *i* $n = 5$. *Uočimo da je* $(5, 13) = 1$. *Promatramo brojeve 5, 10, 15, 20, 25, 30 i njihove najmanje nenegativne ostatke modulo 13, a to su 2, 4, 5, 7, 10, 12. Vidimo da imamo 3 ostatka koji su veći od* $\frac{13}{2}$. *Primjenom Gaussove leme dobivamo da je* $\left(\frac{5}{13}\right) \equiv (-1)^3 \equiv -1 \pmod{13}$, *odnosno 5 je kvadratni neostatak modulo 13.*

Teorem 4 (vidjeti [2, Teorem 4.5.]). *Ako je* p *neparan prost broj i* $(a, 2p) = 1$, *onda je* $\left(\frac{a}{p}\right) = (-1)^t$, *gdje je* $t = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor$. *Također vrijedi*

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

tj. broj 2 je kvadratni ostatak modulo p *ako i samo ako je* p *oblika* $8k \pm 1$.

Dokaz. Označimo s n broj ostataka pri dijeljenju brojeva ja sa p koji su veći od $\frac{p}{2}$, $j = 1, \ldots, \frac{p-1}{2}$. Neka su, nadalje, $r_1, \ldots, r_n$ ostatci veći od $\frac{p}{2}$, a $s_1, \ldots, s_k$ ostali ostatci. Brojevi $r_1, \ldots, r_n, s_1, \ldots, s_k$ međusobno su različiti i nijedan od njih nije jednak nuli te je $n+k = \frac{p-1}{2}$. Kvocijenti pri tome dijeljenju su brojevi $\lfloor \frac{ja}{p} \rfloor$. Ako su brojevi a i p relativno prosti, tj. ako je $(a, p) = 1$, imamo:

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

te

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

Sada, oduzimanjem prethodna dva izraza dobivamo

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

Nadalje, imamo da je

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

te je

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

Ako je a neparan broj, tj ako je $(a, 2p) = 1$, onda iz ovoga slijedi da je $n \equiv \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor \pmod 2$.

Ako imamo da je $a = 2$, onda je $n \equiv \frac{p^2-1}{8} \pmod 2$ jer je $\lfloor \frac{2j}{p} \rfloor = 0$ za $j = 1, \ldots, \frac{p-1}{2}$. Sada je, primjenom Gaussove leme, tvrdnja ovoga teorema dokazana. □

Primjer 8. *Neka je* $p = 17$ *i* $a = 5$. *Vrijedi da je* $(5, 34) = 1$. *Koristeći Teorem 4, za* $t = \sum_{j=1}^{\frac{p-1}{2}} \lfloor \frac{ja}{p} \rfloor = \sum_{j=1}^{8} \lfloor \frac{5j}{17} \rfloor = 7$ *dobivamo da je* $\left(\frac{5}{17}\right) = (-1)^7 = -1$. *Također, primjemom Teorema 4 uočimo da je 2 kvadratni ostatak modulo 17 jer je 17 oblika* $8k + 1$, *za* $k = 2$.

Sada navedimo i dokažimo sam Gaussov zakon reciprociteta:

Teorem 5 (Gaussov (kvadratni) zakon reciprociteta, vidjeti [2, Teorem 4.6.])**.** *Neka su p i q različiti neparni prosti brojeva. Tada vrijedi:*

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

Dokaz. Neka je $S = \{(jp, kq) : j, k \in \mathbb{Z}, 1 \leq j \leq \frac{q-1}{2}, 1 \leq k \leq \frac{p-1}{2}\}$. Broj elemenata skupa S je $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Lako se vidi da $jp \neq kq$ za bilo koji $1 \leq j \leq \frac{q-1}{2}$ i $q \leq k \leq \frac{p-1}{2}$. Osim toga, skup S možemo podijeliti na dva disjunktna podskupa 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 $(jp, kq) \in S_1$, onda je $j < \frac{kq}{p}$. Također, $\frac{kq}{p} \leq \frac{(p-1)q}{2p} < \frac{q}{2}$. Stoga, imamo $\lfloor \frac{kq}{p} \rfloor < \frac{q}{2}$, odakle slijedi da je $\lfloor \frac{kq}{p} \rfloor \leq \frac{q-1}{2}$.

Dakle, broj elemenata skupa S_1 je $\sum_{k=1}^{\frac{(p-1)}{2}} \lfloor \frac{kq}{p} \rfloor$. Slično, broj elemenata skupa S_2 je $\sum_{j=1}^{\frac{(q-1)}{2}} \lfloor \frac{jp}{q} \rfloor$.

Prema tome je

$$\sum_{k=1}^{\frac{p-1}{2}} \lfloor \frac{kq}{p} \rfloor + \sum_{j=1}^{\frac{q-1}{2}} \lfloor \frac{jp}{q} \rfloor = \frac{p-1}{2} \cdot \frac{q-1}{2},$$

te je prema Teoremu 4

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

□

Napomena 1. *Uočimo da množenjem izraza*

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

s $\left(\frac{q}{p}\right)$ *dobivamo:*

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

što je vrlo korisno u rješavanju odgovarajućih zadataka.

Pogledajmo sada kako to funkcionira na primjerima:

Primjer 9. *Odredimo* $\left(\frac{54}{67}\right)$.

Rješenje:
Primjenom Gaussovog zakona reciprociteta i Napomene 1 dobivamo sljedeće:

$$\begin{aligned}\left(\frac{54}{67}\right) &= \left(\frac{2}{67}\right)\cdot\left(\frac{27}{67}\right) = \left(\frac{2}{67}\right)\cdot\left(\frac{3}{67}\right)\cdot\left(\frac{3^2}{67}\right) = (-1)^{\frac{67^2-1}{8}}\cdot\left(\frac{3}{67}\right)\cdot 1\\ &= (-1)\cdot\left(\frac{67}{3}\right)\cdot(-1)^{\frac{67-1}{2}\cdot\frac{3-1}{2}} = (-1)\cdot(-1)\cdot\left(\frac{67}{3}\right) = \left(\frac{1}{3}\right) = 1.\end{aligned}$$

Primjer 10 (vidjeti [2, Primjer 4.10.]). *Proste brojeve p i q zovemo brojevi blizanci ako je $q = p+2$. Pokažimo da postoji cijeli broj a takav da $p \mid (a^2 - q)$ ako i samo ako postoji cijeli broj b takav da $q \mid (b^2 - p)$.*

Rješenje:
Uočimo najprije da je jedan od brojeva p, q oblika $4k+1$, a drugi $4k+3$. Vrijedi:

$$\begin{aligned}\exists a \in \mathbb{Z} : p \mid a^2 - q &\iff \exists a \in \mathbb{Z} : a^2 - q \equiv \pmod p \iff \exists a \in \mathbb{Z} : a^2 \equiv q \pmod p\\ &\iff \left(\frac{q}{p}\right) = 1 \iff \left(\frac{p}{q}\right)(-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}} = 1 \iff \left(\frac{p}{q}\right) = 1\\ &\iff \exists b \in \mathbb{Z} : b^2 \equiv p \pmod q \iff \exists b \in \mathbb{Z} : q \mid b^2 - p.\end{aligned}$$

Još jedna primjena Gaussovog zakona reciprociteta je Pepinov test prostosti. Njega koristimo za ispitivanje prostosti Fermatovih brojeva. Fermatovi brojevi su brojevi oblika $F_n = 2^{2^n}+1$, pri čemu je n nenegativan cijeli broj. Prvih nekoliko Fermatovih brojeva su: 3, 5, 17, 257, 65537, 4294967297, 18446744073709551617,... Zanimljivo je da među Fermatovim brojevima ima i prostih i složenih. Jedini do sada poznati prosti Fermatovi brojevi su F_0, F_1, F_2, F_3, F_4.

Kako bismo uspješno dokazali Pepinov test prostosti navedimo još neke pojmove i rezultate:

Definicija 3. *Neka je $(a,n) = 1$. Najmanji prirodan broj d sa svojstvom da je $a^d \equiv 1 \pmod n$ zove se red od a modulo n.*

Primjer 11. *Red od 8 modulo 3 je 2 jer je $8^2 \equiv 64 \equiv 1 \pmod 3$ i 2 je najmanji takav eksponent.*

Sada bez dokaza navedimo i sljedeći rezultat:

Propozicija 2 (vidjeti [4, Proposition 3.1.]). *Ako su $a \in \mathbb{Z}$, $k, n \in \mathbb{N}$ takvi da je $(a,n) = 1$, tada je $a^k \equiv 1 \pmod n$ ako i samo ako red od a modulo n dijeli k.*

Iskažimo sada i dokažimo Pepinov test prostosti:

Teorem 6 (Pepinov test prostosti, vidjeti [4, Theorem 4.8.]). *Fermatov broj* $F_n = 2^{2^n} + 1$, $n \in \mathbb{N}$ *je prost ako i samo ako je*

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Dokaz. Ako je F_n prost broj, onda primjenom Gaussova zakona reciprociteta vrijedi

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

gdje prva jednakost dolazi od $F_n \equiv 1 \pmod 4$ i $F_n \equiv 2 \pmod 3$, a zadnja jednakost slijedi iz Propozicije 1. Primjenom Teorema 2, dobivamo:

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

Koristeći (1) i (2), imamo:

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

čime je nužnost ovoga teorema dokazana.
Obratno, pretpostavimo da vrijedi

$$3^{(F_n-1)/2} \equiv -1 \pmod{F_n}.$$

Kvadrirajući obje strane dobivamo:

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

Ako je p bilo koji prost djelitelj broja F_n, tada je $3^{(F_n-1)/2} \equiv -1 \pmod p$. Ako je a reda 3 modulo p, prema Propoziciji 2 a dijeli $F_n - 1$, pa a dijeli 2^{2^n}. Prema tome, $a = 2^r$, za $0 \leq r \leq 2^n$. Ako je $r = 2^n - s$, gdje je $s > 0$, tada je $3^{(F_n-1)/2} = 3^{2^{2^n-1}} = 3^{2^{r+s+1}} = (3^{2^r})^{2^{s-1}} = 1$, što je kontradikcija s pretpostavkom $3^{(F_n-1)/2} \equiv -1 \pmod p$. Red za $s = 0$ i 3 je 2^{2^n} modulo p. Prema Propoziciji 2, 2^{2^n} dijeli $p - 1$. Stoga, $2^{2^n} \leq p - 1$ iz čega slijedi da je $F_n \leq p$. Dakle, ako je p prost djelitelj od F_n, tada je $F_n = p$. F_n je prost. □

Primjer 12. *Koristeći Pepinov test prostosti pokažimo da je Fermatov broj* $F_3 = 257$ *prost.*

Rješenje:

$$\begin{aligned} 3^{\frac{257-1}{2}} &\equiv 3^{128} \equiv \left(3^6\right)^{21} \cdot 3^2 \equiv (729)^{21} \cdot 3^2 \equiv (215)^{21} \cdot 3^2 \equiv \left(215^4\right)^1 5 \cdot 215 \cdot 3^2 \\ &\equiv (197)^5 \cdot 215 \cdot 3^2 \equiv (197)^4 \cdot 197 \cdot 215 \cdot 3^2 \equiv 4 \cdot 197 \cdot 215 \cdot 3^2 \equiv 1524780 \equiv 256 \\ &\equiv -1 \pmod{257}. \end{aligned}$$

Dakle, 257 je prost broj.

3 Jacobijev simbol

U ovom poglavlju promatramo Jacobijev simbol koji je poopćenje Legendreova simbola. Kod njega parametri ne moraju biti prosti brojevi. Imamo sljedeću definiciju:

Definicija 4. *Neka je Q neparan prirodan broj te neka je $Q = q_1 \cdot q_2 \cdot \ldots \cdot q_n$, pri čemu su q_i prosti neparni brojevi, ne nužno različiti. Tada se za $a \in \mathbb{Z}$ definira Jacobijev simbol $\left(\frac{a}{Q}\right)$ s*

$$\left(\frac{a}{Q}\right) = \prod_{j=1}^{n} \left(\frac{a}{q_j}\right),$$

gdje je $\left(\frac{a}{q_j}\right)$ pripadni Legendreov simbol, za $j = 1, \ldots, n$.

Za Jacobijev simbol vrijedi sljedeće:

1. Jacobijev simbol se podudara s Legendreovim ako je Q prost broj.
2. Ako a i Q nisu relativno prosti brojevi (tj. ako vrijedi $(a, Q) > 1$), onda je $\left(\frac{a}{Q}\right) = 0$. Inače je $\left(\frac{a}{Q}\right) \in \{-1, 1\}$.
3. Ako je a kvadratni ostatak modulo q_j, za svaki $j = 1, \ldots, n$, tada je a i kvadratni ostatak modulo Q, pa je $\left(\frac{a}{Q}\right) = 1$.
4. Obrat tvrdnje 3 ne vrijedi, odnosno $\left(\frac{a}{Q}\right) = 1$ ne znači da je a kvadratni ostatak modulo Q. Primjerice,

   $$\left(\frac{2}{33}\right) = \left(\frac{2}{3}\right) \cdot \left(\frac{2}{11}\right) = (-1)^{\frac{3^2-1}{8}} \cdot (-1)^{\frac{11^2-1}{8}} = 1,$$

   no direktnom provjerom lako se vidi da kongruencija $x^2 \equiv 2 \pmod{33}$ nema rješenja, tj. 2 nije kvadratni ostatak modulo 33.

Može se pokazati da vrijedi sljedeći teorem:

Teorem 7 (vidjeti [2])**.** *$a \in \mathbb{Z}$ je kvadratni ostatak modulo Q ako i samo ako je a kvadratni ostatak modulo q_j, za svaki $j = 1, \ldots, n$, pri čemu je $Q = q_1, \ldots, q_n$.*

Posljedica Teorema 7 je sljedeća:
Ako je $\left(\frac{a}{Q}\right) = -1$, onda je a kvadratni neostatak modulo Q. Dakle, postoji $j \in \{1, \ldots, n\}$ takav da je $\left(\frac{a}{q_j}\right) = -1$, tj. a je kvadratni neostatak modulo q_j pa je a i kvadratni neostatak modulo Q.

Navedimo sada osnovna svojstva Jacobijeva simbola:

Propozicija 3 (Svojstva Jacobijeva simbola, vidjeti [3, Propozicija 4.3.1.])**.** *Neka su $a, b \in \mathbb{Z}$ i neka su Q_1 i Q_2 neparni prirodni brojevi. Tada vrijedi:*

1. $\left(\frac{a}{Q_1Q_2}\right) = \left(\frac{a}{Q_1}\right) \cdot \left(\frac{a}{Q_2}\right)$.

2. $\left(\frac{ab}{Q_1}\right) = \left(\frac{a}{Q_1}\right) \cdot \left(\frac{b}{Q_1}\right)$.

3. *Ako je* $a \equiv b \pmod{Q_1}$, *onda je* $\left(\frac{a}{Q_1}\right) = \left(\frac{b}{Q_1}\right)$.

4. *Ako je* $(a, Q_1) = 1$, *onda je* $\left(\frac{a^2}{Q_1}\right) = \left(\frac{a}{Q_1^2}\right) = 1$.

5. $\left(\frac{-1}{Q_1}\right) = (-1)^{\frac{Q_1-1}{2}}$, $\left(\frac{2}{Q_1}\right) = (-1)^{\frac{Q_1^2-1}{8}}$.

6. *Ako je* $(Q_1, Q_2) = 1$, *tada vrijedi* $\left(\frac{Q_1}{Q_2}\right) = (-1)^{\frac{Q_1-1}{2}\cdot\frac{Q_2-1}{2}} \left(\frac{Q_2}{Q_1}\right)$.

Dokaz. Prva četiri svojstva slijede izravno iz definicije Jacobijeva simbola i Propozicije 1.

5. Imamo:

$$\left(\frac{-1}{Q_1}\right) = \left(\frac{-1}{q_1}\right) \cdot \left(\frac{-1}{q_2}\right) \cdot \ldots \cdot \left(\frac{-1}{q_n}\right) = \prod_{j=1}^{n} \left(\frac{-1}{q_j}\right) = \prod_{j=1}^{n} (-1)^{\frac{q_j-1}{2}} = (-1)^{\sum_{j=1}^{n} \frac{q_j-1}{2}},$$

gdje je $Q_1 = q_1 \cdot \ldots \cdot q_n$, q_i neparni prosti brojevi za $i = 1, \ldots, n$.
Za neparne brojeve a i b vrijedi:

$$\frac{ab-1}{2} - \left(\frac{a-1}{2} + \frac{b-1}{2}\right) = \frac{(a-1)(b-1)}{2} \equiv 0 \pmod{2}$$

jer je $\frac{(a-1)(b-1)}{2}$ paran broj pa je

$$\frac{ab-1}{2} \equiv \frac{a-1}{2} + \frac{b-1}{2} \pmod{2}.$$

Koristeći se prethodnom relacijom, indukcijom se lako dokaže da vrijedi

$$\frac{q_1 q_2 \cdots q_n - 1}{2} = \sum_{j=1}^{n} \frac{q_j - 1}{2} \equiv \frac{1}{2}\left(\prod_{j=1}^{n} q_j - 1\right) \equiv \frac{Q_1 - 1}{2} \pmod{2},$$

pa je $\left(\frac{-1}{Q_1}\right) = (-1)^{\frac{Q_1-1}{2}}$.
Slično, ako imamo neparne brojeve a i b, onda je

$$\frac{a^2b^2-1}{8} - \left(\frac{a^2-1}{8} + \frac{b^2-1}{8}\right) = \frac{(a^2-1)(b^2-1)}{8} \equiv 0 \pmod{2},$$

te je

$$\left(\frac{2}{Q_1}\right) = \left(\frac{2}{q_1}\right) \cdots \left(\frac{2}{q_n}\right) = \prod_{j=1}^{n} \left(\frac{2}{q_j}\right) = (-1)^{\sum_{j=1}^{n} \frac{q_j^2-1}{8}} = (-1)^{\frac{1}{8}(\sum_{j=1}^{n} q_j^2 - 1)} = (-1)^{\frac{Q_1^2-1}{8}}.$$

6. Neka je $Q_1 = p_1 \cdots p_n$, $Q_2 = q_1 \cdots q_m$, gdje su p_i, q_j neparni prosti brojevi, za $i = 1, \ldots n$, $j = 1, \ldots, m$, $p_i \neq q_j$. Tada je

$$\begin{aligned}\left(\frac{Q_1}{Q_2}\right) &= \prod_{j=1}^{m}\left(\frac{Q_1}{q_j}\right) = \prod_{j=1}^{m}\prod_{i=1}^{n}\left(\frac{p_i}{q_j}\right) = \prod_{j=1}^{m}\prod_{i=1}^{n}\left(\frac{q_j}{p_i}\right)(-1)^{\frac{p_i-q}{2}\cdot\frac{q_j-1}{2}} \\ &= \left(\frac{Q_2}{Q_1}\right)(-1)^{\sum_{j=1}^{m}\sum_{i=1}^{n}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2}}.\end{aligned}$$

Ali,

$$\sum_{j=1}^{m}\sum_{i=1}^{n}\frac{p_i-1}{2}\cdot\frac{q_j-1}{2} = \left(\sum_{i=1}^{n}\frac{p_i-1}{2}\right)\left(\sum_{j=1}^{m}\frac{q_j-1}{2}\right) \equiv \frac{Q_1-1}{2}\cdot\frac{Q_2-1}{2} \pmod 2,$$

pa je

$$\left(\frac{Q_1}{Q_2}\right) = \left(\frac{Q_2}{Q_1}\right)(-1)^{\frac{Q_1-1}{2}\cdot\frac{Q_2-1}{2}}.$$

□

U Propoziciji 3 svojstvo 6 poznato je kao *Zakon reciprociteta za Jacobijev simbol.*

Pogledajmo sada kako to funkcionira na primjerima:

Primjer 13. *Izračunajmo sljedeće Jacobijeve simbole:*

a)

$$\begin{aligned}\left(\frac{27}{385}\right) &= \left(\frac{27}{5}\right)\left(\frac{27}{7}\right)\left(\frac{27}{11}\right) = \left(\frac{2}{5}\right)\left(\frac{6}{7}\right)\left(\frac{5}{11}\right) = \left(\frac{2}{5}\right)\left(\frac{2}{7}\right)\left(\frac{3}{7}\right)\left(\frac{5}{11}\right) \\ &= (-1)^{\frac{5^2-1}{8}}(-1)^{\frac{7^2-1}{8}}\left(\frac{7}{3}\right)(-1)^{\frac{7-1}{2}\cdot\frac{3-1}{2}}\left(\frac{11}{5}\right)(-1)^{\frac{11-1}{2}\cdot\frac{5-1}{2}} \\ &= (-1)\left(\frac{7}{3}\right)(-1)\left(\frac{11}{5}\right) = \left(\frac{1}{3}\right)\left(\frac{1}{5}\right) = 1.\end{aligned}$$

b)

$$\begin{aligned}\left(\frac{-20}{273}\right) &= \left(\frac{253}{273}\right) = \left(\frac{11}{3}\right)\left(\frac{23}{3}\right)\left(\frac{11}{7}\right)\left(\frac{23}{7}\right)\left(\frac{11}{13}\right)\left(\frac{23}{13}\right) \\ &= \left(\frac{2}{3}\right)\left(\frac{2}{3}\right)\left(\frac{2^2}{7}\right)\left(\frac{2}{7}\right)\left(\frac{13}{11}\right)(-1)^{\frac{13-1}{2}\cdot\frac{11-1}{2}}\left(\frac{10}{13}\right) \\ &= (-1)^{\frac{3^2-1}{8}}(-1)^{\frac{3^2-1}{8}}\cdot 1\cdot(-1)^{\frac{7^2-1}{8}}\left(\frac{2}{11}\right)\cdot 1\cdot\left(\frac{2}{13}\right)\left(\frac{5}{13}\right) \\ &= (-1)^{\frac{11^2-1}{8}}(-1)^{\frac{13^2-1}{8}}\left(\frac{13}{5}\right)(-1)^{\frac{13-1}{2}\cdot\frac{5-1}{2}} = \left(\frac{3}{5}\right) \\ &= \left(\frac{5}{3}\right)(-1)^{\frac{5-1}{2}\cdot\frac{3-1}{2}} = \left(\frac{2}{3}\right) = (-1)^{\frac{3^2-1}{8}} = -1.\end{aligned}$$

Primjer 14. *Provjerimo je li 14 kvadratni ostatak modulo 65.*

Rješenje:

$$\left(\frac{14}{65}\right) = \left(\frac{14}{5}\right)\left(\frac{14}{13}\right) = \left(\frac{2^2}{5}\right)\left(\frac{1}{13}\right) = 1 \cdot (-1)^{\frac{13-1}{2}} = 1.$$

Da bi 14 bio kvadratni ostatak modulo 65, potrebno je još izračunati i simbole $\left(\frac{14}{5}\right)$ i $\left(\frac{14}{13}\right)$. Dobivamo:

$$\left(\frac{14}{5}\right) = \left(\frac{4}{5}\right) = 1, \quad \left(\frac{14}{13}\right) = \left(\frac{1}{13}\right) = (-1)^{\frac{13-1}{2}} = 1.$$

Dakle, 14 je kvadratni ostatak modulo 5 te je 14 kvadratni ostatak modulo 13. Sada primjenom Teorema 7 vidimo da je 14 kvadratni ostatak modulo 65 ako i samo ako je 14 kvadratni ostatak modulo 5 i modulo 13.

4 Primjena kvadratnih ostataka pri rješavanju diofantskih jednadžbi

U ovom ćemo poglavlju vidjeti neke primjene kvadratnih ostataka pri rješavanju nekih diofantskih jednadžbi. Diofantske jednadžbe dobile su ime po starogrčkom matematičaru Diofantu. Počnimo s definicijom:

Definicija 5. *Neka je f polinom s n varijabli i s cjelobrojnim koeficijentima. Jednadžba oblika*

$$f(x_1, x_2, \ldots, x_n) = 0,$$

čija su rješenja cijeli brojevi naziva se diofantska jednadžba s n nepoznanica $x_1, \ldots, x_n$.

Primjer 15. *Diofantska jednadžba $5x + 3y - 1 = 0$ ima rješenje $x = 2$ i $y = -3$. Jednadžbe takvoga tipa pripadaju klasi linearnih diofantskih jednadžbi. Postoje algoritmi za traženje njihova rješenja kao primjerice Euklidov algoritam (vidjeti [2, Teorem 2.7.]), ali i drugi također ilustrirani u [2].*

Pogledajmo sada neke posebne tipove diofantskih jednadžbi i analizirajmo postojanje njihova rješenja.

Propozicija 4 (vidjeti [3, Propozicija 4.4.1.])**.** *Diofantska jednadžba oblika*

$$x^2 + 3k + 1 = 0 \tag{3}$$

nema rješenja niti za jedan $k \in \mathbb{Z}$.

Dokaz. Pretpostavimo da postoje $x, k \in \mathbb{Z}$ koji zadovoljavaju diofantsku jednadžbu (3). Tada je $x^2 = -3k - 1$, pa za svaki prost broj p vrijedi $x^2 \equiv -3k - 1 \pmod{p}$. Kako vrijedi za svaki prost broj p, posebno za $p = 3$ dobivamo $x^2 \equiv -1 \pmod{3}$. Iz toga nam slijedi da je -1 kvadratni ostatak modulo 3. Ali, Legendreov simbol $\left(\frac{-1}{3}\right)$ jednak je -1 te polazna jednadžba nema rješenja. □

U ovisnosti o cijelom broju k u sljedećem teoremu okarakterizirana je rješivost diofantske jednadžbe $y^2 = x^3 + k$.

Teorem 8 (vidjeti [1, Theorem 9.12.])**.** *Diofantska jednadžba oblika*

$$y^2 = x^3 + k \tag{4}$$

nema rješenja ako je k oblika

$$k = (4n - 1)^3 - 4m^2,$$

gdje su $m, n \in \mathbb{Z}$ takvi da niti jedan prost broj $p \equiv -1 \pmod{4}$ ne dijeli m.

Dokaz. Pretpostavimo da postoji rješenje diofantske jednadžbe (4) Budući da je $k \equiv -1 \pmod 4$, imamo

$$y^2 \equiv x^3 - 1 \pmod 4.$$

Sada je $y^2 \equiv 0 \pmod 4$ ili $y^2 \equiv 1 \pmod 4$ za svaki y, stoga $y^2 \equiv x^3 - 1 \pmod 4$ ne može biti zadovoljeno ako je x paran broj ili ako je $x \equiv -1 \pmod 4$. Dakle, moramo imati $x \equiv 1 \pmod 4$. Neka je sada

$$a = 4n - 1$$

tako da je $k = a^3 - 4m^2$ i zapišimo jednadžbu (4) u obliku

$$y^2 + 4m^2 = x^3 + a^3 = (x + a)(x^2 - ax + a^2). \tag{5}$$

S obzirom da je $x \equiv 1 \pmod 4$ i da je $a \equiv -1 \pmod 4$, imamo

$$x^2 - ax + a^2 \equiv 1 - a + a^2 \equiv -1 \pmod 4.$$

Stoga je $x^2 - ax + a^2$ neparno i iz prethodne kongruencije vidimo da svi njegovi prosti faktori ne mogu biti $\equiv 1 \pmod 4$. Dakle, neki prosti $p \equiv -1 \pmod 4$ dijeli $x^2 - ax + a^2$ i iz (5) vidimo da dijeli i $y^2 + 4m^2$. Drugim riječima,

$$y^2 \equiv -4m^2 \pmod p$$

za neki $p \equiv -1 \pmod 4$.
Po pretpostavci p ne dijeli m pa je $\left(\frac{-4m^2}{p}\right) = \left(\frac{-1}{p}\right) = -1$ u kontradikciji s prethodnom kongruencijom. Ovo nam dokazuje da diofantska jednadžba (4) nema rješenja kada je k oblika $k = (4n-1)^3 - 4m^2$. □

Primjer 16. *Provjerimo ima li diofantska jednadžba $y^2 = x^3 + 11$ rješenje.*

Rješenje:
Uočimo da Teorem 8 možemo iskazati i na sljedeći način: diofantska jednadžba (4) nema rješenja ako je k oblika $k = (4n-1)^3 - 4m^2$, gdje su $m, n \in \mathbb{Z}$ takvi da m nema prostih faktora oblika $4l + 3$. Uočimo da $k = 11$ možemo zapisati u obliku $k = (4 \cdot 1 - 1)^3 - 4 \cdot 2^2$. Dakle, $m = 2$. Vidimo da 2 nema prostih faktora oblika $4l + 3$. Primjenom Teorema 8 dobivamo da zadana diofantska jednadžba nema rješenja.

Pogledajmo sada kada diofantska jednadžba $x^2 + 3y^2 = n$ ima rješenje.

Teorem 9 (vidjeti [3, Teorem 4.4.2.])**.** *Neka je $n \in \mathbb{N}$. Diofantska jednadžba oblika*

$$x^2 + 3y^2 = n \tag{6}$$

ima rješenje ako i samo ako u rastavu broja n na proste faktore svaki prosti faktor oblika $3k - 1$ dolazi s parnom potencijom.

Dokaz. Pretpostavimo najprije da jednadžba (6) ima rješenje te neka n ima prosti faktor p oblika $3k-1$, odnosno neka je $p \equiv 2 \pmod 3$. Budući da p dijeli n, imamo kongruenciju

$$x^2 + 3y^2 \equiv 0 \pmod p,$$

tj.

$$x^2 \equiv -3y^2 \pmod p.$$

Iz prethodnoga nam slijedi da je $-3y^2$ kvadratni ostatak modulo p ili da p dijeli y. Pretpostavimo da je $(p, y) = 1$, tj. p i y su relativno prosti. Tada je $\left(\frac{-3y^2}{p}\right) = 1$. Budući da po definiciji vrijedi da je

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

jer je $\left(\frac{y^2}{p}\right) = 1$, slijedi da je $\left(\frac{-3}{p}\right) = 1$. Koristeći svojstva Propozicije 1 dobivamo:

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

Budući da je $\left(\frac{-3}{p}\right) = 1$, slijedi i da je $(-1)^{\frac{p-1}{2}}\left(\frac{3}{p}\right) = 1$, tj. $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$. Koristeći Gaussov zakon reciprociteta dobivamo

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

Odatle je $\left(\frac{p}{3}\right) = 1$, iz čega je $p \equiv 1 \pmod 3$ što je u suprotnosti s polaznom pretpostavkom. Dakle, p dijeli y, no tada p mora dijeliti i x pa imamo da p^2 dijeli i x^2 i y^2. Dakle, p^2 dijeli i $x^2 + 3y^2 = n$. Podijelimo li ovu jednadžbu s p^2 dobivamo jednadžbu

$$\left(\frac{x}{p}\right)^2 + 3\left(\frac{y}{p}\right)^2 = \frac{n}{p^2}$$

te indukcijom dobivamo da p u rastavu broja n na proste faktore dolazi s parnom potencijom čime je nužnost dokazana.

Za dokazivanje dovoljnosti uočimo da prost broj p možemo zapisati u obliku $p = x^2 + 3y^2$ ako i samo ako je $p = 3$ ili $p \equiv 1 \pmod 3$. Pretpostavimo da je $p = x^2 + 3y^2$ te da je $p > 3$. Očito je $(p, x) = 1$ i $(p, y) = 1$ jer bi inače bilo $x^2 + 3y^2 > p$, te postoji multiplikativni inverz y_1 od y modulo p. Iz kongruencije $x^2 \equiv -3y^2 \pmod p$ je $(xy_1)^2 \equiv -3 \pmod p$. Iz $(xy_1, 3) = 1$ imamo $\left(\frac{-3}{p}\right) = 1$, odnosno $\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}$ (kao u prethodnom dijelu dokaza). Sada, isto kao i prije, korištenjem Gaussovog zakona reciprociteta slijedi $p \equiv 1 \pmod 3$.

Pretpostavimo sada da je p prost broj oblika $3k+1$. Uočimo da je tada -3 kvadratni ostatak modulo p jer je

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

Dakle, postoji $a \in \mathbb{Z}$ takav da vrijedi $a^2 \equiv -3 \pmod p$.

Očito su a i p relativno prosti, tj. $(a, p) = 1$ te za $b = \lfloor\sqrt{p}\rfloor$ vrijedi $(b+1)^2 > p$. Imamo

$(b+1)^2$ parova $(u,v) \in \{0,1,\ldots,b\}$ te postoji $(b+1)^2$ cijelih brojeva oblika $au+v$, za $u,v \in \{0,1,\ldots,b\}$. Od ovoga imamo različite parove (u_1,v_1) i (u_2,v_2) koji zadovoljavaju $au_1+v_1 \equiv au_2+v_2 \pmod{p}$. Možemo pretpostaviti da je $u_1 \geq u_2$. Uzmimo da je $x = u_1-u_2$, a $y = v_1 - v_2$. Dobivamo:

$$x \leq 0, \quad |y| \leq b < \sqrt{p}, \quad ax+y \equiv 0 \pmod{p}.$$

Dakle, postoje $x, y \in \mathbb{Z}$ za koje vrijedi

$$0 < x, y < \sqrt{p}, \quad p \mid a^2x^2 - y^2 = (ax-y)(ax+y).$$

Iz prethodnoga te zbog $a^2+3 \equiv 0 \ (mod\ p)$ i $p \mid 3x^2+y^2$ slijedi

$$p \mid a^2x^2+3x^2-3x^2-y^2 = (a^2+3)x^2 - (3x^2+y^2).$$

Odatle dobivamo da za neki prirodan broj l vrijedi $3x^2+y^2 = lp$. Iz nejednakosti $0 \leq x^2 < p$ i $0 \leq y^2 < p$ dobivamo da je $3x^2+y^2 < 3p^2+p^2 = 4p^2$, te $l \in \{0,1,2,3\}$. Uočimo odmah da $l \neq 0$ jer bi inače bilo $3x^2+y^2 = 0$ iz čega bi slijedilo $x = y = 0$, a to nije moguće zbog $(u_1,v_1) \neq (u_2,v_2)$.
Dakle, $l \in \{1,2,3\}$. Promotrimo sve mogućnosti:

- $l = 1$: dobivamo jednakost $p = 3x^2+y^2$;
- $l = 2$: dobivamo $2p = 3x^2+y^2$, no ta jednakost nije moguća jer slijedi da su x i y iste parnosti te iz toga dobivamo da je $2p$ djeljivo s 4, što je suprotno pretpostavci;
- $l = 3$: imamo $3p = 3x^2+y^2$, a iz te jednakosti nam slijedi da y možemo zapisati u obliku $y = 3y_1$, odakle je $p = x^2+3y_1^2$.

Uzmimo sada n oblika a^2b te neka je b kvadratno slobodan. Koristeći pretpostavku teorema dobivamo da je $b = \prod_{i=1}^{m} p_i$, pri čemu je ili $p_i \equiv 1 \ (mod\ 3)$ ili je $p_i = 3$, za $i = 1,2,\ldots,m$. Tada svaki p_i možemo zapisati u obliku $p_i = x_i^2+3y_i^2$. Također, iz jednakosti

$$(x_i^2+3y_i^2)(x_j^2+3y_j^2) = (x_ix_j+3y_iy_j)^2 + 3(x_iy_j - x_jy_i)^2$$

slijedi $b = x^2+3y^2$. Dakle,

$$n = a^2b = (ax)^2+3(ay)^2$$

čime je teorem dokazan. □

Pogledajmo sada kako to izgleda na konkretnom primjeru prirodnog broja n te ilustrirajmo Teorem 9.

Primjer 17. *Ispitajmo ima li diofantska jednadžba $x^2+3y^2 = 175$ rješenje.*

Rješenje:
Koristeći Teorem 9, vidimo da u rastavu broja $n = 175$ na proste faktore svaki prost faktor oblika $3k - 1$ dolazi s parnom potencijom, tj. $175 = 5^2 \cdot 7$. Dakle, diofantska jednadžba $x^2 + 3y^2 = 175$ ima rješenje. Uočimo da je desna strana jednadžbe djeljiva s 5. Tada i lijeva strana mora biti djeljiva s 5, tj. x^2 mora biti djeljiv s 5 i $3y^2$ mora biti djeljiv s 5. Primijetimo da za $x = 10$ i $y = 5$ imamo rješenje koje zadovoljava zadanu jednadžbu.

Primjer 18. *Ispitajmo ima li diofantska jednadžba $x^2 + 3y^2 = 10$ rješenje.*

Rješenje:
Primijenimo li Teorem 9, vidimo da u rastavu broja $n = 10$ na proste faktore niti jedan prost faktor oblika $3k - 1$ ne dolazi s parnom potencijom. Dakle, diofantska jednadžba $x^2 + 3y^2 = 10$ nema rješenja.

Literatura

[1] T. M. Apostol, *Introduction to analytic number theory*, Springer-Verlag, New York, 1976.

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

[3] I. Matić, *Uvod u teoriju brojeva*, Sveučilište Josipa Jurja Strossmayera u Osijeku, Odjel za matematiku, Osijek, 2015.

[4] R. A. Mollin, *Fundamental number theory with applications*, University of Calgary, Alberta, 2008.

[5] W. Sierpinski, *Elementary theory of numbers*, North Holland, Amsterdam, 1988.