Tartu Ülikool
Matemaatika-informaatikateaduskond
Matemaatika instituut
Matemaatika eriala

Anu Ahven

Biruutvastavusseadus

Bakalaureusetöö (9 EAP)

Juhendaja: Lauri Tart

Tartu 2015

Biruutvastavusseadus

Bakalaureusetöö
Anu Ahven

Lühikokkuvõte. Käesolevas bakalaureusetöös sõnastatakse biruutvastavusseadus ja esitatakse selle täielik detailne tõestus. Mainitud seadus seob neljanda astme kongruentside lahenduvuse üle Gaussi täisarvude ringi mooduli kujuga analoogiliselt Gaussi ruutvastavusseaduse ning Legendre'i ja Jacobi sümbolitega. Täieliku tõestuseni jõudmiseks kasutatakse Gaussi algarvude ja primaarsete Gaussi täisarvude klassifikatsiooni ning Gaussi ja Jacobi summasid üle lõplike korpuste.

Märksõnad. Gaussi algarvud, biruutvastavusseadus, Gaussi summad, Jacobi summad.

Quartic reciprocity

Bachelor's thesis
Anu Ahven

Abstract. The thesis formulates and gives a complete, fully detailed proof of the law of quartic reciprocity. This law relates the solvability of quartic congruences over the ring of Gaussian integers with the form of the modulus, similar to Gauss' law of quadratic reciprocity and the Legendre and Jacobi symbols. The complete proof requires classifying Gaussian primes and primary Gaussian integers as well as the use of Gauss and Jacobi sums over finite fields.

Keywords. Gaussian primes, quartic reciprocity, Gauss sum, Jacobi sum.

Sisukord

Sissejuhatus

Käesoleva bakalaureusetöö üldiseks valdkonnaks on arvuteooria, täpsemalt algebraline arvuteooria. Töö eesmärgiks on anda täielik detailne tõestus biruutvastavusseadusele, mis seob neljanda astme kongruentside lahenduvuse mooduli kujuga. Biruutvastavusseadus on üks esimesi vaheastmeid tänapäevase algebralise arvuteooria ja Gaussi ruutvastavusseaduse vahel ning selle tõestus illustreerib ilmekalt arvuteoorias kasutatavate algebraliste vahendite arengut.

1796. aastal tõestas Carl Friedrich Gauss nüüd tema nime kandva ruutvastavusseaduse, mida peetakse üheks arvuteooria ilusamaks ja sügavamaks tulemuseks. Esimesed oletused ruutvastavuse üldistuste kohta tegi Leonhard Euler ning nendega jätkas Gauss ise. Peagi taipas viimane, et biruutvastavuse sõnastamiseks ning tõestamiseks on vaja täisarvude mõistet laiendada. Antud laiendust tuntakse tänapäeval kui Gaussi täisarvude ringi $\mathbb{Z}[i]$.

Biruutvastavuse esimene täielik tõestus avaldati aastal 1844 ning selle autoriks oli Ferdinand Gotthold Eisenstein. Tegelikkuses aga oli Carl Gustav Jacob Jacobi antud tõestused esitanud juba aastal 1837 oma Königsbergi loengutes.

Antud bakalaureusetöö on referatiivne ning selle kirjutamisel oli põhiallikaks K. Irelandi ja M. Roseni arvuteooria õpik [3]. Samuti on olulise lähteallikana kasutatud bakalaureusetööd [2], kusjuures käesolevat bakalaureusetööd võib lugeda eelmainitud töö jätkuks. Veel on kasutatud algebra õpikut [4], raamatut [1] ja loengukonspekti [5]. Töö koosneb kuuest peatükist.

Esimene peatükk on sissejuhatav ning selles tuuakse välja olulisemad algebra ja arvuteooria valdkonda kuuluvad põhimõisted ja -omadused, mida antud töös vaja läheb.

Teises peatükis on vaatluse all Gaussi algarvud. Gaussi algarvud jaotatakse esimest ja teist liiki Gaussi algarvudeks ning normiga 2 Gaussi algarvudeks. Samuti kirjeldatakse mõlemat liiki Gaussi algarvude norme.

Kolmandas peatükis vaadeldakse faktoriaalse ringi $\mathbb{Z}[i]$ primaarseid elemente. Tuuakse välja primaarsuseks tarvilikud tingimused Gaussi täisarvude reaal- ja imaginaarosa kordajate jaoks ning näidatakse, et iga primaarne element on avaldatav primaarsete taandumatute elementide korrutisena.

Neljandas peatükis tuuakse sisse biruutjäägi sümbol ja tuletatakse selle põhiomadused, mida on vaja biruutvastavusseaduse tõestamiseks.

Viies peatükk kirjeldab korpuste multiplikatiivseid karakteristikuid ning Gaussi ja Jacobi summasid üle lõplike korpuste. Sealsamas tõestatakse ära rida biruutvastavuse näitamiseks vajalikke seoseid.

Kuuendas ehk viimases peatükis sõnastatakse ja tõestatakse biruutvastavusseadus, liikudes erijuhtudelt üldjuhule.

1 Põhimõisted ja -omadused

Esmalt defineerime antud töös kasutatavad põhimõisted ning sõnastame rea edaspidi vajalikke seoseid.

Definitsioon 1.1. *Gaussi täisarvudeks* nimetatakse kompleksarve, mille reaalosa ja imaginaarosa kordaja on täisarvud.

Kõigi Gaussi täisarvude hulka tähistame edaspidi sümboliga $\mathbb{Z}[i]$. Seega

$$\mathbb{Z}[i] = \{a + bi : a, b \in \mathbb{Z}\}.$$

Sümbolitega $|\alpha|$ ja $\overline{\alpha}$ tähistame vastavalt kompleksarvu α moodulit ja kaaskompleksarvu.

Lause 1.2 ([2], lause 1.2)**.** *Ring $\mathbb{Z}[i]$ on kommutatiivne nulliteguriteta ring.*

Definitsioon 1.3. Gaussi täisarvu $\alpha = a + bi$ *normiks* $N(\alpha)$ nimetatakse tema mooduli ruutu, s.t. mittenegatiivset täisarvu $N(\alpha) = a^2 + b^2$.

Lause 1.4 ([2], lause 2.8)**.** *Kahe Gaussi täisarvu korrutise norm võrdub nende arvude normide korrutisega, s.t. $N(\alpha\beta) = N(\alpha) \cdot N(\beta)$ mistahes $\alpha, \beta \in \mathbb{Z}[i]$ korral.*

Definitsioon 1.5. Öeldakse, et kommutatiivse ringi R element a *jagab* elementi $b \in R$, ja kirjutatakse $a \mid b$, kui leidub element $c \in R$ nii, et $ac = b$.

Lause 1.6 ([2], lause 2.11)**.** *Kui $\beta \mid \alpha$ ringis $\mathbb{Z}[i]$, siis $N(\beta) \mid N(\alpha)$ ringis $\mathbb{Z}$.*

Lause 1.7 ([2], lause 2.14)**.** *Pööratavad Gaussi täisarvud on $1, -1, i$ ja $-i$.*

Tähistame kõigi pööratavate Gaussi täisarvude hulka sümboliga $U(\mathbb{Z}[i])$. Järelikult

$$U(\mathbb{Z}[i]) = \{1, -1, i, -i\}.$$

Lause 1.8 (**Jäägiga jagamine**, [2], lause 2.19)**.** *Kui α ja $\beta \neq 0$ on Gaussi täisarvud, siis leiduvad sellised Gaussi täisarvud q ja r (jagatis ja jääk), et*

$$\alpha = \beta q + r \text{ ning } N(r) < N(\beta).$$

Definitsioon 1.9. Olgu R nulliteguriteta ring. Elemente a ja b nimetatakse *assotsieeritud elementideks*, kui leidub pööratav $c \in R$ nii, et $a = cb$.

Definitsioon 1.10. Nulliteguriteta ringi R nimetatakse *faktoriaalseks ringiks*, kui tema mistahes nullist erinev mittepööratav element on esitatav taandumatute elementide korrutisena ning selline esitus on ühene selles mõttes, et kui mittepööratav element $a \in \mathbb{R}\backslash\{0\}$ on esitatav korrutisena

$$a = p_1 p_2 \dots p_r$$

ja samuti korrutisena

$$a = q_1 q_2 \dots q_s,$$

kus $p_1, p_2, \dots, p_r, q_1, q_2, \dots, q_s$ on taandumatud elemendid, siis $r = s$ ning pärast tegurite võimalikku ümberjärjestamist on elemendid p_i ja q_i assotsieeritud iga $i = 1, 2, \dots, r$ korral.

Teoreem 1.11 ([2], teoreem 2.21)**.** *Gaussi täisarvude ring on faktoriaalne ring.*

Definitsioon 1.12. Kommutatiivse ringi R elemente a ja b nimetatakse *kongruentseteks* mooduli $c \in R$ järgi ja kirjutatakse $a \equiv b \pmod{c}$, kui $c \mid b - a$.

Definitsioon 1.13. Kommutatiivse ringi R mittetühja alamhulka I nimetatakse ringi R *ideaaliks* kui on täidetud järgmised tingimused:

1) $a + b \in I$ mistahes $a, b \in I$ korral,

2) $ar \in I$ mistahes $a \in I$ ja $r \in R$ korral.

Definitsioon 1.14. Ringi, mille nullist erinevad elemendid moodustavad korrutamise suhtes rühma, nimetatakse *korpuseks*.

Definitsioon 1.15. Lõpliku rühma G *elemendi* g *järk* on vähim naturaalarv k, mille korral $g^k = 1$.

Teoreem 1.16 (**Lagrange'i teoreem**)**.** *Lõpliku rühma elemendi järk on rühma järgu jagaja.*

Kui korpus K on lõplik, siis rühm $(K, +)$ on lõplik rühm ning kõik tema elemendid peavad olema lõplikku järku. Olgu p ühikelemendi $1 \in K$ järk aditiivses rühmas $(K, +)$. Siis öeldakse, et korpuse K *karakteristika* on p.

Definitsioon 1.17. Öeldakse, et rühm on *tsükliline*, kui temas leidub element, mille astmetena avalduvad kõik selle rühma elemendid.

Sellist elementi nimetatakse tsüklilise rühma *moodustajaks* ehk tekitajaks.

Teoreem 1.18 ([5], teoreem 7.9)**.** *Iga lõpliku kommutatiivse korpuse multiplikatiivne rühm on tsükliline.*

Definitsioon 1.19. Lõpliku korpuse $\mathbb{F}_q$ multiplikatiivse rühma $\mathbb{F}_q^*$ moodustajat nimetatakse korpuse $\mathbb{F}_q$ *primitiivseks elemendiks*, s.t. $a \in \mathbb{F}_q$ on primitiivne, kui $\mathbb{F}_q^* = \{a, a^2, \ldots, a^{q-2}, a^{q-1} = 1\}$.

Lemma 1.20 ([5], lemma 8.7)**.** *Kui kommutatiivse korpuse K karakteristika on p, siis iga $a, b \in K$ ja $n \in \mathbb{N}$ korral kehtib*

$$(a+b)^{p^n} = a^{p^n} + b^{p^n}.$$

Lemma 1.21 ([5], lemma 8.8)**.** *Kui K on lõplik korpus ning $|K| = q$, siis iga $a \in K^*$ korral $a^{q-1} = 1$.*

Definitsioon 1.22. *n. astme ühejuureks* nimetatakse n. astme juurt kompleksarvust 1.

Definitsioon 1.23. n. astme ühejuurt nimetatakse *n. astme algjuureks*, kui tema astmetena on avaldatavad kõik n. astme ühejuured.

2 Gaussi algarvud

Järgmisena defineerime Gaussi algarvud ja jaotatame need esituse järgi kolme liiki. Lisaks toome ära nende tähtsamad omadused.

Definitsioon 2.1. Olgu R ring. Mittepööratavat elementi $a \in R$ nimetatakse *taandumatuks*, kui teda ei saa esitada kahe mittepööratava elemendi korrutisena, s.t. kui võrdusest $a = bc$, kus $b, c \in R$, järeldub, et kas b on pööratav või c on pööratav.

Tähistame sümboliga $\mathbb{P}$ kõigi algarvude hulka. Ringi $\mathbb{Z}[i]$ taandumatuid elemente nimetatakse *Gaussi algarvudeks*. Iga Gaussi algarvu norm on kas algarv või algarvu ruut ([2], teoreem 4.32).

Definitsioon 2.2. Gaussi algarve, mille norm on paaritu algarv, nimetatakse *esimest liiki* Gaussi algarvudeks. Gaussi algarve, mille norm on algarvu ruut, nimetatakse *teist liiki* Gaussi algarvudeks.

Lemma 2.3 (**Eukleidese lemma**)**.** *Mistahes $a, b, c \in \mathbb{Z}[i]$ korral, kui $a \mid bc$ ja $(a, b) = 1$, siis $a \mid c$.*

TÕESTUS. Et $(a, b) = 1$, siis õpiku [4] lause 6.13.2 põhjal leiduvad sellised Gaussi täisarvud x_0 ja y_0, et $ax_0 + by_0 = 1$. Järelikult $ax_oc + by_0c = c$. Kuna a jagab selle võrduse vasakut poolt, peab ta jagama ka selle paremat poolt, s.t. $a \mid c$. □

Lemma 2.4. *Kui π on Gaussi algarv ja $\pi \mid ab$, siis $\pi \mid a$ või $\pi \mid b$.*

Lemma 2.5. *Kui π on Gaussi algarv, siis leidub algarv $p \in \mathbb{Z}$ nii, et $\pi \mid p$.*

TÕESTUS. Kuna $N(\pi) = \pi\overline{\pi}$, siis $\pi \mid N(\pi)$. Samas $N(\pi) > 1$ ja seega $N(\pi) = p_1 \dots p_s$, kus p_i on algarvud. Järelikult $\pi \mid p_1 \dots p_s$ ning Eukleidese lemmat rakendades näeme, et $\pi \mid p_i$, mingi i korral. □

Teoreem 2.6 ([2], teoreem 4.28)**.** *Kui $\alpha \in \mathbb{Z}[i]$ ja $N(\alpha)$ on algarv, siis α on Gaussi algarv.*

Teoreem 2.7 ([2], teoreem 4.36)**.** *Iga kujul $4n+1$ olevat algarvu, kus $n \in \mathbb{N}$, saab lahutada kahe esimest liiki Gaussi algarvu korrutiseks.*

Järelikult iga kujul $4n + 1$ olev algarv on mingi esimest liiki Gaussi algarvu π norm $N(\pi)$.

Lause 2.8. *Kui π on esimest liiki Gaussi algarv, siis $p \equiv 1 \pmod 4$, kus $p = \pi\overline{\pi} = N(\pi)$.*

TÕESTUS. Vaatleme esimest liiki Gaussi algarvu $\pi = a + bi$. Siis

$$p = N(\pi) = N(a + bi) = a^2 + b^2,\ p \in \mathbb{P},\ a, b \in \mathbb{Z}.$$

Et p on paaritu, siis peab üks täisarvudest a ja b olema paaritu. Üldisust kitsendamata võime eeldada, et a on paaritu ja b paaris, s.t. $a = 2k+1, b = 2l$, $k, l \in \mathbb{Z}$. Seega

$$\begin{aligned} p = a^2 + b^2 &= (2k+1)^2 + (2l)^2 \\ &= 4k^2 + 4k + 1 + 4l^2 \equiv 1 \pmod 4. \end{aligned}$$

□

Lause 2.9 ([2], lause 4.33)**.** *Iga algarv kujul* $4n+3$*, kus* $n \in \mathbb{N} \cup \{0\}$*, on teist liiki Gaussi algarv.*

Lause 2.10. *Kui* q *on teist liiki Gaussi algarv, siis* $|q| \equiv 3 \pmod 4$.

TÕESTUS. Vaatleme teist liiki Gaussi algarvu q. Oletame vastuväiteliselt, et $p = |q| \equiv 1 \pmod 4$. Sel juhul vastavalt teoreemile 2.7 kehtib

$$|q| = p = \pi\overline{\pi}$$

ning oleme saanud vastuolu sellega, et q on taandumatu. □

Teoreemist 2.6 ja bakalaureusetöö [2] teoreemist 4.37 järeldub vahetult järgmine tulemus.

Lemma 2.11. *Gaussi täisarv* $1 + i$ *on Gaussi algarv ja* $2 = -i(1+i)^2$ *on elemendi* 2 *esitus Gaussi algarvude korrutisena.*

Kokkuvõttes saame Gaussi täisarvud jagada kolmeks:

1. Esimest liiki Gaussi algarvud π, kus $N(\pi) = p \equiv 1 \pmod 4$, $p \in \mathbb{P}$.
2. Teist liiki Gaussi algarvud $q = u \cdot p$, kus $u \in U(\mathbb{Z}[i])$ ja $p \in \mathbb{P}$ ning $p \equiv 3 \pmod 4$.
3. Normiga 2 Gaussi algarvud $1 + i,\ 1 - i,\ -1 + i,\ -1 - i$.

3 Primaarsed elemendid

Selles peatükis tõestame Gaussi täisarvude primaarsuseks piisavad ja tarvilikud tingimused nende reaal- ja imaginaarosa kordajate jaoks. Peatüki lõpus veendume, et iga primaarset elementi saab avaldada primaarsete taandumatute elementide korrutisena.

Definitsioon 3.1. Mittepööratavat elementi $\alpha \in \mathbb{Z}[i]$ nimetatakse *primaarseks*, kui $\alpha \equiv 1 \pmod{(1+i)^3}$.

Lemma 3.2. *Mittepööratav element $\alpha = a + bi$ on primaarne parajasti siis, kui $a \equiv 1 \pmod 4$ ja $b \equiv 0 \pmod 4$ või $a \equiv 3 \pmod 4$ ja $b \equiv 2 \pmod 4$.*

Tõestus. Et $(1+i)^3 = 2i(i+1) = -2+2i$, siis $a+bi$ on primaarne parajasti siis, kui

$$\frac{(a-1)+bi}{-2+2i} = \frac{(a-1+bi)(-2-2i)}{8} = \frac{-a+1+b}{4} + \frac{-b-a+1}{4}i \in \mathbb{Z}[i].$$

Siit $a - b \equiv 1 \pmod 4$ ja $a + b \equiv 1 \pmod 4$. Kongruentside liitmisel saame tulemuseks $2a \equiv 2 \pmod 4$ ehk $a \equiv 1 \pmod 2$ ning seega $a \equiv 1 \pmod 4$ või $a \equiv 3 \pmod 4$. Kongruentside lahutamisel saame $2b \equiv 0 \pmod 4$ ehk $b \equiv 0 \pmod 2$ mistõttu $b \equiv 0 \pmod 4$ või $b \equiv 2 \pmod 4$.
Kui $a \equiv 1 \pmod 4$ ja $b \equiv 2 \pmod 4$, siis

$$a - b \equiv 1 - 2 = 3 \pmod 4$$

ning

$$a + b \equiv 1 + 2 = 3 \pmod 4,$$

mis ei ole kooskõlas eelnevaga. Samuti, kui $a \equiv 3 \pmod 4$ ja $b \equiv 0 \pmod 4$, siis $a + b$ ja $a - b$ ei ole kongruentsed arvuga 1 mooduli 4 järgi. Seega on antud variantidest sobilikud vaid paarid $a \equiv 1 \pmod 4$ ja $b \equiv 0 \pmod 4$ ning $a \equiv 3 \pmod 4$ ja $b \equiv 2 \pmod 4$, mis ilmselt rahuldavad tingimusi $a - b \equiv 1 \pmod 4$ ja $a + b \equiv 1 \pmod 4$. □

Pööratavad Gaussi täisarvud on $1, -1, i$ ja $-i$. Järgnevas tabelis on kokku võetud kõik võimalikud pööratavate Gaussi täisarvude vahed. Nüüd on lihtne näha, et kahe pööratava Gaussi täisarvu vahe norm on kas 0, 2 või 4.

$-$	1	-1	i	$-i$
1	0	2	$1-i$	$1+i$
-1	-2	0	$-1-i$	$-1+i$
i	$i-1$	$i+1$	0	$2i$
$-i$	$-i-1$	$-i+1$	$-2i$	0

Tabel 1. *Pööratavate Gaussi täisarvude vahed.*

Lemma 3.3. *Kui* $a \equiv b \pmod{c}$*, kus* $a, b \in U(\mathbb{Z}[i])$ *ja* $|c| > 2$*, siis* $a = b$*.*

TÕESTUS. Olgu $a, b \in U(\mathbb{Z}[i])$ ja $a \equiv b \pmod{c}$. Siis $c \mid a - b$ ja $N(c) \mid N(a-b) \in \{0, 2, 4\}$. Kuid $|c| > 2$ ja seega $N(c) \geq 5$, järelikult oleme jõudnud vastuoluni. □

Lemma 3.4. *Olgu* $\alpha = a + bi \in \mathbb{Z}[i]$ *mittepööratav ja* $(1+i) \nmid \alpha$*. Siis leidub üheselt määratud pööratav element* u *nii, et* $u\alpha$ *on primaarne.*

TÕESTUS. Esimese sammuna näitame, et leidub pööratav element $\varepsilon \in \{1, i\}$ selliselt, et $\varepsilon\alpha = a' + b'i$, kus a' on paaritu ja b' paaris. Veendume esmalt, et a ja b on erineva paarsusega. Oletame, et $2 \mid a$ ja $2 \mid b$. Sellisel juhul, kuna $(1+i)(1-i) = 2$, kehtib $(1+i) \mid \alpha$, mis on vastuolus eeldusega. Kui aga $2 \nmid a$ ja $2 \nmid b$, siis

$$a + bi = a + ai + (b - a)i,$$

kus $2 \mid b - a$. Järelikult $1 + i \mid b - a, 1 + i \mid a(1 + i)$ ja seetõttu $1 + i \mid a + bi$, mis on vastuolus eeldusega $1 + i \nmid \alpha$. Seega a ja b on eri paarsustega. Kui nüüd a on paaris, siis $i(a + bi) = -b + ai$ on selline, kus $-b$ on paaritu ja võime võtta $\varepsilon = i$. Juhul, kui a on paaritu, võtame $\varepsilon = 1$.
Kui meil peaks olema olukord, kus $a \equiv 1 \pmod{4}$ ja $b \equiv 2 \pmod{4}$ või $a \equiv 3 \pmod{4}$ ja $b \equiv 0 \pmod{4}$, siis korrutame kongruentsid elemendiga -1. Seejärel saame

$$-a \equiv -1 = 3 \pmod{4} \quad \text{ja} \quad -b \equiv -2 = 2 \pmod{4}$$

või

$$-a \equiv -3 = 1 \pmod{4} \quad \text{ja} \quad -b \equiv 0 \pmod{4}.$$

Et a ja $-a$ ning b ja $-b$ on assotsieeritud, olemegi saanud olukorra, kus $a \equiv 1 \pmod{4}$ ja $b \equiv 0 \pmod{4}$ või $a \equiv 3 \pmod{4}$ ja $b \equiv 2 \pmod{4}$. Nüüd näeme lemma 3.2 põhjal, et α on assotsieeritud primaarse elemendiga $u\alpha$, kus $u \in U(\mathbb{Z}[i])$ sõltub eelnevatest sammudest.
Näitame, et leidub ainult üks selline u, mille korral $u\alpha$ on primaarne. Oletame vastuväiteliselt, et $u_1 \neq u_2$, kuid $u_1\alpha$ ja $u_2\alpha$ on primaarsed. Seega $u_1\alpha \equiv 1 \pmod{(1+i)^3}$ ja $u_2\alpha \equiv 1 \pmod{(1+i)^3}$. Järelikult

$$(u_1 - u_2)\alpha \equiv 0 \pmod{(1+i)^3}.$$

Nüüd Eukleidese lemmat kasutades näeme, et $1 + i$ algarvulisuse tõttu kehtib $(1 + i)^3 \mid (u_1 - u_2)$. Siis lause 1.6 põhjal $8 = N(1 + i)^3 \mid N(u_1 - u_2)$. Kuid tabelist 1 teame, et $N(u_1 - u_2) \in \{0, 2, 4\}$ ja seetõttu oleme jõudnud vastuoluni. Seega $u_1 = u_2$. □

Lemma 3.5. *Iga primaarne element on avaldatav primaarsete taandumatute elementide korrutisena.*

TÕESTUS. Olgu $\alpha \in \mathbb{Z}[i]$ primaarne, s.t. $\alpha \equiv 1 \pmod{(1+i)^3}$. Kuna $\mathbb{Z}[i]$ on faktoriaalne ring, saame α avaldada Gaussi algarvude korrutisena, s.t. $\alpha = \prod_i r_i$. Siis $N(\alpha) = \prod_i N(r_i)$. Paneme tähele, et $r_i \notin (1+i) \cdot U(\mathbb{Z}[i])$, sest muidu peaks kehtima $1+i \mid \alpha$ ja primaarsuse tõttu $1+i \mid \alpha - 1$, kust $1+i \mid 1$. Lause 1.6 põhjal siis $2 = N(1+i) \mid N(1) = 1$, mis ilmselt ei kehti. Seega võib r_i tegurid jaotada teist liiki Gaussi algarvudeks $q_k = u_k \cdot p_k$, kus $u_k \in U(\mathbb{Z}[i]), p_k \in \mathbb{P}$, $p_k \equiv 3 \pmod 4$ ja esimest liiki Gaussi algarvudeks π_l, $N(\pi_l) = p \equiv 1 \pmod 4$. Et

$$1+i \nmid \pi_l, \text{ sest } N(1+i) = 2 \nmid p = N(\pi_l),$$

siis lemma 3.4 põhjal leidub selline $v_l \in U(\mathbb{Z}[i])$, et $v_l \cdot \pi_l$ on primaarne. Olgu $u = \prod_k (-u_k) \cdot \prod_l v_l^{-1}$. Siis

$$\alpha = u \cdot \prod_k (-p_k) \prod_l v_l \pi_l,$$

kus elemendid $-p_k, v_l\pi_l$ on lemma 3.2 põhjal primaarsed. Siis

$$1 \equiv \alpha = u \cdot \prod_k (-p_k) \prod_l v_l \pi_l \equiv u \cdot 1 \cdot 1 \cdot \ldots \cdot 1 = u \pmod{(1+i)^3},$$

ehk $u \equiv 1 \pmod{(1+i)^3}$. Kui $u \in \{i, -1, -i\}$, siis $N(u-1) \in \{2, 4\}$ ja $(1+i)^3 \mid (u-1)$, mistõttu

$$8 = N((1+i)^3) \mid N(u-1) \in \{2, 4\},$$

mis on võimatu. Järelikult $u = 1$.

□

4 Biruutjäägi sümbol

Olgu R ring ja fikseerime $a \in R$. Siis elemendi a poolt moodustatud *pea-ideaaliks* on hulk

$$I := a \cdot R = \{a \cdot r : r \in R\}.$$

Olgu I ringi R ideaal ja $a \in R$. Hulka

$$\overline{a} = a + I = \{a + b : b \in I\}$$

nimetatakse *kõrvalklassiks* ideaali I järgi esindajaga a. Vaatleme hulka

$$R/I = \{\overline{x} = x + I : x \in R\},$$

kus $\overline{x}$ on ringi R kõrvalklass ideaali I järgi. Defineerime hulgas R/I liitmise ja korrutamise järgmiselt:

$$\overline{x} + \overline{y} = \overline{x + y},$$
$$\overline{x} \cdot \overline{y} = \overline{x \cdot y}$$

mistahes $x, y \in R$ korral. Hulk R/I osutub siis eelnevalt defineeritud tehete suhtes ringiks. [4]

Definitsioon 4.1. Eelnevalt defineeritud ringi R/I nimetatakse ringi R *faktorringiks* ideaali I järgi.

Olgu edaspidi $\pi \in \mathbb{Z}[i]$ taandumatu ja vaatleme faktorringi

$$\mathbb{Z}[i]_\pi := \mathbb{Z}[i]/\pi\mathbb{Z}[i] = \{[\alpha]_\pi = \alpha + \pi\mathbb{Z}[i] : \alpha \in \mathbb{Z}[i]\}.$$

Lause 4.2. *Olgu $\pi \in \mathbb{Z}[i]$ Gaussi algarv. Siis faktorring $\mathbb{Z}[i]_\pi$ on lõplik korpus, milles on $N(\pi)$ elementi.*

Tõestus. Selleks, et $\mathbb{Z}[i]_\pi$ oleks korpus, peame näitama, et tema iga nullist erineva elemendi jaoks leidub samas ringis pöördelement. Olgu $0 \neq [\alpha]_\pi \in \mathbb{Z}[i]_\pi$, s.t. $\pi \not| \alpha$. Paneme tähele, et $(\alpha, \pi) = 1$. Tõepoolest, kui $d := (\alpha, \pi) \neq 1$, siis teoreemi 1.8 põhjal $\alpha = \pi q + r$ ning $N(r) < N(\pi)$, kus $r \neq 0$, sest vastasel juhul $\pi \mid \alpha$. Lause 1.6 põhjal saame, et $N(d) \mid N(r)$. Kuna $N(d) \leq N(r) < N(\pi)$ ning $d \mid \pi$, siis peab kehtima võrratus $N(\frac{\pi}{d}) > 1$, seega $\pi = d \cdot \frac{\pi}{d}$ on Gaussi algarvu esitus kahe mittepööratava elemendi korrutisena, mis on võimatu. Teades nüüd, et $(\alpha, \pi) = 1$ ja rakendades õpiku [4] lauset 6.13.3, saame, et leiduvad elemendid $r_1, r_2 \in \mathbb{Z}[i]$ selliselt, et $1 = \alpha r_1 + \pi r_2$. Seega $\pi \mid 1 - \alpha r_1$ ning $[1 - \alpha r_1]_\pi = [0]_\pi$ ehk $[\alpha]_\pi [r_1]_\pi = [1]_\pi$, mis tähendab, et $[\alpha]_\pi$ on pööratav ringis $\mathbb{Z}[i]/\pi\mathbb{Z}[i]$. Seega faktorring $\mathbb{Z}[i]_\pi$ on tõepoolest korpus.

Teiseks tõestame, et korpuses $\mathbb{Z}[i]_\pi$ on $N(\pi)$ elementi. Kui meil on tegemist II liiki Gaussi algarvuga q, siis $N(q) = p^2, p \in \mathbb{P}$. Veendume, et

$$E := \{a + bi : 0 \leq a, b < p\}$$

on täielik taandatud jääkide süsteem, s.t. $\mathbb{Z}[i]_q = \{[\alpha]_q : \alpha \in E\}$. Esmalt valime vabalt $[\mu]_q = [m + ni]_q \in \mathbb{Z}[i]_q$. Jäägiga jagades saame, et $m = ps + a$ ja $n = pt + b$, kus $a, b, s, t \in \mathbb{Z}, 0 \leq a, b < p$. Siis $\mu \equiv a + bi \pmod{p}$ ehk $[\mu]_\pi = [a + bi]_\pi$, kusjuures $a + bi \in E$. Teiseks, olgu $a + bi \equiv a' + b'i \pmod{p}$, kus $0 \leq a, b, a', b' < p$. Sel juhul $a - a' + (b - b') \cdot i = p \cdot z$, kus $z \in \mathbb{Z}[i]$. Algarvuga p läbi jagades saame, et $\frac{a-a'}{p} + \left(\frac{b-b'}{p}\right) \cdot i = z$ ehk

$$\frac{a - a'}{p} + \left(\frac{b - b'}{p}\right) \cdot i \in \mathbb{Z}[i]$$

ja järelikult $\frac{a-a'}{p}, \frac{b-b'}{p} \in \mathbb{Z}$. Siit $a \equiv a' \pmod{p}$ ja $b \equiv b' \pmod{p}$ ning seetõttu $a = a', b = b'$. Seega $\mathbb{Z}[i]_q = \{[\alpha]_q : \alpha \in E\}$. Ilmselt $|E| = p^2 = N(q)$ ja järelikult $|\mathbb{Z}[i]_q| = |E| = N(q)$.

Kui meil on tegemist I liiki Gaussi algarvuga $\pi = a + bi$, siis $N(\pi) = p$, $p \in \mathbb{P}$. Paneme tähele, et $N(\pi) = N(a + bi) = a^2 + b^2 \nmid b$. Kontrollime, et

$$F = \{0, 1, \ldots, p - 1\}$$

on täielik taandatud jääkide süsteem. Olgu $[\mu]_\pi = [m + ni]_\pi \in \mathbb{Z}[i]_\pi$. Kuna $p \nmid b$, on b pööratav mooduli p järgi ja me saame leida sellise täisarvu c, et $cb \equiv n \pmod{p}$. Siis

$$\mu - c\pi = m + ni - c(a + bi) = m - ca + (n - cb)i \equiv m - ca \pmod{p}.$$

Arvestades, et $\pi \mid p = \pi \cdot \overline{\pi}$, siis kehtib $\mu \equiv m - ca \pmod{\pi}$, kusjuures $m - ca \in \mathbb{Z}$. Seega korpuse $\mathbb{Z}[i]_\pi$ iga elemendi esindajaks võib võtta täisarvu. Olgu $m - ca = sp + r$, kus $s, r \in \mathbb{Z}, 0 \leq r < p$, siis $m - ca \equiv r \pmod{p}$ ja seega $m - ca \equiv r \pmod{\pi}$. Järelikult on korpuse $\mathbb{Z}[i]_\pi$ iga element kongruentne mingi elemendiga hulgast $\{0, 1, \ldots, p - 1\} = F$ mooduli π järgi, ehk

$$\mathbb{Z}[i]_\pi = \{[\alpha]_\pi : \alpha \in F\}.$$

Lõpuks, kui $[r]_\pi = [r']_\pi$ ehk $r \equiv r' \pmod{\pi}$, kus $r, r' \in \mathbb{Z}, 0 \leq r, r' < p$, siis $r - r' = \pi y$, $y \in \mathbb{Z}[i]$. Siit $(r - r')^2 = N(r - r') = N(\pi y) = p \cdot N(y)$, mis tähendab, et $p \mid r - r'$ ringis $\mathbb{Z}$. Seega $r = r'$ ja $|\mathbb{Z}[i]_\pi| = |F| = p$. □

Lause 4.3 (**Fermat' väike teoreem Gaussi täisarvude jaoks**). *Kui π on Gaussi algarv ja $N(\pi) > 2$, siis kui $\pi \nmid \alpha$, siis $\alpha^{N(\pi)-1} \equiv 1 \pmod{\pi}$.*

TÕESTUS. Olgu $\mathbb{Z}[i]_\pi = \{\beta_1, \beta_2, \ldots, \beta_{N(\pi)} = [0]\}$. Et $\pi \nmid \alpha$, siis loengukonspekti [5] järelduse 9.13 põhjal $\mathbb{Z}[i]_\pi = \alpha\mathbb{Z}[i]_\pi$. Kuna kongruentsete elementide korrutamine säilitab kongruentsuse, siis korrutame läbi mõlema hulga nullist erinevad elemendid ja võrdleme neid:

$$\begin{aligned}\beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_{N(\pi)-1} &\equiv (\alpha\beta_1) \cdot (\alpha\beta_2) \cdot \ldots \cdot (\alpha\beta_{N(\pi)-1}) \pmod{\pi} \\ &\equiv \alpha^{N(\pi)-1}\beta_1 \cdot \beta_2 \cdot \ldots \cdot \beta_{N(\pi)-1} \pmod{\pi}.\end{aligned}$$

Tänu valikule $\beta_i \neq 0$ võime nad võrduse mõlemalt poolelt taandada ning saamegi $1 \equiv \alpha^{N(\pi-1)} \pmod{\pi}$. □

Lause 4.4. *Kui $\pi \nmid \alpha$ ja $N(\pi) \neq 2$, siis leidub üheselt määratud täisarv $0 \leq j \leq 3$, nii et*

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

TÕESTUS. Paneme tähele, et π on kas esimest või teist liiki Gaussi algarv, seega

$$N(\pi) = \begin{cases} p \equiv 1 \pmod 4, \text{kui } \pi \text{ on teist liiki Gaussi algarv,} \\ p^2 \equiv 3^2 \equiv 1 \pmod 4, \text{kui } \pi \text{ on esimest liiki Gaussi algarv.} \end{cases}$$

Seega $N(\pi) - 1$ jagub arvuga 4. Tähistame $\beta := \alpha^{\frac{N(\pi)-1}{4}}$. Teame, et polünoomil $x^4 = 1$ on maksimaalselt 4 juurt üle korpuse $\mathbb{Z}[i]_\pi$ ([4], lause 7.1.9). Kuna

$$1^4 = (-1)^4 = i^4 = (-i)^4 = 1,$$

siis ainsad lahendid ongi $1,\ -1,\ i,\ -i$. Need avalduvad kõik kujul i^j, kus $0 \leq j \leq 3$.

□

Definitsioon 4.5. Olgu π Gaussi algarv ja $N(\pi) \neq 2$. Biruutjäägi sümbol $\left(\frac{\alpha}{\pi}\right)_4$ defineeritakse seosega

$$\left(\frac{\alpha}{\pi}\right)_4 = \begin{cases} 0, \text{kui } \pi \mid \alpha, \\ i^j, \text{kui } \pi \nmid \alpha \text{ ja } \alpha^{\frac{N(\pi)-1}{4}} \equiv i^j \pmod{\pi}. \end{cases}$$

Järgmise lause puhul on eriti oluline omadus 1., mis seob omavahel biruutvastavusseaduse ja neljanda astme kongruentside lahenduvuse.

Lause 4.6. *Iga Gaussi algarvu π, kus $N(\pi) \neq 2$, korral on biruutjäägi sümbolil järgmised omadused.*

1. *Kui* $\pi \nmid \alpha$, *siis* $\left(\frac{\alpha}{\pi}\right)_4 = 1$ *parajasti siis, kui kongruents* $x^4 \equiv \alpha \pmod{\pi}$ *on lahenduv hulgas* $\mathbb{Z}[i]$.

2. *Iga* $\alpha, \beta \in \mathbb{Z}[i]$ *korral*

$$\left(\frac{\alpha\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \cdot \left(\frac{\beta}{\pi}\right)_4.$$

3. *Iga* $\alpha \in \mathbb{Z}[i]$ *korral*

$$\overline{\left(\frac{\alpha}{\pi}\right)_4} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 \quad \textit{ja} \quad \left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\overline{\pi}}\right)_4.$$

4. *Kui* $\pi = a + bi$ *on primaarne Gaussi algarv, siis* $\left(\frac{-1}{\pi}\right)_4 = (-1)^{\frac{a-1}{2}}$.

5. *Kui* $\alpha \equiv \beta \pmod{\pi}$, *siis* $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$.

6. *Kui* π *ja* λ *on assotsieeritud Gaussi algarvud, siis* $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\lambda}\right)_4$.

TÕESTUS. Paneme esmalt tähele, et $\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{\frac{N(\pi)-1}{4}} \pmod{\pi}$, kui $\pi \nmid \alpha$.

1. Kehtigu $\pi \nmid \alpha$. Siis $\left(\frac{\alpha}{\pi}\right)_4 = 1$ parajasti siis, kui $\alpha^{\frac{N(\pi)-1}{4}} \equiv 1 \pmod{\pi}$. Näitame, et võrrand $x^n = \alpha \in \mathbb{F}^*$ on lahenduv lõplikus korpuses $\mathbb{F}$ parajasti siis, kui $\alpha^{\frac{q-1}{d}} = 1$, kus $d = (n, q-1)$, $|\mathbb{F}| = q$.

   Olgu γ korpuse $\mathbb{F}^*$ primitiivne element, $\alpha = \gamma^a$ ja $x = \gamma^y$. Siis võrdus $\gamma^{yn} = \gamma^a$ on samaväärne kongruentsiga $yn \equiv a \pmod{q-1}$. Viimane on lahenduv parajasti siis, kui $d = (n, q-1) \mid a$, kusjuures lahenduval juhul on sellel kongruentsil d lahendit ([5], lause 6.2). Teiselt poolt $\alpha^{\frac{q-1}{d}} = \gamma^{\frac{a(q-1)}{d}} = 1$ parajasti siis, kui $\frac{a(q-1)}{d} \equiv 0 \pmod{q-1}$, mis on samaväärne sellega, et $\frac{a}{d} \in \mathbb{Z}$ ehk samuti $d \mid a$.

   Rakendades eelnevat korpuses $\mathbb{Z}[i]_\pi$, on kongruents $x^4 \equiv \alpha \pmod{\pi}$ hulgas $\mathbb{Z}[i]$ lahenduv parajasti siis, kui

$$1 \equiv \alpha^{\frac{N(\pi)-1}{(4,N(\pi)-1)}} = \alpha^{\frac{N(\pi)-1}{4}} \equiv \left(\frac{\alpha}{\pi}\right)_4 \pmod{\pi}.$$

2. Olgu $\alpha, \beta \in \mathbb{Z}[i]$. Kui $\pi \nmid \alpha$ ja $\pi \nmid \beta$, siis

$$\begin{aligned}\left(\frac{\alpha \cdot \beta}{\pi}\right)_4 &\equiv (\alpha \cdot \beta)^{\frac{N(\pi)-1}{4}} = \alpha^{\frac{N(\pi)-1}{4}} \cdot \beta^{\frac{N(\pi)-1}{4}} \\ &\equiv \left(\frac{\alpha}{\pi}\right)_4 \cdot \left(\frac{\beta}{\pi}\right)_4 \pmod{\pi}\end{aligned}$$

ja järelikult lemma 3.3 põhjal $\left(\frac{\alpha\cdot\beta}{\pi}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \cdot \left(\frac{\beta}{\pi}\right)_4$. Vaatame nüüd juhtu, kus $\pi \mid \alpha$ või $\pi \mid \beta$. Siis $\pi \mid \alpha \cdot \beta$ ja

$$\left(\frac{\alpha}{\pi}\right)_4 \cdot \left(\frac{\beta}{\pi}\right)_4 = 0 = \left(\frac{\alpha\beta}{\pi}\right)_4.$$

3. Olgu $\alpha \in \mathbb{Z}[i]$. Kuna $N(\pi) = N(\overline{\pi})$, siis

$$\overline{\left(\frac{\alpha}{\pi}\right)_4} \equiv \overline{\alpha^{\frac{N(\pi)-1}{4}}} \equiv \overline{\alpha}^{\frac{N(\overline{\pi})-1}{4}} \equiv \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 \pmod{\pi}$$

ning

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

Rakendades lemmat 3.3, saamegi, et $\overline{\left(\frac{\alpha}{\pi}\right)_4} = \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4$ ja $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\overline{\pi}}\right)_4$.

4. Et $\pi = a + bi$ on primaarne, siis kas $a \equiv 1 \pmod 4$ ja $b \equiv 0 \pmod 4$ või $a \equiv 3 \pmod 4$ ja $b \equiv 2 \pmod 4$ ehk $a = 4k+1$ ja $b = 4l$ või $a = 4k+3$ ja $b = 4l+2$, kus $k, l \in \mathbb{Z}$ (lemma 3.2). Esimesel juhul

$$\begin{aligned}\left(\frac{-1}{\pi}\right)_4 &\equiv (-1)^{\frac{16k^2+8k+1+16l^2-1}{4}} \\ &= (-1)^{4(k^2+l^2)+2k} = 1 \\ &= (-1)^{2k} = (-1)^{\frac{4k+1-1}{2}} \pmod{\pi}.\end{aligned}$$

Teisel juhul

$$\begin{aligned}\left(\frac{-1}{\pi}\right)_4 &\equiv (-1)^{\frac{16k^2+24k+9+16l^2+16l+4-1}{4}} \\ &= (-1)^{4(k^2+l^2+l)+6k+3} = -1 \\ &= (-1)^{2k+1} = (-1)^{\frac{4k+3-1}{2}} \pmod{\pi}\end{aligned}$$

ja seega omadus kehtib.

5. Kui $\alpha \equiv \beta \pmod{\pi}$, siis

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

Seega jällegi lause 3.3 põhjal $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\beta}{\pi}\right)_4$.

6. Eelduse kohaselt $\pi = u\lambda$, kus $u \in U(\mathbb{Z}[i])$, seega $N(\pi) = N(\lambda)$. Ilmselt iga $\alpha \in \mathbb{Z}[i]$ korral $\pi \mid \alpha$ parajasti siis, kui $\lambda \mid \alpha$. Seega kongruents

$$\left(\frac{\alpha}{\pi}\right)_4 \equiv \alpha^{\frac{N(\pi)-1}{4}} = \alpha^{\frac{N(\lambda)-1}{4}} \pmod{\pi}$$

annab meile ka

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

Lemma 3.3 põhjal saame, et $\left(\frac{\alpha}{\pi}\right)_4 = \left(\frac{\alpha}{\lambda}\right)_4$.

□

Lemma 4.7. *Olgu π Gaussi algarv. Kui $\pi \nmid \alpha$, siis*

$$\left(\frac{\alpha}{\pi}\right)_4^4 = 1.$$

TÕESTUS. Biruutjäägi sümboli definitsiooni kohaselt

$$\left(\left(\frac{\alpha}{\pi}\right)_4\right)^4 = (i^j)^4 = (i^4)^j = 1^j = 1.$$

□

Lause 4.8. *Olgu q teist liiki Gaussi algarv, $|q| \equiv 3 \pmod 4$. Siis $\left(\frac{a}{q}\right)_4 = 1$ iga $a \in \mathbb{Z}$ korral, kui $q \nmid a$.*

TÕESTUS. Et $p = |q| \equiv 3 \pmod 4$, siis $N(q) = q^2$. Kuna $4 \mid p+1$, siis Fermat' väikese teoreemi põhjal ([5], teoreem 5.13)

$$\left(\frac{a}{q}\right)_4 \equiv a^{\frac{q^2-1}{4}} = (a^{p-1})^{\frac{p+1}{4}} \equiv 1 \pmod{p}.$$

Kuna $p > 2$, siis $\left(\frac{a}{q}\right)_4 = 1$. □

Defineerime biruutjäägi sümboli ka mitte-algarvuliste Gaussi täisarvude jaoks.

Definitsioon 4.9. Olgu $\alpha, \beta \in \mathbb{Z}[i]$ ja $(1+i) \nmid \alpha$. Ringi $\mathbb{Z}[i]$ faktoriaalsuse tõttu $\alpha = \prod_i \lambda_i$, kus λ_i on esimest või teist liiki Gaussi algarvud. Juhul kui $(\alpha, \beta) = 1$, siis defineerime $\left(\frac{\beta}{\alpha}\right)_4$ järgmiselt:

$$\left(\frac{\beta}{\alpha}\right)_4 = \prod_i \left(\frac{\beta}{\lambda_i}\right)_4.$$

Lause 4.6 omaduse 6. põhjal on selline definitsioon korrektne.

Lause 4.10. *Olgu $\alpha \in \mathbb{Z} \setminus \{0\}$, $a \in \mathbb{Z}$ paaritu ning $|a| > 1$. Kui $(a, \alpha) = 1$, siis*

$$\left(\frac{\alpha}{a}\right)_4 = 1.$$

TÕESTUS. Lause 4.6 omaduse 6. põhjal võime eeldada, et $a > 0$. Kirjutame $a = \prod_i p_i \prod_j q_j$, kus p_i, q_j on algarvud ning $p_i \equiv 1 \pmod 4$ ja $q_j \equiv 3 \pmod 4$. Lause 4.8 põhjal piisab veenduda, et $\left(\frac{\alpha}{p_i}\right)_4 = 1$. Et $p_i \equiv 1 \pmod 4$, siis $p_i = \pi\overline{\pi}$ (teoreem 2.7), ning kuna $\overline{\alpha} = \alpha$, sest $\alpha \in \mathbb{Z}$, saamegi, et

$$\left(\frac{\alpha}{p_i}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \cdot \left(\frac{\overline{\alpha}}{\overline{\pi}}\right)_4 = \left(\frac{\alpha}{\pi}\right)_4 \cdot \overline{\left(\frac{\overline{\alpha}}{\pi}\right)_4} = \left(\frac{\alpha}{\pi}\right)_4 \cdot \overline{\left(\frac{\alpha}{\pi}\right)_4} = 1.$$

□

Lause 4.11. *Kui $n \neq 1$ on täisarv ja $n \equiv 1 \pmod 4$, siis $\left(\frac{i}{n}\right)_4 = (-1)^{\frac{n-1}{4}}$.*

TÕESTUS. Vaatleme esmalt algarve $n \equiv 1 \pmod 4$. Kirjutades $n = \pi\overline{\pi}$, saame lemma 3.3 tõttu, et

$$\left(\frac{i}{n}\right)_4 = \left(\frac{i}{\pi}\right)_4 \cdot \left(\frac{i}{\overline{\pi}}\right)_4 = i^{\frac{N(\pi)-1}{4}} \cdot i^{\frac{N(\pi)-1}{4}} = (i^{\frac{n-1}{4}})^2 = (i^2)^{\frac{n-1}{4}} = (-1)^{\frac{n-1}{4}}.$$

Kui n on negatiivne algarv, siis $-n \in \mathbb{P}$ ja $-n \equiv 3 \pmod 4$. Järelikult $-n - 1 = 4l + 2$, $l \in \mathbb{Z}$ ja $i^{-n-1} = i^{4l+2} = i^{4l} \cdot i^2 = 1 \cdot (-1) = -1$. Ilmselt $(-1)^{q+1} = (-1)^{-q-1}$ ja seega

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

Juhul, kui $n \equiv 1 \pmod 4$ on suvaline, siis $n = p_1 \cdot \ldots \cdot p_t \cdot q_1 \cdot \ldots \cdot q_s$, kus $p_i \equiv 1 \pmod 4$ ja $-q_i \equiv 1 \pmod 4$ ning algarve q_s on paarisarv tükki. Järelikult [5] lemma 9.20 põhjal

$$\begin{aligned}
\left(\frac{i}{n}\right)_4 &= \left(\frac{i}{p_1}\right)_4 \cdot \ldots \cdot \left(\frac{i}{p_t}\right)_4 \cdot \left(\frac{i}{-q_1}\right)_4 \cdot \ldots \cdot \left(\frac{i}{-q_s}\right)_4 \\
&= (-1)^{\frac{p_1-1}{4}} \cdot \ldots \cdot (-1)^{\frac{p_t-1}{4}} \cdot (-1)^{\frac{-q_1-1}{4}} \cdot \ldots \cdot (-1)^{\frac{-q_s-1}{4}} \\
&= (-1)^{\sum_i \frac{p_i-1}{4} + \sum_j \frac{q_j-1}{4}} \equiv (-1)^{\left(\prod_i p_i \cdot \prod_j q_j - 1\right)/4} = (-1)^{\left(\prod_{i,j} p_i \cdot (-q_j) - 1\right)/4} \\
&= (-1)^{\frac{n-1}{4}}.
\end{aligned}$$

□

5 Gaussi ja Jacobi summad

Ruutvastavusseaduse sõnastamisel ja tõestamisel on otstarbekas kasutada Legendre'i sümbolit. Et tõestada biruutvastavusseadust, defineerime Legendre'i sümboli vaste ehk biruutjäägi sümboli. Kuna viimase omadusi on võimalik vähese vaevaga tõestada ka üldisemalt, toome sisse kõiki eelnevaid sümboleid endasse haarava korpuse multiplikatiivse karakteristiku mõiste ja seome selle Gaussi ning Jacobi summadega.

5.1 Multiplikatiivsed karakteristikud

Lõpliku korpuse $\mathbb{F}_p$, $p \in \mathbb{P}$, *multiplikatiivseks karakteristikuks* nimetatakse kujutust $\chi : \mathbb{F}_p^* \mapsto \mathbb{C} \setminus \{0\}$, mis rahuldab iga $a, b \in \mathbb{F}_p^*$ korral tingimust

$$\chi(ab) = \chi(a) \cdot \chi(b).$$

Üks selline karakteristik on defineeritud võrdusega $\varepsilon(a) = 1$ iga $a \in \mathbb{F}_p^*$ korral. Me võime laiendada karakteristikut tervele korpusele $\mathbb{F}_p$, võttes $\chi(0) = 0$, kui $\chi \neq \varepsilon$, ja $\varepsilon(0) = 1$.

Lause 5.1. *Olgu χ korpuse $\mathbb{F}_p$ multiplikatiivne karakteristik ja $a \in \mathbb{F}_p^*$. Siis karakteristikul χ on järgmised omadused.*

1. $\chi(1) = 1$.
2. $\chi(a)$ *on* $(p-1)$*. astme ühejuur.*
3. $\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}$.

Tõestus.

1. Ilmselt $\chi(1) = \chi(1 \cdot 1) = \chi(1) \cdot \chi(1)$. Kuna $\chi(1) \neq 0$, sest $\chi(1) \in \mathbb{C} \setminus \{0\}$, siis $\chi(1) = 1$.
2. Paneme tähele, et $a^{p-1} = 1$ ([5], lemma 8.8). Nüüd
$$1 = \chi(1) = \chi(a^{p-1}) = \chi(a)^{p-1}.$$
3. Kuna $1 = \chi(1) = \chi(a^{-1}a) = \chi(a^{-1})\chi(a)$, siis $\chi(a^{-1}) = \chi(a)^{-1}$. Et $\chi(a)$ on omaduse 2 põhjal kompleksarv mooduliga 1, siis $\chi(a) \cdot \overline{\chi(a)} = |\chi(a)|^2 = 1$ ja pöördelemendi ühesuse ning korrutamise kommutatiivsuse tõttu ([4], lause 2.1.38) $\chi(a)^{-1} = \overline{\chi(a)}$.

□

Lause 5.2. *Olgu χ korpuse multiplikatiivne karakteristik. Siis*

$$\sum_{t\in\mathbb{F}_p}\chi(t)=\begin{cases} p, \textit{kui } \chi=\varepsilon,\\ 0, \textit{kui } \chi\neq\varepsilon.\end{cases}$$

TÕESTUS. Esimene juht on ilmne, sest $\sum\limits_{t\in\mathbb{F}_p}\varepsilon(t)=\underbrace{1+1+\ldots+1}_{\text{p tükki}}=p.$
Oletame, et $\varepsilon\neq\chi$. Sellisel juhul leidub element $a\in\mathbb{F}_p^*$ nii, et $\chi(a)\neq 1$. Olgu $T=\sum\limits_{t\in\mathbb{F}_p}\chi(t)$. Siis

$$\chi(a)\cdot T=\sum_{t\in\mathbb{F}_p}\chi(a)\cdot\chi(t)=\sum_{t\in\mathbb{F}_p}\chi(at)=T.$$

Viimane võrdus kehtib seetõttu, et kui t omandab kõik väärtused hulgast $\{1,\ldots,p-1\}$, siis loengukonspekti [5] lemma 9.11 põhjal omandab at samad väärtused mooduli p järgi. Kuna $\chi(a)\cdot T=T$ ja $\chi(a)\neq 1$, siis T = 0. □

Multiplikatiivsete karakteristikute hulk moodustab rühma järgmiste tehete suhtes:

1) kui χ ja λ on lõpliku korpuse $\mathbb{F}_p$ multiplikatiivsed karakteristikud, siis $\chi\lambda$ on defineeritud seosega

$$\chi\lambda(a)=\chi(a)\lambda(a) \text{ iga } a\in\mathbb{F}_p^* \text{ korral;}$$

2) kui χ on $\mathbb{F}_p$ multiplikatiivne karakteristik, siis $\chi^{-1}:\mathbb{F}_p^*\mapsto\mathbb{C}\setminus\{0\}$ ja

$$\chi^{-1}(a)=\chi(a)^{-1} \text{ iga } a\in\mathbb{F}_p^* \text{ korral.}$$

Selle rühma ühikelemendiks on karakteristik ε.

Lause 5.3. *Korpuse $\mathbb{F}_p$ karakteristikute rühm on tsükliline rühm järguga $p-1$. Kui $a\in\mathbb{F}_p^*$ ja $a\neq 1$, siis leidub üheselt määratud karakteristik χ selliselt, et $\chi(a)\neq 1$.*

TÕESTUS. Teoreemi 1.18 põhjal teame, et $\mathbb{F}_p^*$ on tsükliline. Olgu $g\in\mathbb{F}_p^*$ primitiivne element. Siis iga $a\in\mathbb{F}_p^*$ on avaldatav g astmena: $a=g^l$, $l\in\mathbb{N}$. Kui nüüd χ on multiplikatiivne karakteristik, siis $\chi(a)=\chi(g)^l$. Seega χ on elemendi $\chi(g)$ poolt täielikult määratud. Et $\chi(g)$ on $(p-1)$. astme ühejuur ja neid on täpselt $p-1$ tükki, siis karakteristikute rühma järk on maksimaalselt $p-1$.

Defineerime funktsiooni λ võrdusega $\lambda(g^l) = e^{\frac{2\pi i}{p-1} \cdot l} \in \mathbb{C} \setminus \{0\}$. Siis λ on multiplikatiivne karakteristik, sest

$$\lambda(g^l \cdot g^{l'}) = \lambda(g^{l+l'}) = e^{\frac{2\pi i}{p-1} \cdot (l+l')} = e^{\frac{2\pi i}{p-1} \cdot l} \cdot e^{\frac{2\pi i}{p-1} \cdot l'} = \lambda(g^l) \cdot \lambda(g^{l'}),$$

kus $l, l' \in \mathbb{N}$. Paneme tähele, et $p-1$ on väikseim täisarv n, mille korral $\lambda^n = \varepsilon$, s.t. λ järk multiplikatiivsete karakteristikute rühmas on $p-1$. Tõepoolest, kui $\lambda^n = \varepsilon$, siis $\lambda^n(g) = \varepsilon(g) = 1$. Kuid

$$1 = \lambda^n(g) = (\lambda(g))^n = e^{2\pi i \cdot \frac{n}{p-1}}$$

ja seega $p-1 \mid n$. Et $\lambda^{p-1}(g) = \lambda(g)^{p-1} = \lambda(g^{p-1}) = \lambda(1) = 1$, siis $\lambda^{p-1} = \varepsilon$. Seega λ järk multiplikatiivsete karakteristikute rühmas on $p-1$. Olgu m multiplikatiivsete karakteristikute rühma järk, siis Lagrange'i teoreemi põhjal $p-1 \mid m$. Kuna eelnevalt veendusime, et $m \leq p-1$, siis $m = p-1$ ja multiplikatiivne karakteristikute rühm on tsükliline rühm moodustajaga λ.

Kui $a \in \mathbb{F}_p^*$ ja $a \neq 1$, siis $a = g^l$, kusjuures $1 \leq l \leq p-2$. Arvutades saame, et $\lambda(a) = \lambda(g)^l = e^{2\pi i \frac{l}{p-1}} \neq 1$, sest vastasel korral $p-1 \mid l$, mis ei saa l valiku tõttu kehtida. □

5.2 Gaussi summad

Nüüd saame defineerida Gaussi summad, mida kasutame korduvalt edaspidistes tõestustes.

Definitsioon 5.4. Olgu $\xi = e^{\frac{2\pi i}{p}}$ p. astme algjuur, χ korpuse $\mathbb{F}_p$ mingi multiplikatiivne karakteristik ja $0 \leq a \leq p-1$. Kompleksarve

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

nimetatakse karakteristiku χ *Gaussi summadeks.*

Lemma 5.5. *Kehtib võrdus*

$$\sum_{t \in \mathbb{F}_p} \xi^{at} = \begin{cases} p, \textit{kui } a = 0, \\ 0, \textit{kui } a \neq 0. \end{cases}$$

Tõestus. Kui $a = 0$, siis $\xi^{at} = (\xi^a)^t = (\xi^0)^t = 1^t = 1$ ja seega

$$\sum_{t \in \mathbb{F}_p} \xi^{at} = \sum_{t \in \mathbb{F}_p} 1 = p.$$

Juhul $a \neq 0$ ka $\xi^a \neq 1$ ja seega $\sum_{t=0}^{p-1} \xi^{at} = \frac{\xi^{ap}-1}{\xi^a-1} = 0$. □

Lemma 5.5 põhjal saame teha järgmise järelduse.

Järeldus 5.6. *Olgu* $\delta(x,y) = \begin{cases} 1, kui\ x \equiv y \pmod{p}, \\ 0, kui\ x \not\equiv y \pmod{p}. \end{cases}$ *Siis*

$$\sum_{t \in \mathbb{F}_p} \xi^{t(x-y)} = p \cdot \delta(x,y).$$

Lause 5.7. *Olgu* $0 \leq a \leq p-1$ *ja* $\chi \neq \varepsilon$ *korpuse* $\mathbb{F}_p$ *multiplikatiivne karakteristik. Siis*

$$g_a(\chi) = \begin{cases} \chi(a^{-1})g_1(\chi), \ kui\ a \neq 0, \\ 0, \ kui\ a = 0, \end{cases}$$

ja

$$g_a(\varepsilon) = \begin{cases} 0, \ kui\ a \neq 0, \\ p, \ kui\ a = 0. \end{cases}$$

TÕESTUS. Olgu $\chi \neq \varepsilon$ ja $a \neq 0$. Siis $g_a(\chi) = \sum\limits_{t=0}^{p-1} \chi(a^{-1})\chi(a)\chi(t)\xi^{at}$, sest $\chi(a^{-1})\chi(a) = \chi(1) = 1$. Seega

$$g_a(\chi) = \chi(a^{-1}) \sum_{t=0}^{p-1} \chi(at)\xi^{at} = \chi(a^{-1})g(\chi),$$

sest kui t omandab väärtused hulgast $\{1, \ldots, p-1\}$, siis ka at omandab need väärtused mooduli p järgi ([5], lemma 9.11). Kui aga $a = 0$, siis lause 5.2 põhjal

$$g_0(\chi) = \sum_{t=0}^{p-1} \chi(t)\xi^{0t} = \sum_{t=0}^{p-1} \chi(t) = 0.$$

Olgu nüüd $\chi = \varepsilon$ ja $a \neq 0$. Sellisel juhul $g_a(\varepsilon) = \sum\limits_{t=0}^{p-1} \varepsilon(t)\xi^{at} = \sum\limits_{t=0}^{p-1} \xi^{at} = 0$ (lemma 5.5). Kui aga $a = 0$, siis lause 5.2 põhjal $g_0(\chi) = \sum\limits_{t} \xi^{0t} = p$.

□

Edaspidi tähistame Gaussi summa $g_1(\chi)$ sümboliga $g(\chi)$ ja summat $g\left(\left(\frac{\cdot}{p}\right)\right)$, *kus* $\left(\frac{\cdot}{p}\right)$ on Legendre sümbol, sümboliga g.

Lemma 5.8. *Kehtib seos*

$$\overline{g(\chi)} = \chi(-1) \cdot g(\overline{\chi}).$$

TÕESTUS. Paneme tähele, et kuna ξ on ühejuur, siis $\overline{\xi} = \xi^{-1}$. Seega

$$\begin{aligned}\overline{g(\chi)} &= \sum_{t\in\mathbb{F}_p} \overline{\chi(t)\cdot\xi^t} = \sum_{t\in\mathbb{F}_p} \overline{\chi(t)}\cdot\overline{\xi}^t = \sum_{t\in\mathbb{F}_p} \overline{\chi(t)}\cdot\xi^{-t} \\ &= \sum_{t\in\mathbb{F}_p} \overline{\chi(-1)\chi(-t)}\cdot\xi^{-t} = \chi(-1)\sum_{t\in\mathbb{F}_p} \overline{\chi(-t)}\cdot\xi^{-t} \\ &= \chi(-1)\sum_{t\in\mathbb{F}_p} \overline{\chi(t)}\cdot\xi^{t} = \chi(-1)\cdot g(\overline{\chi}).\end{aligned}$$

□

Lause 5.9. *Kehtib võrdus* $g^2 = p\cdot(-1)^{\frac{p-1}{2}}$.

TÕESTUS. Tõestamiseks avaldame summa $S = \sum\limits_a g_a g_{-a}$ kahel eri viisil. Kui $a \neq 0$, siis lause 5.7 tõttu

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

ning seega

$$\begin{aligned}S &= \sum_{\substack{a\neq 0\\ a\in\mathbb{F}_p}} g_a g_{-a} = \sum_{\substack{a\neq 0\\ a\in\mathbb{F}_p}} \left(\frac{a^{-1}}{p}\right)\left(\frac{-a^{-1}}{p}\right) g^2 \\ &= \sum_{\substack{a\neq 0\\ a\in\mathbb{F}_p}} \left(\frac{-1}{p}\right) g^2 = (p-1)\left(\frac{-1}{p}\right) g^2.\end{aligned}$$

Samas

$$g_a g_{-a} = \left(\sum_{x\in\mathbb{F}_p}\left(\frac{x}{p}\right)\xi^{ax}\right)\left(\sum_{y\in\mathbb{F}_p}\left(\frac{y}{p}\right)\xi^{-ay}\right),$$

järelikult

$$S = \sum_{a\in\mathbb{F}_p}\sum_{x,y\in\mathbb{F}_p}\left(\frac{x}{p}\right)\xi^{ax}\left(\frac{y}{p}\right)\xi^{-ay} = \sum_{a\in\mathbb{F}_p}\sum_{x,y\in\mathbb{F}_p}\left(\frac{xy}{p}\right)\xi^{a(x-y)}.$$

Muutes summeerimise järjekorda, saame järelduse 5.6 põhjal, et

$$S = \sum_{x,y\in\mathbb{F}_p}\left(\frac{xy}{p}\right)\sum_{a\in\mathbb{F}_p}\xi^{a(x-y)} = \sum_{x,y\in\mathbb{F}_p}\left(\frac{xy}{p}\right)\cdot\delta(x,y)\cdot p.$$

Kui nüüd $x = y$, siis $\left(\frac{xy}{p}\right) = \left(\frac{x^2}{p}\right) = \begin{cases} 1, \text{kui } x \neq 0, \\ 0, \text{kui } x = 0. \end{cases}$ Seega

$$S = \sum_{\substack{x \neq 0 \\ x \in \mathbb{F}_p}} p = (p-1)p.$$

Pannes saadud tulemused kokku, näeme, et

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

Taandades võrduse mõlemalt poolelt $(p-1) \neq 0$ ja korrutades võrdust Legendre'i sümboliga $\left(\frac{-1}{p}\right)$, saamegi $g^2 = \left(\frac{-1}{p}\right) p = (-1)^{\frac{p-1}{2}} p$.

□

Lause 5.10. *Kui $\chi \neq \varepsilon$, siis $|g(\chi)| = \sqrt{p}$.*

TÕESTUS. Tõestamiseks avaldame jällegi summa

$$S = \sum_a g_a(\chi) \cdot \overline{g_a(\chi)}$$

kahel eri viisil. Kui $a \neq 0$, siis lausete 5.1 ja 5.7 põhjal $\overline{\chi(a^{-1})} = \chi(a)$, $g_a(\chi) = \chi(a^{-1}) \cdot g(\chi)$ ja seega

$$\overline{g_a(\chi)} = \overline{\chi(a^{-1}) \cdot g(\chi)} = \chi(a) \cdot \overline{g(\chi)}.$$

Järelikult

$$g_a(\chi) \cdot \overline{g_a(\chi)} = \chi(a^{-1}) \cdot g(\chi) \cdot \chi(a) \cdot \overline{g(\chi)} = |g(\chi)|^2.$$

Kuna $g_0(\chi) = 0$, siis $S = \sum\limits_{a \in \mathbb{F}_p} g_a(\chi) \cdot \overline{g_a(\chi)} = \sum\limits_{a \neq 0} |g(\chi)|^2 = (p-1) \cdot |g(\chi)|^2$.

Teiselt poolt,

$$g_a(\chi) \cdot \overline{g_a(\chi)} = \sum_{x \in \mathbb{F}_p} \sum_{y \in \mathbb{F}_p} \chi(x) \cdot \overline{\chi(y)} \cdot \xi^{ax-ay}.$$

Summeerides mõlemaid pooli üle a ja kasutades järeldust 5.6, kehtib võrdus $\chi(x) \cdot \overline{\chi(x)} = |\chi(x)|^2 = 1$, sest χ on ühejuur ja seega

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

Järelikult $(p-1) \cdot |g(\chi)|^2 = S = (p-1) \cdot p$ ehk $|g(\chi)| = \sqrt{p}$.

□

5.3 Jacobi summad

Peatüki lõpus vaatleme Gaussi multiplikatiivsust muutvaid Jacobi summasid.

Definitsioon 5.11. Olgu χ ja λ korpuse $\mathbb{F}_p$ karakteristikud ning $a, b \in \mathbb{F}_p$. Siis kompleksarve

$$J(\chi, \lambda) = \sum_{\substack{a+b=1 \\ a,b\in\mathbb{F}_p}} \chi(a) \cdot \lambda(b)$$

nimetatakse *Jacobi summadeks.*

Teoreem 5.12. *Olgu χ ja λ mittetriviaalsed karakteristikud ehk $\chi \neq \varepsilon$ ning $\lambda \neq \varepsilon$. Siis*

(a) $J(\varepsilon, \varepsilon) = p$.

(b) $J(\varepsilon, \chi) = 0$.

(c) $J(\chi, \chi^{-1}) = -\chi(-1)$.

(d) *Kui $\chi \cdot \lambda \neq \varepsilon$, siis*

$$J(\chi, \lambda) = \frac{g(\chi) \cdot g(\lambda)}{g(\chi \cdot \lambda)}.$$

TÕESTUS. Osa (a) kehtib vastavalt definitsioonile, sest

$$J(\varepsilon, \varepsilon) = \sum_{\substack{a+b=1 \\ a,b\in\mathbb{F}_p}} \varepsilon(a) \cdot \varepsilon(b) = \sum_{\substack{a+b=1 \\ a,b\in\mathbb{F}_p}} 1 \cdot 1 = p.$$

Osa (b) on vahetu järeldus lausest 5.2, sest

$$J(\varepsilon, \chi) = \sum_{\substack{a+b=1 \\ a,b\in\mathbb{F}_p}} \varepsilon(a) \cdot \chi(b) = \sum_{\substack{a+b=1 \\ a,b\in\mathbb{F}_p}} 1 \cdot \chi(b) = \sum_{b\in\mathbb{F}_p} \chi(b) = 0.$$

Punkti (c) tõestamiseks paneme tähele, et

$$J(\chi, \chi^{-1}) = \sum_{\substack{a+b=1 \\ a,b\in\mathbb{F}_p}} \chi(a)\chi^{-1}(b) = \sum_{\substack{a+b=1 \\ b\neq 0 \\ a,b\in\mathbb{F}_p}} \chi\left(a \cdot b^{-1}\right) = \sum_{\substack{a\neq 1 \\ a\in\mathbb{F}_p}} \chi\left(a \cdot (1-a)^{-1}\right).$$

Olgu $c = \frac{a}{1-a}$. Kui $c \neq -1$, siis $a = \frac{c}{1+c}$. Järelikult kui $a \in \mathbb{F}_p \setminus \{\overline{1}\}$, siis $c \in \mathbb{F}_p \setminus \{-\overline{1}\}$. Seega uuesti lause 5.2 tõttu

$$J(\chi, \chi^{-1}) = \sum_{c\neq -1} \chi(c) = -\chi(-1).$$

Omaduse (d) puhul märgime, et

$$g(\chi)\cdot g(\lambda)=\sum_{x,y\in\mathbb{F}_p}\chi(x)\cdot\lambda(y)\cdot\xi^{x+y}=\sum_{t\in\mathbb{F}_p}\left(\sum_{\substack{x+y=t\\ x,y\in\mathbb{F}_p}}\chi(x)\cdot\lambda(y)\right)\xi^t.$$

Juhul $t=0$ saame lause 5.2 põhjal, et

$$\sum_{\substack{x+y=0\\ x,y\in\mathbb{F}_p}}\chi(x)\cdot\lambda(y)=\sum_{x\in\mathbb{F}_p}\chi(x)\cdot\lambda(-x)=\lambda(-1)\cdot\sum_{x\in\mathbb{F}_p}\chi\lambda(x)=0,$$

sest eelduse kohaselt $\chi\cdot\lambda\neq\varepsilon$. Kui aga $t\neq 0$, võime summas $\sum\limits_{\substack{x+y=t\\ x,y\in\mathbb{F}_p}}\chi(x)\cdot\lambda(y)$ teha asenduse $x=tx', y=ty'$ ning saame

$$\sum_{\substack{x'+y'=1\\ x',y'\in\mathbb{F}_p}}\chi(tx')\cdot\lambda(ty')=\chi\lambda(t)\cdot J(\chi,\lambda).$$

Seega

$$g(\chi)\cdot g(\lambda)=\sum_{t\in\mathbb{F}_p}J(\chi,\lambda)\cdot\chi\lambda(t)\xi^t=J(\chi,\lambda)\cdot g(\chi\lambda)$$

ning jagades mõlemad pooled läbi Gaussi summaga $g(\chi\lambda)\neq 0$ (lause 5.10), saamegi soovitud tulemuse. □

Lause 5.13. *Olgu $p\equiv 1 \pmod n$ ja χ karakteristik, mille järk on $n>2$. Siis*

$$g(\chi)^n=\chi(-1)\cdot p\cdot J(\chi,\chi)\cdot J(\chi,\chi^2)\cdot\ldots\cdot J(\chi,\chi^{n-2}).$$

TÕESTUS. Kasutades teoreemi 5.12 osa (d), kehtib juhul $\chi^2\neq\varepsilon$ võrdus

$$g(\chi)^2=J(\chi,\chi)\cdot g(\chi^2). \tag{1}$$

Kuna $\chi^3\neq\varepsilon$, siis $J(\chi,\chi^2)\,g(\chi^3)=g(\chi^2)g(\chi)$ ning korrutades võrduse (1) mõlemat poolt Gaussi summaga $g(\chi)$, saame, et

$$g(\chi)^3=J(\chi,\chi)\cdot g(\chi^2)\cdot g(\chi)=J(\chi,\chi)\cdot J(\chi,\chi^2)\cdot g(\chi^3).$$

Samamoodi jätkates näeme, et

$$g(\chi)^{n-1}=J(\chi,\chi)\cdot J(\chi,\chi^2)\cdot\ldots\cdot J(\chi,\chi^{n-2})\cdot g(\chi^{n-1}). \tag{2}$$

Nüüd $\chi^{n-1} = \chi^{-1} = \overline{\chi}$ ja seega $g(\chi) \cdot g(\chi^{n-1}) = g(\chi) \cdot g(\overline{\chi})$. Samas teame, et

$$p = |g(\chi)|^2 = g(\chi) \cdot \overline{g(\chi)} = g(\chi) \cdot \chi(-1) \cdot g(\overline{\chi}).$$

Kuna $\chi(-1) = \pm 1$, siis võime kirjutada $\chi(-1) \cdot p = g(\chi) \cdot g(\overline{\chi})$. Järelikult korrutades võrduse (2) mõlemat poolt Gaussi summaga $g(\chi)$, saamegi soovitud tulemuse

$$g(\chi)^n = \chi(-1) \cdot p \cdot J(\chi, \chi) \cdot J(\chi, \chi^2) \cdot \ldots \cdot J(\chi, \chi^{n-2}).$$

□

6 Biruutvastavusseadus

Käesoleva peatüki eesmärgiks on tõestada biruutvastavusseadus, mille võib sõnastada järgmiselt:

Teoreem 6.1. *Olgu λ ja π ühistegurita primaarsed Gaussi täisarvud. Siis*

$$\left(\frac{\lambda}{\pi}\right)_4 = \left(\frac{\pi}{\lambda}\right)_4^{\frac{N(\lambda)-1}{4}\cdot\frac{N(\pi)-1}{4}}.$$

Järgnevalt tõestame rea seoseid biruutjäägi sümboli ja Gaussi ning Jacobi summadel vahel.

Lause 6.2. *Kui λ ja π on primaarsed ning $\lambda = c + di$ ja $\pi = a + bi$, $a, b, c, d \in \mathbb{Z}$, siis $\frac{N(\lambda)-1}{4} \cdot \frac{N(\pi)-1}{4}$ on sama paarsusega mis $\frac{a-1}{2} \cdot \frac{c-1}{2}$.*

TÕESTUS. Tõepoolest,

$$\begin{aligned}\frac{N(\lambda)-1}{4} \cdot \frac{N(\pi)-1}{4} &= \frac{c^2+d^2-1}{4} \cdot \frac{a^2+b^2-1}{4} \\ &= \frac{(a+1)(a-1)+b^2}{4} \cdot \frac{(c+1)(c-1)+d^2}{4}.\end{aligned}$$

Kuna λ ja π on primaarsed, siis kas

$$c \equiv 1 \pmod 4 \quad \text{ja} \quad d \equiv 0 \pmod 4$$

või

$$c \equiv 3 \pmod 4 \quad \text{ja} \quad d \equiv 2 \pmod 4.$$

Samad tingimused kehtivad ka arvude a ja b jaoks. Juhul kui $a \equiv 1 \pmod 4$ ehk $a = 4k + 1$ ja $b \equiv 0 \pmod 4$ ehk $b = 4l$, kus $k, l \in \mathbb{Z}$, siis

$$\frac{(a+1)(a-1)+b^2}{4} = \frac{(4k+2)(4k)+16l^2}{4} = 4k^2 + 2k + 4l^2$$

on paaris ja seega on ka korrutis

$$\frac{(a+1)(a-1)+b^2}{4} \cdot \frac{(c+1)(c-1)+d^2}{4}$$

paaris. Kirjutades lahti murru $\frac{a-1}{2} = \frac{4k}{2} = 2k$, näeme, et ka korrutis $\frac{a-1}{2} \cdot \frac{c-1}{2}$ on paaris ja seega oleme veendunud, et $\frac{N(\lambda)-1}{4} \cdot \frac{N(\pi)-1}{4}$ on tõepoolest sama paarsusega mis $\frac{a-1}{2} \cdot \frac{c-1}{2}$. Sama tulemuse saame ka juhul, kui $c \equiv 1 \pmod 4$

ja $d \equiv 0 \pmod 4$. Kui aga a ja c on kongruentsed arvuga 3 mooduli 4 järgi ning b ja d on kogruentsed arvuga 2 mooduli 4 järgi, siis korrutis

$$\begin{aligned}
&\frac{(a+1)(a-1)+b^2}{4} \cdot \frac{(c+1)(c-1)+d^2}{4} \\
=&\frac{(4k+4)(4k+2)+(4l+2)^2}{4} \cdot \frac{(4m+4)(4m+2)+(4n+2)^2}{4} \\
=&\underbrace{(4k^2+6k+4l^2+4l+3)}_{\text{paaritu}} \cdot \underbrace{(4m^2+6m+4n^2+4n+3)}_{\text{paaritu}}
\end{aligned}$$

on paaritu, nagu ka korrutis

$$\frac{a-1}{2} \cdot \frac{c-1}{2} = \frac{4k+2}{2} \cdot \frac{4m+2}{2} = \underbrace{(2k+1)}_{\text{paaritu}} \cdot \underbrace{(2m+1)}_{\text{paaritu}}.$$

□

Olgu meil edaspidi π primaarne esimest liiki Gaussi algarv, mille norm $N(\pi) = p \equiv 1 \pmod 4$ ja $\left(\frac{\div}{\pi}\right)_4$ sellega seotud biruutjäägi sümbol. Juhul, kui $\left(\frac{\div}{p}\right) = \left(\frac{\div}{\pi}\right)_4^2$, siis $\left(\frac{\div}{p}\right)$ on mittetriviaalne karakteristik ning ühtlasi Legendre'i sümbol. Loengukonspekti [5] lemma 7.5 ütleb, et paarisarvulise järguga tsüklilises rühmas on täpselt üks selline element, mille järk on kaks. Kuna Legendre'i sümbol on karakteristik, mis ei ole võrdne ühikkarakteristikuga ε, aga $\left(\frac{\div}{p}\right)^2 = \varepsilon$, siis tema järk on 2. Samuti biruutjäägi sümboli puhul $\left(\left(\frac{\div}{\pi}\right)_4^2\right)^2 = \varepsilon$, aga $\left(\frac{\div}{\pi}\right)_4^2 \neq \varepsilon$. Seega langevad nad kokku.

Lause 6.3. *Kehtib võrdus* $J\left(\left(\frac{\div}{\pi}\right)_4, \left(\frac{\div}{\pi}\right)_4\right) = \left(\frac{-1}{\pi}\right)_4 \cdot J\left(\left(\frac{\div}{\pi}\right)_4, \left(\frac{\div}{p}\right)\right)$.

TÕESTUS. Teoreemi 5.12 osa (d) põhjal $J\left(\left(\frac{\div}{\pi}\right)_4, \left(\frac{\div}{\pi}\right)_4\right) = \frac{g\left(\left(\frac{\div}{\pi}\right)_4\right)^2}{g\left(\left(\frac{\div}{p}\right)\right)}$ ning seega

lausete 5.9 ja 5.13 kohaselt

$$\begin{aligned}
J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{\pi}\right)_4\right)^2 &= \frac{g\left(\left(\frac{\div}{\pi}\right)_4\right)^4}{g\left(\left(\frac{\div}{p}\right)\right)^2} \\
&= \frac{\left(\frac{-1}{\pi}\right)_4 \cdot p \cdot J\left(\left(\frac{\div}{\pi}\right)_4,\left(\frac{\div}{\pi}\right)_4\right) \cdot J\left(\left(\frac{\div}{\pi}\right)_4,\left(\frac{\div}{p}\right)\right)}{g^2} \\
&= \frac{\left(\frac{-1}{\pi}\right)_4 \cdot p \cdot J\left(\left(\frac{\div}{\pi}\right)_4,\left(\frac{\div}{\pi}\right)_4\right) \cdot J\left(\left(\frac{\div}{\pi}\right)_4,\left(\frac{\div}{p}\right)\right)}{p\cdot(-1)^{\frac{p-1}{2}}} \\
&= \left(\frac{-1}{\pi}\right)_4 \cdot J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{\pi}\right)_4\right) \cdot J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{p}\right)\right)
\end{aligned}$$

ning kuna $J\left(\left(\frac{\div}{\pi}\right)_4,\left(\frac{\div}{\pi}\right)_4\right) \neq 0$ (lause 5.10), võime võrduse selle Jacobi summaga läbi jagada ning saamegi soovitud tulemuse.

□

Lause 6.4. *Kehtib võrdus* $g\left(\left(\frac{\div}{\pi}\right)\right)^4 = p \cdot J\left(\left(\frac{\div}{\pi}\right)_4,\left(\frac{\div}{\pi}\right)_4\right)^2$.

Tõestus. Lausete 5.12 ja 6.3 põhjal

$$\begin{aligned}
g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^4 &= \left(\frac{-1}{\pi}\right)_4 \cdot p \cdot J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{\pi}\right)_4\right) \cdot J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{p}\right)\right) \\
&= \left(\frac{-1}{\pi}\right)_4 \cdot p \cdot J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{\pi}\right)_4\right) \cdot \left(\frac{-1}{\pi}\right)_4 \cdot J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{\pi}\right)_4\right) \\
&= \left(\frac{(-1)^2}{\pi}\right)_4 \cdot p \cdot J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{\pi}\right)_4\right)^2.
\end{aligned}$$

□

Lause 6.5. *Gaussi täisarv* $-\left(\frac{-1}{\pi}\right) \cdot J\left(\left(\frac{\div}{\pi}\right),\left(\frac{\div}{\pi}\right)\right)$ *on primaarne.*

Tõestus. Paneme tähele, et

$$\begin{aligned}
J\left(\left(\frac{\cdot}{\pi}\right)_4,\left(\frac{\cdot}{\pi}\right)_4\right) &= \sum_{\substack{s+t=1\\ s,t\in\mathbb{F}_p}} \left(\frac{s}{\pi}\right)_4 \cdot \left(\frac{t}{\pi}\right)_4 = \sum_{s=1}^{p-1} \left(\frac{s}{\pi}\right)_4 \cdot \left(\frac{1-s}{\pi}\right)_4 \\
&= \sum_{s=1}^{\frac{p-1}{2}} \left(\frac{s}{\pi}\right)_4 \cdot \left(\frac{1-s}{\pi}\right)_4 + \sum_{s=\frac{p+3}{2}}^{p-1} \left(\frac{s}{\pi}\right)_4 \cdot \left(\frac{1-s}{\pi}\right)_4 + \left(\frac{\frac{p+1}{2}}{\pi}\right)_4 \cdot \left(\frac{1-\frac{p+1}{2}}{\pi}\right)_4 \\
&= 2 \cdot \sum_{s=2}^{\frac{p-1}{2}} \left(\frac{s}{\pi}\right)_4 \cdot \left(\frac{1-s}{\pi}\right)_4 + \left(\frac{\frac{p+1}{2}}{\pi}\right)_4^2,
\end{aligned}$$

sest kui $s \in \{(p+3)/2, \ldots, p-1\}$, siis $1-s \in \{-(p+1)/2, \ldots, -p\}$. Viimased aga on mooduli p ja seega ka mooduli π järgi kongruentsed arvudega $(p-1)/2, \ldots, 0$. Samuti võime biruutjäägi sümbolis $\left(\frac{1-\frac{p+1}{2}}{\pi}\right)_4$ liita elemendi p, sest $\pi \mid p$ ja seega saame $\left(\frac{1-((p+1)/2)+p}{\pi}\right)_4 = \left(\frac{(p+1)/2}{\pi}\right)_4$. Paneme tähele, et iga pööratav element hulgas $\mathbb{Z}[i]$ on kongruentne elemendiga 1 mooduli $(1+i)$ järgi. Veendume näiteks, et $-1 \equiv 1 \pmod{1+i}$. Siis kongruentsuse definitsiooni kohaselt $1+i \mid -2 = -(1+i)(1-i)$ ning tõepoolest, -1 ja 1 on mooduli $1+i$ järgi kongruentsed. Ülejäänud variantides saab veenduda analoogiliselt. Järelikult

$$\sum_{s=2}^{\frac{p-1}{2}} \left(\frac{s}{\pi}\right)_4 \cdot \left(\frac{1-s}{\pi}\right)_4 \equiv \sum_{s=2}^{\frac{p-1}{2}} 1 \cdot 1 = \frac{p-3}{2} \pmod{1+i}.$$

Kuna $\frac{p+1}{2} \cdot 2 \equiv p+1 \equiv 1 \pmod{\pi}$, siis $\frac{p+1}{2} = 2^{-1}$, ja et $\left(\frac{2}{\pi}\right)_4^4 = 1$, kehtib $\left(\frac{2}{\pi}\right)_4^2 = \left(\frac{2}{\pi}\right)_4^{-2}$. Nüüd

$$\begin{aligned}\left(\frac{\frac{p+1}{2}}{\pi}\right)_4^2 &= \left(\frac{2^{-1}}{\pi}\right)_4^2 = \left(\frac{2}{\pi}\right)_4^{-2} = \left(\frac{2}{\pi}\right)_4^2 \\ &= \left(\frac{-i\cdot(1+i)^2}{\pi}\right)_4^2 = \left(\frac{-i}{\pi}\right)_4^2 = \left(\frac{-1}{\pi}\right)_4.\end{aligned}$$

Täheldame, et kuna $(p-1)/2$ on paaris, siis $2 \mid (p-1)/2$. Samas kehtib $1+i \mid 2$ ja seega $1+i \mid \frac{p-1}{2}$. Korrutades nüüd viimase jaguvuse elemendiga 2, saame, et $p \equiv 1 \pmod{2+2i}$. Kokkuvõttes

$$\begin{aligned}J\left(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4\right) &\equiv 2 \cdot \left(\frac{p-3}{2}\right) + \left(\frac{-1}{\pi}\right)_4 \\ &\equiv -2 + \left(\frac{-1}{\pi}\right)_4 \pmod{2+2i}.\end{aligned}$$

Teades, et $\left(\frac{-1}{\pi}\right)_4 = \pm 1$ ja korrutades saadud tulemust biruutjäägi sümboliga $-\left(\frac{-1}{\pi}\right)_4$, saamegi, et

$$-\left(\frac{-1}{\pi}\right)_4 \cdot J\left(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4\right) \equiv 2 \cdot \left(\frac{-1}{\pi}\right)_4 - 1 \equiv 1 \pmod{(1+i)^3}.$$

□

Lause 6.6. *Kehtib võrdus* $-\left(\frac{-1}{\pi}\right)_4 \cdot J(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4) = \pi$.

TÕESTUS. Et $-\left(\frac{-1}{\pi}\right)_4 \cdot J(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4)$ on primaarne, piisab lemma 3.4 põhjal veenduda, et võrduse pooled erinevad üksteisest pööratava elemendi võrra. Definitsiooni kohaselt

$$J\left(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4\right) = \sum_{s=1}^{p-1} \left(\frac{s}{\pi}\right)_4 \cdot \left(\frac{1-s}{\pi}\right)_4 \equiv \sum_{s=1}^{p-1} s^{\frac{p-1}{4}} \cdot (1-s)^{\frac{p-1}{4}} \pmod{\pi}.$$

Näitame nüüd, et

$$S = \sum_{x=1}^{p-1} x^k \equiv 0 \pmod{p},$$

kui $1 \leq k < (p-1)$. Veendume selles. Kuna p on algarv, siis leidub algjuur g selliselt, et $\{\overline{1}, \overline{2}, \ldots, \overline{p-1}\} = \{\overline{1}, \overline{g}, \overline{g}^2, \ldots, \overline{g}^{p-2}\}$. Järelikult

$$1^k + \ldots + (p-1)^k \equiv 1 + g^k + \ldots + (g^k)^{p-2} \pmod{p}.$$

Võttes $q = g^k$, kehtib g pööratavavuse tõttu $(q,p) = (g,p) = 1$. Seega Fermat' väikese teoreemi põhjal $q^{p-1} - 1 \equiv 0 \pmod{p}$. Kuna g on algjuur, siis $q \neq 1$, sest $k < p-1$. Seetõttu

$$S \cdot (q-1) = q^{p-1} + q^{p-2} + \ldots + q - q^{p-2} - \ldots - 1 = q^{p-1} - 1 \equiv 0 \pmod{p}.$$

Eelnevast $q - 1 \not\equiv 0 \pmod{p}$ ja seega $S \equiv 0 \pmod{p}$.
Binoomvalemist saame, et

$$s^{\frac{p-1}{4}} \cdot (1-s)^{\frac{p-1}{4}} = \sum_{i=0}^{(p-1)/4} \binom{(p-1)/4}{i} (-s)^i \cdot s^{\frac{p-1}{4}}.$$

Järelikult

$$\begin{aligned} J(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4) &= \sum_{s=1}^{p-1} \sum_{i=0}^{(p-1)/4} \binom{(p-1)/4}{i} (-1)^i \cdot s^{i+\frac{p-1}{4}} \\ &= \sum_{i=0}^{(p-1)/4} \binom{(p-1)/4}{i} (-1)^i \sum_{s=1}^{p-1} s^{i+\frac{p-1}{4}}. \end{aligned}$$

Kuna $1 \leq (p-1)/4$ korral kehtib $1 \leq i + (p-1)/4 \leq (p-1)/2 < p-1$, siis

$$\sum_{s=1}^{p-1} s^{i+\frac{p-1}{4}} \equiv 0 \pmod{p}.$$

Seega $J(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4) \equiv \sum_{i=0}^{(p-1)/4} \binom{(p-1)/4}{i}(-1)^i \cdot 0 = 0 \pmod{p}$ ja kuna $\pi \mid p$, siis tõepoolest

$$J\left(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4\right) \equiv 0 \pmod{\pi}.$$

Kuna $\left(\frac{\cdot}{\pi}\right)_4 \neq \varepsilon$, siis lause 5.10 põhjal $|g(\left(\frac{\cdot}{\pi}\right)_4)| = \sqrt{p}$ ning järelikult tänu faktile $\left(\frac{\cdot}{p}\right) \neq \varepsilon$ kehtib teoreemi 5.12 osa (d) põhjal

$$J(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4) = \frac{g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^2}{g\left(\left(\frac{\cdot}{p}\right)\right)} = \frac{p}{\sqrt{p}} = \sqrt{p}.$$

Nüüd $N\left(J\left(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4\right)\right) = p$ ja seega $J\left(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4\right)$ on Gaussi algarv. Kuid $\pi \mid J\left(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4\right)$ ja järelikult on nad assotsieeritud, mida tahtsimegi näidata. □

Lausete 6.4 ja 6.6 põhjal saame järgmise tulemuse:

Lause 6.7. *Kehtib võrdus* $g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^4 = \pi^3 \cdot \overline{\pi}$.

TÕESTUS. Kuna $g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^4 = p \cdot J(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4)^2$ ning me teame, et $p = \pi \cdot \overline{\pi}$, ja $J(\left(\frac{\cdot}{\pi}\right)_4, \left(\frac{\cdot}{\pi}\right)_4)^2 = \pi^2$, siis saamegi, et

$$g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^4 = \pi^3 \cdot \overline{\pi}.$$

□

Järgmisena vaatame kahte biruutvastavuse erijuhtu.

Lause 6.8. *Olgu* $q > 0$ *algarv kujul* $4k + 3$, $k \in \mathbb{Z}$. *Siis*

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

TÕESTUS. Et $q \equiv 3 \pmod 4$, kehtib lemma 1.20 ning lausete 5.1 ja 5.7

põhjal

$$
\begin{aligned}
g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^q &= \left(\sum_{j=1}^{p-1}\left(\frac{j}{\pi}\right)_4\cdot\xi^j\right)^q \equiv \sum_{j=1}^{p-1}\left(\frac{j}{\pi}\right)_4^q\cdot\xi^{qj}\\
&= \sum_{j=1}^{p-1}\left(\frac{j}{\pi}\right)_4^{4k+3}\cdot\xi^{qj} = \sum_{j=1}^{p-1}\left(\frac{j}{\pi}\right)_4^{4k}\cdot\left(\frac{j}{\pi}\right)_4^3\cdot\xi^{qj} = \sum_{j=1}^{p-1}1\cdot\left(\frac{j}{\pi}\right)_4^3\cdot\xi^{qj}\\
&= \sum_{j=1}^{p-1}\left(\frac{j}{\pi}\right)_4\cdot\left(\frac{j}{\pi}\right)_4^2\cdot\xi^{qj} = \sum_{j=1}^{p-1}\left(\frac{j}{\pi}\right)_4\cdot\overline{\left(\frac{j}{\pi}\right)_4}^2\cdot\xi^{qj}\\
&= \sum_{j=1}^{p-1}\left|\left(\frac{j}{\pi}\right)_4\right|^2\cdot\overline{\left(\frac{j}{\pi}\right)_4}\cdot\xi^{qj} = 1\cdot g_q\left(\overline{\left(\frac{\cdot}{\pi}\right)_4}\right)\\
&= \overline{\left(\frac{q^{-1}}{\pi}\right)_4}\cdot g_1\left(\overline{\left(\frac{\cdot}{\pi}\right)_4}\right) = \left(\frac{q}{\pi}\right)_4\cdot g\left(\overline{\left(\frac{\cdot}{\pi}\right)_4}\right) \pmod q.
\end{aligned}
$$

Seega

$$
\left(g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^4\right)^{\frac{q+1}{4}} = g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^{q+1} \equiv \left(\frac{q}{\pi}\right)_4\cdot g\left(\left(\frac{\cdot}{\pi}\right)_4\right)\cdot g\left(\overline{\left(\frac{\cdot}{\pi}\right)_4}\right) \pmod q.
$$

Paneme tähele, et $\overline{\pi}\equiv\pi^q \pmod q$. Tõepoolest, lemma 1.20 ja Fermat' väikese teoreemi kohaselt

$$
\begin{aligned}
\pi^q &= (a+bi)^q \equiv a^q + (bi)^q\\
&= (-i)b^q + a^q \equiv a - bi = \overline{\pi} \pmod q.
\end{aligned}
$$

Järelikult saame lause 6.7 põhjal, et

$$
\begin{aligned}
\pi^{\frac{(q+3)\cdot(q+1)}{4}} &\equiv \left(\pi^3\cdot\overline{\pi}\right)^{\frac{q+1}{4}} = \left(g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^4\right)^{\frac{q+1}{4}}\\
&= \left(\frac{q}{\pi}\right)_4\cdot g\left(\left(\frac{\cdot}{\pi}\right)_4\right)\cdot g\left(\overline{\left(\frac{\cdot}{\pi}\right)_4}\right)\\
&= \left(\frac{q}{\pi}\right)_4\cdot g\left(\left(\frac{\cdot}{\pi}\right)_4\right)\cdot\left(\frac{-1}{\pi}\right)_4\cdot\overline{g\left(\left(\frac{\cdot}{\pi}\right)_4\right)}\\
&= \left(\frac{-q}{\pi}\right)_4\cdot\left|g\left(\left(\frac{\cdot}{\pi}\right)\right)\right|^2 = \left(\frac{-q}{\pi}\right)_4\cdot p = \left(\frac{-q}{\pi}\right)_4\cdot\pi\cdot\overline{\pi}\\
&\equiv \left(\frac{-q}{\pi}\right)_4\cdot\pi\cdot\pi^q = \left(\frac{-q}{\pi}\right)_4\cdot\pi^{q+1} \pmod q.
\end{aligned}
$$

Veendume, et $\pi \not\equiv 0 \pmod{q}$. Kui $q \mid \pi$, siis kuna π on taandumatu, võime kirjutada $\pi = q \cdot u$, kus $u \in U(\mathbb{Z}[i])$. Seejuures $p = N(\pi) = N(q \cdot u) = q^2$, mis on p ja q algarvulisuse tõttu võimatu. Sarnaselt näeme, et $\overline{\pi} \not\equiv 0 \pmod{q}$. Järelikult jagades kongruentsi läbi arvuga π^{q+1}, saame

$$\pi^{\frac{q^2-1}{4}} \equiv \left(\frac{-q}{\pi}\right)_4 \pmod{q}.$$

Samas teame vastavalt definitsioonile, et $\left(\frac{\pi}{q}\right)_4 \equiv \pi^{\frac{q^2-1}{4}} \pmod{q}$ ja seega

$$\left(\frac{\pi}{q}\right)_4 \equiv \left(\frac{-q}{\pi}\right)_4 \pmod{q}.$$

Kuna ekvivalentsi mõlemal poolel on pööratavad elemendid, saame lemma 3.3 põhjal

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

□

Lause 6.9. *Olgu q algarv ning $q \equiv 1 \pmod{4}$. Siis*

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

TÕESTUS. Kuna $q = 4k+1,\ k \in \mathbb{Z}$, siis

$$\begin{aligned} g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^q &\equiv \sum_{j=1}^{p-1} \left(\frac{j}{\pi}\right)_4^q \cdot \xi^{qj} = \sum_{j=1}^{p-1} \left(\frac{j}{\pi}\right)_4^{4k+1} \cdot \xi^{qj} \\ &= \sum_{j=1}^{p-1} \left(\left(\frac{j}{\pi}\right)_4^4\right)^k \cdot \left(\frac{j}{\pi}\right)_4 \cdot \xi^{qj} \\ &= \sum_{j=1}^{p-1} 1^k \cdot \left(\frac{j}{\pi}\right)_4 \cdot \xi^{qj} \equiv g_q\left(\left(\frac{\cdot}{\pi}\right)_4\right) \\ &= \overline{\left(\frac{q}{\pi}\right)_4} \cdot g\left(\left(\frac{\cdot}{\pi}\right)_4\right) \pmod{q}, \end{aligned}$$

kus viimane võrdus kehtib lausete 5.1 omaduse 3 ja 5.7 põhjal. Seega

$$g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^{q+3} \equiv \overline{\left(\frac{q}{\pi}\right)_4} \cdot g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^4 \pmod{q}.$$

Lause 6.7 põhjal $g\left(\left(\frac{\cdot}{\pi}\right)_4\right)^4 = \pi^3 \cdot \overline{\pi}$, järelikult võime kirjutada

$$(\pi^3 \cdot \overline{\pi})^{\frac{q+3}{4}} \equiv \overline{\left(\frac{q}{\pi}\right)}_4 \cdot \pi^3 \cdot \overline{\pi} \pmod{q}.$$

Nagu eelnevas tõestuses, kehtib ka siin, et $\pi \not\equiv 0 \pmod{q}$ ja $\overline{\pi} \not\equiv 0 \pmod{q}$. Seega võime kongruentsi läbi jagada korrutisega $\pi^3 \cdot \overline{\pi}$ ning saame

$$(\pi^3)^{\frac{q-1}{4}} \cdot \overline{\pi}^{\frac{q-1}{4}} \equiv \overline{\left(\frac{q}{\pi}\right)}_4 \pmod{q}.$$

Kuna teoreemi 2.7 põhjal $q = \lambda \cdot \overline{\lambda}$, kus λ on esimest liiki Gaussi algarv, siis

$$\overline{\left(\frac{q}{\pi}\right)}_4 \equiv \left(\frac{\pi^3}{\lambda}\right)_4 \cdot \left(\frac{\overline{\pi}}{\lambda}\right)_4 \pmod{\lambda},$$

sest $N(\lambda) = q$. Selle kongruentsi mõlemal poolel on pööratavad elemendid, mistõttu võime kirjutada

$$\overline{\left(\frac{q}{\pi}\right)}_4 = \left(\frac{\pi^3}{\lambda}\right)_4 \cdot \left(\frac{\overline{\pi}}{\lambda}\right)_4. \tag{3}$$

Et $\left(\frac{\pi}{\lambda}\right)_4 \cdot \left(\frac{\pi^3}{\lambda}\right)_4 = 1 = \left(\frac{\pi}{\lambda}\right)_4 \cdot \overline{\left(\frac{\pi}{\lambda}\right)_4}$, siis $\left(\frac{\pi^3}{\lambda}\right)_4 = \overline{\left(\frac{\pi}{\lambda}\right)_4}$ ja (3) on samaväärne kirjapildiga

$$\overline{\left(\frac{q}{\pi}\right)}_4 = \overline{\left(\frac{\pi}{\lambda}\right)}_4 \cdot \left(\frac{\overline{\pi}}{\lambda}\right)_4 \quad \text{ehk} \quad \overline{\left(\frac{q}{\pi}\right)}_4 = \left(\frac{\overline{\pi}}{\overline{\lambda}}\right)_4 \cdot \left(\frac{\overline{\pi}}{\lambda}\right)_4.$$

Järelikult $\overline{\left(\frac{q}{\pi}\right)_4} = \left(\frac{\overline{\pi}}{q}\right)_4$. Nüüd saamegi, et kehtib võrdus

$$\left(\frac{q}{\pi}\right)_4 = \overline{\overline{\left(\frac{q}{\pi}\right)}_4} = \overline{\left(\frac{\overline{\pi}}{q}\right)_4} = \left(\frac{\pi}{\overline{q}}\right)_4 = \left(\frac{\pi}{q}\right)_4.$$

□

Lause 6.10. *Olgu a täisarv ja $a \equiv 1 \pmod 4$, $|a| \neq 1$. Olgu λ primaarne Gaussi täisarv ning $(\lambda, a) = 1$. Siis*

$$\left(\frac{\lambda}{a}\right)_4 = \left(\frac{a}{\lambda}\right)_4.$$

TÕESTUS. Aritmeetika põhiteoreemi kohaselt võime kirjutada $a = \prod_i q_i \cdot \prod_j r_j$, kus $q_i \equiv 3 \pmod 4$ ja $r_j \equiv 1 \pmod 4$, $q_i, r_j \in \mathbb{P}$. Paneme tähele, et elemente q_i on paarisarv, sest vastasel korral saaksime $a \equiv 3 \pmod 4$. Et λ on primaarne, siis $\lambda = \prod_k \mu_k \cdot \prod_l \nu_l$, kus μ_k, ν_l on vastavalt primaarsed teist ja esimest liiki Gaussi algarvud (lemma 3.5). Näitame, et q_i, μ_k on ühisteguriteta. Oletame vastuväiteliselt, et $(q_i, \mu_k) \neq 1$. Taandumatuse tõttu on see suurim ühistegur $|q_i| = |\mu_k| \in \mathbb{P}$, kust $q_i \mid a$ ning $q_i \mid \lambda$, mis on vastuolus sellega, et $(a, \lambda) = 1$. Samal põhjusel kehtib ka $(r_j, \mu_k) = 1$. Kuna i on paarisarv, siis $\prod_i \left(\frac{-1}{q_i}\right) = 1$. Võttes $\nu = \prod_l \nu_l$ ja arvestades, et lemma 3.5 tõestuse kohaselt võib võtta μ_k täisarvudeks, $-|\mu_k| = \mu_k$, saame lausete 4.8, 4.10, 6.8 ja 6.9 põhjal, et

$$\begin{aligned}
\left(\frac{a}{\lambda}\right)_4 &= \prod_{i,k} \left(\frac{q_i}{\mu_k}\right)_4 \cdot \prod_{j,l} \left(\frac{r_j}{\nu_l}\right)_4 \cdot \prod_{j,k} \left(\frac{r_j}{\mu_k}\right)_4 \cdot \prod_{i,l} \left(\frac{q_i}{\nu_l}\right)_4 \\
&= \prod_{i,k} \left(\frac{q_i}{|\mu_k|}\right)_4 \cdot \prod_{j,l} \left(\frac{r_j}{\nu_l}\right)_4 \cdot \prod_{j,k} \left(\frac{r_j}{|\mu_k|}\right)_4 \cdot \prod_{i,l} \left(\frac{-1}{\nu_l}\right)_4 \cdot \left(\frac{-q_i}{\nu_l}\right)_4 \\
&= \prod 1 \cdot \prod_{j,l} \left(\frac{\nu_l}{r_j}\right)_4 \cdot \prod 1 \cdot \prod_{i,l} \left(\frac{-1}{\nu_l}\right)_4 \cdot \left(\frac{\nu_l}{q_i}\right)_4 \\
&= \prod_{i,k} \left(\frac{\mu_k}{q_i}\right)_4 \cdot \prod_{j,l} \left(\frac{\nu_l}{r_j}\right)_4 \cdot \prod_{j,k} \left(\frac{\mu_k}{r_j}\right)_4 \cdot \prod_{i,l} \left(\frac{-1}{\nu_l}\right)_4 \cdot \left(\frac{\nu_l}{q_i}\right)_4 \\
&= \left(\frac{\prod_k \mu_k \cdot \prod_l \nu_l}{\prod_i q_i \cdot \prod_j r_j}\right)_4 \cdot \prod_l \left(\frac{-1}{\nu}\right)_4 = \left(\frac{\lambda}{a}\right)_4.
\end{aligned}$$

□

Lause 6.11. *Olgu $\pi = a + bi$ ja $\lambda = c + di$ primaarsed ja ühistegurita. Kui $(a, b) = 1$ ja $(c, d) = 1$, siis*

$$\left(\frac{\lambda}{\pi}\right)_4 = \left(\frac{\pi}{\lambda}\right)_4 \cdot (-1)^{\frac{a-1}{2} \cdot \frac{c-1}{2}}.$$

TÕESTUS. Et π ja λ kordajad on ühistegurita, siis ka $(a, \pi) = (b, \pi) = (c, \lambda) = (d, \lambda) = 1$. Kuna

$$c \cdot \pi \equiv ac + bci - \lambda bi = ac + bci - bci + bd = ac + bd \pmod \lambda,$$

siis $(ac + bd, \lambda) = (ac + bd, \pi) = 1$. Veendume viimase võrduse kehtivuses. Oletame vastuväiteliselt, et $(ac + bd, \pi) = s \neq 1$. Siis $\mathbb{Z}[i]$ faktoriaalsuse tõttu

leidub Gaussi algarv t nii, et $t \mid s$. Vastuväitelise oletuse kohaselt siis

$$t \mid ac+bd \quad \text{ja} \quad t \mid \pi = a+bi.$$

Nüüd, kui $t \mid \pi$, siis ka $t \mid \pi \cdot c = ac + bci$. Järelikult

$$t \mid ac + bd - ac - bci = b(d - ci).$$

Kuna t on taandumatu, siis kas $t \mid b$ või $t \mid d - ci$. Kuid siis kehtib ka $t \mid a$ ja seetõttu jõuame vastuoluni. Samuti, kui $t \mid d - ci = -i\lambda$, siis $t \mid \lambda$. Kuna t jagab ka elementi π ning $(\lambda, \pi) = 1$, oleme saanud vastuolu. Seega tõepoolest $(ac + bd, \pi) = 1$. Kuna $c\pi \equiv ac + bd \pmod 4$, siis

$$\left(\frac{c}{\lambda}\right)_4 \cdot \left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{ac+bd}{\lambda}\right)_4 \tag{4}$$

ja analoogiliselt

$$\left(\frac{a}{\pi}\right)_4 \cdot \left(\frac{\lambda}{\pi}\right)_4 = \left(\frac{ac+bd}{\pi}\right)_4. \tag{5}$$

Võttes võrdusest (5) kaaskompleksarvu ning korrutades seda võrdusega (4), saame seoste $\overline{a} = a$ ja $\overline{ac+bd} = ac + bd$ tõttu võrduse

$$\left(\frac{a}{\overline{\pi}}\right)_4 \cdot \left(\frac{c}{\lambda}\right)_4 \cdot \overline{\left(\frac{\lambda}{\pi}\right)_4} \cdot \left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{ac+bd}{\lambda\overline{\pi}}\right)_4. \tag{6}$$

Korrutades võrdust (6) elementide $\left(\frac{a}{\overline{\pi}}\right)_4$ ja $\left(\frac{c}{\lambda}\right)_4$ pöördelementidega, saame võrdusest (6) lause 5.1 omaduse 3 põhjal võrduse

$$\overline{\left(\frac{\lambda}{\pi}\right)_4} \cdot \left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{c}{\overline{\lambda}}\right)_4 \cdot \left(\frac{a}{\pi}\right)_4 \cdot \left(\frac{ac+bd}{\overline{\pi}\cdot\lambda}\right)_4.$$

Oletame esmalt, et a, c ja $ac + bd$ on mittepööratavad. Defineerime paaritu täisarvu n jaoks funktsiooni $\gamma(n) = (-1)^{\frac{n-1}{2}}$. Siis $\gamma(n) \cdot n \equiv 1 \pmod 4$ ja $\gamma(ac + bd) = (-1)^{\frac{ac+bd-1}{2}} = (-1)^{\frac{ac-1}{2}} = (-1)^{\frac{a-1}{2}} \cdot (-1)^{\frac{c-1}{2}} = \gamma(a) \cdot \gamma(c)$, sest $bd \equiv 0 \pmod 4$ (lemma 3.2). Lause 6.10 põhjal ning teades, et $\left(\frac{x}{\alpha}\right)_4 = \left(\frac{\gamma(x)}{\alpha}\right)_4 \cdot \left(\frac{\gamma(x)\cdot x}{\alpha}\right)_4$, saame

$$\begin{aligned}
&\overline{\left(\frac{\lambda}{\pi}\right)_4} \cdot \left(\frac{\pi}{\lambda}\right)_4 \\
&= \left(\frac{\gamma(c)}{\overline{\lambda}}\right)_4 \cdot \left(\frac{\overline{\lambda}}{\gamma(c)\cdot c}\right)_4 \cdot \left(\frac{\gamma(a)}{\pi}\right)_4 \cdot \left(\frac{\pi}{\gamma(a)\cdot a}\right)_4 \cdot \left(\frac{\gamma(ac+bd)}{\lambda\cdot\overline{\pi}}\right)_4 \cdot \left(\frac{\lambda\cdot\overline{\pi}}{\gamma(ac+bd)\cdot(ac+bd)}\right)_4.
\end{aligned}$$

Märgime, et

$$\gamma(a) = \begin{cases} 1, \text{kui } a \equiv 1 \pmod 4, \\ -1, \text{kui } a \equiv 3 \pmod 4, \end{cases}$$

ja seega lemma 3.3 põhjal

$$\begin{aligned} \left(\frac{\gamma(a)}{\lambda}\right)_4 &= \gamma(a)^{\frac{N(\lambda)-1}{4}} \\ &= \begin{cases} -1 \pmod \lambda, \text{kui } a \equiv 3 \pmod 4 \wedge c \equiv 3 \pmod 4, \\ 1 \pmod \lambda, \text{muudel juhtudel .} \end{cases} \end{aligned}$$

Lause 4.6 omaduse 2 põhjal võime kirjutada

$$\left(\frac{\gamma(ac+bd)}{\lambda\cdot\overline{\pi}}\right)_4 = \left(\frac{\gamma(a)\cdot\gamma(c)}{\lambda\cdot\overline{\pi}}\right)_4 = \left(\frac{\gamma(a)}{\lambda}\right)_4 \cdot \left(\frac{\gamma(c)}{\lambda}\right)_4 \cdot \left(\frac{\gamma(a)}{\overline{\pi}}\right)_4 \cdot \left(\frac{\gamma(c)}{\overline{\pi}}\right)_4$$

ja seetõttu sama lause omaduste 3 ja 6 põhjal

$$\begin{aligned} &\overline{\left(\frac{\lambda}{\pi}\right)_4} \cdot \left(\frac{\pi}{\lambda}\right)_4 \\ &= \left(\frac{\gamma(c)}{\overline{\lambda}}\right)_4 \cdot \left(\frac{\overline{\lambda}}{\gamma(c)c}\right)_4 \cdot \left(\frac{\gamma(a)}{\pi}\right)_4 \cdot \left(\frac{\pi}{\gamma(a)a}\right)_4 \cdot \left(\frac{\gamma(ac+bd)}{\lambda\cdot\overline{\pi}}\right)_4 \cdot \left(\frac{\lambda\cdot\overline{\pi}}{\gamma(ac+bd)(ac+bd)}\right)_4 \\ &= \left(\frac{\gamma(c)}{\overline{\lambda}}\right)_4 \cdot \left(\frac{\overline{\lambda}}{c}\right)_4 \cdot \left(\frac{\gamma(a)}{\pi}\right)_4 \cdot \left(\frac{\pi}{a}\right)_4 \cdot \left(\frac{\gamma(a)}{\lambda}\right)_4 \cdot \left(\frac{\gamma(c)}{\lambda}\right)_4 \cdot \left(\frac{\gamma(a)}{\overline{\pi}}\right)_4 \cdot \left(\frac{\gamma(c)}{\overline{\pi}}\right)_4 \cdot \left(\frac{\lambda\cdot\overline{\pi}}{ac+bd}\right)_4 \\ &= \left(\frac{\gamma(c)}{\lambda}\right)_4^2 \cdot \left(\frac{\gamma(a)}{\pi}\right)_4^2 \cdot \left(\frac{\gamma(a)}{\lambda}\right)_4 \cdot \left(\frac{\gamma(c)}{\pi}\right)_4 \cdot \left(\frac{\overline{\lambda}}{c}\right)_4 \cdot \left(\frac{\pi}{a}\right)_4 \cdot \left(\frac{\lambda\cdot\overline{\pi}}{ac+bd}\right)_4. \end{aligned}$$

Et $\left(\frac{\gamma(a)}{\lambda}\right)_4$ ja $\left(\frac{\gamma(c)}{\pi}\right)_4$ väärtused on samaaegselt kas 1 või -1 ja ruudud $\left(\frac{\gamma(c)}{\lambda}\right)_4^2 = 1$ ning $\left(\frac{\gamma(a)}{\pi}\right)_4^2 = 1$, võime need võrdusest taandada. Nüüd oleme jõudnud olukorrani, kus lause 4.10 ja $a, c, ac+bd$ mittepööratavuse tõttu

$$\begin{aligned} \overline{\left(\frac{\lambda}{\pi}\right)_4} \cdot \left(\frac{\pi}{\lambda}\right)_4 &= \left(\frac{c-di}{c}\right)_4 \cdot \left(\frac{a+bi}{a}\right)_4 \cdot \left(\frac{ac+bd+(ad-cb)i}{ac+bd}\right)_4 \\ &= \left(\frac{-d}{c}\right)_4 \cdot \left(\frac{i}{c}\right)_4 \cdot \left(\frac{b}{a}\right)_4 \cdot \left(\frac{i}{a}\right)_4 \cdot \left(\frac{ad-bc}{ac+bd}\right)_4 \cdot \left(\frac{i}{ac+bd}\right)_4 \\ &= \left(\frac{i}{c}\right)_4 \cdot \left(\frac{i}{a}\right)_4 \cdot \left(\frac{i}{ac+bd}\right)_4 = \left(\frac{i}{ac(ac+bd)}\right)_4. \end{aligned}$$

Kahe järjestikuse paarisarvu korrutis jagub alati arvuga 8, mistõttu

$$(-1)^{\frac{ac(ac+bd)-1}{4}} \begin{cases} (-1)^{\frac{(ac)^2-1}{4}} = (-1)^{\frac{(ac+1)(ac-1)}{4}} = 1, \\ \qquad \text{kui } a \equiv 1 \text{ või } c \equiv 1 \pmod 4, \\ \\ (-1)^{ac+\frac{(ac+1)(ac-1)}{4}} = (-1)^{ac} = -1, \\ \qquad \text{kui } a \equiv 3 \text{ ja } c \equiv 3 \pmod 4, \end{cases}$$

ning ka

$$(-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}} = \begin{cases} 1, \text{kui } a \equiv 1 \pmod 4 \text{ või } c \equiv 1 \pmod 4, \\ -1, \text{kui } a \equiv 3 \pmod 4 \text{ ja } c \equiv 3 \pmod 4. \end{cases} \tag{7}$$

Kuna $ac(ac+bd) \equiv (ac)^2 \equiv 1 \pmod 4$, siis olemegi lause 4.11 kohaselt saanud võrduse

$$\overline{\left(\frac{\lambda}{\pi}\right)}_4 \cdot \left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{i}{ac(ac+bd)}\right)_4 = (-1)^{\frac{ac(ac+bd)-1}{4}} = (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}.$$

Oletame nüüd, et kas a, c või $ac+bd$ on pööratav. Vaatleme näiteks juhtu $a = 1$, sest ülejäänud võimalused on tõestatavad analoogiliselt. Kui $a = 1$, siis $\pi = 1 + bi$, $b \equiv 0 \pmod 4$. Siis eelnevaga sarnaselt saame, et

$$\begin{aligned} \overline{\left(\frac{\lambda}{\pi}\right)}_4 \cdot \left(\frac{\pi}{\lambda}\right)_4 &= \left(\frac{c}{\overline{\lambda}}\right)_4 \cdot \left(\frac{c+bd}{\overline{\pi}\cdot\lambda}\right)_4 \\ &= \left(\frac{\gamma(c)}{\overline{\lambda}}\right)_4 \cdot \left(\frac{\overline{\lambda}}{c}\right)_4 \cdot \left(\frac{\gamma(c)}{\lambda}\right)_4 \cdot \left(\frac{\gamma(c)}{\overline{\pi}}\right)_4 \cdot \left(\frac{\lambda\cdot\overline{\pi}}{c+bd}\right)_4 \\ &= \left(\frac{\overline{\lambda}}{c}\right)_4 \cdot \left(\frac{\lambda\cdot\overline{\pi}}{c+bd}\right)_4 = \left(\frac{c-di}{c}\right)_4 \cdot \left(\frac{c+bd+(d-cb)i}{c+bd}\right)_4 \\ &= \left(\frac{-d}{c}\right)_4 \cdot \left(\frac{i}{c}\right)_4 \cdot \left(\frac{d-bc}{c+bd}\right)_4 \cdot \left(\frac{i}{c+bd}\right)_4 \\ &= \left(\frac{i}{c}\right)_4 \cdot \left(\frac{i}{c+bd}\right)_4 = \left(\frac{i}{c(c+bd)}\right)_4 \end{aligned}$$

Nüüd (7) põhjal, võttes $a = 1$, kehtib

$$(-1)^{\frac{c^2+cbd-1}{4}} = 1 = (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}.$$

Seega

$$\overline{\left(\frac{\lambda}{\pi}\right)}_4 \cdot \left(\frac{\pi}{\lambda}\right)_4 = \left(\frac{i}{c(c+bd)}\right)_4 = (-1)^{\frac{c(c+bd)-1}{4}} = (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}}. \qquad \square$$

Viimase lause põhjal on lihtne tõestada biruutvastavusseadust. Olgu $\pi = a' + b'i$ ja $\lambda = c' + d'i$ primaarsed ning ühistegurita. Võtame $m = \pm(a', b')$ ja $n = \pm(c', d')$ selliselt, et $m \equiv n \equiv 1 \pmod 4$. Siis $(a, b) = 1$ ja $(c, d) = 1$, $\pi = m(a + bi)$ ja $\lambda = n(c + di)$ ning $a + bi$ ja $c + di$ on samuti primaarsed. Vaatleme esiteks juhtu, kus $m \neq 1$ ja $n \neq 1$. Kuna $(\lambda, m) = 1$ ja $(a+bi, n) = 1$ ning ka $(a + bi, c + di) = 1$, siis lausete 6.10 ja 6.11 põhjal

$$\begin{aligned}\left(\frac{\pi}{\lambda}\right)_4 &= \left(\frac{m}{\lambda}\right)_4 \cdot \left(\frac{a+bi}{\lambda}\right)_4 = \left(\frac{\lambda}{m}\right)_4 \cdot \left(\frac{a+bi}{n}\right)_4 \cdot \left(\frac{a+bi}{c+di}\right)_4 \\ &= \left(\frac{\lambda}{m}\right)_4 \cdot \left(\frac{n}{a+bi}\right)_4 \cdot \left(\frac{c+di}{a+bi}\right)_4 \cdot (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}} \\ &= \left(\frac{\lambda}{m}\right)_4 \cdot \left(\frac{\lambda}{a+bi}\right)_4 \cdot (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}} = \left(\frac{\lambda}{\pi}\right)_4 \cdot (-1)^{\frac{a-1}{2}\cdot\frac{c-1}{2}} \\ &= \left(\frac{\lambda}{\pi}\right)_4 \cdot (-1)^{\frac{N(\pi)-1}{4}\cdot\frac{N(\lambda)-1}{4}}.\end{aligned}$$

Viimane võrdus kehtib tänu lausele 6.2. Juhul, kui $m = 1 = n$, on tegemist lausega 6.11. Eelnevaga sarnase arutelu põhjal kehtib biruutvastavusseadus ka juhul, kui $m = 1$ või $n = 1$. Sellega olemegi esitanud biruutvastavusseaduse tõestuse, mida võib nimetada arvuteooria üheks sügavamaks ja ilusamaks tõestuseks.

Kirjandus

[1] F. Lemmermayer, *Reciprocity Laws. From Euler to Eisenstein*, Springer, Berlin, 2000.

[2] G. Brokan, *Gaussi täisarvud*, bakalaureusetöö, Tartu Ülikool, 2014.

[3] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory, second edition*, Springer, New York, 1990.

[4] M. Kilp, *Algebra I*, Eesti Matemaatika Selts, Tartu, 2005.

[5] V. Laan, *Arvuteooria loengukonspekt*, Tartu Ülikool, 2012, http://math.ut.ee/pmi/kursused/arvuteooria/kon.pdf (viimati vaadatud 04.06.2015).

Lihtlitsents lõputöö reprodutseerimiseks ja lõputöö üldsusele kättesaadavaks tegemiseks

Mina, Anu Ahven (sünnikuupäev 28.11.1992),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) enda loodud teose "Biruutvastavusseadus", mille juhendaja on Lauri Tart,
   (a) reprodutseerimiseks säilitamise ja üldsusele kättesaadavaks tegemise eesmärgil, sealhulgas digitaalarhiivi DSpace lisamise eesmärgil kuni autoriõiguse kehtivuse tähtaja lõppemiseni;
   (b) üldsusele kättesaadavaks tegemiseks Tartu Ülikooli veebikeskkonna kaudu, sealhulgas digitaalarhiivi DSpace kaudu kuni autoriõiguse kehtivuse tähtaja lõppemiseni.
2. olen teadlik, et punktis 1 nimetatud õigused jäävad alles ka autorile;
3. kinnitan, et lihtlitsentsi andmisega ei rikuta teiste isikute intellektuaalomandi ega isikuandmete kaitse seadusest tulenevaid õigusi.

Tartus, **05.06.2015**