# Kubni i bikvadratni zakoni reciprociteta

**Boban, Ana**

**SVEUČILIŠTE U ZAGREBU**

**PRIRODOSLOVNO–MATEMATIČKI FAKULTET**

**MATEMATIČKI ODSJEK**

Ana Boban

# KUBNI I BIKVADRATNI ZAKONI RECIPROCITETA

Diplomski rad

Voditelj rada:
prof. dr. sc. Andrej Dujella

Zagreb, rujan, 2014.

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

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

Povjerenstvo je rad ocijenilo ocjenom _____.

Potpisi članova povjerenstva:

1. _____
2. _____
3. _____

# Sadržaj

# Uvod

Promatrajući Gaussov dokaz zakona kvadratnog reciprociteta, Jacobi je pretpostavio zakon kubnog reciprociteta, dok je Gauss pretpostavio zakon bikvadratnog reciprociteta. U ovom radu dati ćemo dokaze ovih zakona na temelju Gaussove i Jacobi sume.
U prvom poglavlju definiramo Gaussovu i Jacobi sumu, te navodimo teoreme koji će nam biti potrebni u idućem poglavlju. Definiramo Legendreovom simbol, te krećemo s Gaussovim kvadratnim zakonom reciprociteta.
Drugo poglavlje započinjemo s kubnim reciprocitetom, definimramo Eisensteinov cijeli broj, simbol kubnog ostatka te dolazimo do dokaza kubnog zakona reciprociteta. Zatim dolazimo do bikvadratnog zakona reciprociteta, gdje prvo definiramo Gaussov cijeli broj nakon čega slijedi dokaz bikvadratnog zakona reciprociteta. Poglavlje završavamo sa zakonom racionalnog reciprociteta u kojemu navodimo dokaz zakona racionalnog kvartičnog reciprociteta.

# Poglavlje 1

# Gaussove i Jacobijeve sume

(Kvadratna) Gaussova suma $\sum_{n=0}^{k-1} e^{\frac{2\pi i m n^2}{k}}$ uvedena je 1801. godine. Tu sumu nije lako izračunati, čak ni u posebnom slučaju kada je $m = 1$ i $k$ neparan prirodni broj. Kasnije je D. L. Dirichlet uveo multiplikativni karakter $\chi$ modulo k i sumu $G(\chi) = \sum_{n=0}^{k-1} \chi(n) e^{\frac{2\pi i m n}{k}}$. Ovaj izraz također se naziva Gaussova suma.
Suma koja se sada naziva Jacobijeva suma, je u biti ona koju je Jacobi uveo 1827. godine, $J(\chi, \psi) = \sum_{n \bmod p} \chi(n)\psi(1-n)$, gdje su $\chi$ i $\psi$ multiplikativni karakteri modulo prost $p$. Jacobi je bio svjestan da su Gaussova i Jacobijeva suma povezane slično kao gama i beta funkcije, tj. za $k = p$ i $m = 1$

$$J(\chi, \psi) = \frac{G(\chi) G(\psi)}{G(\chi\psi)},$$

kada je $\chi\psi$ netrivijalni.
Promatrat ćemo Gaussovu sumu nad konačnim prstenom cijelih brojeva $(\bmod k)$ i Gaussovu i Jacobijevu sumu nad općim konačnim poljima $F_q$, gdje je $q$ potencija od prostog broja $p$.

$F_q$ je konačno polje od $q$ elemenata. $F_q^*$ je oznaka za cikličku multiplikativnu grupu reda $q - 1$.

## 1.1 Kvadratni zakon reciprociteta

**Definicija 1.1.1.** *Neka je* nzd $(a, m) = 1$. *Ako kongruencija* $x^2 \equiv a \pmod m$ *ima rješenja, onda kažemo da je a kvadratni ostatak modulo m. U protivnom kažemo da je a kvadratni neostatak modulo m.*

**Definicija 1.1.2.** *Neka je p neparan prost broj. Legendreov simbol* $\left(\frac{a}{p}\right)$ *je jednak 1, ako je a kvadratni ostatak modulo p, -1, ako je a kvadratni neostatak modulo p, a 0, ako* $p \mid a$.

**Teorem 1.1.3.** *(Gaussov kvadratni zakon reciprociteta) Ako su p i q različiti neparni prosti brojevi, onda vrijedi*

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

*Drugim riječima, ako su p i q oba 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.*

*Dokaz.* Za dokaz ovog teorema potreban nam je sljedeći teorem kojeg nećemo dokazivati.

**Teorem 1.1.4.** *Ako je p neparan prost broj i* nzd $(a, 2p) = 1$, onda 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 $8k \pm 1$.

Neka je $S = \left\{(x,y) : x, y, 1 < x < \frac{p-1}{2}, 1 < y < \frac{q-1}{2}\right\}$. Skup $S$ ima $\frac{p-1}{2} \cdot \frac{q-1}{2}$ članova. Podijelimo $S$ na dva disjunktna podskupa $S_1$ i $S_2$ prema tome da li je $qx > py$ ili $qx < py$. Uočimo da ne može biti $qx = py$. Skup $S_1$ je, dakle, skup svih parova $(x, y)$ takvih da je $1 < x < \frac{p-1}{2}$ i $1 < y < \frac{qx}{p}$. Takvih parova ima $\sum_{x=1}^{\frac{p-1}{2}} \left\lfloor \frac{qx}{p} \right\rfloor$. Slično se $S_2$ sastoji od svih parova $(x, y)$ takvih da je $1 < y < \frac{q-1}{2}$ i $1 < x < \frac{py}{q}$, a takvih parova ima $\sum_{y=1}^{\frac{q-1}{2}} \left\lfloor \frac{py}{q} \right\rfloor$. Prema tome je

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

pa je prema prethodno navedenom teoremu

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

□

## 1.2 Gaussove i Jacobijeve sume

**Definicija 1.2.1.** *Multiplikativni karakter* $\chi$ *u* $F_q$ *je preslikavanje iz* $F_q^*$ *u multiplikativnu grupu kompleksnih korijena iz jedinice koje zadovoljava*

$$\chi(ab) = \chi(a)\chi(b) \quad za \quad sve \quad a, b \in F_p^*.$$

*Trivijalan karakter je karakter $\chi$ takav da je $\chi(\alpha) = 1$ za svaki $\alpha \in F_q^*$. Prikladno je proširiti područje definicije karaktera $\chi$ sa $F_q^*$ na $F_q$ postavljanjem $\chi(0) = 1$ ako je $\chi$ trivijalni karakter i $\chi(0) = 0$ ako je $\chi$ netrivijalni karakter. Ovom definicijom imamo*

$$\sum_{\alpha \in F_q} \chi(\alpha) = \begin{cases} \chi, ako\, je & \chi \quad trivijalan \\ 0, ako\, je & \chi \quad netrivijalan. \end{cases}$$

**Definicija 1.2.2.** *Neka je $\chi$ karakter na $F_q$ i neka je $\beta \in F_q$. Tada je Gaussova suma $G_r(\beta, \chi)$ u $F_q$ definirana sa*

$$G_r(\beta, \chi) = \sum_{\alpha \in F_q} \chi(\alpha)\, e(\alpha\beta).$$

**Teorem 1.2.3.** *Neka je $\chi$ netrivijalan karakter u $F_q$ i neka je $\beta \in F_q^*$. Tada je*

$$G_r(\beta, \chi) = \chi(\beta^{-1}) G_r(\chi),$$

*gdje $\beta^{-1}$ označava inverz od $\beta$ u $F_q^*$.*

*Dokaz.* Neka je $\chi^{-1}$ oznaka za inverz od $\chi$, odnosno $\chi^{-1} = \overline{\chi}$. Tada je

$$G_r(\beta, \chi) = \sum_{\alpha} \chi(\alpha)\, e(\alpha\beta) = \chi^{-1}(\beta) \sum_{\alpha} \chi(\alpha\beta)\, e(\alpha\beta)$$

$$= \chi^{-1}(\beta) \sum_{\gamma} \chi(\gamma)\, e(\gamma) = \chi\left(\beta^{-1}\right) G_r(\chi),$$

budući da je $\chi^{-1}(\beta) = \chi\left(\beta^{-1}\right)$. □

**Definicija 1.2.4.** *Neka su $\chi$ i $\psi$ karakteri konačnog polja $F_q$, gdje je $q = p^r$. Jacobijeva suma definirana je s*

$$J_r(\chi, \psi) = \sum_{a} \chi(\alpha)\, \psi(1 - \alpha),$$

*gdje $\alpha$ prolazi kroz elemente od $F_q$.*

*Kako je $\alpha \mapsto 1 - \alpha$ bijekcija na $F_q$, vidimo da Jacobijeva suma ima svojstvo simetrije*

$$J_r(\chi, \psi) = J_r(\psi, \chi).$$

*Zgodno je staviti*

$$K_r(\chi) = \chi(4)\, J_r(\chi, \chi).$$

*Kada je $r = 1$ ispustimo indeks iz $J_r$ i $K_r$.*

**Teorem 1.2.5.** *Neka su $\chi$ i $\psi$ karakteri u $F_q$. Ako je $\chi\psi$ netrivijalno, tada*

$$(a) \quad J_r(\chi,\psi) = \frac{G_r(\chi)G_r(\psi)}{G_r(\chi\psi)},$$

*a ako su $\chi$, $\psi$ i $\chi\psi$ svi netrivijalni tada je*

$$(b) \quad |J_r(\chi,\psi)| = q^{\frac{1}{2}}.$$

*Dokaz.* (a) Prema definiciji od $G_r(\chi)$ slijedi

$$G_r(\chi)\,G_r(\psi) = \sum_{\alpha}\sum_{\beta}\chi(\alpha)\,\psi(\beta)\,e(\alpha+\beta) = \sum_{\gamma} e(\gamma) \sum_{\alpha+\beta=\gamma}\chi(\alpha)\,\psi(\beta)$$

$$\sum_{\alpha+\beta=0}\chi(\alpha)\,\psi(\beta) + \sum_{\gamma\neq 0} e(\gamma)\sum_{\alpha}\chi(\alpha)\,\psi(\gamma-\alpha)$$

$$= \psi(-1)\sum_{\alpha}\chi\psi(\alpha) + \sum_{\gamma\neq 0} e(\gamma)\sum_{\alpha}\chi(\gamma\alpha)\,\psi(\gamma-\gamma\alpha)$$

$$= 0 + J_r(\chi,\psi)\sum_{\gamma\neq 0}\chi\psi(\gamma)\,e(\gamma) = J_r(\chi,\psi)\,G_r(\chi\psi).$$

(b) Prema (a) i Teoremu 1.2.6 (c) slijedi

$$|J_r(\chi,\psi)|\,\frac{|G_r(\chi)|\,|G_r(\psi)|}{|G_r(\chi\psi)|} = \frac{q^{\frac{1}{2}}q^{\frac{1}{2}}}{q^{\frac{1}{2}}} = q^{\frac{1}{2}}.$$

□

**Teorem 1.2.6.** *Neka je $\beta \in F_q^*$ i neka je $\chi$ netrivijalan karakter u $F_q$. Tada je*

$$(a) \quad G_r(\beta,\chi)\,G_r(\beta,\overline{\chi}) = \chi(-1)\,p^r$$

$$(b) \quad \overline{G_r(\beta,\chi)} = \chi(-1)\,G_r(\beta,\overline{\chi})$$

$$(c) \quad |G_r(\beta,\chi)| = p^{\frac{r}{2}}$$

$$(d) \quad G_r(\beta,\chi^p) = G_r(\beta^p,\chi).$$

Dokaz ovog teorema možemo pronaći u knjizi B.C. Berndt, R. J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, poglavlje *Gauss Sums*, Theorem 1.1.4.

**Teorem 1.2.7.** *Neka je $K = Q(\beta)$, gdje je $\beta = exp\left(\frac{2i\pi}{k}\right)$, $k > 2$. Neka je $p$ prost broj, pa pišemo $q = p^r$, gdje je $r \geq 1$ izabran kao najmanji takav da $p^r \equiv 1 \pmod{k}$. Neka je $\chi$ karakter $\chi_p$ na $O_k/P$ reda $k$, za neki prosti ideal $P$ u $O_k$ koji dijeli $pO_k$. Neka su $m$ i $n$ cijeli brojevi takvi da $0 < m, n < k$ i $m + n \neq k$. Ako je $p \equiv 1 \pmod{k}$, tj. $r = 1$ tada je*

$$J(\chi^m, \chi^n)O_k = \prod_{j \in S} P_{j^{-1}},$$

*gdje je $S = \{j : 0 < j < k\}$, $\text{nzd}(j,k) = 1$ i $L(mj) + L(nj) < k$ i $j^{-1}$ označava inverz od $j \pmod{k}$; posebno*

$$K(\chi)O_k = \prod_{\substack{i \leq j < \frac{k}{2} \\ \text{nzd}(j,k) = 1}} P_{j^{-1}}.$$

*Povrh toga, za opći $r$*

$$J_r(\chi^m, \chi^n) \equiv \begin{cases} 0 \pmod{P}, m + n < k \\ (-1)^{q+mf}\binom{nf}{(k-m)f} \pmod{P}, m + n > k \end{cases}$$

*gdje je $f = \frac{q-1}{k}$.*

Dokaz ovog teorema možemo pronaći u knjizi B.C. Berndt, R. J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, poglavlje *Jacobi Sums and Cyclotomic Numbers*, Theorem 2.1.14.

**Teorem 1.2.8.** *Ako je $g$ primitivan korijen modulo prost $p = 3f + 1$, onda je*

$$ind_g 3 \equiv -\frac{s_3}{3} (\text{mod } 3),$$

*gdje je $ind_g 3$ indeks 3 s obzirom na primitivni korijen $g$, a $s_3$ je cijeli broj dan jedinstveno prema*

$$\begin{cases} 4p = r_3^2 + 3s_3^2, \quad r_3 \equiv 1 \,(\,3), \quad s_3 \equiv 0 \,(\,3), \\ 3s_3 \equiv \left(g^{\frac{p-1}{3}} - g^{\frac{2(p-1)}{3}}\right) r_3 \pmod{p}. \end{cases}$$

Dokaz ovog teorema možemo pronaći u knjizi B.C. Berndt, R. J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, poglavlje *Jacobi Sums and Cyclotomic Numbers* Corollary 2.6.9.

**Teorem 1.2.9.** *Imamo*

$$2J(\chi^2, \chi^2) = r_3 + is_3\sqrt{3}$$

*gdje je $\chi$ karakter $(\text{mod } p)$ reda 6 s $\chi(g) = \beta$, $\beta = exp\left(\frac{2i\pi}{6}\right)$, a $r_3$ i $s_3$ su cijeli brojevi, takvi da je*

$$r_3^2 + 3s_3^2 = 4p,$$

$$s_3 \equiv 0 (\text{mod } 3),$$

$$3s_3 \equiv (2g^{\frac{p-1}{3}} + 1) r_3 (\text{mod } p).$$

Dokaz ovog teorema možemo pronaći u knjizi B.C. Berndt, R. J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, poglavlje *Evaluation of Jacobi Sums over* $F_p$, Theorem 3.1.3.

**Teorem 1.2.10.** *Imamo*

$$K(\chi) = a_4 + ib_4,$$

*gdje je* $\chi$ *karakter* (mod $p$) *reda 4 s* $\chi(g) = i$, *a* $a_4$ *i* $b_4$ *cijeli brojevi takvi da*

$$a_4^2 + b_4^2 = p,$$

$$a_4 \equiv -\left(\frac{2}{p}\right) (\text{mod } 4).$$

*Dokaz.* Kako je $\chi(n) \in Z[i]$ za svaki cijeli broj $n$, slijedi $K(\chi) = a_4 + ib_4$, gdje su $a_4$ i $b_4$ cijeli brojevi. Štoviše, prema Teoremu 1.0.3 (b) $a_4$ i $b_4$ zadovoljavaju $a_4^2 + b_4^2 = p$, pa slijedi

$$a_4 + ib_4 \equiv -p \,(\text{mod } 2(1-i)).$$

Tako 8 mora dijeliti

$$|(a_4 + p) + ib_4|^2 = a_4^2 + b_4^2 + p^2 + 2a_4 p = p(p + 1 + 2a_4)$$

i tako

$$a_4 \equiv -\frac{p+1}{2} \equiv -\left(\frac{2}{p}\right) (\text{mod } 4).$$

□

Neka je $p$ prost broj takav da $p \equiv 1 (\text{mod } 6)$. Neka je $g$ primitivni korijen (u oznaci $ind_g$) (mod $p$) i neka je $\chi$ karakter (mod $p$) reda 6 takav da je $\chi(g) = \beta$, gdje je $\beta = e^{\frac{2i\pi}{6}}$. Stavimo $Z = ind_g 2$ tako da je $\chi(4) = \chi(g^{2ind_g 2}) = \chi(g)^{2ind_g 2} = \beta^{2Z}$.

**Lema 1.2.11.** *Vrijedi:*

$$(a) \quad G^3(\chi^2) = pJ(\chi^2, \chi^2),$$

$$(b) \quad G(\chi) = \beta^{-2Z} i^{\frac{(p-1)^2}{4}} p^{\frac{-1}{2}} G^2 \chi^2.$$

Dokaz ove leme možemo pronaći u knjizi B.C. Berndt, R. J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, poglavlje *Determination of Gauss Sums over* $F_p$, Lemma 4.1.1. Neka je $p$ prost broj oblika $kf + 1$, gdje su $k$ i $f$ prirodni brojevi takvi da je $k \geq 2$.

**Korolar 1.2.12.** *Neka je $\chi$ karakter* (mod $p$) *reda k. Neka je q prost broj takav da je $q \neq p$. Tada je*

$$G^q(\chi)\overline{\chi}^q(q)G(\chi^q)(\text{mod } q).$$

*Također vrijedi:*

$$G^{q-1}(\chi) \equiv \overline{\chi}(q)(\text{mod } q), \textit{ako je} \quad q \equiv 1(\text{mod } k),$$
$$G^{q+1}(\chi) \equiv \chi(-q)p(\text{mod } q), \textit{ako je} \quad q \equiv -1(\text{mod } k).$$

Dokaz ovog teorema možemo pronaći u knjizi B.C. Berndt, R. J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, poglavlje *Residuacity*, Lemma 7.0.1 i Corollary 7.0.2.

**Teorem 1.2.13.** $3 \mid b_4$ *je nužan i dovoljan uvjet da -3 bude kvartičan ostatak* (mod $p$).

Jedan od dokaza ovog teorema je dokaz Teorema 2.2.6 u idućem poglavlju.

**Teorem 1.2.14.** *Neka je $p = 4f + 1$ prost broj. 5 je kvartični ostatak* (mod $p$) *ako i samo ako* $5 \mid b_4$.

*Dokaz.* Prema Korolaru 1.0.11 gdje je $q = 5$ i $k = 4$ vidimo da je $\chi(5) = 1$ ako i samo ako je $G^4(\chi) = pK^2(\chi) \equiv 1 \,(\text{mod } 5)$ ili ekvivalentno $p^2K(\chi) \equiv K\overline{\chi} \,(\text{mod } 5)$. Tako, prema Teoremu 1.0.6 i Eulerovom kriteriju, 5 je kvartični ostatak (mod $p$) ako i samo ako

$$\left(\frac{p}{5}\right)(a_4 + ib_4) \equiv a_4 - ib_4 \,(\text{mod } 5)\,,$$

ili

$$\left\{\left(\frac{p}{5}\right) - 1\right\} a_4 \equiv \left\{\left(\frac{p}{5}\right) + 1\right\} b_4 \equiv 0 \,(\text{mod } 5)\,.$$

Kako je $p = a_4^2 + b_4^2$

$$5 \mid a_4 \Rightarrow \textit{5 ne dijeli} \quad b_4 \quad i \quad \left(\frac{p}{5}\right) = \left(\frac{b_4^2}{5}\right) = 1$$

i

$$5 \mid b_4 \Rightarrow \textit{5 ne dijeli} \quad a_4 \quad i \quad \left(\frac{p}{5}\right) = \left(\frac{a_4^2}{5}\right) = 1,$$

pa je $p$ kvartični ostatak (mod $p$) ako i samo ako $5 \mid b_4$. □

# Poglavlje 2

# Zakoni reciprociteta

U ovom poglavlju, koristit ćemo neke od jednostavnijih svojstava Gaussove i Jacobijeve sume kako bismo dokazali zakone kubične i kvartne recipročnosti. Zakon kvartne recipročnosti, poznat je i kao zakon bikvadratne recipročnosti.

## 2.1 Kubni reciprocitet

Eisensteinov cijeli broj je cijeli broj imaginarnog kvadratnog polja $Q(i\sqrt{3}) = Q(e^{\frac{2i\pi}{3}})$.
Prsten Eisensteinovih cijelih brojeva označavamo sa $Z[\omega]$, gdje je $\omega = exp(\frac{2i\pi}{3})$. Poznato je da je $Z[\omega]$ domena jedinstvene faktorizacije. Prije nego navedemo i dokažemo zakon kubične recipročnosti, trebali bi se prisjetiti nekoliko činjenica o Eisensteinovim cijelim brojevima i utvrditi neke definicije.
Jedinice u $Z[\omega]$ su $\pm 1$, $\pm\omega$, $\pm\omega^2$. Norma $N(\alpha)$ elemenata $\alpha \in Z[\omega]$ je $N(\alpha) = \alpha\overline{\alpha}$.
Eisensteinovi prosti brojevi u $Z[\omega]$ sastoje se od pridruženih elemenata racionalnih prostih brojeva $q \equiv 2(\text{mod } 3)$, pridruženih elemenata broja $1-\omega$ i pridruženih elemenata onih elemenata $\alpha \in Z[\omega]$ čija je norma $N(\alpha)$ racionalan prost broj $p \equiv 1(\text{mod } 3)$. Dogovorili smo se da $p$ označava racionalan prost broj $\equiv 1(\text{mod } 3), \pi \in Z[\omega]$ označava bilo koji (Eisensteinov) prost broj, a $q$ označava racionalan prost broj $\equiv 2(\text{mod } 3)$. Primjetimo da je $N(q) = q^2$ i $N(1-\omega) = 3$. Ako su $\alpha, \pi \in Z[\omega]$, gdje je $\pi$ prost broj takav da $\pi \nmid \alpha$, tada imamo analogiju Malog Fermatovog teorema:

$$\alpha^{N(\pi)-1} \equiv 1(\text{mod } \pi). \tag{2.1}$$

Konačno polje $Z[\omega]/\pi$ ima $N(\pi)$ elemenata.

**Propozicija 2.1.1.** *Neka su $\alpha, \pi \in Z[\omega]$, $\pi$ je prost, $N(\pi) \neq 3$ i $\pi \nmid \alpha$. Tada postoji jedinstveni cijeli broj $m$, $0 \leq m \leq 2$, takav da je*

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m(\text{mod } \pi).$$

*Dokaz.* Prvo primjetimo da za sve proste brojeve $\pi \in Z[\omega]$ gdje $N(\pi) \neq 3$ vrijedi $3 \mid (N(\pi) - 1)$. Stoga možemo pisati

$$\alpha^{N(\pi)-1} = (\alpha^{\frac{N(\pi)-1}{3}} - \omega)(\alpha^{\frac{N(\pi)-1}{3}} - \omega^2). \tag{2.2}$$

Prema (2.1) $\pi$ dijeli lijevu stranu od (2.2). Stoga $\pi$ dijeli barem jedan od faktora s desne strane od (2.2). Pretpostavimo da $\pi$ dijeli dva faktora s desne strane od (2.2)

$$\pi \mid (\alpha^{\frac{N(\pi)-1}{3}} - \omega^r), \pi \mid (\alpha^{\frac{N(\pi)-1}{3}} - \omega^s), 0 \leq r < s \leq 2.$$

Tada $\pi \mid \omega^r(1 - \omega^{s-r})$, zato što je $\omega^r$ jedinica, $\pi \mid 1 - \omega^t$ za $t = 1$ ili $t = 2$. Stoga, $N(\pi) \mid N(1 - \omega^t) = 3$ što je nemoguće jer $N(\pi) \neq 1, 3$. □

Sada definiramo simbol kubnog ostatka.

**Definicija 2.1.2.** *Neka je $\pi$ Eisensteinov prost broj takav da $N(\pi) \neq 3$ i neka je $\alpha \in Z[\omega]$. Ako $\pi \mid \alpha$, uzmimo $\left(\frac{\alpha}{\pi}\right)_3 = 0$. Ako $\pi \nmid \alpha$, neka $\left(\frac{\alpha}{\pi}\right)_3$ bude jedinstvena potencija od $\omega$ definirana kao*

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \pmod{\pi}.$$

*(Ova definicija je jednoznačna prema Propoziciji 2.1.1.)*
*Nadalje ako je $\beta = \pi_1 \cdots \pi_n$, gdje je svaki $\pi_j$ $(1 \leq j \leq n)$ prost iz $Z[\omega]$, $N(\pi_j) \neq 3$, definiramo*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\alpha}{\pi_1}\right)_3 \cdots \left(\frac{\alpha}{\pi_n}\right)_3.$$

*Na kraju, ako je $\beta$ jedinica od $Z[\omega]$, definiramo $\left(\frac{\alpha}{\beta}\right)_3 = 1$ za svaki $\alpha \in Z[\omega]$, $\alpha \neq 0$ i definiramo $\left(\frac{0}{\beta}\right)_3 = 0$.*
*Kada je $N(\pi) \neq 3$ lako vidimo $\left(\frac{\alpha}{\pi}\right)_3 = 1$ ako i samo ako je $\alpha$ kubni ostatak* (mod $\pi$). *Posebno, ako je $\pi = q \equiv 2 \pmod 3$ i $n$ je racionalan cijeli broj, takav da $q \nmid n$, onda je $\left(\frac{n}{q}\right)_3 = 1$ jer je svaki takav cijeli $n$ kubni ostatak* (mod $q$).

**Propozicija 2.1.3.** *Neka je $x \in Z, \theta \in Z[\omega]$ i neka je $p$ racionalan prost broj takav da $p \equiv 1 \pmod 3$, tako da je $p = \pi\overline{\pi}$ za Eisensteinov prost broj $\pi$. Tada*
*(a) $x \equiv \alpha^3 \pmod p$ za neki $\alpha \in Z[\omega]$ ako i samo ako $x \equiv a^3 \pmod p$ za neki $a \in Z$.*
*(b) $\theta \equiv \gamma^3 \pmod p$ za neki $\gamma \in Z[\omega]$ ako i samo ako $\theta \equiv \alpha^3 \pmod \pi$ i $\theta \equiv \beta^3 \pmod{\overline{\pi}}$ za neki $\alpha, \beta \in Z[\omega]$.*

*Dokaz.* Iz $N(\pi) = p$ imamo izomorfizam polja

$$Z(\omega)/(\pi) \approx Z/pZ.$$

Dakle, svaki $\alpha \in Z[\omega]$ zadovoljava $\alpha \equiv a (\text{mod } \pi)$ za neki $\alpha \in Z$ i slijedi dio (a).
Za dane $\alpha, \beta \in Z[\omega]$ postoji $\gamma \in Z[\omega]$ takav da je

$$\gamma \equiv a (\text{mod } \pi), \gamma \equiv \beta (\text{mod } \overline{\pi})$$

prema Kineskom teoremu o ostatcima. Tada lako slijedi (b) dio. □

Produktna formula $\left(\frac{\alpha\beta}{\pi}\right)_3 = \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3$, gdje su $\alpha, \beta \in Z[\omega]$ izravno slijedi iz definicije simbola kubnog ostatka. Također, lako slijedi da je $\alpha \equiv \beta (\text{mod } \pi)$, onda je $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$. Stoga je $\left(\frac{\alpha}{\pi}\right)_3$ kubni karakter na polju $Z(\omega)/(\pi)$ od $N(\pi)$ elemenata i možemo pisati $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$.

**Propozicija 2.1.4.** *Neka su $\alpha, \pi \in Z[\omega]$, $\pi$ je prost, $N(\pi) \neq 3$ i $\pi \nmid \alpha$. Tada je $\overline{\chi}_\pi(\alpha) = \chi_{\overline{\pi}}(\overline{\alpha})$.*

*Dokaz.* Budući da je $\alpha^{\frac{N(\pi)-1}{3}} \equiv \chi_\pi(\alpha) (\text{mod } \pi)$ iz kompleksne konjugacije slijedi $\overline{\alpha}^{\frac{N(\pi)-1}{3}} \equiv \overline{\chi}_\pi(\alpha) (\text{mod } \overline{\pi})$. Po definiciji $\chi_{\overline{\pi}}$, $\chi_{\overline{\pi}} \equiv \chi_{\overline{\pi}}(\overline{\alpha}) (\text{mod } \overline{\pi})$. Zadnje dvije kongruencije povlače željeni rezultat. □

**Definicija 2.1.5.** *Neka je $\alpha \in Z[\omega]$. Kažemo da je $\alpha$ primaran ako $\alpha \equiv \pm 1 (\text{mod } 3)$.*

Primjetino da su $\pm 1$ jedine primarne jedinice u $Z[\omega]$. Ako $(1-\omega) \mid \alpha$ u $Z[\omega]$, tada niti jedan od pridruženih elemenata broja $\alpha$ nije primaran. Za bilo koji drugi $\alpha$ u $Z[\omega]$ točno dva pridružena elementa od $\alpha$ su primarna, kao što prikazujemo u Propoziciji 2.1.6.

**Propozicija 2.1.6.** *Neka je $\alpha \in Z[\omega]$ takav da $(1-\omega) \nmid \alpha$. Tada od šest pridruženih elemenata od $\alpha$, točno dva su primarna i razlikuju se samo po predznaku.*

*Dokaz.* Stavimo da je $\alpha = a + b\omega$, gdje su $a, b \in Z$. Kako $(1-\omega) \nmid (a + b\omega)$ slijedi da $a + b$ nije kongruentno $0 (mod 3)$ te konačna tvrdnja slijedi iz tablice, gdje je $\varepsilon = \pm 1$.

| | $\alpha(\mathrm{mod}3)$ | $b(\mathrm{mod}3)$ | $\pm\alpha(\mathrm{mod}3)$ | $\pm\omega\alpha(\mathrm{mod}3)$ | $\pm\omega^2\alpha(\mathrm{mod}3)$ |
|---|---|---|---|---|---|
| (i) | $\varepsilon$ | 0 | $\pm 1$ | $\pm\omega$ | $\pm\omega^2$ |
| (ii) | $\varepsilon$ | $\varepsilon$ | $\pm\omega^2$ | $\pm 1$ | $\pm\omega$ |
| (iii) | 0 | $\varepsilon$ | $\pm\omega$ | $\pm\omega^2$ | $\pm 1$ |

□

**Propozicija 2.1.7.** *Eisensteinov cijeli broj koji nije jedinica je primaran ako i samo ako se može faktorizirati u produkt primarnih Eisensteinovih prostih brojeva.*

*Dokaz.* Neka je $\alpha$ primaran Eisensteinov cijeli broj koji nije jedinica. $Z[\omega]$ je domena jedinstvene faktorizacije, $\alpha = \pi_1 \cdots \pi_k$, gdje je svaki $\pi_i$ $(1 \leq i \leq k)$ Eisensteinov prost broj. Nadalje, kako je $\alpha$ primaran, niti jedan $\pi_i$ nije pridružen element od prostog broja $(1-\omega)$. Stoga, prema Propoziciji 2.1.6. za $i = 1, ..., k$, $\pi_i = \theta_i\lambda_i$, gdje je $\theta_i$ jedinica od $Z[\omega]$ pa je $\theta_1 \cdots \theta_k = \pm\omega^r$ za neki $r = 0, 1, 2$. Stoga je $\alpha = \pm\omega^r\lambda_1 \cdots \lambda_k$. Uzimajući relaciju modulo 3, budući da je $\alpha \equiv \pm 1(\mathrm{mod}\ 3)$ i svaki $\lambda_i \equiv \pm 1(\mathrm{mod}\ 3)$, vidimo da je $\omega^r \equiv \pm 1(\mathrm{mod}\ 3)$. Ali $3 = -\omega^2(1-\omega)^2$, pa mora biti $r = 0$, i to povlači $\alpha = \pm\lambda_1 \cdots \lambda_k$.
Obrnuto, jasno je da je produkt primarnih Eisensteinovih prostih brojeva primaran. □

**Lema 2.1.8.** *Neka je $\pi$ primaran Eisensteinov prost broj, takav da je $N(\pi) = p \equiv 1(\mathrm{mod}$ 3) Tada je*

$$J(\chi_\pi, \chi_\pi) = \begin{cases} -\pi, \pi \equiv 1(\mathrm{mod}\ 3) \\ \pi, \pi \equiv -1(\mathrm{mod}\ 3) \end{cases},$$

*gdje je J oznaka za Jacobijevu sumu.*

*Dokaz.* Stavimo $\chi_\pi = \chi$ i pišemo $J(\chi,\chi) = a + b\omega$. Prema Teoremu 1.2.9. imamo $2J(\chi,\chi) = r_3 + is_3\sqrt{3}$, gdje je $r_3 \equiv 1(\mathrm{mod}\ 3)$ i $s_3 \equiv 0(\mathrm{mod}\ 3)$. Štoviše, kako je $\omega = \frac{-1+i\sqrt{3}}{2}$, lako vidimo da je $a = \frac{r_3+s_3}{2}$ i $b = s_3$. Stoga, imamo $a \equiv 2(\mathrm{mod}\ 3)$ i $b \equiv 0(\mathrm{mod}\ 3)$. Slijedi da je $J(\chi,\chi)$ primarni Einsteinov prost broj, budući da je $N(J(\chi,\chi)) = p$. Stoga,

$$J(\chi,\chi)\overline{J(\chi,\chi)} = p = N(\pi) = \pi\overline{\pi}.$$

Prema Teoremu 1.2.7., $J(\chi,\chi) \equiv 0(\mathrm{mod}\ \pi)$. Stoga je $J(\chi,\chi) = \pm\pi$. Sada tvrdnja leme slijedi iz $J(\chi,\chi) \equiv -1(\mathrm{mod}\ 3)$.
Sada smo spremni iskazati i dokazati kubni zakon reciprociteta. □

**Teorem 2.1.9.** *(Kubni zakon reciprociteta) Neka su $\alpha$ i $\beta$ relativno prosti primarni Eisensteinovi cijeli brojevi. Tada je*

$$\left(\frac{\alpha}{\beta}\right)_3 = \left(\frac{\beta}{\alpha}\right)_3.$$

*Dokaz.* Ako je $\alpha$ jedinica (tako da je $\alpha = \pm 1$), lako je vidljivo da su oba člana kubnog zakona reciprociteta jednaka 1. Prema Propoziciji 2.1.7. i multiplikativnosti simbola kubnog ostatka, dovoljno je dokazati teorem kada su $\alpha$ i $\beta$ relativno prosti primarni Eisensteinovi cijeli brojevi. Dokaz trebamo podijeliti na tri slučaja.
Prvo pretpostavimo da su $\alpha$ i $\beta$ primarni racionalni Eisensteinovi prosti brojevi. Tada, kako su $\alpha$ i $\beta$ relativno prosti,

$$\left(\frac{\alpha}{\beta}\right)_3 = 1 = \left(\frac{\beta}{\alpha}\right)_3$$

po napomeni koja prethodi Propoziciji 2.1.3.
Drugo, pretpostavimo da je $\alpha = q \equiv 2 (\text{mod } 3)$ i $\beta = \pi$ tako da $N(\pi) = p \equiv 1 (\text{mod } 3)$. Prema Lemi 1.2.11. (a) i Lemi 2.1.8. vrijedi

$$G^3(\chi_\pi) = pJ(\chi_\pi, \chi_\pi) = \pm p\pi$$

i zato je

$$G(\chi_\pi)^{q^2-1} = (p\pi)^{\frac{q^2-1}{3}} \equiv \chi_q(p\pi) = \chi_q(\pi) (\text{mod } q),$$

što implicira

$$G(\chi_\pi)^{q^2} \equiv \chi_q(\pi) G(\chi_\pi) (\text{mod } q). \tag{2.3}$$

S druge strane, prema multinomnom teoremu i Teoremu 1.2.3.,

$$G(\chi_\pi)^{q^2} \equiv \sum_n \chi_\pi^{q^2}(n) e^{\frac{2i\pi q^2 n}{p}} = G(q^2, \chi_\pi) = \overline{\chi_\pi}\left(q^2\right) G(\chi_\pi) = \chi_\pi(q)\, G(\chi_\pi) (\text{mod } q) \tag{2.4}$$

Uspoređujući (2.3) i (2.4) pronalazimo

$$\chi_q(\pi) = \chi_\pi(q).$$

Treće, pretpostavimo da je $\alpha = \pi_1$ takav da $N(\pi_1) = p_1 \equiv 1 (\text{mod } 3)$ i $\beta = \pi_2$ takav da $N(\pi_2) = p_2 \equiv 1 (\text{mod } 3)$. Onda je $\pi_1$ također primaran,

$$G\left(\chi_{\overline{\pi_1}}\right)^{p_2-1} = \left(\pm p_1 \overline{\pi_1}\right)^{\frac{p_2-1}{3}} \equiv \chi_{\pi_2}\left(p_1 \overline{\pi_1}\right) (\text{mod } \pi_2)$$

ili

$$G\left(\chi_{\overline{\pi_1}}\right)^{p_2} \equiv \chi_{\pi_2}\left(p_1 \overline{\pi_1}\right) G\left(\chi_{\overline{\pi_1}}\right) (\text{mod } \pi_2). \tag{2.5}$$

S druge strane, prema multinomnom teoremu i Teoremu 1.2.3.,

$$G\left(\chi_{\overline{\pi_1}}\right)^{p_2} \equiv \sum_n \chi_{\overline{\pi_1}}^{p_2}(n)\, e^{\frac{2i\pi n p_2}{p_1}} = G\left(p_2, \chi_{\overline{\pi_1}}\right) = \chi_{\overline{\pi_1}}(p_2)\, G\left(\chi_{\overline{\pi_1}}\right) (\text{mod } p_2)\,. \tag{2.6}$$

Iz (2.5) i (2.6) slijedi

$$\chi_{\pi_2}\left(p_1\overline{\pi_1}\right) = \chi_{\overline{\pi_1}}\left(p_2^2\right). \tag{2.7}$$

Sada ponovimo isti argument kao u (2.7), ali umjesto $\overline{\pi}_1$ stavimo $\pi_2$, a umjesto $\pi_2$ stavimo $\overline{\pi}_1$. Umjesto (2.7) dobijemo

$$\chi_{\pi_1}\left(p_2\pi_2\right) = \chi_{\pi_2}\left(p_1^2\right). \tag{2.8}$$

Zatim prema Propoziciji (2.1.4.),

$$\chi_{\pi_1}\left(p_2^2\right) = \overline{\chi_{\pi_1}}\left(p_2^2\right) = \chi_{\pi_1}\left(p_2\right). \tag{2.9}$$

Koristeći (2.7), (2.9) i (2.8) u ovom poretku, dobivamo

$$\chi_{\pi_1}(\pi_2)\chi_{\pi_2}\left(p_1\overline{\pi_1}\right) = \chi_{\pi_1}(\pi_2)\chi_{\overline{\pi_1}}\left(p_2^2\right) = \chi_{\pi_1}(\pi_2)\chi_{\pi_1}(p_2)$$

$$= \chi_{\pi_1}(\pi_2 p_2) = \chi_{\pi_2}\left(p_1^2\right) = \chi_{\pi_2}\left(p_1\pi_1\overline{\pi_1}\right) = \chi_{\pi_2}(\pi_1)\chi_{\pi_2}\left(p_1\overline{\pi_1}\right)$$

Stoga, kraćenjem slijedi

$$\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)\,.$$

□

Kriterij da 2 bude ostatak (mod $p$) može se dobiti pomoću zakona kubnog reciprociteta. Prvo trebamo sljedeći rezultat.

**Propozicija 2.1.10.** *Nek je $\pi$ neracionalan primaran Eisensteinov prost broj. Tada je kongruencija $x^3 \equiv 2(\text{mod } \pi)$ rješiva za $x \in Z[\omega]$ ako i samo ako je $\pi \equiv 1(\text{mod } 2)$.*

*Dokaz.* Prema kubnom zakonu reciprociteta imamo

$$\chi_\pi(2) = \chi_2(\pi). \tag{2.10}$$

Budući da je

$$\pi = \pi^{\frac{N(2)-1}{3}} \equiv \chi_2(\pi)(\text{mod } 2) \tag{2.11}$$

i $x^3 \equiv 2(\text{mod } \pi)$ rješivo ako i samo ako je $\chi_\pi(2) = 1$, rezultat slijedi iz (2.10) i (2.11). □

**Teorem 2.1.11.** *Broj 2 je kubni ostatak* (mod $p$) *ako i samo ako je $r_3$ paran.*

*Dokaz.* Napišimo $p = \pi\overline{\pi}$, gdje je $\pi$ Eisensteinov prost broj. Prema Lemi 2.1.8. možemo uzeti $\pi$ tako da je $\pi = J(\chi_\pi, \chi_\pi)$. Vrijedi da je $2J(\chi_\pi, \chi_\pi) = r_3 + is_3\sqrt{3}$, gdje je $r_3 \equiv 1(\text{mod } 3)$ i $s_3 \equiv 0(\text{mod } 3)$. Stoga, prema Propoziciji 2.1.10., 2 je kubni ostatak (mod $p$) ako i samo ako $\left(\frac{r_3 + is_3\sqrt{3}}{2}\right) \equiv 1(\text{mod } 2)$, odnosno ako i samo ako je

$$\frac{r_3 + s_3}{2} \equiv 1(\text{mod } 2) i s_3 \equiv 0(\text{mod } 6).$$

Po ovim kongruencijama odmah vidimo da je $r_3$ paran ako je 2 kubni ostatak ($mod p$). Obrnuto, ako je $r_3$ paran, tada je $s_3$ paran zbog $4p = r_3^2 + 3s_3^2$, stoga možemo napisati $r_3 = 2r$ i $s_3 = 6s$. Tada,

$$\frac{r_3 + s_3}{2} = r + 3s \equiv r^2 + 3(3s)^2 = p \equiv 1(\text{mod } 2),$$

pa je 2 kubni ostatak (mod $p$). □

Činjenica da je $\left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}}$, gdje je $p$ bilo koji neparan prost broj, naziva se Dopuna zakona kvadratnog reciprociteta jer prost broj 2 nije pokriven kvadratnim zakonom reciprociteta. Na isti način, prosti broj $1 - \omega$ nije pokriven zakonom kubnog reciprociteta. U sljedećem teoremu dokazujemo dopunu kubnog zakona reciprocoteta.

**Teorem 2.1.12.** *(Dopuna kubnog zakona reciprociteta) Neka je $\pi$ primaran Eisensteinov proct broj takav da je (bez gubitka općenitosti) $\pi \equiv -1(\text{mod } 3)$. Ako je $\pi = q$, za racionalan prost broj $q$, pišemo $m = \frac{q+1}{3}$. Ako je $N(\pi) = p \equiv 1(\text{mod } 3)$ pišemo $\pi = a + b\omega$, $(a, b \in Z)$ i $m = \frac{a+1}{3}$. Tada je*

$$\chi_\pi(1 - \omega) = \omega^{2m}.$$

*Dokaz.* Budući da je $(1 - \omega^2) = -3\omega$, dovoljno je pokazati da je $\chi_\pi(-3\omega) = \omega^m$. U slučaju $\pi = q$, to slijedi zbog

$$\chi_q(-3\omega) = \chi_q(\omega) = \omega^{\frac{N(q)-1}{3}} = \omega^{\frac{q^2-1}{3}} = \omega^m.$$

Sada pretpostavimo da je $N(\pi) = p \equiv 1(\text{mod } 3)$. Prema Lemi 2.1.8. i Teoremu 1.2.3. vrijedi $\pi = a + b\omega = J(\chi_\pi, \chi_\pi) = \frac{r_3 + is_3\sqrt{3}}{2}$, tako da $a = \frac{r_3 + s_3}{2}$ i $b = s_3$, sa $a \equiv -r_3 \equiv -1(\text{mod } 3)$ i $b \equiv -s_3 \equiv 0(\text{mod } 3)$. Neka je $g$ primitivni korijen (mod $p$) takav da $\chi_\pi(g) = \omega$. Tada slijedi

$$ind_g 3 \equiv \frac{-s_3}{3} \equiv \frac{-b}{3}(\text{mod } 3).$$

Prema Korolaru 1.2.8.

$$\chi_\pi(-3) = \chi_\pi(3) = \omega^{\frac{-b}{3}}.$$

Stoga

$$\chi_\pi(-3\omega) = \omega^{\frac{p-1-b}{3}}.$$

Budući da je $p \equiv \frac{r_3^2}{4} (\text{mod } 9)$, lako se provjeri da je $p - 1 - b \equiv a + 1 (\text{mod } 9)$. Stoga je

$$\chi_\pi(-3) = \omega^{\frac{p-1-b}{3}} = \omega^{\frac{a+1}{3}} = \omega^m$$

kao što je traženo. □

Sljedeći numerički primjer ilustrira manipulaciju simbolom kubnog ostatka.

**Primjer 2.1.13.** *Eisensteinova domena $Z[\omega]$ je Euklidova domena u odnosu na svoju normu, tj. ako je $\alpha \in Z[\omega]$ i $\beta(\neq 0) \in Z[\omega]$, tada postoje $\gamma \in Z[\omega]$ i $\delta \in Z[\omega]$ takvi da je*

$$\alpha = \beta\gamma + \delta, N(\delta) < N(\beta).$$

*Koristeći višestruko ovo svojstvo i zakon kubnog reciprociteta ili njegov dodatak možemo evaluirati simbol kubnog ostatka $\left(\frac{\alpha}{\beta}\right)_3$.*
*Objašnjavamo na primjeru $\left(\frac{-9+4\omega}{5+8\omega}\right)_3$.*
*Prvo primjetimo*

$$5 + 8\omega = -\omega^2(8 + 3\omega),$$

*gdje je $(8 + 3\omega)$ primaran.*
*Zatim*

$$-9 + 4\omega = (8 + 3\omega)(-1 + \omega) + (2 + 2\omega) = (8 + 3\omega)(-1 + \omega) + (-\omega^2)2,$$

*gdje je*

$$N(2 + 2\omega) < N(8 + 3\omega),$$

*$-\omega^2$ je jedinica, a 2 je primaran.*
*Nadalje,*

$$(8 + 3\omega) = 2(4 + \omega) + \omega,$$

*gdje je $N(\omega) < N(2)$ i $\omega$ je jedinica.*
*Stoga,*

$$\left(\frac{-9 + 4\omega}{5 + 8\omega}\right)_3 = \left(\frac{-9 + 4\omega}{8 + 3\omega}\right)_3 = \left(\frac{(-\omega^2)2}{8 + 3\omega}\right)_3 = \omega^2\left(\frac{2}{8 + 3\omega}\right)_3 = \left(\frac{8 + 3\omega}{2}\right)_3 = \omega^2\left(\frac{\omega}{2}\right)_3 = \omega^2\omega = 1.$$

## 2.2 Bikvadratni reciprocitet

Gaussov cijeli broj je cijeli broj imaginarnog kvadratnog polja $Q(\sqrt{-1}) = Q(i) = Q(e^{\frac{2i\pi}{4}})$, odnosno kompleksni broj oblika $x + iy$, gdje su $x, y$ cijeli brojevi. Prsten Gaussovih cijelih brojeva je $Z[i]$. Poznato je da je $Z[i]$ domena jedinstvene faktorizacije. Kratko ćemo ponoviti neke činjenice o Gaussovim cijelim brojevima. Jedinice u $Z[i]$ su $\pm 1, \pm i$. Prosti brojevi u $Z[i]$ sastoje se od pridruženih elemenata od $1 + i$ i pridruženih elemenata onih elemenata $\pi \in Z[i]$ čija je norma $N(\pi)$ racionalan prost broj $p \equiv 1 (\text{mod } 4)$. Ako su $\pi, \alpha \in Z[i]$, gdje je $\pi$ prost i $\pi \nmid \alpha$, tada je $\alpha^{N(\pi)-1} \equiv 1 (\text{mod } \pi)$. Za Gaussov prost broj $\pi$ konačno polje $Z[i]/\pi$ ima $N(\pi)$ elemenata. Uzimajući istu vrstu argumenata kao u dokazu Propozicije 2.1.1. vidimo da imamo jedinstveni cijeli broj m, $0 \leq m \leq 3$, takav da je $\alpha^{\frac{N(\pi)-1}{4}} \equiv i^m (\text{mod } \pi)$ za sve $\pi, \alpha \in Z[i]$, gdje je $\pi$ prost, $\pi \nmid \alpha$ i $N(\pi) \neq 2$. Ovo vodi do sljedeće definicije sumbola kvartičnog ostatka.

**Definicija 2.2.1.** *Neka je $\pi$ Gaussov prost broj takav da je $N(\pi) \neq 2$ i neka je $\alpha \in Z[i]$. Ako $\pi \mid \alpha$, neka je $\left(\frac{\alpha}{\pi}\right)_4 = 0$. Ako $\pi \nmid \alpha$, neka je $\left(\frac{\alpha}{\pi}\right)_4$ jedinstvena potencija od $i$ definirana sa*

$$\alpha^{\frac{N(\pi)-1}{4}} \equiv \left(\frac{\alpha}{\pi}\right)_4 (\text{mod } \pi).$$

*Ako je $\beta = \pi_1 \cdots \pi_n$ gdje je svaki $\pi_j$ $(1 \leq j \leq n)$ Gaussov prost broj takav da je $N(\varpi_j) \neq 2$, definirajmo $\left(\frac{\alpha}{\beta}\right)_4$ sa*

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\alpha}{\pi_1}\right)_4 \cdots \left(\frac{\alpha}{\pi_n}\right)_4.$$

*Na kraju, ako je $\beta$ jedinica od $Z[i]$, definiramo $\left(\frac{\alpha}{\beta}\right)_4 = 1$ za svaki $\alpha \in Z[i]$, $\alpha \neq 0$ i $\left(\frac{0}{\beta}\right)_4 = 0$. Kada je $N(\pi) \neq 2$ lako se vidi da je $\left(\frac{\alpha}{\pi}\right)_4 = 1$ ako i samo ako je $\alpha$ kvartičan ostatak modulo prost $\pi$. Iz definicije simbola kvartičnog ostatka lako se izvodi da je $\left(\frac{\alpha}{\pi}\right)_4$ multiplikativna funkcija od $\alpha$ i da vrijedi $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4$ ako je $\alpha \equiv \beta (\text{mod} \pi)$. Stoga je $\left(\frac{\alpha}{\pi}\right)_4$ kvartičan ostatak karakter na polju $Z[i]/\pi$ od $N(\pi)$ elemenata. Pišemo $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_4$.*

**Definicija 2.2.2.** *Kažemo da je Gaussov cijeli broj $a + ib$ $(a, b \in Z)$ primaran ako je*

$$a \equiv 1 (\text{mod } 2), b \equiv 0 (\text{mod } 2), a + b \equiv 1 (\text{mod } 4).$$

*Ekvivalentno, $a + ib$ je primaran ako i samo ako je $a + ib \equiv 1 (\text{mod } 2 + 2i)$.*

Jedina jedinica koja je primarna je 1. Ako je Gaussov cijeli broj primaran, tada nužno nije djeljiv sa $1 + i$. Kažemo da je Gaussov cijeli broj koji nije djeljiv sa $1 + i$ neparan. Ako

je $\alpha$ neparan cijeli broj, onda od četiri pridružena elementa od $\alpha$, zapravo točno jedan je primaran; ovo je analogno Propoziciji 2.1.6. Gaussov cijeli broj koji nije jedinica je primaran ako i samo ako se može faktorizirati u produkt primarnih Gaussovih prostih brojeva; dokaz je u suštini isti kao u Propoziciji 2.1.7.

**Lema 2.2.3.** *Imamo*

$$\left(\frac{\alpha}{\beta}\right)_4 \left(\frac{\overline{\alpha}}{\overline{\beta}}\right)_4 = 1, \tag{2.12}$$

*ako su* $\alpha, \beta \in Z[i]$, $\alpha \neq 0$, $\beta \neq 0$ *i* nzd $(\alpha, \beta) = 1$;

$$\left(\frac{a}{b}\right)_4 = 1 \tag{2.13}$$

ako su $a, b \neq 0$ i relativno prosti racionalni cijeli brojevi, gdje je $b$ neparan i

$$\left(\frac{i}{a+ib}\right)_4 = i^{\frac{1-a}{2}} \tag{2.14}$$

ako je $a + ib$ primarni.

*Dokaz.* Prema argumentu sličnom onom korištenom u dokazu Propozicije 2.1.4.,

$$\left(\frac{\overline{\alpha}}{\overline{\beta}}\right)_4 = \left(\frac{\overline{\alpha}}{\beta}\right)_4,$$

iz čega slijedi (2.2).
Dovoljno je dokazati (2.13) kad je $b$ neparan prost broj $p$ koji koji ne dijeli $a$. Prema Malom Fermatovom teoremu $a^{p-1} \equiv 1 (\text{mod } p)$. Ako je $p \equiv 3 (\text{mod } 4)$, onda je $a^{\frac{p^2-1}{4}} = a^{\frac{(p-1)(p+1)}{4}} \equiv 1 (\text{mod } p)$ te slijedi željeni rezultat. Ako je $p \equiv 1 (\text{mod } 4)$, onda je $p = \pi\overline{\pi}$ za neki Gaussov prost broj $\pi$ i

$$\left(\frac{a}{p}\right)_4 = \left(\frac{a}{\pi}\right)_4 = \left(\frac{a}{\overline{\pi}}\right)_4 = 1,$$

prema (2.12) što dokazuje (2.13).
Neka su $a + ib$ i $c + id$ primarni Gaussovi cijeli brojevi. Iz $b = 1 - a + 4j$ i $d = 1 - c + 4k$, za neke $j, k \in Z$, lako vidimo da je $(1 - a)(1 - c) \equiv bd (\text{mod } 8)$ i stoga je

$$i^{\frac{1-a}{2}} i^{\frac{1-c}{2}} = i^{\frac{1-ac+bd}{2}}.$$

Dovoljno je dokazati (2.14) za slučaj da je $a + ib$ glavni Gaussov prost $\pi$. Iz $b = 1 - a + 4j$, lako slijedi da je $a^2 + b^2 - 1 \equiv 2 - 2a (\text{mod } 16)$. Dakle, $N(\pi) = a^2 + b^2$,

$$\left(\frac{i}{a+ib}\right)_4 = i^{\frac{a^2+b^2-1}{4}} = i^{\frac{1-a}{2}},$$

što dokazuje (2.2.3) □

Sljedeća lema je analogon Leme 2.1.8. za Gaussove proste brojeve.

**Lema 2.2.4.** *Neka je $\pi$ primarni Gaussov prost broj takav da je $N(\pi) = p \equiv 1(\text{mod } 4)$. Onda je*

$$J(\chi_\pi, \chi_\pi) = (-1)^{\frac{p+3}{4}}\pi.$$

*Dokaz.* Prema Teoremu 1.2.5. (b)

$$J(\chi_\pi, \chi_\pi)\overline{J(\chi_\pi, \chi_\pi)} = p = \pi\overline{\pi}$$

i prema Teoremu 1.2.7.,

$$J(\chi_\pi, \chi_\pi) \equiv 0(\text{mod } \pi).$$

Stoga, $J(\chi_\pi, \chi_\pi) = \theta\pi$ za neku jedinicu $\theta \in Z[i]$.
Sljedeće, prema Teoremu 1.2.10.,

$$(-1)^{\frac{p-1}{4}} J(\chi_\pi, \chi_\pi) = K(\chi_\pi) = a_4 + ib_4,$$

gdje su $a_4$ i $b_4$ cijeli brojevi takvi da

$$a_4 \equiv -1(\text{mod } 4), b_4 \equiv 0(\text{mod } 4), \textit{ako je} \quad p \equiv 1(\text{mod } 8)$$

$$a_4 \equiv 1(\text{mod } 4), b_4 \equiv 2(\text{mod } 4), \textit{ako je} \quad p \equiv 5(\text{mod } 8),$$

tako da je $-a_4 - ib_4 = (-1)^{\frac{p+3}{4}} J(\chi_\pi, \chi_\pi) = (-1)^{\frac{p+3}{4}}\theta\pi$ primaran. Ali, $\pi$ je primaran broj, tako da $(-1)^{\frac{p+3}{4}}\theta$ mora biti primarna jedinica pa je $(-1)^{\frac{p+3}{4}}\theta = 1$, što daje $J(\chi_\pi, \chi_\pi) = (-1)^{\frac{p+3}{4}}\pi$. □

Sada smo spremni dokazati bikvadratni zakon reciprociteta.

**Teorem 2.2.5.** *(Bikvadratni zakon reciprociteta) Neka su $\alpha$ i $\beta$ relativno prosti primarni Gaussovi cijeli brojevi. Stavimo $\alpha = a + ib$ i $\beta = c + id$. Tada je*

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\beta}{\alpha}\right)_4 (-1)^{\frac{bd}{4}}. \tag{2.15}$$

*Dokaz.* Prvo dokazujemo teorem kada je $\alpha$ primaran racionalan cijeli broj. U ovom slučaju pokazat ćemo da je

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\beta}{\alpha}\right)_4. \tag{2.16}$$

Dovoljno je uzeti u obzir primarne $\alpha$ i $\beta$ za koje je $\alpha = \pm q$, gdje je $(q \neq 2)$ racionalan prost broj i $\beta = \pi$ Gaussov prost broj. Ako je $\pi$ realan, onda (2.16) odmah slijedi iz (2.13). Pretpostavimo da $N(\pi) = p \equiv 1 (\text{mod } 4)$. Stavimo $\chi = \chi_\pi$ pa je prema Lemi 2.2.4. $J(\chi, \chi) = \pm\pi$.
Prvo pretpostavimo da je $\alpha = -q$, gdje je $q$ racionalan prost takav da $q \equiv -1 (\text{mod } 4)$. Prema multinomnom teoremu

$$J^q(\chi, \chi) \equiv J(\overline{\chi}, \overline{\chi}) (\text{mod } q)$$

i onda je

$$\pi^{q+1} = J^{q+1}(\chi, \chi) \equiv p (\text{mod } q). \tag{2.17}$$

Također, prema multinomnom teoremu i Teoremu 1.2.3.

$$G^q(\chi) \equiv \overline{\chi}^q(q) G(\chi^q) = \chi(q) G(\overline{\chi}) (\text{mod } q),$$

koji implicira

$$G^{q+1}(\chi) \equiv \chi(-q) p (\text{mod } q). \tag{2.18}$$

Prema (2.17), (2.18) i Teoremu 1.2.5.

$$\chi(-q)\pi^{q+1} \equiv \chi(-q)p \equiv G^{q+1}(\chi) = \left\{G^2(\chi)\right\}^{\frac{q+1}{2}} = \left\{p^{\frac{1}{2}} J(\chi, \chi)\right\}^{\frac{q+1}{2}}$$

$$= \left\{pJ^2(\chi, \chi)\right\}^{\frac{q+1}{4}} = (p\pi^2)^{\frac{q+1}{4}} \equiv \pi^{\frac{(q+3)(q+1)}{4}} (\text{mod } q).$$

Tako,

$$\left(\frac{-q}{\pi}\right)_4 = \chi(-q) \equiv \pi^{\frac{q^2-1}{4}} \equiv \left(\frac{\pi}{-q}\right)_4 (\text{mod } q)$$

i (2.16) slijedi u slučaju da je $\alpha = -q \equiv 1 (\text{mod } 4)$.
Sada pretpostavimo da je $\alpha = q$, gdje je $q$ racionalan prost broj takav da $q \equiv 1 (\text{mod } 4)$. Neka se $q$ može faktorizirati na proste faktore $\gamma\overline{\gamma}$ u $Z[i]$. Prema multinomnom teoremu i Teoremu 1.2.3.

$$G^q(\chi) \equiv \overline{\chi}^q(q) G(\chi^q) = \overline{\chi}(q) G(\chi) (\text{mod } q)$$

i onda

$$G^{q-1}(\chi) \equiv \overline{\chi}(q) (\text{mod } q).$$

Stoga je

$$\overline{\chi}(q) \equiv \left\{pJ^2(\chi,\chi)\right\}^{\frac{q-1}{4}} = \left(\overline{\pi}\pi^3\right)^{\frac{q-1}{4}} \equiv \left(\frac{\overline{\pi}}{\gamma}\right)_4 \left(\frac{\pi}{\gamma}\right)_4^3 = \left(\frac{\overline{\pi}}{\gamma}\right)_4 \overline{\left(\frac{\pi}{\gamma}\right)_4} \pmod{\gamma}.$$

Uzimajući kompleksne konjugate i koristeći (2.12) zaključujemo

$$\left(\frac{q}{\pi}\right)_4 = \chi(q) \equiv \left(\frac{\pi}{\overline{\gamma}}\right)_4 \left(\frac{\pi}{\gamma}\right)_4 = \left(\frac{\pi}{q}\right)_4 \pmod{\overline{\gamma}},$$

pa (2.16) slijedi u slučaju da je $\alpha = q \equiv 1 \pmod 4$. Ovo dovršava dokaz od (2.16).
Sada ćemo dokazati (2.15) za proizvoljne relativno proste Gaussove cijele brojeve $\alpha = a + ib$ i $\beta = c + id$. Gledajući (2.16) možemo pretpostaviti da $\text{nzd}(a,b) = \text{nzd}(c,d) = 1$. Sljedeće, odaberimo $\varepsilon = \pm 1$ takav da je $\varepsilon c$ primaran, neka je $\varepsilon = 1$ ili $-1$ prema tome da li $4 \mid d$ ili $2 \mid d$. Slično, odaberimo $\delta = \pm 1$ takav da je $\delta a$ primaran. Zbog $c\alpha \equiv ac + bd \pmod{\beta}$,

$$\left(\frac{\varepsilon c}{\beta}\right)_4 \left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\varepsilon(ac+bd) + ib\varepsilon(c+id)}{\beta}\right)_4 = \left(\frac{\delta}{\beta}\right)_4 \left(\frac{\delta\varepsilon(ac+bd)}{\beta}\right)_4 \tag{2.19}$$

jer je $\left(\frac{\delta}{\beta}\right)_4 = \pm 1$ prema (2.14). Prema (2.16), (2.13) i (2.14),

$$\left(\frac{\varepsilon c}{\beta}\right)_4 \left(\frac{\beta}{\varepsilon c}\right)_4 = \left(\frac{c+id}{\varepsilon c}\right)_4 = \left(\frac{id}{\varepsilon c}\right)_4 = \left(\frac{i}{\varepsilon c}\right)_4 = i^{\frac{1-\varepsilon c}{2}}.$$

Sljedeće, primjetimo da $\delta\varepsilon(ac+bd) \equiv \delta\varepsilon ac = (\delta a)(\varepsilon c) \equiv 1 \pmod 4$, tako da je $\delta\varepsilon(ac+bd)$ primaran. Zatim, prema (2.16) i (2.19),

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\delta}{\beta}\right)_4 = \left(\frac{\beta}{\delta\varepsilon(ac+bd)}\right)_4 i^{\frac{\varepsilon c-1}{2}}. \tag{2.20}$$

Slično,

$$\left(\frac{\alpha}{\beta}\right)_4 = \left(\frac{\delta}{\beta}\right)_4 \left(\frac{\beta}{\delta\varepsilon(ac+bd)}\right)_4 i^{\frac{\varepsilon c-1}{2}}. \tag{2.21}$$

Sljedeće ćemo pokazati da je

$$nzd(ad-bc, ac+bd) = 1.$$

Pretpostavimo suprotno, da postoji racionalan prost broj $p$ takav da

$$p \mid ad-bc p \mid ad-bc.$$

Jasno $ac+bd$ je neparan, pa onda $p \neq 2$. Neka je $\pi$ Gaussov prost broji koji dijeli $p$. Onda $\pi \mid \overline{\alpha}\beta$ i $\pi \mid \alpha\overline{\beta}$. Ali $\text{nzd}(\alpha,\beta) = \text{nzd}(\overline{\alpha},\overline{\beta}) = 1$, pa mora biti $\pi \mid \alpha$, $\pi \mid \overline{\alpha}$ ili $\pi \mid \beta$, $\pi \mid \overline{\beta}$. Ako

stoji prva mogućnost, imamo $\pi \mid \alpha + \overline{\alpha}$ i $\pi \mid \alpha\overline{\alpha}$, pa onda $\pi \mid 2a$, $\pi \mid a^2 + b^2$. Stoga, kako je $N(\pi) \neq 2$, mora vrijediti $\pi \mid a$, $\pi \mid b$ i onda $p \mid a$, $p \mid b$, kontradikcija nzd $(a, b) = 1$. Druga mogućnost također vodi do kontradikcije, $p \mid c$, $p \mid d$. Ovo upotpunjuje dokaz tvrdnje da su $ad + bc$ i $ac + bd$ relativno prosti brojevi.
Zatim, prema (2.13),

$$\left(\frac{\beta\overline{\alpha}}{\delta\varepsilon(ac+bd)}\right)_4 = \left(\frac{ac+bd+i(ad-bc)}{\delta\varepsilon(ac+bd)}\right)_4 = \left(\frac{i(ad-bc)}{\delta\varepsilon(ac+bd)}\right)_4 = \left(\frac{i}{\delta\varepsilon(ac+bd)}\right)_4. \quad (2.22)$$

Zbog $\varepsilon = i^d$ i $\delta = i^b$, lako slijedi iz (2.14) da

$$\left(\frac{\varepsilon}{\alpha}\right)_4 = \begin{cases} \varepsilon, \varepsilon = 1 \\ \delta, \varepsilon = -1 \end{cases}$$

i

$$\left(\frac{\delta}{\beta}\right)_4 = \begin{cases} \delta, \delta = 1 \\ \varepsilon, \delta = -1 \end{cases},$$

tako da

$$\left(\frac{\varepsilon}{\alpha}\right)_4 \left(\frac{\delta}{\beta}\right)_4 = 1.$$

Sada uzmimo kompleksne konjugate od obje strane od (2.21) za dobivanje ($\left(\frac{\varepsilon}{\alpha}\right)_4 = \pm 1$)

$$\overline{\left(\frac{\beta}{\alpha}\right)_4} = \left(\frac{\varepsilon}{\alpha}\right)_4 \left(\frac{\overline{\alpha}}{\delta\varepsilon\,(ac+bd)}\right)_4 i^{\frac{1-\delta a}{2}}.$$

Iz ove jednakosti i (2.20), množenjem dobivamo

$$\left(\frac{\alpha}{\beta}\right)_4 \overline{\left(\frac{\beta}{\alpha}\right)_4} = \left(\frac{\varepsilon}{\alpha}\right)_4 \left(\frac{\delta}{\beta}\right)_4 \left(\frac{\beta\overline{\alpha}}{\delta\varepsilon\,(ac+bd)}\right)_4 i^{\frac{\varepsilon c-\delta a}{2}} = \left(\frac{\beta\overline{\alpha}}{\varepsilon\delta\,(ac+bd)}\right)_4 i^{\frac{\varepsilon c-\delta a}{2}}.$$

Pozivajući se na (2.22) zaključujemo

$$\left(\frac{\alpha}{\beta}\right)_4 \overline{\left(\frac{\beta}{\alpha}\right)_4} = \left(\frac{i}{\delta\varepsilon\,(ac+bd)}\right)_4 i^{\frac{\varepsilon c-\delta a}{2}}. \quad (2.23)$$

Zbog, $\varepsilon c \equiv \delta a \equiv 1 (\mathrm{mod}\ 4)$, iz (2.14) i (2.23) slijedi

$$\left(\frac{\alpha}{\beta}\right)_4 \overline{\left(\frac{\beta}{\alpha}\right)_4} = i^{\frac{1-\delta\varepsilon(ac+bd)+\varepsilon c-\delta a}{2}} = i^{\frac{(1-\delta a)(1+\varepsilon c)}{2} - \frac{\delta\varepsilon bd}{2}}$$

$$= i^{-\frac{\delta\varepsilon bd}{2}} = (-1)^{-\frac{\delta\varepsilon bd}{4}} = (-1)^{\frac{bd}{4}},$$

dokazuje (2.15). □

**Teorem 2.2.6.** *Za prosti broj $p \equiv 1 (\mathrm{mod}\ 4)$, -3 je kvartičan ostatak* (mod $p$) *ako i samo ako* $3 \mid b_4$.

*Dokaz.* Neka je $\pi$ primaran prost broj takav da $N(\pi) = p \equiv 1 (\mathrm{mod}\ 4)$. Po Teoremu 2.2.5.

$$\left(\frac{-3}{\pi}\right)_4 = \left(\frac{\pi}{-3}\right)_4.$$

Sljedeće imamo

$$\left(\frac{\pi}{-3}\right)_4 = \chi_{-3}(\pi) \equiv \pi^{\frac{N(3)-1}{4}} = \pi^2 (\mathrm{mod}\ 3).$$

Tako da je -3 kvartičan ostatak (mod $p$) ako i samo ako je $\pi^2 \equiv 1 (\mathrm{mod}\ 3)$. Prema Lemi 2.2.4. $J(\chi_\pi, \chi_\pi) = (-1)^{\frac{p+3}{4}}\pi$ tako da je -3 kvartični ostatak (mod $p$) ako i samo ako je $J^2(\chi_\pi, \chi_\pi) \equiv 1 (\mathrm{mod}\ 3)$. Stoga, -3 je kvartični ostatak (mod $p$) ako i samo ako vrijedi

$$a_4\,(p-1) \equiv b_4\,(p+1) \equiv 0\,(\mathrm{mod}\ 3)$$

i slijedi rezultat. □

U Teoremu 2.1.12. dali smo dopunu kubnog zakona reciprociteta za izniman Eisensteinov prost broj $1-\omega$. Za kvartičnu recipročnost, prost broj $1+i$ je izuzetak i sljedeće ćemo dokazati analogon Teorema 2.1.12.

**Teorem 2.2.7.** *(Dopuna zakona o bikvadratnom reciprocitetu) Neka je $\alpha = a + ib$ primarni Gaussov cijeli broj. Tada je*

$$\left(\frac{1+i}{\alpha}\right)_4 = i^{\frac{a-b-1-b^2}{4}}. \tag{2.24}$$

*Dokaz.* Pokažimo prvo (2.24) kada je $\alpha = a$ primarni racionalan cijeli broj. Pokazat ćemo da za $a \equiv 1 (\mathrm{mod}\ 4)$,

$$\left(\frac{1+i}{a}\right)_4 = i^{a-1}4. \tag{2.25}$$

Ako je $a_1 \equiv a_2 \equiv 1 (\mathrm{mod}\ 4)$, lako se provjeri da

$$\frac{a_1 - 1}{4} + \frac{a_2 - 1}{4} \equiv \frac{a_1 a_2 - 1}{4}. \tag{2.26}$$

Dovoljno je dokazati (2.25) kada je $a = p \equiv 1 (\mathrm{mod}\ 4)$ i kada je $a = -q \equiv 1 (\mathrm{mod}\ 4)$, gdje su $p$ i $q$ prosti.
Pretpostavimo prvo da je $a = p = \pi\overline{\pi}$, gdje je $\pi = c + id$ primarni. Onda prema (2.12)

$$\left(\frac{1+i}{p}\right)_4 = \left(\frac{1+i}{\pi}\right)_4 \left(\frac{1+i}{\overline{\pi}}\right)_4 = \left(\frac{1+i}{\pi}\right)_4 \left(\frac{i}{\overline{\pi}}\right)_4 \left(\frac{1-i}{\overline{\pi}}\right)_4$$

$$= \left(\frac{i}{\overline{\pi}}\right)_4 \left(\frac{1+i}{\pi}\right)_4 \overline{\left(\frac{1+i}{\pi}\right)_4} = \left(\frac{i}{\overline{\pi}}\right)_4 = i^{\frac{N\pi-1}{4}} = i^{\frac{p-1}{4}}.$$

Drugo, pretpostavimo da je $a = -q$, gdje je $q$ racionalan prost broj kongruentan 3 modulo 4. Onda

$$\left(\frac{1+i}{-q}\right)_4 \equiv (1+i)^{\frac{q^2-1}{4}} = (2i)^{\frac{q^2-1}{8}} = \left(2^{\frac{q-1}{2}}\right)^{\frac{q+1}{4}} i^{\frac{q^2-1}{8}}$$

$$\equiv \left(\frac{2}{q}\right)^{\frac{q+1}{4}} i^{\frac{q^2-1}{8}} = \left((-1)^{\frac{q+1}{4}}\right)^{\frac{q+1}{4}} i^{\frac{q^2-1}{8}}$$

$$(-1)^{\frac{-(q+1)^2}{16}} i^{\frac{q^2-1}{8}} = i^{\frac{-(q+1)^2}{8}+\frac{q^2-1}{8}} = i^{\frac{-q-1}{4}} \,(\mathrm{mod}\ q)\,.$$

Stoga (2.25) vrijedi za $a = -q$. Ovo upotpunjuje dokaz od (2.25). Prema (2.25) i (2.26), sada je dovoljno dokazati (2.2.13) kada je $a + ib$ primarni, takav da je nzd $(a, b) = 1$. Stavimo da je $a^* = (-1)^{\frac{b}{2}} a$ i primjetimo

$$a^* \equiv 1(\mathrm{mod}\ 4) \quad i \quad \frac{a^*-1}{2} \equiv \frac{a-1}{2} + \frac{b^2}{4} (\mathrm{mod}\ 4). \tag{2.27}$$

Prema (2.13), (2.14), Teoremu 2.2.5. i (2.27) slijedi

$$\left(\frac{1+i}{a+ib}\right)_4 = \left(\frac{i}{a^*}\right)_4^3 \left(\frac{ib}{a^*}\right)_4 \left(\frac{1+i}{a+ib}\right)_4 = i^{\frac{a^*-1}{2}} \left(\frac{a+ib}{a^*}\right)_4 \left(\frac{1+i}{a+ib}\right)_4$$

$$= i^{\frac{a^*-1}{2}} \left(\frac{a^*}{a+ib}\right)_4 \left(\frac{1+i}{a+ib}\right)_4 = i^{\frac{a^*-1}{2}} \left(\frac{i}{a+ib}\right)_4^b \left(\frac{a+ia}{a+ib}\right)_4$$

$$= i^{\frac{a-1}{2}+\frac{b^2}{4}+\frac{b^2}{2}} \left(\frac{i(a-b)}{a+ib}\right)_4 = i^{\frac{3b^2}{4}} \left(\frac{a-b}{a+ib}\right)_4.$$

Kako je $a - b \equiv 1(\mathrm{mod}\ 4)$, vidimo da je $a - b$ primaran: Stoga, prema Teoremu 2.2.5., (2.13) i (2.25) slijedi

$$\left(\frac{1+i}{a+ib}\right)_4 = i^{\frac{-b^2}{4}} \left(\frac{a+ib}{a-b}\right)_4 = i^{\frac{-b^2}{4}} \left(\frac{a-b+b+ib}{a-b}\right)_4$$

$$= i^{\frac{-b^2}{4}} \left(\frac{b}{a-b}\right)_4 \left(\frac{1+i}{a-b}\right)_4 = i^{\frac{-b^2}{4}} \left(\frac{1+i}{a-b}\right)_4 = i^{\frac{-b^2}{4}+\frac{a-b-1}{4}}.$$

Ovo upotpunjuje dokaz. □

Sljedeća dva teorema daju primjenu zakona bikvadratnog reciprociteta.

**Teorem 2.2.8.** *Neka je $p$ prost broj, takav da $p \equiv 1(\text{mod } 4)$ i zapišimo $p = a^2 + b^2$, gdje je $a$ neparan. Ako je $p \equiv 1(\text{mod } 8)$, onda je $b$ kvartični ostatak* (mod $p$). *Ako je $p \equiv 5(\text{mod } 8)$, onda je $\frac{b}{2}$ kvartični ostatak* (mod $p$) *ako je izabran predznak od $b$ tako da vrijedi $\frac{b}{2} \equiv 1(\text{mod } 4)$.*

*Dokaz.* Prvo pretpostavimo da je $p \equiv 1(\text{mod } 8)$. Zamjenom $a$ sa $-a$, ako je potrebno, možemo pretpostaviti bez smanjenja općenitosti da je $a \equiv 1(\text{mod } 4)$. Kako je $p \equiv 1(\text{mod } 8)$, imamo da je $b \equiv 0(\text{mod } 4)$. Tada je $a + b \equiv 1(\text{mod } 4)$ i $\pi = a + ib$ je primaran. Prema Teoremu 2.2.5. i (2.13), slijedi

$$\left(\frac{a}{\pi}\right)_4 = \left(\frac{\pi}{a}\right)_4 = \left(\frac{ib}{a}\right)_4 = \left(\frac{i}{a}\right)_4$$

i stoga prema (2.14) slijedi

$$\left(\frac{b}{\pi}\right)_4 = \left(\frac{i}{\pi}\right)_4 \left(\frac{a}{\pi}\right)_4 = \left(\frac{1}{\pi a}\right)_4 = i^{\frac{1-a^2}{2}} = 1.$$

Stoga je $b$ kvartični ostatak (mod $\pi$), pa je onda $b$ kvartični ostatak (mod $p$).
Sljedeće, pretpostavimo da je $p \equiv 5(\text{mod } 8)$, pa je $\frac{b}{2}$ neparan. Odaberimo predznake za $a$ i $b$ takve da je $a \equiv -1(\text{mod } 4)$ i $\frac{b}{2} \equiv 1(\text{mod } 4)$. Onda su $\pi = a + ib$ i $\frac{b}{2}$ primarni, i onda je prema Teoremu 2.2.5. i (2.2.2)

$$\left(\frac{b/2}{\pi}\right)_4 = \left(\frac{\pi}{b/2}\right)_4 = \left(\frac{a}{b/2}\right)_4 = 1.$$

Slijedi da je $\frac{b}{2}$ kvartični ostatak ( mod $\pi$). Budući da je $N(\pi) = p$ imamo izomorfizam polja

$$Z[i]/\pi \approx Z/pZ$$

pa je $\frac{b}{2}$ kvartični ostatak (mod $p$). □

Neka je $p$ prost, takav da je

$$p = 4f + 1 = a^2 + b^2 \equiv 5(\text{mod } 8) \tag{2.28}$$

i odaberimo predznake od $a$ i $b$ tako da

$$a \equiv -1(\text{mod } 4), b \equiv 2(\text{mod } 8). \tag{2.29}$$

Postoji $\varepsilon = \pm 1$ takav da je

$$2^f + 1 \equiv \varepsilon 2^{\frac{f+1}{2}}(\text{mod } p) \tag{2.30}$$

jer je $(2^f + 1)^2 \equiv 2^{f+1)}(\text{mod } p)$. Brillhart se pitao koji je znak $\varepsilon = \pm 1$ u (2.30) točan. Odgovor se nalazi u idućem teoremu.

**Teorem 2.2.9.** *U oznakama (2.28)-(2.29) vrijedi*

$$2^f \equiv \frac{-b}{a} (\text{mod } p) \tag{2.31}$$

*i*

$$2^f + 1 \equiv (-1)^{\frac{b-10}{8}} 2^{\frac{f+1}{2}} (\text{mod } p). \tag{2.32}$$

*Dokaz.* Neka je $\pi = a + ib$. Prema (2.29) $\pi$ je primaran. Pišemo $\chi = \chi_\pi$. Prema (2.24), (2.14) i (2.29) slijedi

$$\chi(2) = \chi^2(1+i)\overline{\chi}(i) = i^{\frac{a-b-1-b^2}{2}} i^{\frac{a-1}{2}} = i^{a-1} i^{\frac{-b-b^2}{2}} = -i, \tag{2.33}$$

zbog $2^f \equiv \chi(2)(\text{mod } \pi)$ i $-i \equiv \frac{-b}{a}(\text{mod } \pi)$, iz (2.31) slijedi (2.33). Ostaje nam dokazati (2.32). Prema (2.31), (2.16), (2.24), (2.13), (2.14) slijedi

$$\begin{aligned} \chi(-2^f - 1) \equiv \chi(a-b)\overline{\chi}(-a) &= \left(\frac{\pi}{a-b}\right)_4 \left(\frac{\overline{\pi}}{-a}\right)_4 = \left(\frac{b(1+i)}{a-b}\right)_4 \left(\frac{-ib}{-a}\right)_4 = \left(\frac{1+i}{a-b}\right)_4 \left(\frac{i}{-a}\right)_4 \\ &= i^{\frac{a-b-1}{4}} i^{\frac{a+1}{2}} = i^{\frac{3a+1-b}{4}}. \end{aligned} \tag{2.34}$$

Prema (2.33) slijedi

$$\chi(2^{\frac{f+1}{2}}) = i^{\frac{3(f+1)}{2}}. \tag{2.35}$$

Kombinirajući (2.30), (2.34) i (2.35) imamo

$$a \equiv \begin{cases} 1 - 2f(\text{mod } 16), & f \equiv 1(\text{mod } 4) \\ 9 - 2f(\text{mod } 16), & f \equiv 3(\text{mod } 4) \end{cases} \tag{2.36}$$

Stoga je $\chi(-\varepsilon) = (-1)^{\frac{2-b}{8}}$. Kako je $f$ neparan, $\chi(-\varepsilon) = -\varepsilon$ i onda je $\varepsilon = (-1)^{\frac{b-10}{8}}$, što dokazuje (2.2.21). □

Zaključit ćemo ovaj dio numeričkim primjerom da ilustriramo manipulacije oznakom kvartičnog ostatka.

**Primjer 2.2.10.** *Gaussova domena $Z[i]$ je Euklidska s obzirom na normu. To znači, ako su $\alpha \in Z[i]$ i $\beta(\neq 0) \in Z[i]$, onda postoje $\gamma \in Z[i]$ i $\delta \in Z[i]$ takvi da je*

$$\alpha = \beta\gamma + \delta, N(\delta) < N(\beta).$$

*Primjetimo da $\gamma$ i $\delta$ nisu nužno jedinstveno određeni sa $\alpha$ i $\beta$. Da bi to vidjeli, promotrimo*

$$2 + 3i = (1+i)2 + i = (1+i)(3+i) - i.$$

*Koristeći ovo svojstvo, računamo* $\left(\frac{7+2i}{-10+3i}\right)_4$. *Prvo primjetimo,*

$$\left(\frac{7+2i}{-10+3i}\right)_4 = \left(\frac{7+2i}{3+10i}\right)_4 = -\left(\frac{3+10i}{7+2i}\right)_4.$$

*Sada,*

$$3+10i = (7+2i)(1+i)+(-2+i) = (7+2i)(1+i)+(-i)(-1-2i)$$

*gdje je* $-1-2i$ *primarni i* $N(-1-2i) < N(7+2i)$. *Sljedeće,*

$$7+2i = (-1-2i)(-2+2i)+1,$$

*gdje je 1 primarni i* $N(1) < N(-1-2i)$ *kako je 1 jedinica, ne trebamo ići dalje. Tako je*

$$\left(\frac{3+10i}{7+2i}\right)_4 = \left(\frac{(-i)(-1-2i)}{7+2i}\right)_4 = -i\left(\frac{-1-2i}{7+2i}\right)_4$$

$$= i\left(\frac{7+2i}{-1-2i}\right)_4 = i\left(\frac{1}{-1-2i}\right)_4 = i,$$

*i onda*

$$\left(\frac{7+2i}{-10+3i}\right)_4 = -i.$$

## 2.3 Zakoni racionalnog reciprociteta

Započinjemo s definicijom simbola racionalnog ostatka $\left(\frac{a}{q}\right)_{2^r}$ reda $2^r$.

**Definicija 2.3.1.** *Neka je r prirodan broj i pretpostavimo da je a različit od 0 ostatak* $2^{r-1}$*-tog stupnja* (mod $q$)*, gdje je q neparan prost broj. Tada je simbol racionalnog ostatka* $\left(\frac{a}{q}\right)_{2^r}$ *reda* $2^r$ *definiran sa*

$$\left(\frac{a}{q}\right)_{2^r} = \begin{cases} 1, & a \quad ostatak \quad 2^r - tog \quad stupnja \pmod q \\ 1, & u \quad ostalim \quad slučajevima \end{cases}$$

*Kada je* $r = 1$*, ova definicija podudara se s definicijom Legendreovog simbola. U ovom poglavlju* $\left(\frac{a}{q}\right)_{2^r}$ *uvijek označava simbol racionalnog ostatka. Tako, značenje od* $\left(\frac{a}{q}\right)_4$ *u ovom poglavlju nije isto kao značenje* $\left(\frac{a}{q}\right)_4$ *u dijelu 2.2. Neka su p i q različiti prosti brojevi, svaki kongruentan 1 modulo 4. Pišemo*

$$p = a^2 + b^2 \quad i \quad q = A^2 + B^2, b \equiv B \equiv 0 (\text{mod } 2). \tag{2.37}$$

*Nadalje, ako je* $p \equiv q \equiv 1 (\mathrm{mod}\ 8)$*, pišemo*

$$p = c^2 + 2d^2 \quad i \quad q = C^2 + 2D^2, d \equiv D \equiv 0 (\mathrm{mod}\ 2). \tag{2.38}$$

*Dalje, ako je* $p \equiv q \equiv 1 (\mathrm{mod}\ 16)$ *prema Teoremu 1.2.9. možemo pisati*

$$p = x^2 + 2v^2 + 2u^2 + 2w^2, 2xv = u^2 - w^2 - 2uw \tag{2.39}$$

*i*

$$q = X^2 + 2V^2 + 2U^2 + 2W^2, 2XV = U^2 - W^2 - 2UW. \tag{2.40}$$

**Teorem 2.3.2.** *(Zakon racionalnog kvartičnog reciprociteta) Neka su p i q različiti prosti brojevi takvi da je* $p \equiv q \equiv 1 (\mathrm{mod}\ 4)$ *i* $\left(\frac{p}{q}\right) = 1$*. Onda je*

$$\left(\frac{p}{q}\right)_4 = \left(\frac{q}{p}\right)_4 = \left(\frac{aA + bB}{q}\right) = (-1)^{\frac{q-1}{4}} \left(\frac{aB + bA}{q}\right), \tag{2.41}$$

*gdje vrijednosti simbola ne ovise o izboru predznaka od a, b, A, B.*

*Dokaz.* Primjetimo prvo da je

$$\left(\frac{aA + bB}{q}\right)\left(\frac{aA - bB}{q}\right) = \left(\frac{a^2A^2 - b^2B^2}{q}\right) = \left(\frac{a^2A^2 + b^2A^2 - b^2A^2 - b^2B^2}{q}\right)$$

$$= \left(\frac{pA^2 + b^2q}{q}\right) = \left(\frac{pA^2}{q}\right) = 1$$

i onda

$$\left(\frac{aA + bB}{q}\right) = \left(\frac{aA - bB}{q}\right) = \left(\frac{-aA + bB}{q}\right) = \left(\frac{-aA - bB}{q}\right)$$

tako da vrijednost od $\left(\frac{aA+bB}{q}\right)$ ne ovisi o izboru predznaka $a$, $b$, $A$, $B$. Sličan argument pokazuje da vrijednost od $\left(\frac{aB+bA}{q}\right)$ također ne ovisi o izboru predznaka $a$, $b$, $A$, $B$.
Neka je $\chi$ kvartični karakter (mod $p$). Prema Teoremu 1.2.10. možemo odabrati predznake za $a$ i $b$ tako da $K(\chi) = a + ib$. Prema Korolaru 1.2.12. i Teoremu 1.2.5. imamo (podsjetivši se $G(\chi^2) = p^{\frac{1}{2}}$)

$$1 \equiv \chi(q) G^{q-1}(\chi) = \left(\frac{p}{q}\right)_4 p^{\frac{q-1}{4}} K^{\frac{q-1}{2}}(\chi) (\mathrm{mod}\ q).$$

Prema Eulerovom kriteriju,

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 \equiv (a + ib)^{\frac{q-1}{2}} (\mathrm{mod}\ q). \tag{2.42}$$

Sljedeće, pozivajući se na kvadratni zakon reciprociteta imamo

$$A^{\frac{q-1}{2}} \equiv \left(\frac{A}{q}\right) = \left(\frac{|A|}{q}\right) = \left(\frac{q}{|A|}\right) = \left(\frac{A^{2+B^2}}{|A|}\right) = \left(\frac{B^2}{|A|}\right) = 1(\text{mod } q). \tag{2.43}$$

Stoga, prema (2.42) i (2.43) slijedi

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 \equiv (aA + iAb)^{\frac{q-1}{2}} = (aA + bB + ib(A + iB))^{\frac{q-1}{2}} (\text{mod } q).$$

Zatim, računajući modulo $A + iB$ imamo

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 \equiv (aA + bB)^{\frac{q-1}{2}} \equiv \left(\frac{aA + bB}{q}\right) (\text{mod } A + iB)\,.$$

Ovo dokazuje prvu jednakost u (2.41). Konačno,

$$\left(\frac{aA + bB}{q}\right)\left(\frac{aB + bA}{q}\right) = \left(\frac{abq + ABp}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{2AB}{q}\right) = \left(\frac{2}{q}\right)\left(\frac{(A + B)^2 - q}{q}\right) = \left(\frac{2}{q}\right) = (-1)^{\frac{q-1}{4}},$$

iz čega slijedi druga jednakost iz (2.41) □

**Primjer 2.3.3.** *Koristimo zakon racionalnog kvartičnog reciprociteta da odredimo je li kongruencija* $x^4 \equiv 73(\text{mod } 137)$ *rješiva. Stavimo da je* $p = 73$ *i* $q = 137$. *Prvo*

$$\left(\frac{p}{q}\right) = \left(\frac{73}{137}\right) = \left(\frac{137}{73}\right) = \left(\frac{64}{73}\right) = 1$$

*Možemo uzeti* $a = 3$, $b = 8$, $A = 11$, $B = 4$ *i onda*

$$\left(\frac{aA + bB}{q}\right) = \left(\frac{65}{137}\right) = \left(\frac{7}{65}\right) = \left(\frac{2}{5}\right)\left(\frac{7}{13}\right) = -\left(\frac{13}{7}\right) = -\left(\frac{-1}{7}\right) = 1.$$

*Stoga, prema Teoremu 2.3.2.,*

$$\left(\frac{73}{137}\right)_4 = \left(\frac{137}{73}\right)_4 = \left(\frac{64}{73}\right)_4 = \left(\frac{8}{73}\right) = \left(\frac{2}{73}\right) = 1.$$

*Kongruencija* $x^4 \equiv 73(mod 137)$ *je rješiva. Doista,* $61^4 \equiv 73(mod 137)$.

Ako postoje cijeli $m$ i $n$ za koje vrijedi

$$p = m^2 + qn^2, \tag{2.44}$$

onda zakon racionalnog kvartičnog reciprociteta ima jednostavniji oblik, što pokazuje sljedeći teorem.

**Teorem 2.3.4.** *Neka su $p$ i $q$ različiti prosti brojevi takvi da je $p \equiv q \equiv 1(\mod 4)$ i $\left(\frac{p}{q}\right) = 1$. Pretpostavimo da postoje cijeli brojevi $m$ i $n$ takvi da vrijedi (2.44). Onda je*

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \begin{cases} 1, & q \equiv 1(\mod 8) \\ (-1)^n, & q \equiv 5(\mod 8) \end{cases}$$

*Dokaz.* Iz (2.44) dobivamo

$$\left(\frac{p}{q}\right)_4 = \left(\frac{m}{q}\right)$$

i

$$\left(\frac{p}{q}\right)_4 = \left(\frac{pn^{-2} - m^2n^{-2}}{p}\right)_4 = \left(\frac{-m^2n^2}{p}\right)_4 = \left(\frac{2mn}{p}\right).$$

Stoga je

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{m}{pq}\right)\left(\frac{2n}{p}\right). \tag{2.45}$$

Sljedeće, stavimo $m = 2^\lambda m_1$ i $n = 2^\nu n_1$, gdje su $m_1$ i $n_1$ neparni. Točno jedan od $\lambda$ i $\nu$ je 0. Zatim prema (2.44)

$$\left(\frac{2}{p}\right)^\nu \left(\frac{n}{p}\right) = \left(\frac{n_1}{p}\right) = \left(\frac{p}{|n_1|}\right) = \left(\frac{m^2}{|n_1|}\right) = 1$$

i

$$\left(\frac{2}{pq}\right)^\lambda \left(\frac{m}{pq}\right) = \left(\frac{m_1}{pq}\right) = \left(\frac{pq}{|m_1|}\right) = \left(\frac{q^2n^2}{|m_1|}\right) = 1.$$

Zatim iz (2.45) zaključujemo,

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 = \left(\frac{2}{p}\right)^{\nu+\lambda+1} \left(\frac{2}{q}\right)^\lambda. \tag{2.46}$$

Prvo, pretpostavimo da $2 \mid n$ tako da je $\nu \geq 1$ i $\lambda = 0$. Ako je $p \equiv 1(\mod 8)$, onda je $\left(\frac{2}{p}\right) = 1$, dok ako je $p \equiv 5(\mod 8)$ vidimo da je $\nu = 1$ iz (2.44). Stoga je desna strana od (2.46) jednaka 1 u oba slučaja.
Drugo, pretpostavimo da $2 \nmid n$, tako da je $\nu = 0$. Ako $p$ nije kongruentno $q(\mod 8)$, iz (2.44) vidimo da je $\lambda = 1$ i ako je $p \equiv q(\mod 8)$, $\left(\frac{2}{p}\right) = \left(\frac{2}{q}\right)$. Stoga je u oba slučaja desna strana od (2.46) jednaka $\left(\frac{2}{q}\right)$. □

**Korolar 2.3.5.** *Neka je $q = 5$, 13 ili 37 i neka je $p$ prost broj takav da je $p \equiv 1(\mod 4)$ i $\left(\frac{p}{q}\right) = 1$. Onda je $p = m^2 + qn^2$ za neke cijele brojeve $m$ i $n$ i*

$$\left(\frac{p}{q}\right)_4 \left(\frac{q}{p}\right)_4 (-1)^n.$$

*Dokaz.* Dovoljno je pokazati da je

$$p = m^2 + qn^2$$

za neke cijele brojeve $m$ i $n$. Tada ostatak teorema odmah slijedi iz Teorema 2.3.4. Iz

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

postoji cijeli broj $s (\text{mod } p)$ takav da je $s^2 \equiv -q (\text{mod } p)$. Promotrimo skup $\{x - sy : 0 \leq x, y < \sqrt{p}\}$. Ovaj skup sadrži više od p elemenata, pa su dva različita elementa skupa međusobno kongruentna (mod $p$). Uzimajući njihovu razliku, vidimo da je $m - sn \equiv 0 (\text{mod } p)$, za neke cijele brojeve $m$ i $n$ takve da je $0 < |m| < \sqrt{p}$, $0 < |n| < \sqrt{p}$. Stoga je

$$m^2 + qn^2 = Mp$$

za neki prirodan broj M takav da je $Mp < (q + 1)p$, tj. $M \leq q$.
Sada uzimamo u obzir samo slučaj kada je $q = 5$ jer su slučajevi $q = 13$, $q = 37$ analogni. Zbog $m^2 \equiv Mp (\text{mod } 5)$ i $\left(\frac{p}{5}\right) = 1$, ne možemo imati $\left(\frac{M}{5}\right) = -1$, pa je $M = 1, 4$ ili 5. Ako je $M = 1$, onda je $p = m^2 + qn^2$. Ako je $M = 5$, onda $5 \mid m$ i

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

Konačno, ako je $M = 4$, onda i $m$ i $n$ moraju biti parni brojevi i

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

□

**Korolar 2.3.6.** *Neka je p prost takav da je* $p \equiv 1$ *ili* $9 (\text{mod } 20)$*, tada (prema Korolaru 2.3.5.) postoje cijeli brojevi a, b, u, v takvi da je*

$$p = a^2 + b^2 = u^2 + 5v^2, \tag{2.47}$$

*gdje je a neparan. Ako je* $p \equiv 1 (\text{mod } 20)$*, onda*

$$p \mid a \text{ ako i samo ako } 2 \mid u;$$

*a ako je* $p \equiv 9 (\text{mod } 20)$*, onda*

$$p \mid a \text{ ako i samo ako } 2 \nmid u.$$

*Dokaz.* Prema Korolaru 2.3.5. slijedi,

$$\left(\frac{p}{5}\right)_4 \left(\frac{5}{p}\right)_4 = (-1)^v = (-1)^{u+1}.$$

Jasno je da

$$\left(\frac{p}{5}\right)_4 = \begin{cases} \left(\frac{1}{5}\right)_4 = 1, & p \equiv 1 (\text{mod } 20) \\ \left(\frac{9}{5}\right)_4 = \left(\frac{3}{5}\right) = -1, & p \equiv 9 (\text{mod } 20) \end{cases} \tag{2.48}$$

Prema Teoremu 1.2.14. (jer je upravo jedan od a i b djeljiv s 5),

$$\left(\frac{p}{5}\right)_4 = \begin{cases} 1, b \equiv 0 (\text{mod } 5) \\ -1, a \equiv 0 (\text{mod } 5) \end{cases} \tag{2.49}$$

Korolar slijedi korištenjem zajedno (2.47), (2.48), (2.49). □

# Bibliografija

B.C. Berndt, R. J. Evans, K.S. Williams, *Gauss and Jacobi Sums*, John Wiley and Sons, Inc., 1998.
K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1998.

# Sažetak

U ovom radu govorimo o kubnim i bikvadratnim zakonima reciprociteta. Polazimo od definicije Gaussove i Jacobi sume, te od kvadratnog zakona reciprociteta. Koristimo neka jednostavnija svojstva Gaussove i Jacobi sume kako bismo dokazali zakone kubne i bikvadratne recipročnosti.

# Summary

In this thesis we talk about cubic and quartic reciprocity laws. We start from the definition of Gauss and Jacobi sums and quadratic reciprocity law. We use some of the simpler properties of Gauss and Jacobi sums to prove the cubic and quartic reciprocity laws.

# Životopis

Zovem se Ana Boban. Rođena sam 29.04.1988. godine u Ogulinu. Osnovnu školu Ivane Brlić-Mažuranić u Ogulinu, upisala sam 1995. godine. Nakon završene osnovne škole 2003. godine, upisala sam Opću gimnaziju Bernardina Frankopana u Ogulinu. Preddiplomski studij na Prirodoslovno-matematičkom fakultetu u Zagrebu, matematika - smjer nastavnički, upisala sam 2007. godine nakon završene srednje škole. Diplomski studij na istom fakultetu upisala sam 2010. godine.