Matematički fakultet u Beogradu

Diplomski master rad

Ilustracija opšte ideje zakona reciprociteta preko kvadratnog, kubnog i bikvadratnog

Student:
Emir Zogić, 1178/2011

Mentor:
Dragana Todorić

Beograd 2012.

Sadržaj

Uvod

Istorija zakona reciprociteta je zapravo istorija algebarske teorije brojeva. Čuveni matematičar Heke je ovu činjenicu formulisao na sledeći način:

> Moderna teorija brojeva datira od otkrića zakona reciprociteta. Ovaj zakon još uvek pripada teoriji racionalnih brojeva jer može biti potpuno formulisan kao jednostavna relacija između racionalnih brojeva; međutim, njegov koncept izlazi van domena racionalnih brojeva. [...] Razvoj algebarske teorije brojeva koji je aktuelan, ukazuje na to da koncept zakona reciprociteta postaje razumljiv ako se pređe na generalnu algebarsku teoriju brojeva i da se dokaz svrsishodan prirodi problema može najbolje sprovesti sa visokim metodama algebarske teorije brojeva.

Šta predstavlja zapravo zakon reciprociteta? Ojlerov način proučavanja ovog zakona je bio sledeći: kvadratni karakter od a mod p zavisi jedino od klase ostataka p mod $4a$. Za Ležandra, koji je i uveo termin reciprocitet, zakon reciprociteta je bio iskazan na sledeći način: neparni prost broj p je kvadratni ostatak modulo neki drugi neparan prost broj q ako i samo ako je q kvadratni ostatak modulo p, izuzev kada je $p \equiv q \equiv 3 \bmod 4$. Preciznije, Ležandr je za neparne proste brojeve q definisao simbol $\left(\frac{p}{q}\right)$ sa vrednostima $\{-1, +1\}$ zahtevajući da važi $\left(\frac{p}{q}\right) \equiv p^{\frac{q-1}{2}} \bmod q$ i najavio

Kvadratni zakon reciprociteta: Neka su $p, q \in \mathbb{N}$ različiti neparni prosti brojevi. Tada je

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

Štaviše, imamo da je

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}} \quad \text{i} \quad \left(\frac{2}{p}\right) = (-1)^{\frac{p^2-1}{8}};$$

gde se prva i druga jednakost zovu prvi i drugi dopunski zakon, respektivno.

Gaus je napomenuo da u formulaciji fundamentalne teoreme o bikvadratnim ostacima je potreban skup $\mathbb{Z}[i]$ poznat kao Gausov prsten celih. Simbol bikvadratnog ostatka $\left[\frac{\pi}{\lambda}\right]$, gde su $\pi, \lambda \in \mathbb{Z}[i]$ prosti koji ne dele 2, je jedinstven element u skupu $\{\pm 1, \pm i\}$ tako da važi kongruencija $\left[\frac{\pi}{\lambda}\right] \equiv \pi^{\frac{N(\lambda)-1}{4}} \bmod \lambda$. Zakon reciprociteta koji je otkrio Gaus glasi

Bikvadratni zakon reciprociteta: Neka su $\pi, \lambda \in \mathbb{Z}[i]$ različiti primarni prosti, tj. pretpostavimo da je $\pi \equiv \lambda \equiv 1 \bmod (2+2i)$. Tada važi:

$$\left[\frac{\pi}{\lambda}\right] = (-1)^{\frac{N(\pi)-1}{4}\cdot\frac{N(\lambda)-1}{4}} \left[\frac{\lambda}{\pi}\right].$$

Slično, poslednja formula važi i za kubne ostatke i primarne proste u $\mathbb{Z}[\omega]$, gde je ω primitivni treći koren jedinice. Naime, za prosti $\pi \in \mathbb{Z}[\omega]$ kažemo da je primaran ako je $\pi \equiv 2 (\mathrm{mod}\, 3)$.

Kubni zakon reciprociteta: Neka su π_1 i π_2 primarni, $N(\pi_1), N(\pi_2) \neq 3$ i $N(\pi_1) \neq N(\pi_2)$. Tada važi:

$$\left(\frac{\pi_2}{\pi_1}\right)_3 = \left(\frac{\pi_1}{\pi_2}\right)_3.$$

Prvi kompletni dokazi kubnog i bikvadratnog zakona reciprociteta su objavljeni 1844. godine od strane Ajzenštajna , koji je takođe dao odgovarajuće dopunske zakone. Jakobi je međutim, prvi dao dokaze još 1837. godine. Jakobi je radio na realizaciji kubnog i bikvadratnog zakona reciprociteta koristeći ciklotomičnost, ali se ispostavilo da nedostatak jedinstvene faktorizacije je bio glavni kamen spoticanja. Posle Kumerovog uvoda u njegove idealne brojeve (sa namerom da nađe uopšteni zakon reciprociteta) postalo je moguće raditi sa aritmetikom u ciklotomičnim poljima $\mathbb{Q}(\zeta_p)$. Ajzenštajn je brzo priznao superiornost Kumerovog pristupa i uspeo u nalaženju specijalnog slučaja opšteg zakona reciprociteta nazvanog:

Ajzenštajnov zakon reciprociteta: Neka je l neparan prost i pretpostavimo da je $\alpha \in \mathbb{Z}[\zeta_l]$ primaran, tj. kongruentan sa racionalnim celim modulo $(1-\zeta_l)^2$. Tada

$$\left(\frac{\alpha}{a}\right)_l = \left(\frac{a}{\alpha}\right)_l$$

za sve cele $a \in \mathbb{Z}$ uzajamno proste sa l.

Ovde l-ti stepen simbola ostatka $\left(\frac{\alpha}{\mathfrak{p}}\right)_l$ je jedinstveni l-ti koren jedinice tako da je $\left(\frac{\alpha}{\mathfrak{p}}\right)_l \equiv \alpha^{\frac{N(\mathfrak{p})-1}{l}} \mod \mathfrak{p}$.

Ovo je bio kratak istorijski pregled o kvadratnom, kubnom, bikvadratnom i Ajzenštajnovom zakonu reciprociteta. U ovom radu bavimo se kvadratnim zakonom reciprociteta čije izučavanje se oslanja na osnovne teoreme i rezultate iz elementarne teorije brojeva vezano za skup $\mathbb{Z}$. Treba istaći da kvadratni zakon reciprociteta se može formulisati i u nekim drugim prstenima, a ne samo u prstenu $\mathbb{Z}$. Dirihle je dokazao ovaj zakon za prsten $\mathbb{Z}[i]$. Hilbert je uspeo da dokaže da kvadratni zakon reciprociteta važi u bilo kom brojnom polju. Takođe, može se pokazati da kvadratni zakon reciprociteta važi i u prstenu $k[x]$, gde je k konačno polje. Ovaj rezultat je formulisan (mada ne i dokazan) od strane Dedekinda 1857. godine. Kvadratni zakon reciprociteta je kao što je to već navedeno vezan za kvadratne ostatke, tj. za rešavanje jednačine $x^2 \equiv a (\mathrm{mod}\, p)$. U ovom radu pored izučavanja kvadratnog zakona reciprociteta idemo dalje, želimo pokazati kako funkcioniše zakon reciprociteta za kubne i bikvadratne ostatke, tj. ispitujemo kada su rešive jednačine $x^3 \equiv a (\mathrm{mod}\, p)$ i $x^4 \equiv a (\mathrm{mod}\, p)$. Za kubni i bikvadratni zakon reciprociteta kao što je i navedeno u istorijskom pregledu, potrebni su nam prsteni $\mathbb{Z}[\omega]$ i $\mathbb{Z}[i]$ i samim tim za uvođenje kubnog i bikvadratnog zakona reciprociteta neophodno je prvo utvrditi osnovna svojstva pomenutih prstena i karakterizaciju njihovih prostih i inverzibilnih elemenata.

Napomene

Uvodno izlaganje je prikazano uz korišćenje [2] i [3].

1 Kvadratni zakon reciprociteta

U ovoj sekciji bavićemo se kvadratnim ostacima, izložićemo tri različita dokaza kvadratnog zakona reciprociteta a zatim ćemo izložiti primenu kvadratnog zakona reciprociteta na faktorizaciju u kvadratnim raširenjima polja i primenu u vidu Solovej-Štrasenovog testa primalnosti.

U domenu izučavanja kvadratnih kongruencija nameće se sledeće pitanje: ako je a ceo broj, za koje proste brojeve p kongruencija $x^2 \equiv a(\mathrm{mod}\, p)$ ima rešenja? Odgovor nam daje kvadratni zakon reciprociteta. Ovaj zakon je formulisan od strane Ojlera i Ležandra ali Gaus je bio prvi koji je izneo kompletan dokaz. Gaus je bio veoma ponosan na svoj rezultat i nazvao je teoremu koja govori o kvadratnom zakonu reciprociteta zlatnom teoremom.

1.1 Kvadratni ostaci

Da bismo razmatrali i dokazivali kvadratni zakon reciprociteta, neophodno je da prvo iznesemo neke osnovne pojmove i rezultate u vezi kvadratnih ostataka. Izlaganje počinjemo definicijom kvadratnog ostatka.

Definicija 1.1. *Ako je $(a, m) = 1$, a se zove kvadratni ostatak mod m ako kongruencija $x^2 \equiv a(mod\, m)$ ima rešenja. U suprotnom za a kažemo da je kvadratni neostatak mod m.*

Za bilo koji fiksiran ceo broj m moguće je odrediti kvadratne ostatke modulo m, tako što ispišemo pozitivne cele brojeve koji su manji i uzajamno prosti sa m, kvadriramo ih i redukujemo modulo m.

Na primer, 2 je kvadratni ostatak mod 7, ali 3 nije. U stvari, $1^2, 2^2, 3^2, 4^2, 5^2$ i 6^2 su kongruentni mod 7 sa 1,4,2,2,4 i 1 respektivno. Zato 1,2 i 4 su kvadratni ostaci a 3, 5 i 6 nisu.

Navedimo sada neke teoreme o kvadratnim ostacima.

Teorema 1.1. *Neka p označava prost broj. Tada $x^2 \equiv -1(mod\, p)$ ima rešenja ako i samo ako $p = 2$ ili $p \equiv 1(mod\, 4)$.*

Dokaz. Ako je $p = 2$ tada imamo rešenje $x = 1$.

Za bilo koji neparan prost broj p, možemo zapisati Vilsonovu teoremu na sledeći način:

$$\left(1 \cdot 2 \cdots j \cdots \frac{p-1}{2}\right)\left(\frac{p+1}{2} \cdots (p-j) \cdots (p-2)(p-1)\right) \equiv -1(\mathrm{mod}\, p).$$

Proizvod na levoj strani poslednje kongruencije je podeljen na dva dela u kome svaki deo ima isti broj faktora. Ovaj proizvod možemo zapisati i na sledeći način:

$$\prod_{j=1}^{\frac{p-1}{2}} j(p-j) \equiv -1(\mathrm{mod}\, p).$$

Kako je $j(p-j) \equiv -j^2 (\mathrm{mod}\, p)$, na osnovu prethodnog je

$$j(p-j) \equiv \prod_{j=1}^{\frac{p-1}{2}} (-j^2) = (-1)^{\frac{p-1}{2}} \left(\prod_{j=1}^{\frac{p-1}{2}} j \right)^2 (\mathrm{mod}\, p).$$

Ako je $p \equiv 1 (\mathrm{mod}\, 4)$, tada je prvi faktor na desnoj strani poslednje kongruencije jednak 1, i sledi da je $x = \left(\frac{p-1}{2}\right)!$ rešenje jednačine $x^2 \equiv -1 (\mathrm{mod}\, p)$.

Pretpostavimo, obrnuto, da postoji x, tako da je $x^2 \equiv -1 (\mathrm{mod}\, p)$. Primetimo da za takvo x, važi $p \nmid x$. Pretpostavimo da je $p > 2$ i stepenujmo obe strane poslednje kongruencije stepenom $\frac{p-1}{2}$. Dobijamo

$$(-1)^{\frac{p-1}{2}} \equiv (x^2)^{\frac{p-1}{2}} = x^{p-1} (\mathrm{mod}\, p).$$

Na osnovu Male Fermaove teoreme, desna strana poslednje kongruencije je $\equiv 1 (\mathrm{mod}\, p)$. Leva strana je ± 1, i kako je $-1 \not\equiv 1 (\mathrm{mod}\, p)$, zaključujemo da je

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

Zato je $\frac{p-1}{2}$ paran, odnosno $p \equiv 1 (\mathrm{mod}\, 4)$. □

Teorema 1.2. *Ako je p prost broj i (a,p)=1, tada kongruencija $x^n \equiv a (mod\, p)$ ima (n,p-1) rešenja ili nema rešenja u zavisnosti od toga da li važi ili ne važi sledeća kongruencija*

$$a^{\frac{p-1}{(n,p-1)}} \equiv 1 (mod\, p).$$

Dokaz. Neka je g primitivni koren modulo p i izaberimo i tako da je $g^i \equiv a (\mathrm{mod}\, p)$. Ako postoji x takvo da je $x^n \equiv a (\mathrm{mod}\, p)$ tada je $(x, p) = 1$ odakle je $x \equiv g^u (\mathrm{mod}\, p)$ za neko u. Zato data kongruencija je zapravo $g^{nu} \equiv g^i (\mathrm{mod}\, p)$, što je ekvivalentno sa $nu \equiv i (\mathrm{mod}\, p-1)$. Stavimo $k = (n, p-1)$. Poslednja kongruencija ima rešenja ako $k \mid i$ i nema rešenja ako $k \nmid i$. Ako $k \mid i$, tada je $i\frac{p-1}{k} \equiv 0 (\mathrm{mod}\, p-1)$, pa je $a^{\frac{p-1}{k}} \equiv g^{i\frac{p-1}{k}} = (g^{p-1})^{\frac{i}{k}} \equiv 1 (\mathrm{mod}\, p)$. Sa druge strane, ako $k \nmid i$ tada $i\frac{p-1}{k} \not\equiv 0 (\mathrm{mod}\, p-1)$, i sledi $a^{\frac{p-1}{k}} \equiv g^{i\frac{p-1}{k}} \not\equiv 1 (\mathrm{mod}\, p)$. □

Teorema 1.3. *(Ojlerov kriterijum) Ako je p neparan prost broj i (a,p)=1, tada $x^2 \equiv a (mod\, p)$ ima dva rešenja ili nema rešenja u zavisnosti od toga da li je $a^{\frac{p-1}{2}} \equiv 1$ ili $\equiv -1 (mod\, p)$.*

Dokaz. Neka je $b = a^{\frac{p-1}{2}}$. Na osnovu Male Fermaove teoreme važi $b^2 = a^{p-1} \equiv 1 (\mathrm{mod}\, p)$. Sada je $b = \pm 1 (\mathrm{mod}\, p)$. Ako je $b \equiv -1 (\mathrm{mod}\, p)$ tada kongruencija $x^2 \equiv a (\mathrm{mod}\, p)$ nema rešenja na osnovu Teoreme 1.2. Ako je $b \equiv 1 (\mathrm{mod}\, p)$ tada kongruencija ima tačno dva rešenja, na osnovu Teoreme 1.2. Za $a = -1$ dobijamo drugi deo dokaza Teoreme 1.1. □

Definišimo sada Ležandrov simbol koji je izuzento važan za razmatranje kvadratnih ostataka.

Definicija 1.2. *Neka je p neparan prost broj i $(a,p)=1$. Ležandrov simbol broja a u odnosu na p, u oznaci $\left(\frac{a}{p}\right)$ je definisan na sledeći način:*

$$\left(\frac{a}{p}\right)=\begin{cases}+1, & \text{ako je } a \text{ kvadratni ostatak mod } p\\ -1, & \text{ako } a \text{ nije kvadratni ostatak mod } p.\end{cases}$$

Navedimo sada neke osobine Ležandrovog simbola.

Teorema 1.4. *Neka su dati celi brojevi a i b i prost broj p, pri čemu $p\nmid a$ i $p\nmid b$. Tada za Ležandrov simbol važe sledeće osobine:*

1. $\left(\frac{a}{p}\right)\equiv a^{\frac{p-1}{2}}(mod\, p)$,
2. $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.
3. *Ako* $a\equiv b(mod\, p)$, *tada* $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.
4. $\left(\frac{a^2}{p}\right)=1, \left(\frac{a^2b}{p}\right)=\left(\frac{b}{p}\right)$,
5. $\left(\frac{1}{p}\right)=1, \left(\frac{-1}{p}\right)=(-1)^{\frac{p-1}{2}}$.

Dokaz. Dokaz pod 1. sledi na osnovu Ojlerovog kriterijuma.

Dokaz pod 2. : primenimo Ojlerov kriterijum.

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

Zato $\left(\frac{ab}{p}\right)\equiv\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)(\text{mod } p)$ odakle sledi $\left(\frac{ab}{p}\right)=\left(\frac{a}{p}\right)\left(\frac{b}{p}\right)$.

Dokaz pod 3. : primenimo ponovo Ojlerov kriterijum.

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

$\left(\frac{b}{p}\right)\equiv b^{\frac{p-1}{2}}(\text{mod } p)\equiv a^{\frac{p-1}{2}}(\text{mod } p)$ odakle sledi da je $\left(\frac{a}{p}\right)\equiv\left(\frac{b}{p}\right)(\text{mod } p)$, odnosno $\left(\frac{a}{p}\right)=\left(\frac{b}{p}\right)$.

Dokaz pod 4. : $\left(\frac{a^2}{p}\right)\equiv a^{2\frac{p-1}{2}}=a^{p-1}\equiv 1(\text{mod } p)\Rightarrow\left(\frac{a^2}{p}\right)=1$.

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

Dokaz pod 5. : Koristeći 1. za $a=-1$ i $a=1$ sledi dokaz □

Posledica 1.1. *Broj kvadratnih ostataka je jednak broju kvadratnih neostataka.*

Dokaz. Jednačina $a^{\frac{p-1}{2}} \equiv 1(\mathrm{mod}\, p)$ ima $\frac{p-1}{2}$ rešenja. Zato postoji $\frac{p-1}{2}$ kvadratnih ostataka i $p-1-\frac{p-1}{2}=\frac{p-1}{2}$ kvadratnih neostataka. □

Posledica 1.2. *Proizvod dva kvadratna ostatka je kvadratni ostatak, proizvod dva kvadratna neostatka je kvadratni ostatak, i proizvod kvadratnog ostatka i kvadratnog neostatka je kvadratni neostatak.*

Dokaz. a je kvadratni ostatak modulo p ako je $\left(\frac{a}{p}\right)=1$, i a je kvadratni neostatak ako je $\left(\frac{a}{p}\right)=-1$. Dakle, za proizvod dva kvadratna ostatka a_1 i a_2 imamo $\left(\frac{a_1a_2}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)=1$, pa je a_1a_2 zaista kvadratni ostatak. Ako su sada a_1 i a_2 kvadratni neostaci, onda imamo $\left(\frac{a_1a_2}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)=(-1)(-1)=1$, pa je zaista a_1a_2 kvadratni ostatak. I ako je recimo a_1 kvadrani ostatak i a_2 kvadratni neostatak, tada je a_1a_2 kvadratni neostatak jer $\left(\frac{a_1a_2}{p}\right)=\left(\frac{a_1}{p}\right)\left(\frac{a_2}{p}\right)=1\cdot(-1)=-1$. □

Teorema 1.5. *(*Gausova lema*) Neka je μ broj ostataka u skupu $ak, 1\le k\le\frac{p-1}{2}$, čija je vrednost veća od $\frac{p-1}{2}$. Tada je*

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

Dokaz. Neka je $la\equiv\pm m_l(\mathrm{mod}\, p)$, gde je $1\le m_l\le\frac{p-1}{2}$. Kako $k\pm l\not\equiv 0(\mathrm{mod}\, p)$, za $1\le k<l\le\frac{p-1}{2}$, to je $m_l\neq m_k$, za sve $1\le k<l\le\frac{p-1}{2}$. Dakle, $\{1,2,...,\frac{p-1}{2}\}=\{m_1,m_2,...,m_{\frac{p-1}{2}}\}$, pa množenjem kongruencija $la\equiv\pm m_l(\mathrm{mod}\, p)$ dobijamo

$$\left(\frac{p-1}{2}\right)!\cdot a^{\frac{p-1}{2}}\equiv\left(\frac{p-1}{2}\right)!\cdot(-1)^{\mu}(\mathrm{mod}\, p).$$

Tvrđenje sada sledi na osnovu Ojlerovog kriterijuma. □

Teorema 1.6. *2 je kvadratni ostatak prostih brojeva oblika 8k+1 i 8k+7. 2 je kvadratni neostatak prostih brojeva oblika 8k+3 i 8k+5. Ova dva tvrđenja su ekvivalentna sa formulom:*

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

Dokaz. Neka je p neparan prost broj i primetimo da je broj μ definisan u Gausovoj lemi jednak broju elemenata skupa $2\cdot 1, 2\cdot 2, ..., 2\cdot\frac{p-1}{2}$, koji prelaze $\frac{p-1}{2}$.

Neka je m definisan sa dva uslova $2m\le\frac{p-1}{2}$ i $2(m+1)>\frac{p-1}{2}$. Tada je $\mu=\frac{p-1}{2}-m$.

Ako je $p=8k+1$, tada je $\frac{p-1}{2}=4k$ i $m=2k$. Zato $\mu=4k-2k=2k$ je paran i $\left(\frac{2}{p}\right)=1$.

Ako je $p = 8k + 7$, tada je $\frac{p-1}{2} = 4k + 3, m = 2k + 1$ i $\mu = 4k + 3 - (2k + 1) = 2k + 2$ je paran. Zato je $\left(\frac{2}{p}\right) = 1$.

Ako je $p = 8k + 3$, tada je $\frac{p-1}{2} = 4k + 1, m = 2k$ i $\mu = 4k + 1 - 2k = 2k + 1$ je neparan. Zato je $\left(\frac{2}{p}\right) = -1$.

Ako je $p = 8k + 5$, tada je $\frac{p-1}{2} = 4k + 2, m = 2k + 1$, i $\mu = 4k + 2 - (2k + 1) = 2k + 1$ je neparan. Zato je $\left(\frac{2}{p}\right) = -1$. □

1.2 Kvadratni zakon reciprociteta

Sada ćemo dati dokaz kvadratnog zakona reciprociteta, koristeći Gausovu lemu. Kvadratni zakon reciprociteta se još zove i Gausov kvadratni zakon reciprociteta.

Teorema 1.7. *(Kvadratni zakon reciprociteta) Ako su p i q različiti prosti brojevi, tada je*

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

Dokaz. Na osnovu Gausove leme važi $\left(\frac{q}{p}\right) = (-1)^{\nu}$ gde je ν broj celih brojeva x takvih da je $1 \leq x \leq \frac{p-1}{2}$ i $qx = py + r$, gde je $-\frac{p}{2} < r < 0$, i y je ceo broj.

Takođe, važi da je $1 \leq y \leq \frac{q-1}{2}$, jer je y nenegativan i

$$py = xq - r < \frac{p-1}{2}q + \frac{p}{2} < \frac{p}{2}(q+1)$$

odakle sledi $y < \frac{q+1}{2}$ odnosno $y \leq \frac{q-1}{2}$.

Slično, $\left(\frac{p}{q}\right) = (-1)^{\mu}$, gde je μ broj celih brojeva y, takvih da je $1 \leq y \leq \frac{q-1}{2}$, tako da je $py = qx + s$ gde je $-\frac{q}{2} < s < 0$ i x je ceo broj. Sada ponovo imamo $1 \leq x \leq \frac{p-1}{2}$.

Zato je $\left(\frac{q}{p}\right)\left(\frac{p}{q}\right) = (-1)^{\nu+\mu}$.

Zaključujemo da je $\nu+\mu$ broj uređenih parova celih brojeva (x, y) takvih da je $1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}$ i $-\frac{p}{2} < qx - py < \frac{q}{2}$.

Posmatrajmo sledeće skupove uređenih parova celih brojeva:

$S = \{(x, y) | 1 \leq x \leq \frac{p-1}{2}, 1 \leq y \leq \frac{q-1}{2}\}$

$S_1 = \{(x, y) \in S | qx - py \leq -\frac{p}{2}\}$

$S_0 = \{(x, y) \in S | -\frac{p}{2} < qx - py < \frac{q}{2}\}$

$S_1' = \{(x, y) \in S | \frac{q}{2} \leq qx - py\}$.

Preslikavanje $\theta : S \to S$, definisano sa $\theta(x, y) = (x', y')$, gde su $x' = \frac{p+1}{2} - x, y' = \frac{q+1}{2} - y$ je bijekcija, θ^2 je identitet, $\theta(S_1) = S_1', \theta(S_1') = S_1, \theta(S_0) = S_0$.

Imamo da je $|S| = |S_1| + |S_0| + |S_1'| \equiv |S_0| (\mathrm{mod}\ 2)$ odakle sledi

$$\frac{p-1}{2} \cdot \frac{q-1}{2} \equiv \nu + \mu (\mathrm{mod}\ 2).$$

Zato je

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

□

Sa ovim rezultatom, možemo odgovoriti na pitanje: Za fiksirano a, za koje proste brojeve p jednačina $x^2 \equiv a(\mathrm{mod}\, p)$ ima rešenja? Ovo pitanje se sada svodi na pitanje: Kada je $\left(\frac{a}{p}\right)$ jednako 1. Neka je $a = q_1^{e_1} \cdots q_n^{e_n}$. Kako je Ležandrov simbol multiplikativan (Teorema 1.4) sledi

$$\left(\frac{a}{p}\right) = \left(\frac{q_1}{p}\right)^{e_1} \cdots \left(\frac{q_n}{p}\right)^{e_n}.$$

Sada se naše pitanje svodi na izračunavanje Ležandrovog simbola $\left(\frac{q}{p}\right)$ za svako prosto q. Takođe, sada znamo na osnovu Teoreme 1.4 i Teoreme 1.6 kako da izračunamo $\left(\frac{-1}{p}\right)$ i $\left(\frac{2}{p}\right)$. Zato se sav problem svodi na izračunavanje $\left(\frac{q}{p}\right)$. Sledeća teorema nam pomaže da odgovorimo na postavljeno pitanje.

Teorema 1.8. *Neka su p i q neparni prosti brojevi.*

1. *Ako je $q \equiv 1(mod\, 4)$, tada je q kvadratni ostatak mod p ako i samo ako $p \equiv r(mod\, q)$, gde je r kvadratni ostatak mod q.*
2. *Ako je $q \equiv 3(mod\, 4)$, tada je q kvadratni ostatak mod p ako i samo ako $p \equiv \pm b^2(mod\, 4q)$, gde je b neparan ceo broj uzajamno prost sa q.*

Dokaz. Kako je $q \equiv 1(\mathrm{mod}\, 4)$, $\frac{q-1}{2}$ je paran, pa imamo da na osnovu Teoreme 1.7 važi

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

Odavde sada sledi da važi da je ili $\left(\frac{p}{q}\right) = 1 = \left(\frac{q}{p}\right)$ ili $\left(\frac{p}{q}\right) = -1 = \left(\frac{q}{p}\right)$.

Dokaz pod 1. :

($\Rightarrow$:) Ako je $\left(\frac{q}{p}\right) = 1$, tada je $\left(\frac{p}{q}\right) = 1$ odakle na osnovu Teoreme 1.4 pod 3. važi $p \equiv r(\mathrm{mod}\, q)$, gde je r kvadratni ostatak mod q.

($\Leftarrow$:) Pretpostavimo da je $p \equiv r(\mathrm{mod}\, q)$, i $\left(\frac{r}{q}\right) = 1$. Tada je $\left(\frac{p}{q}\right) = \left(\frac{r}{q}\right)$ i zato je $\left(\frac{p}{q}\right) = 1$. Kako je $\left(\frac{q}{p}\right) = \left(\frac{p}{q}\right)$ na osnovu Teoreme 1.7 takođe imamo da je $\left(\frac{q}{p}\right) = 1$, odakle sledi da je q kvadratni ostatak mod p.

Dokaz pod 2. : Pretpostavimo da je $q \equiv 3(\text{mod } 4)$. Tada je prema Teoremi 1.7

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

($\Rightarrow$:) Pretpostavimo da je $\left(\frac{q}{p}\right) = 1$. Razlikujemo dva slučaja:

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

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

Slučaj 1. Primetimo da iz $(-1)^{\frac{p-1}{2}} = -1$ sledi $p \equiv 3(\text{mod } 4)$. Iz $q \equiv 3(\text{mod } 4)$ sledi da na osnovu Teoreme 1.4 pod 5 važi:

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

Tada takođe važi:

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

Dakle, $\left(\frac{p}{q}\right) = \left(\frac{-b^2}{q}\right)$ i $p \equiv -b^2(\text{mod } q)$. Možemo pretpostaviti da je b neparan. Ako nije, onda ga možemo zameniti sa $b' = b + q$, koji je neparan. Kako je b neparan sledi $b = 2n + 1$. Zato je $b^2 = 4n^2 + 4n + 1$, i $-b^2 \equiv 3(\text{mod } 4)$. Kako već važi $p \equiv 3(\text{mod } 4)$, imamo da je $p \equiv -b^2(\text{mod } q)$. Sada iz $p \equiv -b^2(\text{mod } q)$, možemo zaključiti da je $p \equiv -b^2(\text{mod } 4q)$.

Slučaj 2. $(-1)^{\frac{p-1}{2}} = 1$ sledi da je $p \equiv 1(\text{mod } 4)$. Takođe, $\left(\frac{p}{q}\right) = \left(\frac{b^2}{q}\right)$. Pretpostavimo da je b neparan broj iz istih razloga kao što je navedeno u slučaju 1. Dakle, $p \equiv b^2(\text{mod } q)$. Kako je b neparan, sledi $b = 2n + 1$ što znači da je $b^2 \equiv 1(\text{mod } 4)$. Iz $p \equiv 1(\text{mod } 4)$ sledi $p \equiv b^2(\text{mod } 4)$. A kako takođe znamo da je $p \equiv b^2(\text{mod } q)$, možemo zaključiti $p \equiv b^2(\text{mod } 4q)$.

($\Leftarrow$:) Pretpostavimo da je $p \equiv \pm b^2(\text{mod } 4q)$, gde je b uzajamno prost sa q. Razlikujemo dva slučaja:

Slučaj 1. $p \equiv b^2(\text{mod } 4q)$

Slučaj 2. $p \equiv -b^2(\text{mod } 4q)$

Slučaj 1. Imamo da je $p \equiv b^2 \equiv 1(\text{mod } 4)$, i $p \equiv b^2(\text{mod } q)$. Iz $p \equiv 1(\text{mod } 4)$ sledi $(-1)^{\frac{p-1}{2}} = 1$. Kako je $p \equiv b^2(\text{mod } q)$ sledi da je

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

Dakle,

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

pa je q kvadratni ostatak mod p.

Slučaj 2. Sada imamo $p \equiv -b^2 \equiv 3(\text{mod } 4)$, i $p \equiv -b^2(\text{mod } q)$. Iz činjenice da je $p \equiv 3(\text{mod } 4)$ sledi da je $(-1)^{\frac{p-1}{2}} = -1$. Iz $p \equiv -b^2(\text{mod } q)$, možemo zaključiti da je

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

Kako je $q \equiv 3(\text{mod } 4)$ sledi da je $\left(\frac{-1}{q}\right) = -1$. Dakle, $\left(\frac{p}{q}\right) = -1$. Zato je

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

Sada sledi da je q kvadratni ostatak mod p. □

Primer 1. Izračunati Ležandrov simbol $\left(\frac{34}{79}\right)$.

$\left(\frac{34}{79}\right) = \left(\frac{2}{79}\right)\left(\frac{17}{79}\right)$

$\left(\frac{2}{79}\right) = (-1)^{(79^2-1)/8} = 1$

$\left(\frac{17}{79}\right)\left(\frac{79}{17}\right) = (-1)^{(17-1)/2(79-1)/2} = 1 \Rightarrow \left(\frac{17}{79}\right) = \left(\frac{79}{17}\right)$

$\left(\frac{79}{17}\right) = \left(\frac{11}{17}\right) = \left(\frac{17}{11}\right)$ jer je $79 \equiv 11(\text{mod } 17)$ i $\left(\frac{17}{11}\right)\left(\frac{11}{17}\right) = 1$.

$\left(\frac{17}{11}\right) = \left(\frac{6}{11}\right)$ jer je $17 \equiv 6(\text{mod } 11)$.

$\left(\frac{6}{11}\right) = \left(\frac{2}{11}\right)\left(\frac{3}{11}\right)$

$\left(\frac{2}{11}\right) = (-1)^{(121-1)/8} = -1$

$\left(\frac{3}{11}\right)\left(\frac{11}{3}\right) = -1 \Rightarrow \left(\frac{3}{11}\right) = -\left(\frac{11}{3}\right) = -\left(\frac{2}{3}\right) = -(-1) = 1$

Dakle, $\left(\frac{34}{79}\right) = 1 \cdot (-1) = -1$.

Primer 2. Za koje vrednosti prostog broja p jednačine $x^2 \equiv 5(\text{mod } p)$ i $x^2 \equiv 7(\text{mod } p)$ imaju rešenja?

Izračunajmo $\left(\frac{5}{p}\right)$. Kako je $5 \equiv 1(\text{mod } 4)$, primenimo Teoremu 1.8 pod 1. Dakle, $\left(\frac{5}{p}\right) = 1$ ako i samo ako $p \equiv r(\text{mod } 5)$, gde je r kvadratni ostatak mod 5. Proverimo sada za koje je vrednosti r kvadratni ostatak mod 5: $1^1 \equiv 1, 2^2 \equiv 4, 3^2 \equiv 4, 4^2 \equiv 1$. Dakle, 1 i 4 su kvadratni ostataci mod 5 dok 2 i 3 nisu. Zato imamo:

$$\left(\frac{5}{p}\right) = \begin{cases} 1 & \text{ako je } p \equiv 1, 4 (\text{mod } 5), \\ -1 & \text{ako je } p \equiv 2, 3 (\text{mod } 5), \\ 0 & \text{ako je } p = 5. \end{cases}$$

Izračunajmo sada $\left(\frac{7}{p}\right)$. Kako je $7 \equiv 3 (\text{mod } 4)$, primenimo Teoremu 1.8 pod 2. To znači da treba odrediti sve ostatke mod 28 od svih kvadrata neparnih celih brojeva uzajamno prostih sa 7.

$$1^2, 13^2, 15^2, 27^2 \equiv 1 (\text{mod } 28)$$
$$3^2, 11^2, 17^2, 25^2 \equiv 9 (\text{mod } 28)$$
$$5^2, 9^2, 17^2, 23^2 \equiv 25 (\text{mod } 28)$$

$$\left(\frac{7}{p}\right) = \begin{cases} 1 & \text{ako je } p \equiv \pm 1, \pm 9, \pm 25 (\text{mod } 28), \\ -1 & \text{ako je } p \equiv \pm 5, \pm 11, \pm 13 (\text{mod } 28), \\ 0 & \text{ako je } p = 7. \end{cases}$$

1.3 Jakobijev simbol

Definicija 1.3. *Neka je b neparan i pozitivan ceo broj i a bilo koji ceo broj. Neka je $b = p_1 p_2 \cdots p_m$, gde su p_i-ovi prosti (pri čemu nije neophodno da su i različiti). Simbol $\left(\frac{a}{b}\right)$ definisan sa*

$$\left(\frac{a}{b}\right) = \left(\frac{a}{p_1}\right)\left(\frac{a}{p_2}\right)\cdots\left(\frac{a}{p_m}\right)$$

se zove Jakobijev simbol.

Jakobijev simbol ima slične osobine kao Ležandrov simbol. Jedna razlika između ova dva simbola se ogleda u sledećem: $\left(\frac{a}{b}\right)$ može biti jednak 1 ali da pri tom a nije kvadratni ostatak mod b. Na primer, $\left(\frac{2}{15}\right) = \left(\frac{2}{3}\right)\left(\frac{2}{5}\right) = (-1)(-1) = 1$, ali 2 nije kvadratni ostatak mod 15.

Međutim, ako je $\left(\frac{a}{b}\right) = -1$, tada je a kvadratni neostatak mod b.

Teorema 1.9. *Neka su b, b_1, b_2 neparani, pozitivni, celi brojevi i a, a_1, a_2 bilo koji celi brojevi. Tada za Jakobijev simbol važe sledeće osobine:*

1. $\left(\frac{a_1}{b}\right) = \left(\frac{a_2}{b}\right)$ *ako je* $a_1 \equiv a_2 (mod\, b)$.
2. $\left(\frac{a_1 a_2}{b}\right) = \left(\frac{a_1}{b}\right) \cdot \left(\frac{a_2}{b}\right)$.
3. $\left(\frac{a}{b_1 b_2}\right) = \left(\frac{a}{b_1}\right) \cdot \left(\frac{a}{b_2}\right)$.

Dokaz. Dokaz pod 1. i 2. sledi direktno iz odgovarajućih osobina Ležandrovog simbola dok dokaz pod 3. sledi direktno iz definicije Jakobijevog simbola. □

Lema 1.1. *Neka su r i s neparni celi brojevi. Tada važi:*

1. $\frac{rs-1}{2} \equiv \frac{r-1}{2} + \frac{s-1}{2} (mod\ 2)$.
2. $\frac{r^2 s^2 - 1}{8} \equiv \frac{r^2-1}{8} + \frac{s^2-1}{8} (mod\ 2)$.

Dokaz. Dokaz pod 1.: Kako je $(r-1)(s-1) \equiv 0 (\text{mod } 4)$ imamo da je $rs - 1 \equiv (r-1) + (s-1) (\text{mod } 4)$ odakle deljenjem poslednje kongruencije sa 2 sledi dokaz.

Dokaz pod 2.: $r^2 - 1$ i $s^2 - 1$ su oba deljivi sa 4. Zato je $(r^2-1)(s^2-1) \equiv 0 (\text{mod } 16)$ i $r^2 s^2 - 1 \equiv (r^2-1) + (s^2-1) (\text{mod } 16)$ odakle deljenjem poslednje kongruencije sa 8 sledi dokaz.

□

Teorema 1.10. *Neka su a i b pozitivni neparni celi brojevi. Tada važe sledeće osobine Jakobijevog simbola:*

1. $\left(\frac{-1}{b}\right) = (-1)^{\frac{b-1}{2}}$.
2. $\left(\frac{2}{b}\right) = (-1)^{\frac{b^2-1}{8}}$.
3. $\left(\frac{a}{b}\right)\left(\frac{b}{a}\right) = (-1)^{\frac{a-1}{2}\cdot\frac{b-1}{2}}$.

Dokaz. Dokaz pod 1.: $\left(\frac{-1}{b}\right) = \left(\frac{-1}{p_1}\right)\cdot\left(\frac{-1}{p_2}\right)\cdots\left(\frac{-1}{p_m}\right) = (-1)^{\frac{p_1-1}{2}}(-1)^{\frac{p_2-1}{2}}\cdots(-1)^{\frac{p_m-1}{2}} = (-1)^{\sum\limits_{i=1}^{m}\frac{p_i-1}{2}}$.

Na osnovu Leme 1.1 imamo da je $\sum\limits_{i=1}^{m}\frac{p_i-1}{2} \equiv \frac{p_1p_2\cdots p_m-1}{2} \equiv \frac{b-1}{2} (\text{mod } 2)$ odakle sledi dokaz.

Dokaz pod 2.: $\left(\frac{2}{b}\right) = \left(\frac{2}{p_1}\right)\cdot\left(\frac{2}{p_2}\right)\cdots\left(\frac{2}{p_m}\right) = (-1)^{\frac{p_1^2-1}{8}}(-1)^{\frac{p_2^2-1}{8}}\cdots(-1)^{\frac{p_m-1}{8}} = (-1)^{\sum\limits_{i=1}^{m}\frac{p_i^2-1}{8}}$

Na osnovu Leme 1.1 imamo da je $\sum\limits_{i=1}^{m}\frac{p_i^2-1}{8} \equiv \frac{p_1^2p_2^2\cdots p_m^2-1}{8} \equiv \frac{b^2-1}{8} (\text{mod } 2)$ odakle sledi dokaz.

Dokaz pod 3.:

$$\left(\frac{a}{b}\right)\cdot\left(\frac{b}{a}\right) = \prod_i\prod_j\left(\frac{q_i}{p_j}\right)\left(\frac{p_j}{q_i}\right) = (-1)^{\sum_i\sum_j((q_i-1)/2)(p_j-1)/2)}$$

Na osnovu Leme 1.1 imamo:
$\sum\limits_i\sum\limits_j\left(\frac{(p_j-1)}{2}\right)\left(\frac{(q_i-1)}{2}\right) \equiv \frac{(a-1)}{2}\sum\limits_i\frac{(p_j-1)}{2} \equiv \left(\frac{(a-1)}{2}\right)\left(\frac{(b-1)}{2}\right) (\text{mod } 2)$ odakle sledi dokaz. □

1.4 Ajzenštajnov dokaz

U ovoj podsekciji dokaćemo kvadratni zakon reciprociteta na jedan drugačiji način, koji se pripisuje Ajzenštajnu.

Kompleksan broj ζ se zove n-ti koren jedinice ako je $\zeta^n = 1$ za neki ceo broj $n > 0$. Ako je n najmanji ceo broj sa takvom osobinom, onda za ζ kažemo da je primitivni n-ti koren jedinice. Brojevi 1, $e^{\frac{2\pi i}{n}}, e^{\frac{2\pi i}{n}2}, ..., e^{\frac{2\pi i}{n}(n-1)}$ su n-ti koreni jedinice. Među njima primitivni su koreni jedinice $e^{\frac{2\pi i}{n}k}$ za koje je $(k, n) = 1$.

Ako je ζ n-ti koren jedinice i $m \equiv l (\mathrm{mod}\, n)$, tada je $\zeta^m = \zeta^l$. Ako je ζ primitivni n-ti koren jedinice i $\zeta^m = \zeta^l$, tada je $m \equiv l (\mathrm{mod}\, n)$.

Posmatrajmo funkciju $f(z) = e^{2\pi iz} - e^{-2\pi iz} = 2i \sin 2\pi z$. Ova funkcija zadovoljava relacije $f(z + 1) = f(z)$ i $f(-z) = -f(z)$. Takođe, ako je r realan broj i $2r \notin \mathbb{Z}$, tada je $f(r) \neq 0$.

Lema 1.2. *Ako je $n > 0$ neparan, onda*

$$x^n - y^n = \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y), \quad \textit{gde je } \zeta = e^{\frac{2\pi i}{n}}.$$

Dokaz. $1, \zeta, \zeta^2, ..., \zeta^{n-1}$ su koreni polinoma $z^n - 1$. Kako njih ima n i kako su svi različiti, imamo $z^n - 1 = \prod_{k=0}^{n-1} (z - \zeta^k)$. Neka je $z = \frac{x}{y}$ i pomnožimo obe strane poslednje jednakosti sa y^n. Tada dobijamo $x^n - y^n = \prod_{k=0}^{n-1} (x - \zeta^k y)$.

Broj n je neparan. Kada k prolazi kroz kompletan sistem ostataka mod n, isto to važi i za $-2k$. Sada imamo:

$$\begin{aligned} x^n - y^n &= \prod_{k=0}^{n-1} (x - \zeta^{-2k} y) \\ &= \zeta^{-(1+2+\cdots n-1)} \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y) \\ &= \prod_{k=0}^{n-1} (\zeta^k x - \zeta^{-k} y). \end{aligned}$$

jer je $1 + 2 + 3 + \cdots + (n - 1) = n\frac{n-1}{2}$ deljivo sa n.

□

Teorema 1.11. *Ako je n pozitivan ceo broj i $f(z) = e^{2\pi iz} - e^{-2\pi iz}$, tada je*

$$\frac{f(nz)}{f(z)} = \prod_{k=1}^{\frac{n-1}{2}} f\left(z+\frac{k}{n}\right) f\left(z-\frac{k}{n}\right).$$

Dokaz. U Lemi 1.2, stavimo $x = e^{2\pi iz}$ i $y = e^{-2\pi iz}$. Tada dobijamo:

$$f(nz) = \prod_{k=0}^{n-1} f\left(z+\frac{k}{n}\right).$$

Uočimo da važi $f\left(z+\frac{k}{n}\right) = f\left(z+\frac{k}{n}-1\right) = f\left(z-\frac{n-k}{n}\right)$. Kako k ide od $\frac{n+1}{2}$ do $n-1$, $n-k$ ide od $\frac{n-1}{2}$ do 1. Zato imamo:

$$\begin{aligned}
\frac{f(nz)}{f(z)} &= \prod_{k=1}^{\frac{n-1}{2}} f\left(z+\frac{k}{n}\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z+\frac{k}{n}\right) \\
&= \prod_{k=1}^{\frac{n-1}{2}} f\left(z+\frac{k}{n}\right) \prod_{k=\frac{n+1}{2}}^{n-1} f\left(z-\frac{n-k}{n}\right) \\
&= \prod_{k=1}^{\frac{n-1}{2}} f\left(z+\frac{k}{n}\right) f\left(z-\frac{k}{n}\right).
\end{aligned}$$

□

Teorema 1.12. *Ako je p neparan prost broj, $a \in \mathbb{Z}$, i $p \nmid a$, tada*

$$\prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{la}{p}\right) = \left(\frac{a}{p}\right) \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p}\right).$$

Dokaz. $la \equiv \pm m_l (\mathrm{mod}\, p)$, gde $1 \le m_l \le \frac{p-1}{2}$. Zato se $\frac{la}{p}$ i $\pm\frac{m_l}{p}$ razlikuju za neki ceo broj. Odavde sledi da je $f\left(\frac{la}{p}\right) = f\left(\pm\frac{m_l}{p}\right) = \pm f\left(\frac{m_l}{p}\right)$.

Dokaz teoreme sada sledi uzimanjem proizvoda na levoj i desnoj strani poslednje jednakosti kada l ide od 1 do $\frac{p-1}{2}$ i primenom Gausove leme. □

Dokažimo sada na još jedan način (koji se pripisuje Ajzenštajnu) kvadratni zakon reciprociteta.

Neka su p i q prosti neparni brojevi. Tada, prema Teoremi 1.12 imamo

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

Iz Teoreme 1.11 imamo

$$\frac{f\left(\frac{ql}{p}\right)}{f\left(\frac{l}{p}\right)} = \prod_{m=1}^{\frac{q-1}{2}} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right).$$

Iz poslednje dve jednačine dobijamo da je

$$\left(\frac{q}{p}\right) = \prod_{m=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{l}{p} + \frac{m}{q}\right) f\left(\frac{l}{p} - \frac{m}{q}\right).$$

Na isti način nalazimo da je

$$\left(\frac{p}{q}\right) = \prod_{m=1}^{\frac{q-1}{2}} \prod_{l=1}^{\frac{p-1}{2}} f\left(\frac{m}{q} + \frac{l}{p}\right) f\left(\frac{m}{q} - \frac{l}{p}\right).$$

Kako je $f\left(\frac{m}{q} - \frac{l}{p}\right) = -f\left(\frac{l}{p} - \frac{m}{q}\right)$ sledi da je

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

odnosno

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

1.5 Kvadratne Gausove sume

U ovom delu izložićemo još jedan dokaz kvadratnog zakona reciprociteta u kome ćemo koristiti kvadratne Gausove sume. Zato, na početku će biti predstavljeni definicija i nekoliko rezulutata vezano za kvadratne Gausove sume.

Neka ζ sada označava p-ti primitivni koren jedinice, tj. $\zeta = e^{\frac{2\pi i}{p}}$.

Lema 1.3. $\sum_{t=0}^{p-1} \zeta^{at}$ *je jednaka* p *ako je* $a \equiv 0(mod\, p)$. *U suprotnom je jednaka nuli.*

Dokaz. Ako je $a \equiv 0(\mathrm{mod}\, p)$,onda je $\zeta^a = e^{\frac{2\pi i}{p}a} = e^{2k\pi i} = 1$, i tada je $\sum_{t=0}^{p-1} \zeta^{at} = p$. Ako je $a \not\equiv 0(\mathrm{mod}\, p)$, tada $\zeta^a \neq 1$ i $\sum_{t=0}^{p-1} \zeta^{at} = \frac{\zeta^{ap}-1}{\zeta^a-1} = 0$.

□

Posledica 1.3. $p^{-1} \sum_{t=0}^{p-1} \zeta^{t(x-y)} = \delta(x,y)$, *gde je* $\delta(x,y) = 1$ *ako je* $x \equiv y(mod\, p)$ *i* $\delta(x,y) = 0$ *ako je* $x \not\equiv y(mod\, p)$.

Dokaz. Dokaz sledi direktno iz Leme 1.3. □

Lema 1.4. $\sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0$, *gde je* $\left(\frac{t}{p}\right)$ *Ležandrov simbol.*

Dokaz. Na osnovu definicje Ležandrovog simbola važi $\left(\frac{0}{p}\right) = 0$. Među preostalih $p-1$ članova, polovina njih su +1 a druga polovina njih su -1 na osnovu Posledice 1.1. □

Definicija 1.4. $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) \zeta^{at}$ *se zove kvadratna Gausova suma.*

Teorema 1.13. $g_a = \left(\frac{a}{p}\right) g_1$.

Dokaz. Ako je $a \equiv 0(\mathrm{mod}\, p)$, onda je $\zeta^{at} = 1$ za svako t, i $g_a = \sum_{t=0}^{p-1} \left(\frac{t}{p}\right) = 0$ na osnovu Leme 1.4. odakle sledi dokaz teoreme za slučaj $a \equiv 0(\mathrm{mod}\, p)$.

Pretpostavimo sada da je $a \not\equiv 0(\mathrm{mod}\, p)$. Tada je

$$\left(\frac{a}{p}\right) g_a = \sum_{t=0}^{p-1} \left(\frac{at}{p}\right) \zeta^{at} = \sum_{x=0}^{p-1} \left(\frac{x}{p}\right) \zeta^{x} = g_1.$$

U poslednjoj jednakosti koristili smo činjenicu da at prolazi kroz kompletan sistem ostataka mod p kada i t takođe i zato $\left(\frac{x}{p}\right)$ i ζ^x zavisi samo od klase ostataka x mod p.

Kako je $\left(\frac{a}{p}\right)^2 = 1$ kada $a \not\equiv 0(\mathrm{mod}\, p)$, dokaz teoreme sledi množeći obe strane jednačine $\left(\frac{a}{p}\right) g_a = g_1$ sa $\left(\frac{a}{p}\right)$. □

Označimo sada g_1 sa g. Iz Teoreme 1.13. sledi $g_a^2 = g^2$ ako je $a \not\equiv 0(\mathrm{mod}\, p)$.

Teorema 1.14. $g^2 = (-1)^{\frac{p-1}{2}} p$.

Dokaz. Ideaja dokaza teoreme jeste da sumu $\sum_a g_a g_{-a}$ razvijemo na dva načina.

Ako je $a \not\equiv 0(\mathrm{mod}\, p)$, tada je $g_a g_{-a} = \left(\frac{a}{p}\right)\left(\frac{-a}{p}\right) g^2 = \left(\frac{-1}{p}\right) g^2$ odakle sledi

$$\sum_a g_a g_{-a} = \left(\frac{-1}{p}\right)(p-1)g^2.$$

S druge strane imamo

$$g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \zeta^{a(x-y)}.$$

Sumirajući obe strane poslednje jednakosti po a i koristeći Posledicu 1.3. dobijamo

$$\sum_a g_a g_{-a} = \sum_x \sum_y \left(\frac{x}{p}\right)\left(\frac{y}{p}\right) \delta(x,y)p = (p-1)p.$$

Iz dva prikazana razvoja sume $\sum_a g_a g_{-a}$ dobijamo $\left(\frac{-1}{p}\right)(p-1)g^2 = (p-1)p$ odakle sledi $g^2 = \left(\frac{-1}{p}\right) p$.

□

Pre nego što pređemo na dokaz kvadratnog zakona reciprociteta, navedimo jednu teoremu koja je vezana za algebarske cele a koju ćemo koristiti u dokazu.

Teorema 1.15. *Neka je A prsten algebarskih celih. Ako $w_1, w_2 \in A$ i $p \in \mathbb{Z}$ prost, tada je*

$$(w_1 + w_2)^p \equiv w_1^p + w_2^p (mod\, p).$$

Dokaz. $(w_1 + w_2)^p = \sum_{k=0}^{p} \binom{p}{k} w_1^k w_2^{p-k}$. Na osnovu činjenice da je A prsten i $p \mid \binom{p}{k}$ za $1 \leq k \leq p-1$ sledi dokaz teoreme.

□

Dokažimo sada kvadratni zakon reciprociteta koristeći kvadratne Gausove sume. Neka je $p^* = (-1)^{\frac{p-1}{2}} p$. Neka je $q \neq p$ takođe neparan prost broj.

$$g^{q-1} = (g^2)^{\frac{q-1}{2}} = {p^*}^{\frac{q-1}{2}} \equiv \left(\frac{p^*}{q}\right) (\text{mod } q)$$

$$g^q \equiv \left(\frac{p^*}{q}\right) g(\text{mod } q).$$

Koristeći Teoremu 1.15. dobijamo

$$g^q = \left(\sum \left(\frac{t}{p}\right) \zeta^t\right)^q \equiv \sum \left(\frac{t}{p}\right)^q \zeta^{qt} \equiv g_q(\text{mod } q).$$

odakle sledi $g^q \equiv g_q \equiv \left(\frac{q}{p}\right) g(\text{mod } q)$ i

$$\left(\frac{q}{p}\right) g \equiv \left(\frac{p^*}{q}\right) g(\text{mod } q).$$

Množeći obe strane poslednje jednakosti sa g i koristeći da je $g^2 = p^*$, dobijamo:

$$\left(\frac{q}{p}\right) p^* \equiv \left(\frac{p^*}{q}\right) p^*(\text{mod } q),$$

odakle sledi

$$\left(\frac{q}{p}\right) \equiv \left(\frac{p^*}{q}\right) (\text{mod } q)$$

i konačno

$$\left(\frac{q}{p}\right) = \left(\frac{p^*}{q}\right).$$

Sada dokaz sledi iz

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

1.6 Faktorizacija ideala

U ovoj podsekciji prikazujemo primenu kvadratnog zakona reciprociteta na faktorizaciju ideala u kvadratnim raširenjima polja. Pozivaćemo se na rezultate iz kvadratnih raširenja polja $\mathbb{Q}$ koja navodimo u Dodatku A.

Neka je A Dedekindov domen, K njegovo polje razlomaka i neka je $L|K$ separabilno raširenje stepena n i neka je B integralno zatvorenje od A u L. B je takođe Dedekindov domen.

Ako je I bilo koji ideal od A, označimo sa $B.I$ ideal od B generisan sa I. Ovaj ideal sadrži sve sume $\sum_{i=1}^{m} b_i x_i$ gde je $m \geq 1, b_i \in B, x_i \in I$ za sve $i = 1, ..., m$.

Neka je sada A prsten celih algebarskog brojnog polja K. Ako je P nenula prost ideal od A, tada se $B.P$ može predstaviti na jedinstven način kao proizvod prostih ideala od P:

$$B.P = \prod_{i=1}^{g} Q_i^{e_i}.$$

Navedimo sada nekoliko definicija vezanih za faktorizaciju ideala.

Definicija 1.5. *Broj g se zove dekompozicioni broj od P u raširenju $L|K$. Važi da je $g \geq 1$ zato što je $B.P \neq B$.*

Definicija 1.6. *Za svako $i = 1, ..., g$, e_i se zove indeks grananja od Q_i u $L|K$. Ako je $e_i = 1$, kažemo da je Q_i negranajući u $L|K$ (ili nad P). Ako je $e_1 = \cdots = e_g = 1$ kažemo da je P negranajući u $L|K$.*

Primetimo da je $Q_i \cap A \supseteq B.P \cap A = P$ odakle je $Q_i \cap A = P$ i B/Q_i je konačno polje koje sadrži A/P.

Definicija 1.7. *Stepen f_i od B/Q_i nad A/P se zove inercijalni stepen od Q_i nad $L|K$. Ako je $f_i = 1$ kažemo da je Q_i inertan u $L|K$ (ili nad P). Ako je $f_1 = \cdots = f_g = 1$ tada za P kažemo da je inertan u $L|K$.*

Ako odredimo za svaki prost ideal P od A dekompozicioni broj, indekse grananja, i inercijalne stepene u $L|K$, tada, kako se svaki nenula ideal I od A može na jedinstven način prikazati kao proizvod prostih ideala od A, dekompozicija od $B.I$ će biti poznata.

Glavna činjenica ovde je da postoji samo konačno mnogo ramifikovanih (razgranatih) ideala P u $L|K$. Specijalno, samo konačno prostih ideala Q od B će biti ramifikovano (razgranato) u $L|K$.

Teorema 1.16. *Ako je $B.P = \prod_{i=1}^{g} Q_i^{e_i}$ i $f_i = [B/Q_i : A/P]$ za $i = 1, ..., g$, tada*

$$\sum_{i=1}^{g} e_i f_i = n.$$

Specijalno, ako je $L|K$ Galuaovo raširenje, tada formula navedena u prethodnoj teoremi postaje $n = efg$, gde je $e = e_1 = \cdot = e_g$ i $f = f_1 = \cdots = f_g$.

Dekompozicioni broj g od P u $L|K$ je najviše jednak stepenu $n = [L : K]$. Ako je $g = n$ kažemo da je P kompletno dekomponovan u $L|K$.

Pređimo sada konkretnije na primenu kvadratnog zakona reciprociteta. Neka je sada $K = \mathbb{Q}(\sqrt{d})$, gde je d slobodno kvadratan ceo broj i neka je p prost broj. Odredimo dekompoziciju Ap na proste ideale od A.

Imamo da je $n = 2$ odakle na osnovu prethodne teoreme jedine mogućnosti su sledeće:

1. $g = 2, e_1 = e_2 = 1, f_1 = f_2 = 1$. U ovom slučaju je $Ap = P_1P_2$ gde je $P_1 \neq P_2, N(P_1) = N(P_2) = p$. Kažemo da je p (totalno) dekomponovan u $\mathbb{Q}(\sqrt{d})$. (Ili još i kažemo da se p cepa u K.)

2. $g = 1, e = 1, f = 2$. $Ap = P$ je prost ideal, $N(Ap) = p^2$, i kažemo da je p inertan u $\mathbb{Q}(\sqrt{d})$.

3. $g = 1, e = 2, f = 1$. $Ap = P^2, N(P) = p$ i kažemo da se p ramifikuje ili grana u $\mathbb{Q}(\sqrt{d})$.

Navedimo sada neke rezultate vezano za ideale. Ako je $Ap = P_1P_2$, tada je $A/Ap \cong A/P_1 \times A/P_2$, pa je A/Ap kartezijski proizvod dva polja. Posebno, A/Ap_1 nema nilpotentnih elemenata, osim 0. Ako je $Ap = P$, tada je A/Ap polje. Konačno, ako je $Ap = P^2$ tada A/Ap je prsten koji ima nenula ideal P/P^2, koji je nilpotentan.

Glavno pitanje koje se nameće u ovoj podsekciji je sledeće: Za dati prost broj p, za koje vrednosti d, imamo navedene slučajeve 1., respektivno 2., 3.? Sledeća teorema govori o tome.

Teorema 1.17. *Neka je p prost i $p \neq 2$. Tada:*

1. *p se grana u $\mathbb{Q}(\sqrt{d})$ ako i samo ako p deli d;*

2. *p je inertan ako i samo ako $\left(\frac{d}{p}\right) = -1$;*

3. *p se cepa ako i samo ako $\left(\frac{d}{p}\right) = 1$.*

Dokaz. Ako je $d \equiv 2$ ili $d \equiv 3 (\mathrm{mod}\, 4)$, tada je prsten celih A od $\mathbb{Q}(\sqrt{d})$ dat sa $A = \mathbb{Z} + \mathbb{Z}\sqrt{d}$; ako je $d \equiv 1 (\mathrm{mod}\, 4)$ tada je $A = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$.

U oba slučaja, $A/Ap = (\mathbb{Z} + \mathbb{Z}\sqrt{d})/Ap$. Naime, ako je $d \equiv 1 (\mathrm{mod}\, 4)$ i b je neparan, tada

$$\left[a + b\left(\frac{1+\sqrt{d}}{2}\right)\right] - \left[a + (b+p)\left(\frac{1+\sqrt{d}}{2}\right)\right] \in Ap,$$

gde je $b+p$ paran.

Sada je $\mathbb{Z}+\mathbb{Z}\sqrt{d} \cong \mathbb{Z}[X]/(X^2-d)$, na osnovu preslikavanja indukovanog sa $\theta : \mathbb{Z}[X] \to \mathbb{Z}+\mathbb{Z}\sqrt{d}, \theta(h) = h(\sqrt{d})$, koje ima jezgro (X^2-d) (glavni ideal generisan sa X^2-d u $\mathbb{Z}[X]$).

Sada imamo:

$$\begin{aligned}(\mathbb{Z}+\mathbb{Z}\sqrt{d})/Ap &\cong \mathbb{Z}[X]/(X^2-d, p\mathbb{Z}[X]) \\ &\cong (\mathbb{Z}[X]/p\mathbb{Z}[X])/((X^2-d, p\mathbb{Z}[X])/p\mathbb{Z}[X]) \\ &\cong \mathbb{F}_p[X]/(X^2-\bar{d})\end{aligned}$$

gde $(X^2-d, p\mathbb{Z}[X])$ označava ideal od $\mathbb{Z}[X]$ generisan sa $X^2-d, p\mathbb{Z}[X]$, $\bar{d}$ klasu ostataka od d modulo p. Ovde smo koristili poznate teoreme o izomorfizmima.

Prikažimo sada detaljnije kako smo dobili da je $(\mathbb{Z}+\mathbb{Z}\sqrt{d})/Ap \cong \mathbb{F}_p[X]/(X^2-\bar{d})$.

Neka je $\bar{h} \in \mathbb{F}_p[X]$ i neka je $h \in \mathbb{Z}[X]$ tako da koeficijenti od $\bar{h}$ su dobijeni uzimanjem klasa ostataka modulo p koeficijenata od h; izbor takvih polinoma nije jedinstven. Neka je $\theta(f) = h(\sqrt{d}) \in \mathbb{Z}+\mathbb{Z}\sqrt{d} \subseteq A$. Označimo sa $\pi : A \to A/Ap$ kanonski homomorfizam. Definišimo $\psi : \mathbb{F}_p[X] \to A/Ap$ sa $\psi(\bar{h}) = \pi(\theta(h))$. Ako $k \in p\mathbb{Z}[X]$, tada $\theta(k) \in Ap$, pa ako su h', h takvi da je $\bar{h'} = \bar{h}$ tada $h-h' = k \in p\mathbb{Z}[X]$ i $\pi(\theta(h)) = \pi(\theta(h'))$. Dakle, ψ je dobro definisano. Direktnom proverom sledi da je ψ izomorfizam prstena. Kako je $A/Ap = (\mathbb{Z}+\mathbb{Z}\sqrt{d})/Ap$, preslikavanje ψ je sirjektivno. $X^2-\bar{d}$ pripada jezgru od ψ. Obrnuto, ako je $\bar{h}$ u jezgru, tada $h(\sqrt{d}) \in Ap$. Kako je $\mathbb{Z}[\sqrt{d}] \cap Ap = p\mathbb{Z}[\sqrt{d}]$ sledi $h(\sqrt{d}) = a+b\sqrt{d}, a, b \in \mathbb{Z}p$. Zato se $h-(a+bX)$ anulira sa $\sqrt{d}$, pa X^2-d deli $h-(a+bX)$. Dakle, posmatrajući klase ostataka modulo p od koeficijenata dobijamo da $X^2-\bar{d}$ deli $\bar{h}$, odakle sledi da jezgro od ψ je ideal generisan sa $X^2-\bar{d}$. Sada ψ indukuje traženi izomorfizam:

$$\bar{\psi} : \mathbb{F}_p[X]/(X^2-\bar{d}) \to (\mathbb{Z}+\mathbb{Z}\sqrt{d})/Ap = A/Ap.$$

Ako je $X^2-\bar{d}$ ireducibilan u $\mathbb{F}_p[X]$, tada je A/Ap izomorfno nekom domenu, pa je Ap prost ideal, odnosno p je inertan u $\mathbb{Q}(\sqrt{d})$.

Ako je $X^2-\bar{d} = h_1h_2$ gde su h_1, h_2 različiti ireducibilni polinomi i koji su stepena 1, tada iz $(h_1h_2) = (h_1) \cap (h_2), (h_1)+(h_2) = \mathbb{F}_p[X]$, imamo da je

$$A/Ap \cong \mathbb{F}_p[X]/(h_1h_2) \cong \mathbb{F}_p[X]/(h_1) \times \mathbb{F}_p/(h_2) \cong \mathbb{F}_p \times \mathbb{F}_p.$$

($\mathbb{F}_p[X]/(h_i)$ je algebarsko raširenje stepena 1 nad $\mathbb{F}_p$.) Dakle, p se cepa u $\mathbb{Q}(\sqrt{d})$.

Ako je $X^2-\bar{d}$ kvadrat ireducibilnog polinoma, $X^2-\bar{d} = \bar{h}^2$, tada je $A/Ap \cong \mathbb{F}_p[X]/(h^2)$ i ideal $(h)/(h^2)$ je nenula i nilpotentan. Zato se p grana u $\mathbb{Q}(\sqrt{d})$.

U poslednjem slučaju, uzimajući za $\bar{h} = X + \bar{a}$ imamo $X^2 - \bar{d} = X^2 + 2\bar{a}X + \bar{a}^2$ i kako je $p \neq 2$, sledi da je $\bar{a} = \bar{0}$, pa p deli a; zato $-d \equiv a^2 (\mathrm{mod}\, p)$ implicira $p \mid d$. Obrnuto, ako $p \mid d$ tada $X^2 - \bar{d} = X^2$, pa se p grana.

Ako p ne deli d, tada se p cepa tačno kada je $X^2 - \bar{d} = (X + \bar{a})(X + \bar{b})$ gde je $\bar{a} \neq \bar{b}$, pa je $\bar{a} + \bar{b} = 0, \bar{a}\bar{b} = -\bar{d}$. Dakle, imamo da je $\bar{a}^2 = \bar{d}$ odnosno $\left(\frac{d}{p}\right) = 1$. Zato p je inertan kada p ne deli d i $\left(\frac{d}{p}\right) = -1$. □

Teorema 1.18. *Prost broj 2 se grana u $\mathbb{Q}(\sqrt{d})$ ako i samo ako je $d \equiv 2 (mod\, 4)$ ili $d \equiv 3 (mod\, 4)$; 2 je inertno u $\mathbb{Q}(\sqrt{d})$ ako i samo ako je $d \equiv 5 (mod\, 8)$; 2 se cepa u $\mathbb{Q}(\sqrt{d})$ ako i samo ako je $d \equiv 1 (mod\, 8)$.*

Dokaz. Ako je $d \equiv 2$ ili $d \equiv 3 (\mathrm{mod}\, 4)$, tada prsten algebarskih celih je $A = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ i $A/2A \cong \mathbb{F}_2[X]/(X^2 - \bar{d})$ (sa istim dokazom kao u prethodnoj teoremi). Kako je $\bar{d} = \bar{0}$ ili $\bar{d} = \bar{1}$ sledi da je $X^2 - \bar{d}$ je kvadrat u $\mathbb{F}_2[X]$ ($X^2 - \bar{1} = (X - \bar{1})^2$). Zato $A/2A$ ima nenula nilpotentne elemente, pa se 2 grana u $\mathbb{Q}(\sqrt{d})$.

Ako je $d \equiv 1 (\mathrm{mod}\, 4)$ tada je

$$A = \mathbb{Z} + \mathbb{Z}\left(\frac{1 + \sqrt{d}}{2}\right) \cong \mathbb{Z}[X]/\left(X^2 - X - \frac{d-1}{4}\right),$$

zato što je $X^2 - X - \frac{d-1}{4}$ minimalni polinom od $\frac{1+\sqrt{d}}{2}$. Dakle, $A/2A \cong \mathbb{F}_2[X]/(X^2 - X - \bar{a})$ gde je $a = \frac{d-1}{4}$.

Ako je $a \equiv 1 (\mathrm{mod}\, 2)$ tada $d \equiv 5 (\mathrm{mod}\, 8)$. U ovom slučaju, kako je $X^2 - X - \bar{1} = X^2 + X + \bar{1} \in \mathbb{F}_2[X]$ ireducibilan nad $\mathbb{F}_2$, $A/2A$ je polje, pa je 2 inertno u $\mathbb{Q}(\sqrt{d})$.

Konačno, ako je $a \equiv 0 (\mathrm{mod}\, 2)$ tada je $d \equiv 1 (\mathrm{mod}\, 8), X^2 - X - \bar{a} = X^2 + X = X(X + \bar{1})$, pa je $A/2A$ proizvod dva polja i 2 se cepa u $\mathbb{Q}(\sqrt{d})$. □

Sada ćemo izneti nekoliko primera u kojima se primenjuju navedeni rezultati.

Primer 1. Neka je $K = \mathbb{Q}(\sqrt{17})$. Imamo da je $d = 17$ i $d \equiv 1 (\mathrm{mod}\, 4)$ odakle sledi da je prsten celih $A = \mathbb{Z} + \mathbb{Z}\left(\frac{1+\sqrt{17}}{2}\right)$. Faktorišimo brojeve $p < 20$ koji su prosti u $\mathbb{Z}$ na proizvod prostih elemenata iz A. Ako sam p nije prost, faktori će biti prosti u A zato što im je norma prost ceo broj p. Neka je $\alpha = \frac{1+\sqrt{17}}{2}$ i $\beta = \sqrt{17}$. Tada je $1 + \sqrt{17} = 0 \cdot 1 + 2 \cdot \frac{1}{2}(1 + \sqrt{17}) \Rightarrow 1 + \sqrt{17} \in A \Rightarrow \sqrt{17} \in A$, tj. $\beta \in A$ i $K = \mathbb{Q}[\beta] = \mathbb{Q}[\alpha]$.

$\underline{p = 2}$: Kako je $17 \equiv 1 (\mathrm{mod}\, 8)$ sledi da se 2 cepa u K.

$(2) = (2, \alpha - 2)(2, \alpha + 1)$.

$2 = \alpha^2 - \alpha - 2 = (\alpha - 2)(\alpha + 1)$.

$\underline{p=3:}$ $\left(\frac{d}{p}\right)=\left(\frac{17}{3}\right)=\left(\frac{2}{3}\right)=-1 \Rightarrow 3$ je inertan u K.

$\underline{p=5:}$ $\left(\frac{d}{p}\right)=\left(\frac{17}{5}\right)=\left(\frac{2}{5}\right)=-1 \Rightarrow 5$ je inertan u K.

$\underline{p=7:}$ $\left(\frac{d}{p}\right)=\left(\frac{17}{7}\right)=\left(\frac{3}{7}\right)=-1 \Rightarrow 7$ je inertan u K.

$\underline{p=11:}$ $\left(\frac{d}{p}\right)=\left(\frac{17}{11}\right)=\left(\frac{6}{11}\right)=-1 \Rightarrow 11$ je inertan u K.

$\underline{p=13:}$ Kako je $\left(\frac{d}{p}\right)=\left(\frac{17}{13}\right)=\left(\frac{4}{13}\right)=1$ sledi da se 13 cepa u K.

$(13)=(13,\beta^2-17)=(13,\beta^2-4)=(13,\beta-2)(13,\beta+2)$.

$13=(\beta-2)(\beta+2)$

$\underline{p=17:}$ Kako je $\left(\frac{d}{p}\right)=\left(\frac{17}{17}\right)=0$ sledi da se 17 grana u K.

$(17)=(\beta^2)=(\beta)^2$.

$17=\beta^2$

$\underline{p=19:}$ Kako je $\left(\frac{d}{p}\right)=\left(\frac{17}{19}\right)=1$ sledi da se 19 cepa u K.

$(19)=(19,\beta^2-17)=(19,\beta^2-36)=(19,\beta-6)(19,\beta+6)$

$19=(6-\beta)(6+\beta)$

Primer 2. Neka je $K=\mathbb{Q}(\sqrt{7})$. Imamo da je $d=7$ i $d\equiv 3(\text{mod } 4)$ odakle sledi da je prsten celih $A=\mathbb{Z}+\mathbb{Z}\sqrt{7}$. Faktorišimo brojeve $p<20$ koji su prosti u $\mathbb{Z}$ na proizvod prostih elemenata iz A. Ako sam p nije prost, faktori će biti prosti u A zato što im je norma prost ceo broj p.

$\underline{p=2:}$ Kako je $d\equiv 3(\text{mod } 4)$ sledi da se 2 cepa u K.

$(2)=(2,\alpha^2-7)=(2,\alpha^2-9)=(2,\alpha-3)(2,\alpha+3)$

$2=(3-\alpha)(3+\alpha)$

$\underline{p=3:}$ $\left(\frac{d}{p}\right)=\left(\frac{7}{3}\right)=1 \Rightarrow 3$ se cepa u K.

$(3)=(3,\alpha^2-7)=(3,\alpha^2-4)=(3,\alpha-2)(3,\alpha+2)$

$3=(-2+\alpha)(2+\alpha)$

$\underline{p=5:}$ $\left(\frac{d}{p}\right)=\left(\frac{7}{5}\right)=-1 \Rightarrow 5$ je inertan u K.

$\underline{p=7:}$ Kako je $\left(\frac{d}{p}\right)=\left(\frac{7}{7}\right)=0$ sledi da se 7 grana u K.

$(7)=(\alpha)^2$

$7=\alpha^2$

$\underline{p = 11:}$ $\left(\frac{d}{p}\right) = \left(\frac{7}{11}\right) = -1 \Rightarrow 11$ je inertan u K.

$\underline{p = 13:}$ $\left(\frac{d}{p}\right) = \left(\frac{7}{13}\right) = -1 \Rightarrow 13$ je inertan u K.

$\underline{p = 17:}$ $\left(\frac{d}{p}\right) = \left(\frac{7}{17}\right) = -1 \Rightarrow 17$ je inertan u K.

$\underline{p = 19:}$ Kako je $\left(\frac{d}{p}\right) = \left(\frac{7}{19}\right) = 1$ sledi da se 19 cepa u K.

$(19) = (19, \alpha^2 - d) = (19, \alpha^2 - 7) = (19, 4\alpha^2 - 9) = (19, 2\alpha - 3)(2\alpha + 3)$

$19 = (2\alpha - 3)(2\alpha + 3)$

1.7 Solovej-Štrasenov test primalnosti

U ovom delu rada prikazaćemo primenu kvadratnog zakona reciprociteta na Solovej-Štrasenov test primalnosti brojeva. Pozivamo se na Jakobijev simbol i njegove osobine. Prvo ćemo prikazati algoritam za računanje Jakobijevog simbola $\left(\frac{m}{n}\right)$ a onda ćemo prikazati i algoritam za Solovej-Štrasenov test primalnosti.

Primetimo da za cele brojeve m i n, $\left(\frac{m}{n}\right)$ zavisi jedino od m modulo n i zato problem algoritma za određivanje Jakobijevog simbola svodimo na računanje m modulo n. Kada je $m < n$, koristeći reciprocitet dolazimo do $\left(\frac{n}{m}\right)$ i ponovo problem redukujemo na isti način. Bazični slučajevi su 1. kada je jedan od m ili n 1; 2. Kada je $(m, n) > 1$; 3. $m = 2^k m'$ ili $n = 2^k m'$. Sledeći algoritam predstavlja algoritam za računanje Jakobijevog simbola $\left(\frac{m}{n}\right)$.

Algorithm 1 JAKOBIJEV SIMBOL $\left(\frac{m}{n}\right)$

if $(m, n) > 1$ **then**
  return 0
else if $m = 1$ **then**
  return 1
else if $m = 2$ **then**
  return $(-1)^{\frac{n-1}{2}}$
else if $m = 2^k m'$ **then**
  return $\left(\frac{2}{n}\right)^k \left(\frac{m'}{n}\right)$
else if $n = 2^k n'$ **then**
  return $\left(\frac{m}{2}\right)^k \left(\frac{m}{n'}\right)$
end if
//bazični slučajevi su završeni
if $m > n$ **then**
  return $\left(\frac{m \bmod n}{n}\right)$
else
  return $(-1)^{\frac{m-1}{2}\frac{n-1}{2}} \left(\frac{n}{m}\right)$
end if

Pređimo sada na test primalnosti. Uopštena filozofija testova primalnosti je sledeća:

- Naći osobinu koju zadavoljovaju tačno prosti brojevi.
- Naći efikasan način za proveru zadovoljenja ove osobine na proizvoljnim brojevima.
- Pokazati da za bilo koji složen broj, može se ,,lako" doći do toga da data osobina prostog broja nije zadovoljena.

Kod Solovej-Štrasenovog testa primalnosti koristimo grupu $E(n)$ koja definisana na sledeći način:

$$E(n) = \{a \in (\mathbb{Z}/(n))^* : \left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} (\mathrm{mod}\, n)\}.$$

Na primer, $E(65) = \{1, 8, 14, 18, 47, 51, 57, 64\}$.

Pre nego što pređemo na lemu na kojoj je baziran Solovej-Štrasenov test primalnosti, uvedimo pojam Karmajklovog broja i neke rezultate o ovom broju koji nam je potreban u daljem radu.

Definicija 1.8. *Ako je n složen broj tako da je $a^{n-1} \equiv 1 (mod\, n)$ za svako $a \in (\mathbb{Z}/(n))^*$, tada za n kažemo da je Karmajklov broj.*

Teorema 1.19. *Ako je n Karmajklov broj, tada je n neparan, kvadratno slobodan i deljiv sa najmanje 3 različita prosta broja.*

Solovej-Štrasenov test primalnosti je baziran na sldećoj lemi.

Lema 1.5. *Neka je n neparan ceo broj i $n \geq 3$. Tada je n prost ako i samo ako $E(n) = (\mathbb{Z}/(n))^*$.*

Dokaz. Ako je n neparan prost broj, tada je $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} (\mathrm{mod}\, n)$ na osnovu Teoreme 1.4 pod 1.

Neka je sada $E(n) = (\mathbb{Z}/(n))^*$. Pretpostavimo suprotno, tj. neka je n složen broj. Tada je

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

za svako $a \in (\mathbb{Z}/(n))^*$. Zato je n Karmajklov broj i na osnovu Teoreme 1.19., n mora biti kvadratno slobodan. Zato n možemo predstaviti kao $n = pr$ gde je p prost, $r > 1$ i $(p, r) = 1$. Neka je g kvadratni neostatak modulo p i neka je $a \equiv g (\mathrm{mod}\, p)$ i $a \equiv 1 (\mathrm{mod}\, r)$. Na osnovu Teoreme 1.9. imamo:

$$\left(\frac{a}{n}\right) = \left(\frac{a}{pr}\right) = \left(\frac{a}{p}\right)\left(\frac{a}{r}\right) = \left(\frac{g}{p}\right)\left(\frac{1}{r}\right) = (-1)(+1) = -1.$$

Kako je na osnovu pretpostavke $\left(\frac{a}{n}\right) \equiv a^{\frac{n-1}{2}} (\mathrm{mod}\, n)$ za svako $a \in (\mathbb{Z}/(n))^*$, sledi da je $a^{\frac{n-1}{2}} \equiv -1 (\mathrm{mod}\, r)$. Ali ovo je u kontradikciji sa $a \equiv 1 (\mathrm{mod}\, r)$. □

Konstruišimo sada Solovej-Štrasenov test primalnosti za neparne brojeve koji su veći ili jednaki od 3.

Algorithm 2 SOLOVAY-STRASSEN(n)

1: Izaberi slučajan broj a iz skupa $\{1, 2, ..., n-1\}$
2: **if** $(a, n) \neq 1$ **then**
3: **return** SLOŽEN
4: **end if**
5: **if** $\left(\frac{a}{n}\right) \not\equiv a^{\frac{n-1}{2}} (\mathrm{mod}\, n)$ **then**
6: **return** SLOŽEN
7: **else**
8: **return** PROST
9: **end if**

Napomene

Definicije i rezultati o kvadratnim ostacima se mogu naći u [2] i [5]. Prvi dokaz kvadratnog zakona reciprociteta koji je ovde prikazan izveden je uz korišćenje [6]. Razmatranja u vezi Jakobijevog simbola, Ajzenštajnovog dokaza i dokaza uz pomoć Gausovih kvadradnih suma su prikazana uz korišćenje [2]. Za primenu Gausovog zakona reciprociteta na faktorizaciju u kvadratnim raširenjima polja, korišćena je [6]. Za razmatranja Solovaj-Štrasenovog testa primalnosti korišćena su izlaganja iz [1] i [8].

2 Kubni zakon reciprociteta

U prethodnoj sekciji smo videli da kvadratni zakon reciprociteta daje odgovor na pitanje: za koje proste brojeve p kongruencija $x^2 \equiv a(\mathrm{mod}\, p)$ je rešiva. Ovde je a fiksiran ceo broj. Ako se isto pitanje posmatra za kongruencije $x^n \equiv a(\mathrm{mod}\, p)$, gde je n fiksiran pozitivan ceo broj, dolazimo do zakona reciprociteta višeg stepena od 2. Kada je $n = 3$ odnosno $n = 4$ govorimo o kubnom odnosno o bikvadratnom zakonu reciprociteta.

Gaus u uvodu u njegova dva poznata rada ,, Theorie der biquadratischen Reste I, II" tvrdi da teorija kvadratnih ostataka je dovedena do perfekcije tako da se više ništa ne može poželeti. Sa druge strane, ,, Teorija kubnih i bikvadratnih ostataka je teža."

Zanimljivo je da je Gaus otkrio i formulisao bikvadratni zakon reciprociteta, ali da ga nije kompletno dokazao. Prvi kompletni dokazi kubnog i bikvadratnog zakona reciprociteta se pripisuju Ajzenštajnu.

Za izučavanje kubnog zakona reciprociteta neophodno je da navedemo osnovna svojstva prstena $\mathbb{Z}[\omega]$ gde je $\omega = \frac{-1+\sqrt{-3}}{2}$.

2.1 Prsten $\mathbb{Z}[\omega]$

U ovoj podsekciji dokazaćemo da je prsten $\mathbb{Z}[\omega]$ euklidski domen a samim tim i domen sa jedinstvenom faktorizacijom. Zatim ćemo izučavati inverzibilne i proste elemente ovog prstena.

Definicija 2.1. *Integralni domen R se naziva euklidskim domenom ako postoji funkcija (norma) $N : R\backslash\{0\} \to \mathbb{N}_0$ tako da ako $a, b \in R, b \neq 0$, postoje $c, d \in R$ sa osobinom $a = cb + d$ pri čemu ili važi da je $d = 0$ ili je $N(d) < N(b)$. .*

Teorema 2.1. *$\mathbb{Z}[\omega] = \{a + b\omega | a, b \in \mathbb{Z}\}$ je eukldiski domen.*

Dokaz. Pre svega primetimo da je $\omega^2 = \frac{-1-\sqrt{-3}}{2}$ kao i da važi $1 + \omega + \omega^2 = 0$. Dokažimo prvo da je $\mathbb{Z}[\omega]$ integralni domen. $\mathbb{Z}[\omega]$ je zatvoren u odnosu na sabiranje i množenje. Naime, $a + b\omega + c + d\omega = a + c + (b + d)\omega$ i $(a + b\omega)(c + d\omega) = ac + (ad + bc)\omega + bd\omega^2 = ac + (ad + bc)\omega + bd(-1 - \omega) = ac - bd + (ad + bc - bd)\omega$. Zato je $\mathbb{Z}[\omega]$ prsten. Kako je $\mathbb{Z}[\omega]$ podskup skupa kompleksnih brojeva sledi da je $\mathbb{Z}[\omega]$ integralni domen.

Dokažimo sada da $\mathbb{Z}[\omega]$ zadovoljava drugi deo definicije euklidskog domena. Primetimo da je $\mathbb{Z}[\omega]$ zatvoren u odnosu na kompleksnu konjugaciju. Naime, kako je $\overline{\sqrt{-3}} = \overline{\sqrt{3}i} = -\sqrt{-3}$ sledi da je $\overline{\omega} = \omega^2$. Zato, ako $\alpha = a + b\omega \in \mathbb{Z}[\omega]$, tada $\overline{\alpha} = a + b\overline{\omega} = a + b\omega^2 = a + b(-1 - \omega) = a - b - b\omega \in \mathbb{Z}[\omega]$.

Za element $\alpha = a + b\omega \in \mathbb{Z}[\omega]$ definišimo normu na sledeći način $N(\alpha) = \alpha\overline{\alpha} = a^2 - ab + b^2$. Neka je $\alpha, \beta \in \mathbb{Z}[\omega]$ i pretpostavimo da je $\beta \neq 0$. Tada je $\frac{\alpha}{\beta} = \frac{\alpha\overline{\beta}}{\beta\overline{\beta}} = r + s\omega$ gde su r i s racionalni brojevi. Ovde smo koristili činjenicu da je $\beta\overline{\beta} = N(\beta)$ pozitivan ceo broj i $\alpha\overline{\beta} \in \mathbb{Z}[\omega]$

jer $\alpha, \overline{\beta} \in \mathbb{Z}[\omega]$. Neka su m i n celi brojevi takvi da je $|r-m| \leq \frac{1}{2}$ i $|s-n| \leq \frac{1}{2}$. Tada stavimo da je $\gamma = m + n\omega$. Sada je $N(\frac{\alpha}{\beta} - \gamma) = (r-m)^2 - (r-m)(s-n) + (s-n)^2 \leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1$. Neka je $\rho = \alpha - \gamma\beta$. Tada je ili $\rho = 0$ ili je $N(\rho) = N(\beta(\frac{\alpha}{\beta} - \gamma)) = N(\beta)N(\frac{\alpha}{\beta} - \gamma) < N(\beta)$. □

Teorema 2.2. *$\alpha \in \mathbb{Z}[\omega]$ je inverzibilni element ako i samo ako je $N(\alpha) = 1$. Inverzibilni elementi u $\mathbb{Z}[\omega]$ su $1, -1, \omega, -\omega, \omega^2, -\omega^2$.*

Dokaz. Ako je $N(\alpha) = 1$ onda je $\alpha\overline{\alpha} = 1$ odakle sledi da je α inverzibilan jer $\overline{\alpha} \in \mathbb{Z}[\omega]$.

Ako je α inverzibilni element, onda postoji $\beta \in \mathbb{Z}[\omega]$ tako da je $\alpha\beta = 1$ odakle sledi $N(\alpha)N(\beta) = 1$. Kako su $N(\alpha)$ i $N(\beta)$ pozitivni celi brojevi sledi da je $N(\alpha) = 1$.

Pretpostavimo sada da je $\alpha = a + b\omega$ inverzibilan element. Tada $1 = a^2 - ab + b^2$ odakle množenjem sa 4 i sređivanjem dobijamo $4 = (2a-b)^2 + 3b^2$. Razlikujemo dva slučaja:

1) $2a - b = \pm 1, b = \pm 1$

2) $2a - b = \pm 2, b = 0$.

Rešavanje ovih parova jednačina nam daje rezultate za $\alpha : 1, -1, \omega, -\omega, -1-\omega$ i $1+\omega$. Uzimajući u obzir da je $\omega^2 + \omega + 1 = 0$ dva poslednja elementa su ω^2 i $-\omega^2$. □

Pređimo sada na izučavanje prostih elemenata u $\mathbb{Z}[\omega]$. Primetimo da prosti elementi u skupu $\mathbb{Z}$ ne moraju biti prosti i u $\mathbb{Z}[\omega]$. Na primer, $7 = (3+\omega)(2-\omega)$. Zato ćemo u nastavku proste elemente skupa $\mathbb{Z}$ nazivati racionalnim prostim.

Teorema 2.3. *Ako je π prost u $\mathbb{Z}[\omega]$, tada postoji racionalan prost broj p tako da važi $N(\pi) = p$ ili $N(\pi) = p^2$. U prvom slučaju π nije asociran sa racionalnim prostim p; u drugom slučaju π je asociran sa p.*

Dokaz. Imamo da je $N(\pi) = n > 1$ odnosno $\pi\overline{\pi} = n$. Kao što znamo n se može prikazati kao proizvod racionalnih prostih. Zato $\pi \mid p$ za neki racionalan prost broj p. Ako je $p = \pi\gamma, \gamma \in \mathbb{Z}[\omega]$, tada je $N(\pi)N(\gamma) = N(p) = p^2$. Zato je ili $N(\pi) = p^2$ i $N(\gamma) = 1$ ili $N(\pi) = p$. U prvom slučaju γ je inverzibilan i zato je π asociran sa p. U drugom slučaju ako je $\pi = uq$, gde je u inverzibilan i q racionalan prost, tada je $p = N(\pi) = N(u)N(q) = q^2$, što je kontradikcija odakle sledi da π nije asociran racionalnom prostom broju. □

Teorema 2.4. *Ako je $\pi \in \mathbb{Z}[\omega]$ tako da važi $N(\pi) = p$, gde je p racionalan prost, tada je π prost u $\mathbb{Z}[\omega]$.*

Dokaz. Ako π ne bi bio prost u $\mathbb{Z}[\omega]$, tada bi $\pi = \rho\gamma$, gde su $N(\rho), N(\gamma) > 1$. Tada je $p = N(\pi) = N(\rho)N(\gamma)$, što nije tačno jer je p racionalan prost. Zato je π prost u $\mathbb{Z}[\omega]$. □

Teorema 2.5. *Neka je p racionalan prost. Ako je $p \equiv 2 (mod\, 3)$, tada je p prost u $\mathbb{Z}[\omega]$. Ako je $p \equiv 1 (mod\, 3)$, tada je $p = \pi\overline{\pi}$, gde je π prost u $\mathbb{Z}[\omega]$. Takođe, $3 = -\omega^2(1-\omega)^2$, i $1-\omega$ je prost u $\mathbb{Z}[\omega]$.*

Dokaz. Neka je $p \equiv 2(\mathrm{mod}\, 3)$. Ako p ne bi bio prost, tada imamo $p = \pi\gamma$, gde je $N(\pi) > 1, N(\gamma) > 1$. Zato je $p^2 = N(\pi)N(\gamma)$ i $N(\pi) = p$. Neka je $\pi = a + b\omega$. Tada je $p = a^2 - ab + b^2$ odnosno $4p = (2a - b)^2 + 3b^2$ odakle sledi da je $p \equiv (2a - b)^2(\mathrm{mod}\, 3)$, što je kontradikcija jer 2 nije kvadrat mod 3.

Pretpostavimo sada da je $p \equiv 1(\mathrm{mod}\, 3)$. Na osnovu kvadratnog zakona reciprociteta imamo da je

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

Dakle, postoji $a \in \mathbb{Z}$ tako da je $a^2 \equiv -3(\mathrm{mod}\, p)$ odnosno $pb = a^2 + 3$ za neko $b \in \mathbb{Z}$. Zato p deli $(a + \sqrt{-3})(a - \sqrt{-3}) = (a + 1 + 2\omega)(a - 1 - 2\omega)$. Ako bi p bio prost u $\mathbb{Z}[\omega]$, tada bi p delio jedan od navedenih faktora ali ovo je nemoguće jer $p \neq 2$ i $\frac{2}{p} \notin \mathbb{Z}$. Zato je $p = \pi\gamma$ gde su π i γ elementi koji nisu inverzibilni. Prelazeći na norme u poslednjoj jednakosti dobijamo $p^2 = N(\pi)N(\gamma)$ i $p = N(\pi) = \pi\overline{\pi}$.

Poslednja stavka teoreme sledi iz sledećeg: iz $x^3 - 1 = (x-1)(x-\omega)(x-\omega^2)$ sledi $x^2 + x + 1 = (x-\omega)(x-\omega^2)$. Uzimajući da je $x = 1$ sledi $3 = (1-\omega)(1-\omega^2) = (1+\omega)(1-\omega)^2 = -\omega^2(1-\omega)^2$. Prelazeći na norme dobijamo $9 = N(1-\omega)^2$ i $3 = N(1-\omega)$ Zato je $1 - \omega$ prost. □

Kao i u prstenu $\mathbb{Z}$, kongruencije su veoma važne u prstenu $\mathbb{Z}[\omega]$. Ako su $\alpha, \beta, \gamma \in \mathbb{Z}[\omega]$ i $\gamma \neq 0$ element koji nije inverzibilan, kažemo da je $\alpha \equiv \beta(\mathrm{mod}\, \gamma)$ ako γ deli $\alpha - \beta$. Kao i u prstenu $\mathbb{Z}$ klase kongruencija modulo γ formiraju prsten $\mathbb{Z}[\omega]/\gamma\mathbb{Z}[\omega]$, koji se zove prsten ostataka po modulu γ.

Teorema 2.6. *Neka je $\pi \in \mathbb{Z}[\omega]$ prost. Tada je $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ konačno polje sa $N(\pi)$ elemenata.*

Dokaz. Pokažimo prvo da je $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ polje. Neka je $\alpha \in \mathbb{Z}[\omega]$ tako da je $\alpha \not\equiv 0(\mathrm{mod}\, \pi)$. Kako je $\mathbb{Z}[\omega]$ glavnoidealski (kao euklidski), sledi da postoje $\beta, \gamma \in \mathbb{Z}[\omega]$, takvi da je $\beta\alpha + \gamma\pi = 1$. Zato je $\beta\alpha \equiv 1(\mathrm{mod}\, \pi)$, što nam pokazuje da je klasa ostataka od α inverzibilni element u $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$.

Da bi smo pokazali da $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ ima $N(\pi)$ elemenata, posmatrajmo pojedinačne slučajeve iz Teoreme 2.5.

Pretpostavimo da je $\pi = q$ racionalan prost kongruentan sa 2 modulo 3. Tvrdimo da je $\{a + b\omega | 0 \leq a < q, 0 \leq b < q\}$ kompletan skup reprezentativnih koseta. Ovo će pokazati da $\mathbb{Z}[\omega]/q\mathbb{Z}[\omega]$ ima $q^2 = N(q)$ elemenata. Neka je $\mu = m + n\omega \in \mathbb{Z}[\omega]$. Tada je $m = qs + a$ i $n = qt + b$, gde $s, t, a, b \in \mathbb{Z}$ i $0 \leq a, b < q$. Važi da je $\mu \equiv a + b\omega(\mathrm{mod}\, q)$. Naime, pretpostavimo da je $a + b\omega \equiv a' + b'\omega(\mathrm{mod}\, q)$, gde je $0 \leq a, b, a', b' < q$. Tada je $\frac{a-a'}{q} + (\frac{b-b'}{q})\omega \in \mathbb{Z}[\omega]$, odakle sledi $\frac{a-a'}{q}, \frac{b-b'}{q} \in \mathbb{Z}$. Ovo je moguće jedino ako je $a = a'$ i $b = b'$.

Pretpostavimo sada da je $p \equiv 1(\mathrm{mod}\, 3)$ racionalan prost i $\pi\bar{\pi} = N(\pi) = p$. Tvrdimo da je $\{0, 1, ..., p-1\}$ kompletan skup reprezentativnih koseta. Ovo će pokazati da $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ ima $p = N(\pi)$ elemenata. Neka je $\pi = a + b\omega$. Kako je $p = a^2 - ab + b^2$ sledi da $p \nmid b$. Neka je $\mu = m + n\omega$. Postoji ceo broj c tako da $cb \equiv n(\mathrm{mod}\, p)$. Tada je $\mu - c\pi \equiv m - ca(\mathrm{mod}\, p)$ i

$\mu \equiv m - ca (\mathrm{mod}\, \pi)$. Svaki element iz $\mathbb{Z}[\omega]$ je kongruentan racionalnom celom modulo π. Ako $l \in \mathbb{Z}$, tada $l = sp + r$, gde $s, r \in \mathbb{Z}$ i $0 \leq r < p$. Zato je $l \equiv r (\mathrm{mod}\, p)$ i $l \equiv r (\mathrm{mod}\, \pi)$. Pokazali smo da svaki element iz $\mathbb{Z}[\omega]$ je kongruentan elementu iz skupa $\{0, 1, 2, ..., p-1\}$ modulo π. Ako je $r \equiv r' (\mathrm{mod}\, \pi)$ gde su $r, r' \in \mathbb{Z}$ i $0 \leq r, r' < p$, tada je $r - r' = \pi\gamma$ i $(r - r')^2 = pN(\gamma)$, odakle sledi $p \mid r - r'$. Zato je $r = r'$. □

2.2 Kubni karakter ostatka

Kubni karakter ostatka u teoriji kubnih ostataka ima istu ulogu kao Ležandrov simbol u teoriji kvadratnih ostataka. Sada ćemo dati nekoliko teorema koje vode definiciji kubnog karaktera ostatka.

Teorema 2.7. *Neka su $\pi, \alpha \in \mathbb{Z}[\omega]$ i π prost. Ako $\pi \nmid \alpha$, tada je $\alpha^{N(\pi)-1} \equiv 1 (mod\, \pi)$.*

Ako je norma od π različita od 3, tada su klase ostataka od $1, \omega$ i ω^2 različite u $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$. Naime, uzmimo da je $\omega \equiv 1 (\mathrm{mod}\, \pi)$. Tada $\pi \mid (1-\omega)$, i kako je $1-\omega$ prost, π i $1-\omega$ su asocirani. Zato je $N(\pi) = N(1-\omega) = 3$, što je kontradikcija.

Kako je $\{1, \omega, \omega^2\}$ ciklična grupa reda 3 sledi da 3 deli red grupe inverziblinih elemenata $(\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega])^*$, tj. $3 \mid N(\pi) - 1$. Ovo se može pokazati koristeći Teoremu 2.6. Ako je $\pi = q$, racionalan prost, tada je $N(\pi) = q^2 \equiv 1 (\mathrm{mod}\, 3)$. Ako je π takav da je $N(\pi) = p$, tada je $p \equiv 1 (\mathrm{mod}\, 3)$.

Teorema 2.8. *Pretpostavimo da je π prost takav da $N(\pi) \neq 3$ i $\pi \nmid \alpha$. Tada postoji jedinstveni ceo broj $m = 0, 1$ ili 2 tako da je $\alpha^{\frac{N(\pi)-1}{3}} \equiv \omega^m (mod\, \pi)$.*

Dokaz. Imamo da $\pi \mid \alpha^{N(\pi)-1} - 1$. Sada je:

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

Kako je π prost sledi da on mora deliti jedan od tri faktora na desnoj strani poslednje jednakosti. Na osnovu prethodnog razmatranja π može deliti najviše jedan faktor odakle sledi dokaz teoreme. □

Sada možemo dati definiciju kubnog karaktera ostatka.

Definicija 2.2. *Ako je $N(\pi) \neq 3$, kubni karakter ostatka od α modulo π je dat sa:*

- $\left(\frac{\alpha}{\pi}\right)_3 = 0$ *ako* $\pi \mid \alpha$.
- $\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 (mod\, \pi)$, *gde je* $\left(\frac{\alpha}{\pi}\right)_3$ *jednako* $1, \omega$ *ili* ω^2.

U sledećim teoremama ispitaćemo neke osobine kubnog karaktera ostatka.

Teorema 2.9. *Za kubni karakter ostatka važi sledeće:*

1. $\left(\frac{\alpha}{\pi}\right)_3 = 1$ *ako i samo ako je* $x^3 \equiv \alpha (mod\, \pi)$ *rešiva, tj. ako i samo ako je* α *kubni ostatak.*
2. $\alpha^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 (mod\, \pi)$.

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

4. *Ako je* $\alpha \equiv \beta (mod\, \pi)$, *tada je* $\left(\frac{\alpha}{\pi}\right)_3 = \left(\frac{\beta}{\pi}\right)_3$.

Dokaz. Dokaz pod 1. : Ako $x^3 \equiv \alpha (\mathrm{mod}\, \pi)$ ima rešenja, tada je na osnovu Teoreme 2.6 $\alpha^{\frac{N(\pi)-1}{3}} \equiv 1 (\mathrm{mod}\, \pi)$ odakle sledi da je $\left(\frac{\alpha}{\pi}\right) = 1$.

Obrnuto, neka je g primitivni koren iz $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$. Tada za $\alpha = g^r$ nalazimo da je $g^{\frac{r(N(\pi)-1)}{3}} \equiv 1 (\mathrm{mod}\, \pi)$ pa je

$$\frac{r(N(\pi)-1)}{3} \equiv 0 (\mathrm{mod}\, N(\pi)-1).$$

Dakle, $3 \mid r$, i α je kub mod π. Otuda jednačina $x^3 \equiv \alpha (\mathrm{mod}\, \pi)$ ima rešenje.

Dokaz pod 2. sledi direktno iz definicije.

Dokaz pod 3.:

$$\left(\frac{\alpha\beta}{\pi}\right)_3 \equiv (\alpha\beta)^{\frac{N(\pi)-1}{3}} \equiv \alpha^{\frac{N(\pi)-1}{3}} \beta^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\alpha}{\pi}\right)_3 \left(\frac{\beta}{\pi}\right)_3 (\mathrm{mod}\, \pi).$$

Dokaz pod 4. : Ako je $\alpha \equiv \beta (\mathrm{mod}\, \pi)$, tada je

$$\left(\frac{\alpha}{\pi}\right)_3 \equiv \alpha^{\frac{N(\pi)-1}{3}} \equiv \beta^{\frac{N(\pi)-1}{3}} \equiv \left(\frac{\beta}{\pi}\right)_3 (\mathrm{mod}\, \pi).$$

□

U daljem izlaganju o kubnim karakterima ostatka uvodimo sledeću oznaku $\chi_\pi(\alpha) = \left(\frac{\alpha}{\pi}\right)_3$.

Teorema 2.10. *Za kubni karakter ostatka važe sledeće osobine:*

1. $\overline{\chi_\pi(\alpha)} = \chi_\pi(\alpha)^2 = \chi_\pi(\alpha^2)$.
2. $\overline{\chi_\pi(\alpha)} = \chi_{\bar{\pi}}(\bar{\alpha})$.

Dokaz. Dokaz pod 1.: $\chi_\pi(\alpha)$ je po definiciji $1, \omega$ ili ω^2, i svaki od njih od ovih brojeva kada se kvadrira je jednak svom konjugatu.

Dokaz pod 2.: Kako je

$$\alpha^{\frac{N(\pi)-1}{3}} \equiv \chi_\pi(\alpha) (\mathrm{mod}\, \pi),$$

dobijamo da je

$$\bar{\alpha}^{\frac{N(\pi)-1}{3}} \equiv \overline{\chi_\pi(\alpha)} (\mathrm{mod}\, \bar{\pi}).$$

Kako je $N(\bar{\pi}) = N(\pi)$ sledi da je $\chi_{\bar{\pi}}(\overline{\alpha}) \equiv \overline{\chi_\pi(\alpha)} (\mathrm{mod}\, \bar{\pi})$ i zato je $\overline{\chi_\pi(\alpha)} = \chi_{\bar{\pi}}(\bar{\alpha})$. □

Posledica 2.1. *Ako je n racionalan ceo uzajamno prost sa pozitivnim racionalnim prostim q, tada je $\chi_q(\bar{\alpha}) = \chi_q(\alpha^2)$ i $\chi_q(n) = 1$.*

Dokaz. Kako je $\bar{q} = q$ imamo $\chi_q(\bar{\alpha}) = \chi_{\bar{q}}(\bar{\alpha}) = \overline{\chi_q(\alpha)} = \chi_q(\alpha^2)$ odakle sledi dokaz za prvu relaciju.

Kako je $\bar{n} = n$ imamo $\chi_q(n) = \overline{\chi_q(n)} = \chi_q(n)^2$. Kako je $\chi_q(n) \neq 0$ sledi da je $\chi_q(n) = 1$. □

U Posledici 2.1 imamo da je n kubni ostatak mod q. Zato, ako su $q_1 \neq q_2$ dva racionalna prosta kongruentna sa 2 mod 3, tada imamo (trivijalno) $\chi_{q_1}(q_2) = \chi_{q_2}(q_1)$. Ovo je specijalni slučaj kubnog zakona reciprociteta. Da bismo formulisali opšti zakon, potrebno je da definišemo pojam primarnog broja.

Definicija 2.3. *Neka je π prost u $\mathbb{Z}[\omega]$. Za π kažemo da je primarni ako je $\pi \equiv 2 (mod\, 3)$.*

Ako je $\pi = q$ racionalan, onda nema ništa novo po pitanju prethodne definicije. Ako je $\pi = a + b\omega$ kompleksan prost, tada je prethodna definicija ekvivalentna sa $a \equiv 2 (\mathrm{mod}\, 3)$ i $b \equiv 0 (\mathrm{mod}\, 3)$.

Teorema 2.11. *Neka je $N(\pi) = p \equiv 1 (mod\, 3)$. Tada među svim asociranim elementima sa π postoji tačno jedan koji je primarni.*

Dokaz. Neka je $\pi = a + b\omega$. Asocirani elementi sa π su $\pi, \omega\pi, \omega^2\pi, -\pi, -\omega\pi$ i $-\omega^2\pi$. Zapišimo asocirane elemente sada preko a i b :

(a) $a + b\omega$.

(b) $-b + (a - b)\omega$.

(c) $(b - a) - a\omega$.

(d) $-a - b\omega$.

(e) $b + (b - a)\omega$.

(f) $(a - b) + a\omega$.

Kako je $p = a^2 - ab + b^2$, sledi da jedan od a i b nije deljiv sa 3. Uzimajući u obzir (a) i (b) možemo pretpostaviti da $3 \nmid a$. Posmatrajući (a) i (d) možemo dalje pretpostaviti da je $a \equiv 2 (\mathrm{mod}\, 3)$. Sa ovim pretpostavkama iz $p = a^2 - ab + b^2$ sledi $1 \equiv 4 - 2b + b^2 (\mathrm{mod}\, 3)$ ili $b(b-2) \equiv 0 (\mathrm{mod}\, 3)$. Ako $3 \mid b$, tada je $a + b\omega$ primaran. Ako je $b \equiv 2 (\mathrm{mod}\, 3)$, tada je $b + (b-a)\omega$ primaran.

Da bismo dokazali jedinstvenost, pretpostavimo da je $a + b\omega$ primaran. Posmatrajući klasu kongruencije prvog člana od (b) do (e) vidimo da ni jedan od ovih elemenata nije primaran. Ni elemenat u (f) nije primaran jer koeficijent uz ω, a nije deljiv sa 3. □

Na primer, $3+\omega$ je prost jer je $N(3+\omega)=7$, i $-\omega^2(3+\omega)=2+3\omega$ je primaran i asociran sa $3+\omega$.

Sada možemo iskazati kubni zakon reciprociteta.

Kubni zakon reciprociteta: Neka su π_1 i π_2 primarni, $N(\pi_1), N(\pi_2) \neq 3$, i $N(\pi_1) \neq N(\pi_2)$. Tada je

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

Pre nego što pređemo na dokaz kubnog zakona reciprociteta istaknimo dve važne napomene.

1. Postoje tri slučaja za razmatranje kubnih ostataka. Naime, kada su oba π_1 i π_2 racionalni, zatim kada je π_1 racionalan i π_2 kompleksan i kada su oba π_1 i π_2 kompleksni. Prvi slučaj, kao što smo videli, je trivijalan.

2. Kubni karakter inverzibilnih elemenata se može posmatrati na sledeći način. Kako je $-1=(-1)^3$ imamo da je $\chi_\pi(-1)=1$ za sve proste π. Za $N(\pi)\neq 3$, iz Teoreme 2.8 sledi da je $\chi_\pi(\omega)=\omega^{\frac{N(\pi)-1}{3}}$. Zato je $\chi_\pi(\omega)=1,\omega$ ili ω^2 u zavisnosti od toga da li je $N(\pi)\equiv 1,4$ ili 7 mod 9.

2.3 Gausove i Jakobijeve sume

Za dokaz kubnog zakona reciprociteta potrebne su nam Gausove i Jakobijeve sume. Zato ćemo sada izneti neke rezultate vezane za pomenute sume.

Neka $\mathbb{F}_p$ označava konačno polje sa p elemenata. Multiplikativni karakter na $\mathbb{F}_p$ je homomorfizam $\chi : \mathbb{F}_p^* \to \mathbb{C}^*$. Ležandrov simbol $\left(\frac{a}{p}\right)$ je primer jednog takvog karaktera. Trivijalni karakter χ_0 definisan sa $\chi_0(a) = 1$ za svako $a \in \mathbb{F}_p^*$ je još jedan primer multiplikativnog karaktera. Stavimo da je $\chi(0) = 0$ za $\chi \neq \chi_0$ i $\chi_0(0) = 1$.

Teorema 2.12. *Neka je χ multiplikativni karakter i $a \in \mathbb{F}_p^*$. Tada je*

1. $\chi(1) = 1$.
2. $\chi(a)$ *je* $(p-1)$*-ti koren jedinice.*
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Dokaz. Dokaz pod 1.: $\chi(1) = \chi(1 \cdot 1) = \chi(1)\chi(1)$. Kako je $\chi(1) \neq 0$ sledi da je $\chi(1) = 1$.

Dokaz pod 2.: Kako je $a^{p-1} = 1$ sledi da je $1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}$.

Dokaz pod 3.: Kako je $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$ sledi da je $\chi(a^{-1}) = \chi(a)^{-1}$. Sada $\chi(a)^{-1} = \overline{\chi(a)}$ sledi iz činjenice da je $\chi(a)$ kompleksan broj apsolutne vrednosti 1 na osnovu dela 2. ove teoreme. □

Teorema 2.13. *Neka je χ multiplikativni karakter. Ako je $\chi \neq \chi_0$, tada je $\sum_t \chi(t) = 0$, gde se suma vrši po svim elementima $t \in \mathbb{F}_p$. Ako je $\chi = \chi_0$, tada je vrednost sume jednaka p, gde je p racionalan prost.*

Dokaz. Drugi deo teoreme je očigledan jer je $\chi(t) = 1, t \in \mathbb{F}_p$. Dokažimo prvi deo. Neka je $a \in \mathbb{F}_p^*$ tako da je $\chi(a) \neq 1$. Neka $T = \sum_t \chi(t)$. Tada je

$$\chi(a)T = \sum_t \chi(a)\chi(t) = \sum_t \chi(at) = T.$$

Poslednja jednakost važi jer at prolazi skupom $\mathbb{F}_p$ kada t takođe prolazi skupom $\mathbb{F}_p$. Kako je $\chi(a)T = T$ i $\chi(a) \neq 1$ sledi da je $T = 0$. □

U podsekciji 1.5 definisali smo kvadratne Gausove sume. Sledeća definicija uopštava definiciju kvadratnih Gausovih suma.

Definicija 2.4. *Za $a \in \mathbb{F}_p^*$, definišiemo Gausovu sumu na sledeći način:*

$$g_a(\chi) = \sum_{t \in \mathbb{F}_p} \chi(t)\zeta^{at},$$

gde je $\zeta = e^{\frac{2\pi i}{p}}$ *primitivni p-ti koren jedinice.*

Teorema 2.14. *Ako je* $a \neq 0$ *i* $\chi \neq \chi_0$*, tada je* $g_a(\chi) = \chi(a^{-1})g_1(\chi)$*. Ako je* $a \neq 0$ *i* $\chi = \chi_0$ *tada je* $g_a(\chi_0) = 0$*. Ako je* $a = 0$ *i* $\chi \neq \chi_0$*, tada je* $g_0(\chi) = 0$*. Ako je* $a = 0$ *i* $\chi = \chi_0$ *tada je* $g_0(\chi_0) = p$*.*

Dokaz. Pretpostavimo da je $a \neq 0$ i $\chi \neq \chi_0$. Tada je

$$\chi(a)g_a(\chi) = \chi(a)\sum_t \chi(t)\zeta^{at} = \sum_t \chi(at)\zeta^{at} = g_1(\chi).$$

Ovim smo dokazali prvi deo teoreme.

Ako je $a \neq 0$, tada je

$$g_a(\chi_0) = \sum_t \chi_0(t)\zeta^{at} = \sum_t \zeta^{at} = 0.$$

Primetimo da je $g_0(\chi) = \sum_t \chi(t)\zeta^{0t} = \sum_t \chi(t)$. Ako je $\chi = \chi_0$ rezultat je p; ako je $\chi \neq \chi_0$, rezultat je nula na osnovu Teoreme 2.13. □

U daljem tekstu $g_1(\chi)$ označavaćemo sa $g(\chi)$.

Teorema 2.15. *Ako je* $\chi \neq \chi_0$*, tada je* $|g(\chi)| = \sqrt{p}$*.*

Dokaz. Dokaz ove teoreme je sličan dokazu Teoreme 1.14.

Ideja dokaza jeste da sumu $\sum_a g_a(\chi)\overline{g_a(\chi)}$ prikažemo na dva načina.

Ako je $a \neq 0$, tada je na osnovu Teoreme 2.14. $\overline{g_a(\chi)} = \overline{\chi(a^{-1})g(\chi)} = \chi(a)\overline{g(\chi)}$ i $g_a(\chi) = \chi(a^{-1})g(\chi)$. Zato je $g_a(\chi)\overline{g_a(\chi)} = \chi(a^{-1})\chi(a)g(\chi)\overline{g(\chi)} = |g(\chi)|^2$. Kako je $g_0(\chi) = 0$ sledi da je $\sum_a g_a(\chi)g_a(\chi) = (p-1)|g(\chi)|^2$.

Sa druge strane imamo da je

$$g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\zeta^{ax-ay}.$$

Sumirajući obe strane po a u poslednjoj jednakosti i koristeći Posledicu 1.3. dobijamo

$$\sum_a g_a(\chi)\overline{g_a(\chi)} = \sum_x \sum_y \chi(x)\overline{\chi(y)}\delta(x,y)p = (p-1)p.$$

Zato je $(p-1)|g(\chi)|^2 = (p-1)p$ odakle sledi dokaz teoreme. □

Definicija 2.5. *Neka su $\chi_1, \chi_2, ..., \chi_r$ karakteri na $\mathbb{F}_p$. Jakobijevu sumu definišemo na sledeći način:*

$$J(\chi_1, ..., \chi_r) = \sum_{t_1+\cdots+t_r=1} \chi_1(t_1)\cdots\chi_r(t_r),$$

gde se suma vrši po svim rešenjima jednačine $t_1 + \cdots + t_r = 1$ u $\mathbb{F}_p$.

Sledeća teorema nam daje vezu između Gausovih i Jakobijevih suma.

Teorema 2.16. *Ako su $\chi_1, ..., \chi_r$ netrivijalni karakteri i ako je njihov proizvod $\chi_1 \cdots \chi_r$ takođe netrivijalan, tada je $g(\chi_1)\cdots g(\chi_r) = J(\chi_1, ..., \chi_r)g(\chi_1 \cdots \chi_r)$.*

Dokaz. Definišimo preslikavanje $\psi : \mathbb{F}_p \to \mathbb{C}$ sa $\psi(t) = \zeta^t$. Tada je $\psi(t_1 + t_2) = \psi(t_1)\psi(t_2)$ i možemo zapisati da je $g(\chi) = \sum_t \chi(t)\psi(t)$. Sada je

$$g(\chi_1)\cdots g(\chi_r) = \left(\sum_{t_1} \chi_1(t_1)\psi(t_1)\right)\cdots\left(\sum_{t_r} \chi_r(t_r)\psi(t_r)\right) = \sum_s \psi(s)\left(\sum_{t_1+\cdots+t_r=s} \chi_1(t_1)\cdots\chi_r(t_r)\right).$$

Ako je $s \neq 0$, za $t_i = su_i$, unutrašnja suma je jednaka $(\chi_1 \cdots \chi_r)(s)J(\chi_1, ..., \chi_r)$.

Ako je $s = 0$, tada unutrašnja suma je jednaka $\sum_{t_1+\cdots t_r=0} \chi_1(t_1)\cdots\chi_r(t_r) = 0$ jer $t_1, ..., t_{r-1}$ mogu biti proizvoljno izabrani pa je $t_r = -t_1 - \cdots - t_{r-1}$, i svaka od suma korespodentna sa $t_1, ..., t_{r-1}$ je nula jer su $\chi_1, ..., \chi_r$ netrivijalni. □

Teorema 2.17. *Ako su $\chi_1 ..., \chi_r$ netrivijalni, i ako je $\chi_1 \cdots \chi_r$ trivijalan, tada je*

$$g(\chi_1)\cdots g(\chi_r) = \chi_r(-1)pJ(\chi_1, ..., \chi_{r-1}).$$

Dokaz. Na osnovu Teoreme 2.16. imamo da je

$$g(\chi_1)\cdots g(\chi_{r-1}) = J(\chi_1, ..., \chi_{r-1})g(\chi_1 \cdots \chi_{r-1}).$$

Množeći sa $g(\chi_r)$ obe strane poslednje jednakosti dolazimo do izračunavanja

$$g(\chi_r)g(\chi_1 \cdots \chi_{r-1}).$$

Međutim, $(\chi_1 \cdots \chi_{r-1})\chi_r = \chi_0$ znači da je

$$g(\chi_1 \cdots \chi_{r-1})g(\chi_r) = g(\bar{\chi_r})g(\chi_r) = \chi_r(-1)p$$

na osnovu dokaza Teoreme 2.15. □

2.4 Kubni zakon reciprociteta

Lema 2.1. $g(\chi)^3 = p\pi$

Dokaz. Na osnovu Teoreme 2.17. važi $g(\chi)^3 = pJ(\chi,\chi)$. Dokažimo da je $J(\chi,\chi) = \pi$ odakle će slediti da je $g(\chi)^3 = p\pi$. Neka je $J(\chi,\chi) = \pi'$. Kako je $\pi\bar{\pi} = p = \pi'\bar{\pi}'$ imamo da $\pi \mid \pi'$ ili $\pi \mid \bar{\pi}'$. Kako su svi posmatrani prosti primarni, imamo da je $\pi = \pi'$ ili $\pi = \bar{\pi}'$. Eliminisaćemo poslednju mogućnost.

Na osnovu definicije važi:

$$J(\chi,\chi) = \sum_x \chi(x)\chi(1-x) \equiv \sum_x x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} (\mathrm{mod}\ \pi),$$

gde se suma vrši nad skupom $\mathbb{Z}/p\mathbb{Z}$. Polinom $x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}}$ je stepena $\frac{2}{3}(p-1) < p-1$. Pokažimo sada da važi sledeća formula:

$$p-1 \nmid k \Rightarrow 1^k + 2^k + \cdots + (p-1)^k \equiv 0 (\mathrm{mod}\ p). \tag{1}$$

Neka je x primitivan koren mod p. Tada je $1^k+2^k+\cdots+(p-1)^k \equiv 1+x^k+\cdots+x^{(p-2)k} (\mathrm{mod}\ p)$. Kako $x^k \not\equiv 1 (\mathrm{mod}\ p)$ i $x^{(p-1)k} \equiv 1 (\mathrm{mod}\ p)$ sledi da je $1^k+2^k+\cdots+(p-1)^k \equiv \frac{x^{(p-1)k}-1}{x^k-1} \equiv 0 (\mathrm{mod}\ p)$ čime je dokazana formula (1). Sada na osnovu formule (1) sledi $\sum\limits_x x^{\frac{p-1}{3}}(1-x)^{\frac{p-1}{3}} \equiv 0 (\mathrm{mod}\ p)$. Ovim je pokazano da važi $J(\chi,\chi) \equiv 0 (\mathrm{mod}\ \pi)$, tj. $\pi \mid \pi'$ odakle sledi da je $\pi = \pi'$. □

Lema 2.2. *Neka je* $\pi_1 = q \equiv 2 (mod\, 3)$ *i* $\pi_2 = \pi$ *prost u* $\mathbb{Z}[\omega]$ *norme p. Tada je* $\chi_\pi(q) = \chi_q(\pi)$.

Dokaz. Neka je $\chi_\pi = \chi$, i posmatrajmo Jakobijevu sumu $J(\chi,...,\chi)$ sa q članova. Kako $3|q+1$, imamo na osnovu Teoreme 2.17 da je $g(\chi)^{q+1} = pJ(\chi,...,\chi)$. Na osnovu Leme 2.1 je $g(\chi)^3 = p\pi$, pa važi:

$$g(\chi)^{q+1} = (p\pi)^{\frac{q+1}{3}}.$$

Podsetimo se da je

$$J(\chi,...,\chi) = \sum \chi(t_1)\cdots\chi(t_q),$$

gde se suma vrši po svim $t_1,...,t_q \in \mathbb{Z}/p\mathbb{Z}$ tako da je $t_1+\cdots+t_q = 1$. Član u kome je $t_1 = \cdots = t_q$ zadovoljava $qt_1 = 1$ i $\chi(q)\chi(t_1) = 1$. Stepenujući obe strane poslednje jednakosti q-tim stepenom i uzimajući u obzir da je $q \equiv 2 (\mathrm{mod}\ 3)$ dobijamo da je

$$\chi(q)^2\chi(t_1)^q = 1$$

i otuda dobijamo da je $\chi(t_1)^q = \chi(q)$. Zato, ,,dijagonalni"element koji korespondira sa $t_1 = \cdots = t_q$ ima vrednost $\chi(q)$. Ako nisu svi t_i međusobno jednaki, tada dobijamo q različitih q-torki iz ciklične permutacije $(t_1, ..., t_q)$. Zato je $J(\chi, ..., \chi) \equiv \chi(q) (\mathrm{mod}\, q)$.

Dakle, $(p\pi)^{\frac{q+1}{3}} \equiv p\chi(q) (\mathrm{mod}\, q)$ odakle sledi

$$p^{\frac{q-2}{3}} \pi^{\frac{q+1}{3}} \equiv \chi(q) (\mathrm{mod}\, q).$$

Imajući u vidu $q - 1 \equiv 1 (\mathrm{mod}\, 3)$ stepenujmo poslednju jednakost do $(q-1)$-tog stepena:

$$p^{\frac{(q-2)(q-1)}{3}} \pi^{\frac{q^2-1}{3}} \equiv \chi(q)^{q-1} \equiv \chi(q) (\mathrm{mod}\, q).$$

Na osnovu Male Fermaove teoreme važi $p^{q-1} \equiv 1 (\mathrm{mod}\, q)$. Zato je

$$\chi_\pi(q) \equiv \pi^{\frac{q^2-1}{3}} \equiv \chi_q(\pi) (\mathrm{mod}\, q)$$

odakle sledi $\chi_\pi(q) = \chi_q(\pi)$. □

Teorema 2.18. *Neka su π_1 i π_2 primarni prosti u $\mathbb{Z}[\omega]$ sa normama p_1, p_2 respektivno. Tada je*

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

Dokaz. Neka je $\gamma_1 = \overline{\pi_1}, \gamma_2 = \overline{\pi_2}$. Tada je $p_1 = \pi_1\gamma_1, p_2 = \pi_2\gamma_2$, i $p_1, p_2 \equiv 1 (\mathrm{mod}\, 3)$. Sada je

$$g(\chi_{\gamma_1})^{p_2} = J(\chi_{\gamma_1}, ..., \chi_{\gamma_1}) g(\chi_{\gamma_1}^{p_2})$$

na osnovu Teoreme 2.16. (Postoji p_2 karaktera u Jakobijevoj sumi.) Kako je $p_2 \equiv 1 (\mathrm{mod}\, 3)$ sledi $\chi_{\gamma_1}^{p_2} = \chi_{\gamma_1}$. Zato je

$$[g(\chi_{\gamma_1})^3]^{\frac{p_2-1}{3}} = J(\chi_{\gamma_1}, ..., \chi_{\gamma_1}).$$

Kao u dokazu prethode teoreme, izostavljajući ,,dijagonalni" član u Jakobijevoj sumi i posmatrajući članove kongruentne sa 0 mod p_2, dobijamo

$$J(\chi_{\gamma_1}, ..., \chi_{\gamma_1}) \equiv \chi_{\gamma_1}(p_2^{-1}) \equiv \chi_{\gamma_1}(p_2^2) (\mathrm{mod}\, p_2).$$

Na osnovu Leme 2.1 je $g(\chi_{\gamma_1})^3 = p_1\gamma_1$ odakle sledi

$$(p_1\gamma_1)^{\frac{p_2-1}{3}} \equiv \chi_{\gamma_1}(p_2^2) (\mathrm{mod}\, p_2).$$

Dakle, $\chi_{\pi_2}(p_1\gamma_1) = \chi_{\gamma_1}(p_2^2)$. Slično, $\chi_{\pi_1}(p_2\pi_2) = \chi_{\pi_2}(p_1^2)$. Sada je na osnovu Teoreme 2.10. $\chi_{\gamma_1}(p_2^2) = \chi_{\pi_1}(p_2)$. Zato je

$$\chi_{\pi_2}(p_1\gamma_1) = \chi_{\pi_1}(p_2),$$
$$\chi_{\pi_1}(p_2\gamma_2) = \chi_{\pi_2}(p_1).$$

Sada imamo

$$\begin{aligned}\chi_{\pi_1}(\pi_2)\chi_{\pi_2}(p_1\gamma_1) &= \chi_{\pi_1}(\pi_2 p_2)\\ &= \chi_{\pi_2}(p_1^2)\\ &= \chi_{\pi_2}(p_1\pi_1\gamma_1)\\ &= \chi_{\pi_2}(\pi_1)\chi_{\pi_2}(p_1\gamma_1),\end{aligned}$$

odakle sledi $\chi_{\pi_1}(\pi_2) = \chi_{\pi_2}(\pi_1)$.

□

2.5 Kubni karakter broja 2

Sada ćemo se baviti sledećim pitanjem: Za koje sve proste $\pi \in \mathbb{Z}[\omega]$, 2 je kubni ostatak. Na početku, primetimo da $x^3 \equiv 2(\text{mod } \pi)$ je rešiva ako i samo ako $x^3 \equiv 2(\text{mod } \pi')$ je rešiva za svaki asocirani element od π. Zato možemo pretpostaviti da je π primaran. Ako je $\pi = q$ racionalan prost, tada je $\chi_q(2) = 1$, pa je 2 kubni ostatak za sve ovakve proste π.

Pretpostavimo sada da je $\pi = a + b\omega$ primaran, kompleksan i prost. Na osnovu kubnog zakona reciprociteta je $\chi_\pi(2) = \chi_2(\pi)$. Norma od 2 je $2^2 = 4$. Zato je

$$\pi = \pi^{\frac{4-1}{3}} \equiv \chi_2(\pi)(\text{mod } 2).$$

Sada sledi da je $\chi_\pi(2) = 1$ ako i samo ako $\pi \equiv 1(\text{mod } 2)$. Upravo smo dokazali sledeću teoremu.

Teorema 2.19. *$x^3 \equiv 2(mod\, \pi)$ je rešiva ako i samo ako je $\pi \equiv 1(mod\, 2)$, tj. ako i samo ako $a \equiv 1(mod\, 2)$ i $b \equiv 0(mod\, 2)$.*

Poslednju teoremu je moguće iskazati na još jedan način. Neka je $\pi = a + b\omega$ primaran, kompleksan i prost i $p = N(\pi) = a^2 - ab + b^2$. Tada je $4p = (2a - b)^2 + 3b^2$. Ako stavimo da je $A = 2a - b$ i $B = \frac{b}{3}$, tada je $4p = A^2 + 27B^2$.

Teorema 2.20. *Ako je $p \equiv 1(mod\, 3)$, tada je $x^3 \equiv 2(mod\, p)$ rešiva ako i samo ako postoje celi brojevi C i D takvi da je $p = C^2 + 27D^2$.*

Dokaz. Ako je $x^3 \equiv 2(\text{mod } p)$ rešiva, onda je rešiva i $x^3 \equiv 2(\text{mod } \pi)$ i zato je $\pi \equiv 1(\text{mod } 2)$ na osnovu Teoreme 2.19. Sada imamo:

$$4p = A^2 + 27B^2, \quad \text{gde je} \quad A = 2a - b, B = \frac{b}{3}.$$

Kako je b, paran, sledi da su to i A i B. Neka je $D = \frac{B}{2}$ i $C = \frac{A}{2}$. Tada je $p = C^2 + 27D^2$.

Pretpostavimo obrnuto, neka je $p = C^2 + 27D^2$. Tada je $4p = (2C)^2 + 27(2D)^2$. Na osnovu jedinstvenosti broja B, sledi da je $B = \pm 2D$; tj. B je paran, pa je i b paran. Kako $\mathbb{Z}[\omega]/\pi\mathbb{Z}[\omega]$ ima $p = N(\pi)$ elemenata, postoji ceo broj h, takav da je $h^3 \equiv 2(\text{mod } \pi)$. Takođe, sada važi i da je $h^3 \equiv 2(\text{mod } p)$. Ako $\pi \mid h^3 - 2$, tada $\bar{\pi} \mid h^3 - 2$ i $\pi\bar{\pi} = p \mid (h^3 - 2)^2$. Sada $p \mid h^3 - 2$. □

Na primer, uzmimo da je $p = 7$. Tada $x^3 \equiv 2(\text{mod } 7)$ nije rešiva jer ne postoje celi brojevi C i D takvi da je $7 = C^2 + 27D^2$.

Sa druge strane, ako uzmemo da je $p = 31 = 2^2 + 27 \cdot 1^2$, tada je jednačina $x^3 \equiv 2(\text{mod } 31)$ rešiva. Zaista, $4^3 \equiv 2(\text{mod } 31)$.

Napomene

Razmatranja o prstenu $\mathbb{Z}[\omega]$, i kubni karakter ostatka i kubni karakter broja 2 su prikazani uz korišćenje [2]. Dokaz kubnog zakona reciprociteta, zajedno sa Gausovim i Jakobijevim sumama je prikazan uz korišćenje [2] i [4].

3 Bikvadratni zakon reciprociteta

U svom drugom memoaru o bikvadratnim ostacima, 1832. godine, Gaus je naveo bez dokaza bikvadratni zakon reciprociteta. Dokaz, koji je on tvrdio, pripadao je misterijama više aritmetike. Detalji su publikovani u trećem meomaru, što se nažalost nije nikad pojavilo. Kasnije je Ajzenštajn publikovao nekoliko dokaza 1844. godine, koristeći Jakobijeve i Gausove sume. Glavna ideja je ista kao i kod kubnih ostataka s tim da su neki detalji sada obimniji.

U ovoj sekciji, prvo ćemo se baviti prstenom $\mathbb{Z}[i]$, bikvadratnim (kvartnim) karakterom ostatka, formulacijom i dokazom bikvadratnog zakona reciprociteta.

3.1 Prsten $\mathbb{Z}[i]$

U toku narednog izlaganja neka D označava prsten $\mathbb{Z}[i] = \{a + bi | a, b \in \mathbb{Z}\}$ koji se još zove prsten Gausovih celih. Ako $\alpha \in D$ tada $(\alpha) = \alpha D$ je glavni ideal generisan sa α. Takođe, u narednom izlaganju kada kažemo prost, mislićemo na pozitivan prost broj iz $\mathbb{Z}$.

Teorema 3.1. *Prsten D je euklidski domen.*

Dokaz. Skup D je očigledno zatvoren u odnosu na sabiranje i oduzimanje. Šta više, ako $a + bi, c + di \in D$, tada $(a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i \in D$. Zato je D zatvoren i u odnosu na množenje, pa je D jedan prsten. Kako je D sadržan u skupu kompleksnih brojeva, sledi da je D integralni domen.

Za $a + bi \in \mathbb{Q}[i]$ definišemo normu $N(a + bi) = a^2 + b^2$. Neka je $\alpha = a + bi$ i $\gamma = c + di$ i pretpostavimo $\gamma \neq 0, \frac{\alpha}{\gamma} = r + si$, gde $r, s \in \mathbb{Q}$. Izaberimo cele brojeve $m, n \in \mathbb{Z}$ takve da je $|r - m| \leq \frac{1}{2}$ i $|s - n| \leq \frac{1}{2}$. Neka je sada $\delta = m + ni$. Tada $\delta \in D$ i $N(\frac{\alpha}{\gamma} - \delta) = (r - m)^2 + (s - n)^2 \leq \frac{1}{4} + \frac{1}{4} = \frac{1}{2}$. Neka je $\rho = \alpha - \gamma\delta$. Tada $\rho \in D$ i važi ili $\rho = 0$ ili $N(\rho) = N(\gamma(\frac{\alpha}{\gamma} - \delta)) = N(\gamma)N(\frac{\alpha}{\gamma} - \delta) \leq \frac{1}{2}N(\gamma) < N(\gamma)$. □

Kako je D euklidski domen, imamo da ako je π ireducibilan i $\pi \mid \alpha\beta$ tada ili $\pi \mid \alpha$ ili $\pi \mid \beta$. Ako $N(\alpha) = \alpha\bar{\alpha}$ norma od α, tada važi $N(\alpha) = 1$ ako i samo ako α je inverzibilan. Odavde dobijamo da su inverzibilni elementi u D, $\pm 1, \pm i$.

Lema 3.1. *Ako je π ireducibilan, tada postoji prost $p \in \mathbb{Z}$ tako da $\pi | p$.*

Dokaz. $N(\pi) = \pi\bar{\pi} = n = p_1 \cdots p_s$, p_i je prost, $p_i \in \mathbb{Z}$. Zato $\pi \mid p_i$ za neko i. □

Lema 3.2. *Ako $\alpha \in D$, i $N(\alpha)$ je prost, tada je α ireducibilan.*

Dokaz. Ako $\alpha = \mu\lambda$, tada $N(\alpha) = N(\mu)N(\lambda)$. Kako je $N(\alpha)$ prost, sledi da je $N(\mu) = 1$ ili $N(\lambda) = 1$. Zato je jedan od λ i μ inverzibilan, odakle sledi da je α ireducibilan. □

Lema 3.3. *$1 + i$ je ireducibilan i $2 = -i(1 + i)^2$ je prosta faktorizacija od 2 u D.*

Dokaz. Kako je $N(1+i)=2$ sledi na osnovu Leme 3.2 da je $1+i$ ireducibilan. Drugi deo leme se dokazuje direktnom proverom. □

Lema 3.4. *Ako je $q \equiv 3(mod\, 4)$ prost u $\mathbb{Z}$, tada je q ireducibilan posmatran kao element od D.*

Dokaz. Ako q ne bi bio ireducibilan u D, tada $q=\alpha\beta$ gde je $N(\alpha)>1$ i $N(\beta)>1$. Prelazeći na norme dobijamo $q^2=N(\alpha)N(\beta)$. Sledi da je $q=N(\alpha)$. Ako je $\alpha=a+bi, a,b\in\mathbb{Z}$, tada je $q=a^2+b^2$. Ovo je kontradikcija jer zbir dva kvadrata u $\mathbb{Z}$ je kongruentan sa 0 ili 1 modulo 4, a q je kongruentno sa 3 modulo 4. □

Lema 3.5. *Ako je p prost, $p \equiv 1(mod\, 4)$, tada postoji ireducibilni π tako da $p=\pi\bar{\pi}$.*

Dokaz. Pokažimo da postoji $n\in\mathbb{Z}$ tako da $p \mid n^2+1$.

Na osnovu Vilsonove teoreme imamo da $p \mid (p-1)!+1$. Imamo da je

$$(p-1)! = \prod_{a=1}^{\frac{p-1}{2}} a(p-a) \equiv \prod_{a=1}^{\frac{p-1}{2}} (-a^2) = (-1)^{\frac{p-1}{2}} \left(\prod_{a=1}^{\frac{p-1}{2}} a\right)^2 \equiv n^2 (\mathrm{mod}\, p)$$

jer je $\frac{p-1}{2}$ paran. Dakle, $p \mid n^2+1$. Na osnovu Leme 3.1. $\pi \mid p$. Kako $p \mid n^2+1=(n-i)(n+i)$ i kako je π prost u $\mathbb{Z}[i]$ sledi da $\pi \mid n-i$ ili $\pi \mid n+i$. Ako bi π bio asociran sa p, onda bi važilo $N(\pi)=N(p)=p^2$. Tada bi još i važilo da $p \mid n-i$ ili $p \mid n+i$ što je kontradikcija. Dakle, $N(\pi)=p$, odnosno $p=\pi\bar{\pi}$ i $\pi,\bar{\pi}$ su prosti jer je $\mathbb{Z}[i]$ glavnoidealski. □

Sa iznetim lemama i teoremama je kompletiran opis ireducibilnih elemenata u D.

Definicija 3.1. *Za element $\alpha\in D$ koji nije inverzibilan kažemo da je primaran ako $\alpha \equiv 1(mod\,(1+i)^3)$.*

Lema 3.6. *Element $\alpha=a+bi\in D$ koji nije inverzibilan je primaran ako i samo ako je ili $a\equiv 1(mod\,4), b\equiv 0(mod\,4)$ ili $a\equiv 3(mod\,4), b\equiv 2(mod\,4)$.*

Dokaz. Kako je $(1+i)^3=2i(1+i)$ sledi da je $a+bi$ primaran ako i samo ako

$$\frac{(a-1)+bi}{2+2i} = \frac{a+b-1}{4} + \frac{b-a+1}{4} i \in D.$$

Ovo je ekvivalento sa kongruencijama $a+b\equiv 1(\mathrm{mod}\,4), a-b\equiv 1(\mathrm{mod}\,4)$. □

Napomenimo da bilo koji neinverzibilni $\alpha\equiv 1(\mathrm{mod}\,4)$ je primaran. Šta više, ako je α primaran, tada $(1+i)\nmid\alpha$. Ako je q realan prost, $q\equiv 3(\mathrm{mod}\,4)$, tada je $-q$ primarni ireducibilni.

Lema 3.7. *Neka je $\alpha\in D$ neinverzibilni, $(1+i)\nmid\alpha$. Tada postoji jedinstveni inverzibilni element u tako da je $u\alpha$ primarni.*

Dokaz. Postoji inverzibilni ϵ tako da je $\epsilon\alpha = a + bi$ gde je a neparan i b paran. Množeći ako je potrebno sa -1, Lema 3.6 nam pokazuje da je α asociran sa nekim primarnim elementom. Ako su u_1 i u_2 inverzibilni elementi takvi da su $u_1\alpha$ i $u_2\alpha$ primarni tada kako $(1+i) \nmid \alpha$ sledi da je $u_1 \equiv u_2(1+i)^3$. Odavde je $u_1 = u_2$. □

Lema 3.8. *Primarni element se može prikazati kao proizvod primarnih ireducibilnih elemenata.*

Dokaz. Neka je $\alpha \in D$ primaran. Tada postoje racionalni prosti $q_i \equiv 3(\text{mod } 4)$, primarni ireducibilni $\pi_i, N(\pi_i) \equiv 1(\text{mod } 4)$ i inverzibilni u tako da je $\alpha = u\pi_1 \cdots \pi_t(-q_1) \cdots (-q_s)$. Redukcijom modulo $(1+i)^3$ dobijamo da je $1 \equiv u(1+i)^3$. Odavde sledi da je $u = 1$. □

3.2 Bikvadratni karakter ostatka

U ovoj podsekciji posmatramo ireducibilni $\pi \in D$.

Teorema 3.2. *Prsten ostataka $D/\pi D$ je konačno polje sa $N(\pi)$ elemenata.*

Dokaz. Dokaz se izvodi na isti način kao i u Teoremi 2.6, zamenom odgovarajućih ireducibilnih iz $\mathbb{Z}[\omega]$ sa odgovarajućim ireducibilnim u $D = \mathbb{Z}[i]$. □

Iz ove teoreme dobijamo jednostavnu posledicu.

Posledica 3.1. *Ako $\pi \nmid \alpha$ tada $\alpha^{N(\pi)-1} \equiv 1 (mod\, \pi)$.*

Teorema 3.3. *Ako $\pi \nmid \alpha, (\pi) \neq (1+i)$ tada postoji jedinstven ceo broj $j, 0 \leq j \leq 3$ tako da*

$$\alpha^{\frac{N(\pi)-1}{4}} \equiv i^j (mod\, \pi).$$

Dokaz. Klase ostataka od $1, -1, i, -i$ su različite. One su koreni od $x^4 \equiv 1 (\text{mod}\, \pi)$. Međutim, klasa ostataka od $\alpha^{\frac{N(\pi)-1}{4}}$ je takođe rešenje za $x^4 \equiv 1 (\text{mod}\, \pi)$ na osnovu prethodne posledice. □

Definicija 3.2. *Ako je π ireducibilan, $N(\pi) \neq 2$, tada bikvadratni karakter ostatka od α, za $\pi \nmid \alpha$, je definisan sa $\chi_\pi(\alpha) = i^j$ gde je j određen na osnovu Teoreme 3.3. Ako $\pi \mid \alpha$, tada je $\chi_\pi(\alpha) = 0$.*

Teorema 3.4. *Za bikvadratni simbol ostatka važi sledeće:*

1. *Ako $\pi \nmid \alpha$ tada $\chi_\pi(\alpha) = 1 \Leftrightarrow x^4 \equiv \alpha (mod\, \pi)$ ima rešenje u D.*
2. $\chi_\pi(\alpha\beta) = \chi_\pi(\alpha) \cdot \chi_\pi(\beta)$.
3. $\overline{\chi_\pi(\alpha)} = \chi_{\bar{\pi}}(\bar{\alpha})$.
4. *Ako je π primaran ireducibilni tada je $\chi_\pi(-1) = (-1)^{\frac{a-1}{2}}$, gde je $\pi = a + bi$.*
5. *Ako je $\alpha \equiv \beta (mod\, \pi)$ tada je $\chi_\pi(\alpha) = \chi_\pi(\beta)$.*
6. $\chi_\pi(\alpha) = \chi_\lambda(\alpha)$ *ako* $(\pi) = (\lambda)$.

Dokaz. 1. Dokaz sledi iz činjenice da $x^n = \alpha$ ima rešenja ako i samo ako $\alpha^{\frac{q-1}{d}} = 1$, gde $\alpha \in F^*, d = (n, q-1), F$ je konačno polje.

2., 3., 5. i 6. slede direktno iz definicije.

4. sledi iz Leme 3.6. □

Teorema 3.5. *Neka je q prost, $q \equiv 3 (mod\, 4)$. Tada je $\chi_q(a) = 1$ za $a \in \mathbb{Z}, q \nmid a$.*

Dokaz. Imamo da je $N(q) = q^2$. Zato je

$$\chi_q(a) \equiv a^{\frac{q^2-1}{4}} = (a^{q-1})^{\frac{q+1}{4}} \equiv 1(\text{mod } q)$$

na osnovu Male Fermaove teoreme. □

Bikvadratni karakter ostatka se generalizuje na sledeći način.

Definicija 3.3. *Neka je $\alpha \in D$ neinverzibilni element tako da $(1+i) \nmid \alpha$, i $\beta \in D$. Zapišimo α kao $\alpha = \prod_i \lambda_i$ gde je λ_i ireducibilan. Ako je $(\alpha, \beta) = 1$ definišemo $\chi_\alpha(\beta)$ na sledeći način:*

$$\chi_\alpha(\beta) = \prod_i \chi_{\lambda_i}(\beta).$$

Ovo je dobro definisano na osnovu Teoreme 3.4 pod 6. Na osnovu 5. Teoreme 3.4 sledi da ako je $\beta \equiv \gamma(\text{mod } \alpha)$ tada $\chi_\alpha(\beta) = \chi_\alpha(\gamma)$.

Teorema 3.6. *Neka je $\alpha \in \mathbb{Z}, \alpha \neq 0$, i $a \in \mathbb{Z}$ neparan neinverzibilni. Ako je $(a, \alpha) = 1$, tada je*

$$\chi_a(\alpha) = 1.$$

Dokaz. Možemo pretpostaviti da je $a > 0$. Pretstavimo a na sledeći način: $a = \prod p_i \prod q_i$ gde su p_i, q_i prosti, $p_i \equiv 1(\text{mod } 4)$ i $q_i \equiv 3(\text{mod } 4)$. Na osnovu Teoreme 3.5 ostalo još samo da proverimo da je $\chi_{p_i}(\alpha) = 1$. Ako je $p_i = \pi\bar{\pi}$ gde je π ireducibilan, tada $\chi_{p_i}(\alpha) = \chi_\pi(\alpha)\chi_{\bar{\pi}}(\bar{\alpha}) = \chi_\pi(\alpha)\overline{\chi_\pi(\alpha)} = 1$ na osnovu Teoreme 3.4 pod 3. □

Teorema 3.7. *Ako je $n \neq 1$ ceo broj $n \equiv 1(mod\, 4)$,tada je $\chi_n(i) = (-1)^{\frac{n-1}{4}}$.*

Dokaz. Primetimo da n može biti negativan. Ako je n pozitivan prost $p \equiv 1(\text{mod } 4)$ tada je $p = \pi\bar{\pi}$. Sada imamo

$$\chi_p(i) = \chi_\pi(i)\chi_{\bar{\pi}}(i) = (i^{\frac{p-1}{4}})^2 = (-1)^{\frac{p-1}{4}}.$$

Ako je $n = -q, q \equiv 3(\text{mod } 4)$ i prost, tada je $\chi_{-q}(i) = i^{\frac{q^2-1}{4}} = (i^{q-1})^{\frac{q+1}{4}} = (-1)^{\frac{-q-1}{4}}$. Ako je $n \equiv 1(\text{mod } 4)$ proizvoljan tada je $n = p_1 \cdots p_t(-q_1) \cdots (-q_s), p_i \equiv 1(\text{mod } 4), q_i \equiv 3(\text{mod } 4)$ odakle dokaz sledi iz činjenice da je $\frac{n-1}{4} \equiv \sum_{i=1}^{t} \frac{p_1-1}{4}(\text{mod } 4)$. □

3.3 Bikvadratni zakon reciprociteta

Uopšteni bikvadratni zakon reciprociteta se može izraziti na sledeći način. Neka su λ i π uzajamno prosti primarni elementi od D. Tada

Teorema 3.8. $\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{N(\lambda)-1}{4}\cdot\frac{N(\pi)-1}{4}}$.

Ako su λ i π primarni, gde je $\lambda = c + di$ i $\pi = a + bi$, može se pokazati da su $\frac{N(\lambda)-1}{4} \cdot \frac{N(\pi)-1}{4}$ i $\frac{a-1}{2} \cdot \frac{c-1}{2}$ iste parnosti, odakle sledi

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}.$$

Drugim rečima, ako su ili π ili λ kongruentni sa 1 modulo 4 tada π i λ imaju isti bikvadratni karakter. Takođe, ako su π i λ kongruentni sa $3 + 2i$ tada važi $\chi_\pi(\lambda) = -\chi_\lambda(\pi)$.

Posmatrajmo primarni ireducibilni elemenat π sa normom $N(\pi) = p \equiv 1(\text{mod } 4)$ i neka je χ_π odgovarajući bikvadratni karakter. Tada se χ_π može posmatrati kao multiplikativni karakter na konačnom polju $D/\pi D = F$. Podsetimo se da je F konačno polje sa p elemenata koje sadrži klase ostataka od $0, 1, ..., p-1$. Neka je $\zeta = e^{\frac{2\pi i}{p}}$ i neka je $g(\chi_\pi) = \sum_{j\in F} \chi_\pi(j)\zeta^j$ Gausova suma koja odgovara χ_π. Ako je $\psi = \chi_\pi^2$, tada je ψ netrivijalni karakter reda 2 na polju F i zato je ψ Ležandrov simbol.

Pre nego što pređemo na dokaz specijalnih slučajeva bikvadratnog zakona reciprociteta i generalnog oblika ovog zakona, navedimo nekoliko rezultata vezano za Gausove i Jakobijeve sume, koji će nam biti potrebni.

Teorema 3.9. $J(\chi_\pi, \chi_\pi) = \chi_\pi(-1)J(\chi_\pi, \psi)$.

Dokaz. $J(\chi_\pi, \chi_\pi) = \frac{g(\chi_\pi)^2}{g(\psi)}$ odakle sledi $J(\chi_\pi, \chi_\pi)^2 = \frac{g(\chi_\pi)^4}{g(\psi)^2} = \chi_\pi(-1)J(\chi_\pi, \chi_\pi)J(\chi_\pi, \psi)$. □

Teorema 3.10. $g(\chi_\pi)^4 = pJ(\chi_\pi, \chi_\pi)^2$.

Dokaz. Dokaz sledi iz prethodne Teoreme 3.9 i Teoreme 2.17. □

Teorema 3.11. $-\chi_\pi(-1)J(\chi_\pi, \chi_\pi)$ *je primaran.*

Dokaz. $J(\chi_\pi, \chi_\pi) = 2\sum_{t=2}^{\frac{p-1}{2}} \chi_\pi(t)\chi_\pi(1-t) + \chi_\pi\left(\frac{p+1}{2}\right)^2$. Svaki inverzibilni element u D je kongruentan sa 1 modulo $1 + i$. Takođe, $p \equiv 1(\text{mod } 2 + 2i)$. Sada imamo $\chi_\pi(\frac{p+1}{2})^2 = (\chi_\pi(2^{-1}))^2 = \chi_\pi(2)^{-2} = \chi_\pi(2)^2 = \chi_\pi(-i(1+i)^2)^2 = \chi_\pi(-i)^2 = \chi_\pi(-1)$. Zato je

$$\begin{aligned} J(\chi_\pi, \chi_\pi) &\equiv 2\left(\frac{p-3}{2}\right) + \chi_\pi(-1)(\text{mod } 2+2i) \\ &\equiv -2 + \chi_\pi(-1)(\text{mod } 2+2i). \end{aligned}$$

Otuda imamo

$$\begin{aligned} -\chi_\pi(-1)J(\chi,\chi) &\equiv 2\chi_\pi(-1) - 1(\mathrm{mod}\, 2+2i) \\ &\equiv 1(\mathrm{mod}\, 2+2i), \end{aligned}$$

jer je $\chi_\pi(-1) = \pm 1$. □

Teorema 3.12. $-\chi_\pi(-1)J(\chi_\pi,\chi_\pi) = \pi$.

Dokaz. Na osnovu Leme 3.7 dovoljno je dokazati da se leva i desna strana razlikuju za neki inverzibilni element. $J(\chi_\pi,\chi_\pi) \equiv \sum_{t=1}^{p-1} t^{\frac{p-1}{4}}(1-t)^{\frac{p-1}{4}}(\mathrm{mod}\,\pi)$. Na osnovu dokaza Leme 2.1 sledi da je $J(\chi_\pi,\chi_\pi) \equiv 0(\mathrm{mod}\,\pi)$. Kako je $N(J(\chi_\pi,\chi_\pi)) = p$ sledi da je $J(\chi_\pi,\chi_\pi)$ ireducibilan. □

Kombinujući Teoremu 3.12. i Teoremu 3.10. dobijamo faktorizaciju od $g(\chi)^4$ u D.

Teorema 3.13. $g(\chi_\pi)^4 = \pi^3\bar{\pi}$.

Pređimo sada na neke specijalne slučajeve bikvadratnog zakona reciprociteta.

Teorema 3.14. *Neka je $q > 0$ realan i ireducibilan u D. Tada važi*

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

Dokaz. Kako je $q \equiv 3(\mathrm{mod}\,4)$ imamo da je

$$g(\chi_\pi)^q \equiv \sum_{j=1}^{p-1} \chi_\pi(j)^q \zeta^{qj} \equiv \sum \chi_\pi^3(j)\zeta^{qj}(\mathrm{mod}\, q) \equiv \chi_\pi(q)g(\bar{\chi_\pi})(\mathrm{mod}\, q).$$

Zato je

$$(g(\chi_\pi)^4)^{\frac{q+1}{4}} = g(\chi_\pi)^{q+1} \equiv \chi_\pi(q)g(\chi_\pi)\cdot g(\bar{\chi}_\pi)(\mathrm{mod}\, q).$$

Na osnovu Teoreme 2.15. dobijamo da je $\bar{\pi} \equiv \pi^q(\mathrm{mod}\, q)$. Sada na osnovu Teoreme 3.13 imamo

$$\pi^{\frac{(q+3)(q+1)}{4}} \equiv \chi_\pi(-1)\chi_\pi(q)\pi^{q+1}(\mathrm{mod}\, q),$$

odakle je

$$\pi^{\frac{q^2-1}{4}} \equiv \chi_\pi(-q)(\mathrm{mod}\, q).$$

Kako je $\pi^{\frac{q^2-1}{4}} \equiv \chi_q(\pi)(\text{mod } q)$, imamo da je

$$\chi_q(\pi) \equiv \chi_\pi(-q)(\text{mod } q),$$

odakle na osnovu činjenice da sa obe strane poslednje jednakosti su inverzibilni elementi, sledi da je

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

□

Primetimo da je $-q$ primarni ireducibilni i da je $\frac{N(q)-1}{4} = \frac{q^2-1}{4}$ paran. Zato je prethodna teorema zaista jedan specijalan slučaj bikvadratnog zakona reciprociteta.

Teorema 3.15. *Neka je q prost i $q \equiv 1(mod\, 4)$. Tada je $\chi_\pi(q) = \chi_q(\pi)$.*

Dokaz. Kako je $q \equiv 1(\text{mod } 4)$ imamo da je

$$g(\chi_\pi)^q \equiv \sum \chi_\pi(j)^q \zeta^{qj} \equiv \sum \chi_\pi(j)\zeta^{qj} \equiv \bar{\chi}_\pi(q) g(\chi_\pi)(\text{mod } q).$$

Zato je

$$g(\chi_\pi)^{q+3} \equiv \bar{\chi}_\pi(q) g(\chi_\pi)^4(\text{mod } q).$$

Na osnovu Teoreme 3.13 poslednja jednakost postaje

$$(\pi^3\bar{\pi})^{\frac{q+3}{4}} \equiv \bar{\chi}_\pi(q)\pi^3\bar{\pi}(\text{mod } q).$$

Obe strane posledednje kongruencije pripadaju D i $(q, \pi) = (q, \bar{\pi}) = 1$. Zato dobijamo da je

$$(\pi^3)^{\frac{q-1}{4}}(\bar{\pi})^{\frac{q-1}{4}} \equiv \bar{\chi}_\pi(q)(\text{mod } q).$$

Ako je $q = \lambda\bar{\lambda}$ gde je λ ireducibilan u D sledi da je

$$\chi_\lambda(\pi^3)\chi_\lambda(\bar{\pi}) \equiv \bar{\chi}_\pi(q)(\text{mod } \lambda).$$

Sada možemo zaključiti da je

$$\chi_\lambda(\pi^3)\chi_\lambda(\bar{\pi}) = \bar{\chi}_\pi(q).$$

Poslednju jednakost možemo zapisati i na sledeći način

$$\overline{\chi_\lambda(\pi)}\chi_\lambda(\bar{\pi}) = \overline{\chi}_\pi(q)$$

ili

$$\chi_{\bar{\lambda}}(\bar{\pi})\chi_\lambda(\bar{\pi}) = \overline{\chi}_\pi(q)$$

odakle na osnovu definicije imamo

$$\chi_q(\bar{\pi}) = \bar{\chi}_\pi(q).$$

Sada uzimanjem konjugacije na poslednju jednakost sledi dokaz teoreme. □

Teorema 3.16. *Neka je a relan i $a \equiv 1(mod\,4)$ i neka je λ primaran i $(\lambda, a) = 1$. Tada je $\chi_a(\lambda) = \chi_\lambda(a)$.*

Teorema 3.17. *Neka su $\pi = a + bi$ i $\lambda = c + di$ primarni i uzajamno prosti brojevi u D. Ako je $(a, b) = 1$ i $(c, d) = 1$ tada*

$$\chi_\pi(\lambda) = \chi_\lambda(\pi)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}.$$

Dokaz. Iz pretpostavke sledi da je $(a, \pi) = (b, \pi) = (c, \lambda) = (d, \lambda) = 1$. Relacija $c\pi \equiv ac + bd(\text{mod } \lambda)$ implicira $(ac + bd, \lambda) = (ac + bd, \pi) = 1$. Šta više

$$\chi_\lambda(c)\chi_\lambda(\pi) = \chi_\lambda(ac + bd).$$

Slično

$$\chi_\pi(a)\chi_\pi(\lambda) = \chi_\pi(ac + bd).$$

Uzimanjem konjugacije u poslednjoj jednakosti i množeći je sa prethodnom dobijamo sledeće:

$$\chi_\lambda(c)\chi_{\bar{\pi}}(a)\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\lambda\bar{\pi}}(ac + bd).$$

Na osnovu Teoreme 3.4 pod 3. važi:

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_{\bar{\lambda}}(c)\chi_\pi(a)\chi_{\lambda\bar{\pi}}(ac + bd). \tag{1}$$

Pretpostavimo da su c, a, i $ac+bd$ neinverzibilni elementi. Tri člana na desnoj strani jednakosti (1) se jednostavno računaju. Za neparan ceo broj n stavimo $\chi_0(n) = (-1)^{\frac{n-1}{2}}$. Tada je $\chi_0(n)n \equiv 1(\text{mod } 4)$ i $\chi_0(ac + bd) = \chi_0(a)\chi_0(c)$ jer je $bd \equiv 0(\text{mod } 4)$.

Kako je $\chi_\alpha(x) = \chi_\alpha(\chi_0(x))\chi_\alpha(\chi_0(x)x)$ za svaki član na desnoj strani jednakosti (1), može se dobiti da je $\chi_\alpha(\chi_0(x)) = \chi_{\bar{\alpha}}(\chi_0(x))$ i koristeći Teoremu 3.16. i Teoremu 3.4 pod 3. dobijamo

$$\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} = \chi_c(\bar{\lambda})\chi_a(\pi)\chi_{ac+bd}(\lambda\bar{\pi}).$$

Koristeći Teoremu 3.6. dobijamo

$$\begin{aligned}\chi_c(\bar{\lambda}) = \chi_c(c-di) = \chi_c(-di) = \chi_c(i),\\ \chi_a(\pi) = \chi_a(a+bi) = \chi_a(bi) = \chi_a(i),\\ \chi_{ac+bd}(\bar{\pi}\lambda) = \chi_{ac+bd}((ad-bc)i) = \chi_{ac+bd}(i).\end{aligned}$$

Zato imamo relaciju:

$$\begin{aligned}\chi_\lambda(\pi)\overline{\chi_\pi(\lambda)} &= \chi_{(ac+bd)ac}(i)\\ &= (-1)^{\frac{(ac+bd)ac-1}{4}}\\ &= (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}.\end{aligned}$$

□

Uopšteni bikvadratni zakon reciprociteta sledi iz Teoreme 3.17. Neka je $\pi = m(a+bi), \lambda = n(c+di), (\pi,\lambda) = 1$ gde je $m \equiv n \equiv 1(\mathrm{mod}\,4), (a,b) = 1, (c,d) = 1$. Na osnovu Teoreme 3.16. je $\chi_\pi(n) = \chi_n(\pi)$ i $\chi_\lambda(m) = \chi_m(\lambda)$. Takođe je $\chi_m(n) = \chi_n(m) = 1$ na osnovu Teoreme 3.6. Kako su $a+bi$ i $c+di$ primarni imamo

$$\begin{aligned}\chi_\lambda(\pi) &= \chi_\lambda(m)\chi_\lambda(a+bi)\\ &= \chi_m(\lambda)\chi_n(a+bi)\chi_{c+di}(a+bi)\\ &= \chi_m(\lambda)\chi_{a+bi}(n)\chi_{a+bi}(c+di)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}\\ &= \chi_\pi(\lambda)(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}\\ &= \chi_\pi(\lambda)(-1)^{\frac{N(\pi)-1}{4}\cdot\frac{N(\lambda)-1}{4}},\end{aligned}$$

gde smo u posledjnoj jednakosti koristili činjenicu $m \equiv n \equiv 1(\mathrm{mod}\,4)$.

3.4 Bikvadratni karakter broja 2

Neka je dat broj $p \equiv 1(\mathrm{mod}\, 4)$. Tada se on može napisati kao zbir kvadrata nekih prirodnih brojeva $p = a^2 + b^2$, pri čemu uzimamo da je a neparan.

Teorema 3.18. *Kongruencija $x^4 \equiv 2(mod\, p)$ ima rešenja za $p \equiv 1(mod\, 4)$ ako i samo ako je p oblika $A^2 + 64B^2$ za neke cele brojeve A i B.*

Dokaz. Ideja dokaza jeste da $\left(\frac{a+b}{p}\right)$ izrazimo na dva načina. Neka je f takvo da važi $b \equiv af(\mathrm{mod}\, p)$. Tada je $p = a^2 + b^2 = a^2(1 + f^2) \equiv 0(\mathrm{mod}\, p)$ odakle sledi da je $f^2 \equiv -1(\mathrm{mod}\, p)$.

Prvo, primetimo da je $(a + b)^2 + (a - b)^2 = 2p$ odakle je $1 = \left(\frac{2p}{a+b}\right) = \left(\frac{2}{a+b}\right)\left(\frac{p}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}}\left(\frac{p}{a+b}\right)$. Zato je $\left(\frac{a+b}{p}\right) = (-1)^{(a+b-1)\frac{p-1}{4}}\left(\frac{p}{a+b}\right) = (-1)^{\frac{(a+b)^2-1}{8}} \equiv f^{\frac{(a+b)^2-1}{4}}(\mathrm{mod}\, p)$.

Drugo, kako je $(a+b)^2 \equiv 2ab(\mathrm{mod}\, p)$ sledi da je $\left(\frac{a+b}{p}\right) \equiv (a+b)^{\frac{p-1}{2}} \equiv (2ab)^{\frac{p-1}{4}} \equiv (2f)^{\frac{p-1}{4}}(\mathrm{mod}\, p)$ jer je $\left(\frac{a}{p}\right) = (-1)^{(p-1)\frac{a-1}{4}}\left(\frac{p}{a}\right) = 1$.

Izjednačavajući dva dobijena prikaza $\left(\frac{a+b}{p}\right)$ dobijamo da je $2^{\frac{p-1}{4}} \equiv f^{\frac{ab}{2}}(\mathrm{mod}\, p)$. 2 je bikvadratni ostatak ako i samo ako je poslednja kongruencija je jednaka 1, ali kako je f reda 4, ovo je moguće ako i samo 8 deli b odakle sledi dokaz teoreme. □

Napomene

Definicije i rezultati o bikvadratnom zakonu reciprociteta su prikazani uz korišćenje [2].

A Kvadratna raširenja polja

Definicija A.1. *Svako raširenje nad poljem $\mathbb{Q}$ stepena 2 se zove kvadratno raširenje. (Kažemo još i da se takvo polje naziva kvadratno polje.)*

Ako je K kvadratno polje, svaki element $x \in K\backslash\mathbb{Q}$ je stepena 2 nad $\mathbb{Q}$ i zato je x primitivni element od K (tj. $K = \mathbb{Q}[x]$ i $(1, x)$ je baza za K nad $\mathbb{Q}$). Neka je $F(X) = X^2+bX+c$ $(b, c \in \mathbb{Q})$ minimalni polinom elementa $x \in K$. Rešavajući jednačinu $x^2 + bx + c = 0$ dobijamo $2x = -b \pm \sqrt{b^2 - 4c}$. Zato je $K = \mathbb{Q}(\sqrt{b^2 - 4c})$. (Ovde se misli da je $\sqrt{b^2 - 4c}$ jedan od dva elementa iz K čiji je kvadrat b^2-4c.) Sada je b^2-4c racionaln broj $\frac{u}{v} = \frac{uv}{v^2}$, $u, v \in \mathbb{Z}$. Ustvari, $K = \mathbb{Q}(\sqrt{d})$ gde je d kvadratno slobodan ceo broj. Zato važi sledeća teorema.

Teorema A.1. *Svako kvadratno polje je oblika $\mathbb{Q}(\sqrt{d})$ gde je d kvadratno slobodan ceo broj.*

Razmotrimo sada kako izgleda prsten celih kvadratnog raširenja $\mathbb{Q}(\sqrt{d})$ za dato d. Element $\sqrt{d}$ je koren ireducibilnog polinoma $X^2 - d$. Ovaj element ima svoj konjugat u K i to je $-\sqrt{d}$. Postoji automorfizam σ polja K koji $\sqrt{d}$ slika u $-\sqrt{d}$. Svaki element iz K je oblika $a + b\sqrt{d}$, $a, b \in \mathbb{Q}$. Sada imamo

$$\sigma(a + b\sqrt{d}) = a - b\sqrt{d}. \tag{2}$$

Posmatrajmo prsten celih A kvadratnog polja K. Njega čine elementi $x \in K$ koji su integralni nad $\mathbb{Z}$. Ako $x \in A$, tada je $\sigma(x)$ koren iste jednačine integralne zavisnosti kao i x, odakle sledi $\sigma(x) \in A$. Sada imamo da je $x + \sigma(x) \in A$ i $x\sigma(x) \in A$. Ako je $x = a + b\sqrt{d}$ gde je $a, b \in \mathbb{Q}$, tada na osnovu (1) imamo

$$x + \sigma(x) = 2a \in \mathbb{Q} \quad \text{i} \quad x \cdot \sigma(x) = a^2 - db^2 \in \mathbb{Q}. \tag{3}$$

Kako je $\mathbb{Z}$ glavnoidealski i integralno zatvoren, dobijamo

$$2a \in \mathbb{Z}; \quad a^2 - db^2 \in \mathbb{Z} \tag{4}$$

Uslovi (3) su potrebni u slučaju da je $x = a + b\sqrt{d}$ integralan nad $\mathbb{Z}$. Oni su takođe i dovoljni, jer je x koren od $X^2 - 2aX + a^2 - db^2 = 0$. Na osnovu (3), $(2a)^2 - d(2b)^2 \in \mathbb{Z}$. Kako $2a \in \mathbb{Z}$, imamo da je $d(2b)^2 \in \mathbb{Z}$. S druge strane, d je kvadratno slobodan, pa ako $2b$ ne bi bio ceo broj, njegov imenilac bi sadržao prost faktor p. Ovaj prosti faktor bi se pojavljivao kao p^2 u imeniocu od $(2b)^2$. Množenjem sa d, $(2b)^2$ neće pripadati $\mathbb{Z}$. Možemo zaključiti da $2b \in \mathbb{Z}$.

Ukratko, možemo uzeti da je $a = \frac{u}{2}, b = \frac{v}{2}$, gde je $u, v \in \mathbb{Z}$. Uslovi (3) sada postaju:

$$u^2 - dv^2 \in 4\mathbb{Z}. \tag{5}$$

Ako je v paran, (4) nam pokazuje da je u paran takođe. U ovom slučaju $a, b \in \mathbb{Z}$. Ako je v neparan, tada $v^2 \equiv 1(\text{mod } 4)$. u^2 je 0 ili 1 modulo 4 (jedini kvadrati mod 4). Kako je d kvadratno slobodan, on nije umnožak od 4. Sada je $u^2 \equiv 1(\text{mod } 4)$ i $d \equiv 1(\text{mod } 4)$. Upravo smo pokazali da važi sledeća teorema:

Teorema A.2. *Neka je $K = \mathbb{Q}(\sqrt{d})$ kvadratno polje gde je $d \in \mathbb{Z}$ kvadratno slobodan.*

(a) Ako je $d \equiv 2$ ili $d \equiv 3(\text{mod } 4)$, tada prsten celih A polja K sadrži sve elemente oblika $a + b\sqrt{d}$ gde je $a, b \in \mathbb{Z}$.

(b) Ako je $d \equiv 1(\text{mod } 4)$, tada prsten celih A polja K sadrži sve elemente oblika $\frac{1}{2}(u + v\sqrt{d})$ gde $u, v \in \mathbb{Z}$ i u i v su iste parnosti.

Prsten A u slučaju (a) možemo zapisati kao $A = \mathbb{Z} + \mathbb{Z}\sqrt{d}$ a u slučaju (b) kao $A = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{d}}{2}$, jer je $\frac{u-v+v(1+\sqrt{d})}{2} = \frac{u-v}{2} + v \cdot \frac{1+\sqrt{d}}{2}$ i $\frac{u-v}{2} \in \mathbb{Z}$.

U slučaju (a), $(1, \sqrt{d})$ je baza za A kao $\mathbb{Z}$-modula. U slučaju (b), $(1, \frac{1}{2}(1 + \sqrt{d}))$ je baza za A nad $\mathbb{Z}$. Zaista, na osnovu (b) 1 i $\frac{1}{2}(1 + \sqrt{d})$ pripadaju A. Da bismo pokazali da se $\frac{1}{2}(u + v\sqrt{d})$ može prikazati kao $\mathbb{Z}$-linearna kombinacija od 1 i $\frac{1}{2}(1 + \sqrt{d})$, može se oduzimanjem $\frac{1}{2}(1 + \sqrt{d})$ problem svesti na slučaj kada su u i v parni. U ovom slučaju

$$\frac{1}{2}(u + v\sqrt{d}) = \left(\frac{u}{2} - \frac{v}{2}\right) \cdot 1 + v \cdot \frac{1}{2}(1 + \sqrt{d}).$$

Definišimo sada realna kvadratna i imaginarna kvadratna polja.

Ako je $d > 0$, $\mathbb{Q}(\sqrt{d})$ se zove realno kvadrano polje.

Ako je $d < 0$, $\mathbb{Q}(\sqrt{d})$ se zove imaginarno kvadratno polje.

Navedimo sada neke primere.

Primer 1. Odrediti prsten celih u kvadratnom raširenju $K = \mathbb{Q}(\sqrt{17})$ i odrediti bar jednu njegovu integralnu bazu.

Kako je $17 \equiv 1(\text{mod } 4)$ imamo slučaj (b) Teoreme A.2. Prsten celih je $A = \mathbb{Z} + \mathbb{Z}\frac{1+\sqrt{17}}{2}$. Integralna baza je $(1, \frac{1}{2}(1 + \sqrt{17}))$.

Primer 2. Odrediti prsten celih u kvadratnom raširenju $K = \mathbb{Q}(i)$ i odrediti bar jednu njegovu integralnu bazu.

Kako je $-1 \equiv 3(\text{mod } 4)$ imamo slučaj (a) Teoreme A.2. Prsten celih je $A = \mathbb{Z} + \mathbb{Z}\sqrt{d}$. Integralna baza je $(1, i)$.

Napomene

Izvor za ovaj dodatak je [7].

Literatura

[1] E. Bach, J. Shallit, *Algorithmic Number Theory, Volume I: Efficient Algorithms*, Cambridge, Massachusetts, London, 1996.

[2] K. Ireland, M. Rosen *A Classical Introduction to Modern Number Theory*, Springer, New York, 1992.

[3] F. Lemmermeyer, *Reciprocity Laws From Euler to Eisenstein*, Springer, Heidelberg, 1999.

[4] M.R. Murty, J. Esmonde *Problems in Algebaric Number Theory*, Springer, Kingston 2004.

[5] I. Niven, H. S. Zuckerman, H.L. Montgomery *An Introduction to the Theory of Numbers*, John Wiley and Sons, New York, 1991.

[6] P. Ribenboim, *Algebaric Numbers*, Wiley-interscience, Kingston, 1972.

[7] P. Samuel, *Algebaric Theory of Numbers*, Hermann, Paris, 1970.

[8] R. Saptharishi, *Lecture notes on Solovay-Strassen Primality Testing*, Chennai Mathematical Institute