Tartu Ülikool
Loodus- ja täppisteaduste valdkond
Matemaatika ja statistika instituut

Johanna Charlotte Jeltsch

Eisensteini kuupvastavusseadus

Matemaatika

Bakalaureusetöö (9 EAP)

Juhendajad: PhD Lauri Tart ja prof. Valdis Laan

Tartu 2025

EISENSTEINI KUUPVASTAVUSSEADUS

Bakalaureusetöö

Johanna Charlotte Jeltsch

Lühikokkuvõte

Eisensteini kuupvastavusseadus on oluline tulemus algebralises arvuteoorias, mis käsitleb kongruentsi $x^3 \equiv p \pmod{q}$ lahenduvustingimusi. Kuupvastavusseadus võimaldab lahenduvuse taandamist kuupjäägi sümboli arvutamisele analoogiliselt Gaussi ruutvastavusseadusega, mis seob ruutkongruentside lahenduvuse Legendre'i sümboliga. Töös esitatakse kuupvastavusseaduse täielik ja detailne tõestus Gaussi ja Jacobi summade abil.

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria.

Märksõnad: Algebraline arvuteooria, kongruentsid, kommutatiivne algebra, kompleksarvud, algarvud, korpused.

EISENSTEIN'S CUBIC RECIPROCITY LAW

Bachelor thesis

Johanna Charlotte Jeltsch

Abstract

Eisenstein's cubic reciprocity law is a major result in algebraic number theory concerning the solvability of the congruence $x^3 \equiv p \pmod{q}$. The cubic reciprocity law allows reducing the question of solvability to the computation of the cubic reciprocity symbol, in a manner analogous to how Gauss's law of quadratic reciprocity relates the question of solvability of quadratic congruences to the Legendre symbol. We present a complete and detailed proof of Eisenstein's cubic reciprocity law using Gauss and Jacobi sums.

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory.

Key Words: Algebraic number theory, congruences, commutative algebra, complex numbers, prime numbers, fields.

Sisukord

Sissejuhatus

Käesolev töö viib meid algebralise arvuteooria valdkonda. Põhiküsimus on siin järgmine: milliste arvude p ja q korral on kongruents $x^3 \equiv p \pmod{q}$ lahenduv? Juba Gaussilt pärinev ruutvastavusseadus vastab sellele küsimusele ruutkongruentside $x^2 \equiv p \pmod{q}$ jaoks. Kuid kõrgema astme kongruentse uurides pidi Gauss lõpuks tunnistama, et sarnaste tulemuste tõestamiseks ei piisa täisarvudest — tuleb arvuvalda hoopis laiendada sobivate kompleksarvuliste ühejuurtega.

Kuupkongruentside uurimiseks moodustame täisarvude laiendi kolmanda astme ühejuure $\omega := \frac{-1+\sqrt{3}i}{2}$ abil. Tulemuseks on ring $\mathbb{Z}[\omega] := \{a+b\omega | a, b \in \mathbb{Z}\}$. Neljanda astme kongruentse uurides laiendame täisarvude ringi analoogiliselt neljanda astme ühejuurega i, saades Gaussi täisarvude ringi $\mathbb{Z}[i]$. Mõlemas ringis kehtib faktoriaalsus, s.t. leidub elementide ühene lahutus algteguriteks, kuid üldisematel juhtudel see tavaliselt enam ei kehti — nende puhul tuleb sarnaste tulemuste tõestamiseks juba teisi meetodeid kasutada.

Gauss ise ei suutnud ei kuup- ega biruutvastavusseadust täielikult tõestada. Jacobi sõnastas ja hiljem tõestas mõned tulemused mõlema kohta, kuid esimesed täielikud avaldatud tõestused pärinevad Eisensteinilt.

Bakalaureusetöö on referatiivne ning selle põhiallikaks on K. Irelandi ja M. Roseni õpik "A Classical Introduction to Modern Number Theory" [1]. Lisaks on kasutatud A. Ahvena bakalaureusetööd biruutvastavusseadusest [2], arvuteooria loengukonspekti [3] ning algebra loengukonspekte [4], [5] ja [6].

A. Ahvena bakalaureusetöös on lahti kirjutatud biruutvastavusseaduse tõestus, käesoleva töö sihiks on teha sama kuupvastavusseaduse jaoks. Õpiku tõestus on napisõnaline ja vajaminevad tulemused on üle mitme peatükki laiali jaotatud — meie eesmärgiks on need lahti kirjutada ja esitada kuupvastavusseaduse täielik ja detailne tõestus. Oma olemuselt on see tõestus suuresti Eisensteini oma.

Töö koosneb kuuest peatükist.

Esimeses peatükis on välja toodud kasutatud üldmõistete definitsioonid algebra ja arvuteooria valdkonnast, ning on loetletud põhitööks vajalikud eelteadmised.
Teises peatükis konstrueeritakse Eisensteini täisarvude ring. Käsitletakse selle ringi elementide normi mõistet ja tõestatakse normi omadused. Lisaks defineeritakse Eisensteini algarvud ja uuritakse nende struktuuri ja seost täisarvudega.
Kolmas peatükk on pühendatud Eisensteini täisarvude jäägiklassiringidele. Tuuakse välja sarnasused täisarvude jäägiklassiringidega ning näidatakse, kuidas moodustada Eisensteini täisarvude baasil lõplikke jäägiklassikorpusi.
Neljandas peatükis defineeritakse kuupjäägi sümbol, mis täidab analoogilist rolli Legendre'i sümboliga ruutjääkide analüüsis. Lisaks tõestatakse selle olulisemad omadused.
Viiendas peatükis tuuakse sisse karakteri mõiste ning kuupvastavusseaduse tõestamiseks vajalikud tulemused Gaussi ja Jacobi summade kohta.
Kuuendas peatükis defineeritakse primaarsuse mõiste ja sõnastatakse ning tõestatakse Eisensteini kuupvastavusseadus Gaussi ja Jacobi summade abil.

1 Põhimõisted ja -tulemused

Enne põhitöö juurde asumist on meil vaja sõnastada mõned definitsioonid ja tulemused, mida hiljem tulemuste tõestamiseks tarvis on. Nende peamised allikad on ainete Algebra I [4], Arvuteooria [3] ja Sissejuhatus algebra struktuuridesse [6] loengukonspektid ning A. Ahvena bakalaureusetöö biruutvastavusseadusest [2]. Tulemuste sõnastus ja/või tähistus on osaliselt muudetud.

1.1 Rühmad

Definitsioon 1.1 ([6], definitsioon 2.9)**.** Lõpliku rühma **järguks** nimetame tema elementide arvu.

Teoreem 1.2 ([6], teoreem 2.10)**.** (Lagrange'i teoreem) *Lõpliku rühma iga alamrühma järk jagab selle rühma järku.*

Definitsioon 1.3 ([6], definitsioon 3.15)**.** Olgu A Abeli rühm tehtega $*$, $a \in A$ ja $n \in \mathbb{N}$. Ütleme, et **elemendi** a **järk on** n, kui $a^n = \underbrace{a * \cdots * a}_{n} = 0$, kusjuures n on vähim naturaalarv, mille korral see võrdus kehtib. Kui sellist naturaalarvu ei leidu, siis ütleme, et a on lõpmatut järku.

Definitsioon 1.4 ([6], definitsioon 8.17)**.** Rühma R nimetame **tsükliliseks**, kui leidub selline $g \in R$, et kõik R elemendid on esitatavad g astmetena. Sel juhul ütleme, et g on rühma R **moodustaja**.

1.2 Ringid ja korpused

Selles töös mõistame ringi all kommutatiivset ühikelemendiga ringi.

Definitsioon 1.5 ([6], definitsioon 4.9)**.** Ringi R mittetühja alamhulka I nimetame **ideaaliks**, kui

1. $a + b \in I$ iga $a, b \in I$ korral;

2. $ra \in I$ iga $a \in I$ ja $r \in R$ korral.

Definitsioon 1.6 ([6], definitsioon 4.13)**.** Ringi R elemendi a poolt tekitatud **peaideaaliks** nimetame ideaali $aR := \{ar | r \in R\}$.

Definitsioon 1.7 ([5], definitsioon 1.63)**.** Ringi R **faktorringiks** ideaali I järgi nimetame ringi, mille elementideks on ideaali I kõrvalklassid, rühmas $(R; +)$ ning mille liitmine ja korrutamine on defineeritud võrdustega

$$(x + I) + (y + I) = (x + y) + I,$$
$$(x + I) \cdot (y + I) = (xy) + I,$$

kus $x, y \in R$. Seda ringi tähistame R/I.

Definitsioon 1.8 ([4], definitsioon 9.12)**.** Olgu R ring ja $a, b \in R$. Ütleme, et element a **jagab** elementi b ja tähistame $a|b$, kui leidub selline $c \in R$, et $ac = b$.

Definitsioon 1.9 ([4], definitsioon 9.15)**.** Ütleme, et ringi elemendid a ja b on **assotsieeritud** (tähistame $a \sim b$), kui $a|b$ ja $b|a$.

Lause 1.10 ([4], lause 9.16)**.** *Olgu R ring ja $a, b \in R\backslash\{0\}$. Elemendid a ja b on assotsieeritud parajasti siis, kui leidub selline pööratav element $u \in R$, et $a = bu$.*

Definitsioon 1.11 ([4], definitsioon 9.30)**.** Nulliteguriteta ringi R nimetame **Eukleidese ringiks**, kui leidub selline kujutus $\delta : R\backslash\{0\} \to \mathbb{N} \cup \{0\}$, et

1. iga $a, b \in R\backslash\{0\}$ korral $\delta(ab) \geq \delta(a)$,

2. iga $a \in R, b \in R\backslash\{0\}$ korral leiduvad sellised $q, r \in R$, et $a = bq + r$, kusjuures $r = 0$ või $\delta(r) < \delta(b)$. Elementi q nimetame sel juhul a ja b **jagatiseks** ning elementi r jagamisel tekkivaks **jäägiks**.

Definitsioon 1.12 ([4], definitsioon 9.18)**.** Olgu R ring ja $a, b, d \in R$. Elementi d nimetame a ja b **suurimaks ühisteguriks** (tähistame $d = (a, b)$), kui

1. $d|a$ ja $d|b$,

2. iga $c \in R$ korral kehtib, et kui $c|a$ ja $c|b$, siis $c|d$.

Lause 1.13 ([4], lause 9.21)**.** *Olgu a, b, c, d ringi R elemendid. Kui kehtib $d = (a, b)$ ja $d \sim c$, siis ka $c = (a, b)$.*

See tähendab, et Eukleidese ringis on suurim ühistegur defineeritud assotsieerituse täpsuseni.

Definitsioon 1.14 ([4], definitsioon 9.34)**.** Nulliteguriteta ringi R mittepööratavat elementi $p \neq 0$ nimetame **taandumatuks**, kui mistahes $a, b \in R$ korral võrdusest $p = ab$ järeldub, et kas a või b on pööratav.

Definitsioon 1.15 ([4], definitsioon 9.36)**.** Nulliteguriteta ringi R nimetame **faktoriaalseks**, kui iga nullist erinev mittepööratav element $a \in R$ on esitatav taandumatute elementide korrutisena

$$a = p_1 \dots p_n, \quad \text{kus } n \in \mathbb{N},\ p_1, \dots, p_n \text{ on taandumatud}$$

ning see esitus on ühene tegurite järjekorra ja assotsieerituse täpsuseni.

Teoreem 1.16 ([3], teoreem 1.19)**.** (Aritmeetika põhiteoreem) *Iga naturaalarvu $n > 1$ saab esitada algarvude korrutisena ning see esitus on ühene järjekorra täpsuseni.*

Teoreem 1.17 ([4], teoreem 9.39)**.** *Iga Eukleidese ring on faktoriaalne.*

Lause 1.18 ([4], lause 9.32)**.** *Kui R on Eukleidese ring, $a, b \in R$ ja $d = (a, b)$, siis leiduvad sellised $u, v \in R$, et $ua + vb = d$.*

Definitsioon 1.19 ([6], ptk. 8.1)**.** **Korpus** on kommutatiivne ring, milles on vähemalt kaks elementi ja mille kõik nullist erinevad elemendid on pööratavad. Korpust, milles on lõplik arv elemente, nimetame **lõplikuks korpuseks**. Kui K on korpus, siis tähistame $K^* := K \backslash \{0\}$ ja ütleme, et $(K^*, \cdot)$ on korpuse K **multiplikatiivne rühm**.

Teoreem 1.20 ([3], teoreem 10.14)**.** *Iga lõpliku korpuse multiplikatiivne rühm on tsükliline.*

Definitsioon 1.21 ([3], ptk. 10.1)**.** Lõpliku korpuse K **karakteristika** on vähim naturaalarv n, mille korral $\underbrace{1+\cdots+1}_{n \text{ tükki}} = 0$.

Lause 1.22 ([3], lause 10.1)**.** *Lõpliku korpuse karakteristika on algarv.*

1.3 Arvuteooria

Lemma 1.23 ([3], järeldus 1.11)**.** (Eukleidese lemma) *Mistahes $a, b, c \in \mathbb{Z}$ korral kehtib, et kui $a|bc$ ja $(a, b) = 1$, siis $a|c$.*

Lemma 1.24 ([3], lemma 7.17)**.** *Kui p on algarv ja $1 \leq k \leq p-1$ on naturaalarv, siis p jagab binoomkordajat $\binom{p}{k}$.*

Lause 1.25 ([3], lause 6.2)**.** *Olgu $a, b \in \mathbb{Z}$, $n \in \mathbb{N}$. Lineaarkongruents $ax \equiv b \pmod{n}$ on lahenduv parajasti siis, kui $(a, n)|b$.*

Lause 1.26 ([3], lause 7.30)**.** *Olgu q algarv ja $[g]$ korpuse $\mathbb{Z}_q$ multiplikatiivse rühma $\mathbb{Z}_q^*$ moodustaja. Kongruents $g^u \equiv g^v \pmod{q}$ on samaväärne kongruentsiga $u \equiv v \pmod{q-1}$.*

Definitsioon 1.27 ([3], definitsioon 8.1)**.** Olgu $p > 2$ algarv ja $a \in \mathbb{Z}$ selline, et $p \nmid a$. Arvu a nimetame **ruutjäägiks**, kui elemendil $[a] \in \mathbb{Z}_p$ leidub ruutjuur korpuses $\mathbb{Z}_p$, ja mitteruutjäägiks, kui ei leidu.

Definitsioon 1.28 ([3], definitsioon 8.3)**.** Olgu a täisarv ja $p > 2$ algarv. **Legendre'i sümboli** $\left(\frac{a}{p}\right)$ defineeritakse järgmiselt:

$$\left(\frac{a}{p}\right) = \begin{cases} 0, & \text{kui } p|a, \\ 1, & \text{kui } a \text{ on ruutjääk mooduli } p \text{ järgi}, \\ -1, & \text{kui } a \text{ ei ole ruutjääk mooduli } p \text{ järgi}. \end{cases}$$

Lemma 1.29 ([3], lemma 8.4)**.** *Olgu a, b täisarvud ja $p > 2$ algarv. Kui $a \equiv b \pmod{p}$, siis $\left(\frac{a}{p}\right) = \left(\frac{b}{p}\right)$.*

Lause 1.30 ([3], lause 8.8)**.** *Suvalise argarvu $p > 2$ ja täisarvude a, b korral kehtib*

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

Teoreem 1.31 ([3], teoreem 8.14)**.** (Gaussi ruutvastavusseadus) *Kui $p > 2$ ja $q > 2$ on erinevad algarvud, siis*

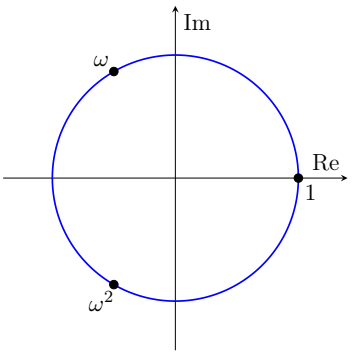
$$\left(\frac{p}{q}\right) = (-1)^{\frac{(p-1)(q-1)}{4}} \left(\frac{q}{p}\right).$$

Antud töö eesmärgiks on esitada ja tõestada Gaussi ruutvastavusseaduse analoog kuupjääkide jaoks.

2 Eisensteini täisarvude ring ja selle algarvud

Uurides võrrandi $x^2 \equiv a \pmod{p}$ lahenduvust üle täisarvude puutume kokku Legendre'i sümboliga (vt. definitsioon 1.28). Paneme tähele, et 1 ja -1 on parajasti võrrandi $x^2 = 1$ kompleksarvulised lahendid ehk teise astme ühejuured.

Kuupvõrrandi $x^3 \equiv a \pmod{p}$ lahenduvust uurides defineerime kuupjäägi sümboli analoogiliselt. Selleks on tarvilik kasutusele võtta hoopis kolmanda astme ühejuured $\{1, \frac{-1+\sqrt{3}i}{2}, \frac{-1-\sqrt{3}i}{2}\}$ ning sellest lähtudes ka vastavalt täisarvude ringi laiendada. Tähistame edaspidi $\omega := \frac{-1+\sqrt{3}i}{2}$, siis võrrandi $x^3 = 1$ kompleksarvulised lahendid on parajasti $\{1, \omega, \omega^2\}$. Geomeetriliselt need juured asuvad komplekstasandi ühikringil.



Joonis 1: Kolmanda astme ühejuured

Lisaks paneme tähele, et $\omega^2 = \overline{\omega} = -1 - \omega$. Tõepoolest,

$$\omega^2 = \left(\frac{-1+\sqrt{3}i}{2}\right)^2 = \frac{-2(1+\sqrt{3}i)}{4} = \frac{-1-\sqrt{3}i}{2} = \overline{\omega}$$

ja

$$\overline{\omega} = \frac{-1-\sqrt{3}i}{2} = -(1+\frac{-1+\sqrt{3}i}{2}) = -1-\omega.$$

2.1 Ringi $\mathbb{Z}[\omega]$ konstrueerimine

Defineerime kompleksarvude hulga $\mathbb{Z}[\omega] := \{a + b\omega | a, b \in \mathbb{Z}\}$.

Näitame, et tegemist on ringiga. Kui $a + b\omega, c + d\omega \in \mathbb{Z}[\omega]$, siis

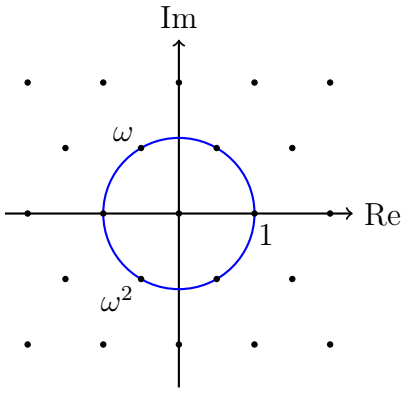
$$(a + b\omega) + (c + d\omega) = (a + c) + (b + d)\omega \in \mathbb{Z}[\omega]$$

ja

$$\begin{aligned}(a+b\omega)(c+d\omega) &= ac + (ad+bc)\omega + bd\omega^2 \\ &= ac + (ad+bc)\omega + bd(-1-\omega) \\ &= (ac-bd) + (ad+bc-bd)\omega \in \mathbb{Z}[\omega],\end{aligned}$$

ehk $\mathbb{Z}[\omega]$ on kinnine liitmise ja korrutamise suhtes. Null- ja ühikelemendiks on vastavalt $0 = 0 + 0\omega$ ja $1 = 1 + 0\omega$; ülejäänud ringi tehete omadused kehtivad seetõttu, et $\mathbb{Z}[\omega]$ elemendid on kompleksarvud. Lisaks on $\mathbb{Z}[\omega]$ kompleksarvude korpuse alamringina kommutatiivne ja nulliteguriteta. Paneme ka tähele, et $\mathbb{Z}[\omega]$ on kinnine kaaskompleksarvu võtmise suhtes:

$$\overline{a+b\omega} = a + b\overline{\omega} = a + b\omega^2 = a + b(-1-\omega) = (a-b) + (-b)\omega \in \mathbb{Z}[\omega].$$



Joonis 2: Ringi $\mathbb{Z}[\omega]$ elemendid komplekstasandil

2.2 Ringi $\mathbb{Z}[\omega]$ elementide norm

Kompleksarvu $a + bi$ norm ehk moodul on tavaliselt defineeritud kui $|a + bi| = \sqrt{a^2 + b^2}$. Edaspidi mõistame kompleksarvu $a + b\omega$ normi all avaldist

$$N(a + bi) = a^2 + b^2$$

ehk mooduli ruutu. (NB! Tegemist ei ole normiga analüüsi kontekstis, vaid sellest sõltumatult defineeritud nimetusega.) Teame, et iga kompleksarvu z korral $N(z) = z\overline{z}$. Tõepoolest, $z\overline{z} = (a+bi)(a-bi) = a^2 - b^2 i^2 = a^2 + b^2 = N(z)$. Seega, elementide $a + b\omega \in \mathbb{Z}[\omega]$ korral

$$\begin{aligned} N(a+b\omega) &= (a+b\omega)(a+b\overline{\omega}) \\ &= (a+b\omega)(a-b-b\omega) \\ &= a^2 - ab - ab\omega + ab\omega - b^2\omega - b^2(-1-\omega) \\ &= a^2 - ab + b^2. \end{aligned}$$

Tõestame mõningad normi omadused.

Lause 2.1. *Olgu $z, z' \in \mathbb{Z}[\omega]$, kus $z = a + b\omega, z' = a' + b'\omega$. Siis*

1. *norm $N(z)$ on mittenegatiivne täisarv, kusjuures $N(z) = 0$ parajasti siis, kui $z = 0$;*
2. *$N(zz') = N(z) \cdot N(z')$.*

Tõestus.

1. Kuna a ja b on täisarvud, siis $N(a + b\omega) = a^2 - ab + b^2$ on samuti täisarv. Ülejäänud järeldub otse mooduli omadustest: $N(z) = |z|^2$ ja $|z| = 0 \Leftrightarrow z = 0$, seega $N(z) \geq 0$ ja $N(z) = 0 \Leftrightarrow z = 0$.

2. Kasutame jälle mooduli omadusi ja kompleksarvude korrutamise kommutatiivsust:

$$N(zz') = |zz'|^2 = (|z||z'|)^2 = |z|^2|z'|^2 = N(z) \cdot N(z').$$

■

Soovime nüüd näidata, et ringis $\mathbb{Z}[\omega]$ on võimalik iga element üheselt esitada taandumatute elementide korrutisena. Selleks näitame, et $\mathbb{Z}[\omega]$ on Eukleidese ring.

Lause 2.2. *Ring $\mathbb{Z}[\omega]$ on Eukleidese ring kujutuse $N : \mathbb{Z}[\omega]\backslash\{0\} \to \mathbb{N} \cup \{0\}$ suhtes.*

Tõestus. Olgu $z_1, z_2 \in \mathbb{Z}[\omega]$ suvalised.

1. Näitame, et kui $z_1 \neq 0$, $z_2 \neq 0$, siis $N(z_1 z_2) \geq N(z_1)$. Kuna eelduste kohaselt $N(z_2) \geq 1$, siis

$$N(z_1 z_2) = N(z_1) \cdot N(z_2) \geq N(z_1) \cdot 1 = N(z_1).$$

2. Näitame nüüd, et kui $z_2 \neq 0$, siis leiduvad sellised $q, r \in \mathbb{Z}[\omega]$, et $z_1 = qz_2 + r$, kusjuures $r = 0$ või $N(r) < N(z_2)$. Vaatleme $\frac{z_1}{z_2}$ kui kompleksarvude jagatist. Siis

$$\frac{z_1}{z_2} = \frac{z_1\overline{z_2}}{z_2\overline{z_2}} = \frac{z_1\overline{z_2}}{N(z_2)}, \tag{1}$$

kus $z_1\overline{z_2} \in \mathbb{Z}[\omega]$ ja $N(z_2)$ on naturaalarv. Järelikult saame selle jagatise kirjutada kujul $x + y\omega$, kus $x, y \in \mathbb{Q}$. Kui x ja y peaksid olema täisarvud, siis $q = \frac{z_1}{z_2}$ ja $r = 0$. Vastasel juhul leiame täisarvud m, n selliselt, et $|x - m| \leq \frac{1}{2}$ ja $|y - n| \leq \frac{1}{2}$. See on alati võimalik, kuna iga ratsionaalarv on ülimalt kaugusel $\frac{1}{2}$ talle lähimast täisarvust. Valime $q := m + n\omega \in \mathbb{Z}[\omega]$. Siis

$$\begin{aligned} N\left(\frac{z_1}{z_2} - q\right) &= N((x - m) + (y - n)\omega) \\ &= (x - m)^2 - (x - m)(y - n) + (y - n)^2 \\ &\leq \frac{1}{4} + \frac{1}{4} + \frac{1}{4} < 1. \end{aligned}$$

(NB! Arv $\frac{z_1}{z_2} - q$ ei ole $\mathbb{Z}[\omega]$ element, tegemist on tavalise kompleksarvuga.) Valime $r = z_1 - qz_2$. Siis $r \in \mathbb{Z}[\omega]$ ja $N(r) = N(z_1 - qz_2) = N(z_2) \cdot N(\frac{z_1}{z_2} - q) < N(z_2)$ ning väide on tõestatud. ■

Iga Eukleidese ring on faktoriaalne (teoreem 1.17), seega oleme soovitud tulemuse tõestanud. Kui $z \in \mathbb{Z}[\omega]$ ja $z = p_1^{k_1} \dots p_n^{k_n}$ on tema lahutus taandumatuteks elementideks, siis neid taandumatuid elemente hakkame edaspidi kutsuma arvu z **algteguriteks**.

2.3 Ringi $\mathbb{Z}[\omega]$ pööratavad elemendid

Selles paragrahvis kirjeldame ära ringi $\mathbb{Z}[\omega]$ pööratavad elemendid.

Lause 2.3. *Element $z \in \mathbb{Z}[\omega]$ element on pööratav parajasti siis, kui $N(z) = 1$.*

Tõestus. Olgu $z \in \mathbb{Z}[\omega]$.

Tarvilikkus. Kui z on pööratav, siis leidub selline $z' \in \mathbb{Z}[\omega]$, et $zz' = 1$. Teame, et $N(z) \cdot N(z') = N(zz') = 1$. Kuna $\mathbb{Z}[\omega]$ elementide normid on mittenegatiivsed täisarvud, siis peab kehtima, et $N(z) = 1$.

Piisavus. Kui $N(z) = 1$, siis $z\overline{z} = 1$ ehk $z^{-1} = \overline{z} \in \mathbb{Z}[\omega]$. ■

Leiame nüüd ringi $\mathbb{Z}[\omega]$ kõik pööratavad elemendid. Teame, et kui $a + b\omega \in \mathbb{Z}[\omega]$ on pööratav, siis

$$\begin{aligned} a^2 - ab + b^2 &= 1, \\ 4a^2 - 4ab + 4b^2 &= 4, \\ \left(4a^2 - 4ab + b^2\right) + 3b^2 &= 4, \\ (2a - b)^2 + 3b^2 &= 4. \end{aligned} \tag{2}$$

Kuna täisarvude ruudud on alati mittenegatiivsed, siis ainsad võimalikud b^2 väärtused on 0 ja 1. Seega on kaks võimalust: kas $b^2 = 0$, $(2a - b)^2 = 4$ või $b^2 = 1, (2a - b)^2 = 1$.

- Kui $b^2 = 0$, siis $b = 0$ ja $a = \pm 1$. See annab meile lahenditeks 1 ja -1.
- Kui $b^2 = 1$, siis on kaks võimalust:
  - Kui $b = 1$, siis kas $a = 0$ või $a = 1$ ning lahenditeks on vastavalt ω ja $1 + \omega = -\omega^2$.
  - Kui $b = -1$, siis kas $a = 0$ või $a = -1$, millest saame lahendid $-\omega$ ja $-1 - \omega = \omega^2$.

Seega ringi $\mathbb{Z}[\omega]$ pööratavate elementide hulk on $\{1, \omega, \omega^2, -1, -\omega, -\omega^2\}$, kusjuures $\omega^{-1} = \omega^2, (-\omega)^{-1} = -\omega^2$ ja $(-1)^{-1} = -1$. Antud hulga elemendid on täpselt

kuuenda astme ühejuured, mis asuvad komplekstasandil ühikringjoonel korrapärase kuusnurga tippudes.

2.4 Ringi $\mathbb{Z}[\omega]$ taandumatud elemendid

Eelmises paragrahvis näitasime, et ring $\mathbb{Z}[\omega]$ on faktoriaalne, ehk iga ringi $\mathbb{Z}[\omega]$ nullist erinev mittepööratav element on üheselt esitatav taandumatute elementide korrutisena. Järelikult taandumatute elementide uurimine võimaldab meile nende kaudu kõikide $\mathbb{Z}[\omega]$ elementide kohta järeldusi teha.

Lemma 2.4. *Olgu n täisarv ja $a+b\omega \in \mathbb{Z}[\omega]$. Ringis $\mathbb{Z}[\omega]$ kehtib $n|a+b\omega$ parajasti siis, kui ringis $\mathbb{Z}$ kehtivad $n|a$ ja $n|b$.*

Tõestus. Tõepoolest,

$$\begin{aligned} n|a+b\omega &\Leftrightarrow \exists x+y\omega \in \mathbb{Z}[\omega] : n(x+y\omega) = a+b\omega \\ &\Leftrightarrow \exists x, y \in \mathbb{Z} : nx = a, ny = b \\ &\Leftrightarrow n|a \wedge n|b. \end{aligned}$$

Seega on väide tõestatud. ■

Edaspidi kutsume ringi $\mathbb{Z}[\omega]$ taandumatuid elemente **Eisensteini algarvudeks**, ehk lühidalt **E-algarvudeks**, ning hakkame nende omadusi uurima. Tõestame esiteks Eukleidese lemma analoogi ringis $\mathbb{Z}[\omega]$.

Lemma 2.5. *Kui p on E-algarv ja $p|ab$, kus $a, b \in \mathbb{Z}[\omega]$, siis $p|a$ või $p|b$.*

Tõestus. Kehtigu $p|ab$, kus $a = p_1^k \dots p_n^{k_n}$, $b = p_{n+1}^{k_{n+1}} \dots p_m^{k_m}$ on a ja b lahutused algteguriteks. Siis leidub selline $t \in \mathbb{Z}[\omega]$, et $pt = ab = p_1^k \dots p_m^{k_m}$. (NB! Kui $i \neq j$, siis ei pruugi kehtida, et $p_i \neq p_j$, kuna mõned a ja b algteguritest võivad ühtida.) Kuna algteguriteks lahutus on ühene assotsieerituse täpsuseni, siis peab leiduma selline ab algtegur p_i, $i \in \{1, \dots, m\}$, et $p \sim p_i$. Kui $1 \leq i \leq n$, siis p_i on elemendi

a algtegur ehk $p|a$. Kui $n+1 \leq i \leq m$, siis p on elemendi b algtegur ja kehtib $p|b$.
■

Järeldus 2.6. *Olgu p E-algarv ja $a_1, \ldots, a_n \in \mathbb{Z}[\omega]$. Kui $p|a_1 \ldots a_n$, siis leidub selline $i \in \{1, \ldots, n\}$, et $p|a_i$.*

Tõestus. Tõestame väite induktsiooniga n järgi. Kui $n = 1$, siis on väide ilmne. Kui $n = 2$, siis väide kehtib eelneva lemma tõttu. Kui $n > 2$ ja väide kehtib iga $n-1$ tegurist moodustatud korrutise puhul, siis $p|a_1$ või $p|a_2 \ldots a_n$ samuti eelneva lemma pärast. Kui $p|a_1$, siis oleme jõudnud sobiva tegurini. Kui $p|a_2 \ldots a_n$, siis induktsiooni eelduse tõttu leidub selline $i \in \{2, \ldots, n\}$, et $p|a_i$. ■

Teoreem 2.7. *Kui p on E-algarv, siis leidub selline algarv q, et $N(p) = q$ või $N(p) = q^2$. Seejuures kui $N(p) = q$, siis p ei ole ühegi algarvuga assotsieeritud, ja kui $N(p) = q^2$, siis p on assotsieeritud algarvuga q.*

Tõestus. Eeldame, et p on E-algarv. Olgu $N(p) = n$. Kuna p ei ole pööratav ega võrdu nulliga, siis $n > 1$, seega tal leidub ühene algarvude korrutise esitus $n = q_1^{k_1} \ldots q_n^{k_n}$. Kuna $N(p) = p\overline{p} = n$, siis $p|n = q_1^{k_1} \ldots q_n^{k_n}$ ringis $\mathbb{Z}[\omega]$. Järelduse 2.6 tõttu leidub selline $i \in \{1, \ldots, n\}$, et $p|q_i$ ringis $\mathbb{Z}[\omega]$, ehk $ps = q_i$ mingi $s \in \mathbb{Z}[\omega]$ korral. Nüüd

$$N(p)N(s) = N(ps) = N(q_i) = q_i^2.$$

Kuna $N(p) > 1$, siis on kaks võimalust: kas $N(p) = N(s) = q_i$ või $N(p) = q_i^2$ ja $N(s) = 1$.

Viimasel juhul s on pööratav, millest saame, et p ja q_i on assotsieeritud, seega võime võtta $q = q_i$. Esimesel juhul, s.t. kui $N(p) = N(s) = q_i$, oletame vastuväiteliselt, et p on assotsieeritud mingi algarvuga q'. Siis leidub pööratav element $u \in \mathbb{Z}[\omega]$ selliselt, et $p = uq'$ ja

$$q_i = N(p) = N(uq') = N(u) \cdot N(q') = 1 \cdot (q')^2,$$

mis on võimatu, kuna q_i on algarv. Järelikult p ei ole assotsieeritud ühegi algarvuga.
■

See tähendab, et iga E-algarv on normi kaudu seotud mingi algarvuga. Tuleb välja, et kehtib ka vastupidine väide.

Lause 2.8. *Olgu $z \in \mathbb{Z}[\omega]$. Kui $N(z)$ on algarv, siis z on E-algarv.*

Tõestus. Paneme tähele, et $N(z) > 0$, seega $z \neq 0$. Oletame vastuväiteliselt, et z ei ole E-algarv. Siis leiduvad mittepööratavad elemendid $z_1, z_2 \in \mathbb{Z}[\omega]$ selliselt, et $z = z_1 z_2$, kusjuures $N(z_1), N(z_2) > 1$. Siis $N(z) = N(z_1 z_2) = N(z_1) \cdot N(z_2)$, ehk $N(z)$ on kahe mittepööratava täisarvu $N(z_1), N(z_2)$ korrutis. See on vastuolu, seega z peab olema E-algarv. ■

Teoreem 2.9. *Olgu $q \in \mathbb{Z}$ algarv. Kui $q \equiv 2 \pmod 3$, siis q on E-algarv. Kui $q \equiv 1 \pmod 3$, siis q on mingi E-algarvu norm. Kui $q \equiv 0 \pmod 3$, siis $q = 3 = -\omega^2(1-\omega)^2$, kus $1-\omega$ on E-algarv.*

Tõestus. Oletame, et q ei ole E-algarv. Siis leiduvad mittepööratavad $\mathbb{Z}[\omega]$ elemendid q_1, q_2 selliselt, et $q = q_1 q_2$. Siis ka $q^2 = N(q) = N(q_1 q_2) = N(q_1) \cdot N(q_2)$, ja kuna $N(q_1), N(q_2) > 1$ ning q on algarv, siis sellest järeldub, et $q = N(q_1)$. Olgu $q_1 = a + b\omega$. Siis saame, et $q = N(q_1) = a^2 - ab + b^2$. Analoogiliselt teisendustega (2) järeldub siit, et $4q = (2a-b)^2 + 3b^2$. Arvutades nüüd mooduli 3 järgi saame, et $q \equiv (2a-b)^2 \pmod 3$. Kuna ainsad ruudud ringis $\mathbb{Z}_3$ on 0 ja 1, siis $q \neq 3$ korral kehtib, et $q \equiv 1 \pmod 3$. Sellest omakorda järeldub, et kui $q \neq 3$ ja $q \not\equiv 1 \pmod 3$, siis q peab olema E-algarv. Sellega on esimene väide tõestatud.
Olgu nüüd $q \equiv 1 \pmod 3$. Näitame, et q on E-algarvu norm. Kasutame Legendre'i sümbolit ja selle omadusi:

$$\begin{aligned}\left(\frac{-3}{q}\right) &= \left(\frac{-1}{q}\right)\cdot\left(\frac{3}{q}\right) = (-1)^{\frac{q-1}{2}}\cdot(-1)^{\frac{(q-1)(3-1)}{2\cdot 2}}\left(\frac{q}{3}\right) && \text{(teoreem 1.31)}\\ &= (-1)^{(q-1)\cdot 1}\cdot\left(\frac{q}{3}\right) = \left(\frac{q}{3}\right) = \left(\frac{1}{3}\right) = 1. && (q \equiv 1 \pmod 3)\end{aligned}$$

See tähendab, et -3 on korpuse $\mathbb{Z}_q$ ruutjääk ehk leidub selline $a \in \mathbb{Z}_q$, et $a^2 \equiv -3 \pmod{q}$, mida võime ka väljendada kui $a^2 + 3 \equiv 0 \pmod{q}$. Nüüd teame, et mingi $b \in \mathbb{Z}$ korral kehtib

$$qb = a^2 + 3 = (a + \sqrt{3}i)(a - \sqrt{3}i) = (a + 1 + 2\omega)(a - 1 - 2\omega).$$

Kui nüüd q oleks E-algarv, siis lemma 2.5 tõttu ta peaks jagama vähemalt ühte antud teguritest. Lemmast 2.4 saame, et kui $q|a+1+2\omega$, siis $q|a+1$ ja $q|2$, kuid $q > 2$ tõttu see ei saa kehtida. Analoogiliselt saame, et q ei jaga arvu $a-1-2\omega$. Seega q on taanduv element ringis $\mathbb{Z}[\omega]$ ning teda saab esitada mittepööratavate elementide $q_1, q_2 \in \mathbb{Z}[\omega]$ korrutisena. Siis kehtib, nagu teoreemi 2.7 tõestuses näidatud, et $q = N(q_1)$. Lause 2.8 tõttu q_1 on E-algarv. Sellega on teine väide tõestatud.

Kui $q \equiv 0 \pmod{3}$, siis

$$\begin{aligned} q = 3 &= 3 + 3\omega - 3\omega = -3\omega - 3(-1 - \omega) \\ &= -3\omega - 3\omega^2 = -3\omega(1 + \omega) \\ &= (1 + \omega)(1 - 2\omega - 1 - \omega) \\ &= -\omega^2(1 - 2\omega + \omega^2) = -\omega^2(1 - \omega)^2, \end{aligned}$$

kus $-\omega^2$ on pööratav. Kuna $N(1 - \omega) = 1^2 - 1 \cdot (-1) + (-1)^2 = 3$, siis lause 2.8 tõttu teame, et $1 - \omega$ on E-algarv. ■

3 Ringi $\mathbb{Z}[\omega]$ jäägiklassiringid

Nii nagu võime jaotada täisarvud jäägiklassidesse suvalise naturaalarvu järgi, võime ringis $\mathbb{Z}[\omega]$ analoogiliselt tegutseda. Meenutame, et täisarvude a, b, n korral kirjutame $a \equiv b \pmod{n}$, kui $n|b-a$, ning sel juhul ütleme, et a ja b on kongruentsed mooduli n järgi. Algebra I konspektist [4] teame, et kongruentsi ekvivalentsiklassid on ringi $\mathbb{Z}_n$ elementideks. Teame arvuteooria konspektist [3], et $\mathbb{Z}_n$ on korpus parajasti siis, kui n on algarv. Sarnane tulemus kehtib ka E-algarvude puhul.

Olgu $p \in \mathbb{Z}[\omega]$. Moodustame peaideaali $p\mathbb{Z}[\omega] := \{pz | z \in \mathbb{Z}[\omega]\}$ ning vaatleme ringi $\mathbb{Z}[\omega]$ faktorringi $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$. Selle elementideks on peaideaali $p\mathbb{Z}[\omega]$ kõrvalklassid kujul $r + p\mathbb{Z}[\omega] = \{r + pz | z \in \mathbb{Z}[\omega]\}$, $r \in \mathbb{Z}[\omega]$. Teame, et kõrvalklasside $r + p\mathbb{Z}[\omega]$, $s + p\mathbb{Z}[\omega]$ liitmine ja korrutamine on defineeritud järgmiselt:

$$(r + p\mathbb{Z}[\omega]) + (s + p\mathbb{Z}[\omega]) := (r + s) + p\mathbb{Z}[\omega],$$
$$(r + p\mathbb{Z}[\omega])(s + p\mathbb{Z}[\omega]) := rs + p\mathbb{Z}[\omega].$$

Definitsioon 3.1. Olgu $a, p \in \mathbb{Z}[\omega]$. Elemendi a **jäägiklassiks** mooduli p järgi nimetame kõrvalklassi $[a] := a + p\mathbb{Z}[\omega]$.

Definitsioon 3.2. Jäägiklassidest $\{[a] | a \in \mathbb{Z}[\omega]\}$ moodustatud faktorringi nimetame **jäägiklassiringiks** mooduli $p \in \mathbb{Z}[\omega]$ järgi.

Paneme tähele, et faktorringi $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ nullelemendiks on kõrvalklass $[0] = 0 + p\mathbb{Z}[\omega] = p\mathbb{Z}[\omega]$. Kuna peaideaali järgi moodustatud faktorring on ring, siis jäägiklassiringid on korrektselt defineeritud. Näitame nüüd, et kui p on E-algarv, siis faktorring $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ on korpus. Meenutame, et $r + p\mathbb{Z}[\omega] = s + p\mathbb{Z}[\omega]$ parajasti siis, kui $r - s \in p\mathbb{Z}[\omega]$ ehk $p|r - s$ ringis $\mathbb{Z}[\omega]$. Sarnaselt täisarvude juhuga kirjutame $x, y, p \in \mathbb{Z}[\omega]$ korral $x \equiv y \pmod{p}$ (ja ütleme, et x ja y on **kongruentsed** mooduli p järgi), kui $p|y - x$ ringis $\mathbb{Z}[\omega]$. Seda arvestades võime öelda, et kehtib järgmine tulemus.

Lemma 3.3. *Olgu $a, b, p \in \mathbb{Z}[\omega]$. Kongruents $a \equiv b \pmod{p}$ kehtib parajasti siis, kui $[a] = [b]$ ringis $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$.*

Nüüd võime tõestada järgmise teoreemi.

Teoreem 3.4. *Kui p on E-algarv, siis ring $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ on lõplik korpus, milles on $N(p)$ elementi.*

Tõestus. Näitame, et $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ on korpus. Olgu $z \in \mathbb{Z}[\omega], z \not\equiv 0 \pmod{p}$. Kuna ainsad E-algarvu jagajad on temaga assotsieeritud E-algarvud ja pööratavad elemendid ning me teame, et $(z, p) \neq p$, siis peab kehtima $(z, p) = 1$. Lause 1.18 tõttu leiduvad sellised $u, v \in \mathbb{Z}[\omega]$, et

$$uz + vp = 1,$$

ehk mingi $u \in \mathbb{Z}[\omega]$ korral $uz \equiv 1 \pmod{p}$. Lemma 3.3 põhjal

$$[u][z] = [uz] = [1]$$

ja $[z]$ on pööratav. Kuna ainsaks eelduseks oli, et $[z] \neq [0]$, siis ring $\mathbb{Z}[\omega]/p\mathbb{Z}[\omega]$ on korpus. Edaspidi kasutame tähist

$$\mathbb{K}_p := \mathbb{Z}[\omega]/p\mathbb{Z}[\omega].$$

Näitame, et korpuses $\mathbb{K}_p$ on $N(p)$ elementi. Teame, et iga E-algarvu $p \neq 1 - \omega$ puhul kehtib, et kui p on mingi algarvuga assotsieeritud, siis $p \equiv 2 \pmod{3}$, ja kui p ei ole ühegi algarvuga assotsieeritud, siis $N(p) \equiv 1 \pmod{3}$. Vaatleme eraldi kolme juhtu.

Oletame, et $p \neq 1 - \omega$ on algarvuga p' assotsieeritud. Kui ringi elemendid on assotsieeritud, siis nad moodustavad sama peaideaali, seega $\mathbb{K}_p = \mathbb{K}_{p'}$. Seetõttu

võime üldisust kitsendamata eeldada, et p on algarv. Näitame, et hulk

$$A := \{a + b\omega | a, b \in \mathbb{Z}, 0 \leq a < p, 0 \leq b < p\}$$

on selline, et igal $\mathbb{K}_p$ jäägiklassil on hulgas A täpselt üks esindaja. Sel juhul väide on tõestatud, sest $|\mathbb{K}_p| = |A| = p \cdot p = N(p)$.
Olgu $z = m + n\omega \in \mathbb{Z}[\omega]$. Jagame m ja n jäägiga algarvuga p:

$$m = ps + a,$$
$$n = pt + b,$$

kus $s, a, t, b \in \mathbb{Z}$ ning $0 \leq a, b < p$. Ilmselt $z = m + n\omega \equiv a + b\omega \pmod{p}$. Seega iga $\mathbb{Z}[\omega]$ elemendi z jäägiklassile leidub hulgas A esindaja. Näitame nüüd ühesust. Oletame, et

$$a + b\omega \equiv a' + b'\omega \pmod{p},$$

kus $a + b\omega, a' + b'\omega \in A$. Sel juhul

$$p|(a - a') + (b - b')\omega,$$

ehk $p|a - a'$ ja $p|b - b'$ (lause 2.4). Kuna aga $0 \leq a, a', b, b' < p$, siis ainus võimalik olukord on see, et $a - a' = 0 = b - b'$, ehk peab kehtima võrdus

$$a + b\omega = a' + b'\omega.$$

Seega on esindaja ühesus samuti tõestatud.

Vaatleme nüüd juhtu, kus E-algarv $p \neq 1 - \omega$ ei ole täisarv. Sel juhul tema norm $N(p) = p\overline{p} =: q$ on algarv, kusjuures $q \equiv 1 \pmod{3}$. Sarnaselt eelmisele arutelule näitame, et hulka

$$B := \{0, \ldots, q - 1\} \in \mathbb{Z}$$

kuulub iga $\mathbb{K}_p$ jäägiklassi täpselt üks esindaja. Olgu $p = a + b\omega$. Siis kehtib $q \nmid b$. Tõepoolest, kui oletame vastuväiteliselt, et $q|b$, siis võrduse $q = a^2 - ab + b^2$ tõttu peaks ka kehtima $q|a^2 - ab = a(a - b)$, millest järelduks, et $q|a$. See aga omakorda tähendaks, et $q|a + b\omega = p$, ehk

$$q^2 = N(q)|N(p) = q,$$

mis on vastuolu. Seega $b \not\equiv 0 \pmod{q}$, mis tähendab, et $[b]$ on korpuses $\mathbb{Z}_q$ pööratav: leidub täisarv b^{-1} selliselt, et $bb^{-1} \equiv 1 \pmod{q}$. Olgu $z = m+n\omega \in \mathbb{Z}[\omega]$ suvaline. Defineerime $c := b^{-1}n \in \mathbb{Z}$, nii et kehtib $bc \equiv n \pmod{q}$. Kuna $p\overline{p} = q|n - bc$ ringis $\mathbb{Z}[\omega]$, siis ka $p|n - bc$. Järelikult

$$z = m + n\omega \equiv m + bc\omega = m + c(p - a) \equiv m - ca \pmod{p}$$

ringis $\mathbb{Z}[\omega]$. See aga tähendab, et iga $\mathbb{Z}[\omega]$ element z on kongruentne mingi täisarvuga $x := m - ca$ mooduli p järgi. Jagame täisarvu x jäägiga algarvuga q:

$$x = ql + y,$$

kus $y \in \mathbb{Z}$ ning $0 \leq y < q$. Siis $y \in B$ ja me valime täisarvu y elemendi x jäägiklassi esindajaks. Tõepoolest, kuna $q|x - y$, siis $[z] = [x] = [y]$. Järelikult suvalisel $\mathbb{Z}[\omega]$ elemendi jäägiklassil $[z]$ leidub esindaja hulgas B.
Näitame nüüd ühesust. Olgu $r, r' \in B$ ja kehtigu $r \equiv r' \pmod{p}$. Siis leidub $t \in \mathbb{Z}[\omega]$ selliselt, et $r - r' = pt$. Järelikult

$$(r - r')^2 = N(r - r') = N(pt) = q \cdot N(t).$$

See aga tähendab, et $q|r - r'$ ringis $\mathbb{Z}$ (lemma 1.23). Kuna $0 \leq r, r' < q$, siis $r - r' = 0$ ehk $r = r'$. Järelikult leidub igale korpuse $\mathbb{K}_p$ elemendile täpselt üks esindaja hulgas B ja seega $|\mathbb{K}_p| = |B| = q$.

Vaatleme nüüd juhtu $p = 1 - \omega$. Kongruentsi

$$1 - \omega \equiv 0 \pmod{1 - \omega}$$

tõttu kehtib korpuses $\mathbb{K}_{1-\omega}$ võrdus $[1] = [\omega]$. Seega suvalise $a + b\omega \in \mathbb{Z}[\omega]$ korral

$$a + b\omega \equiv a + b \pmod{1 - \omega}$$

ehk iga $\mathbb{Z}[\omega]$ element on mooduli $1 - \omega$ järgi kongruentne mingi täisarvuga.
Kuna $(1 - \omega)(1 - \overline{\omega}) = 3$, siis $1 - \omega | 3$ ringis $\mathbb{Z}[\omega]$, ehk kui $x \equiv y \pmod 3$ ringis $\mathbb{Z}[\omega]$, siis ka $x \equiv y \pmod{1 - \omega}$ ringis $\mathbb{Z}[\omega]$. See tähendab, et korpuse $\mathbb{K}_{1-\omega}$ iga element $[a + b\omega]$ on võrdne ühega elementidest $[0], [1], [2] \in \mathbb{K}_{1-\omega}$. Näitame, et antud jäägiklassid on korpuses $\mathbb{K}_{1-\omega}$ paarikaupa erinevad. Kasutame vastuväitelist tõestust:

- Kui $1 \equiv 0 \pmod{1 - \omega}$, siis $1 - \omega | 1 - 0$ ehk $(1 - \omega)k = 1$ mingi $k \in \mathbb{Z}[\omega]$ korral. See on vastuolu, kuna $N(1 - \omega) = 3$, ehk $1 - \omega$ ei ole pööratav.
- Kui $1 \equiv 2 \pmod{1 - \omega}$, siis $1 - \omega | 2 - 1$ ning vastuolu tekib analoogiliselt.
- Kui $0 \equiv 2 \pmod{1 - \omega}$, siis $1 - \omega | 2$ ja $N(1 - \omega) \cdot N(k) = N(2)$ mingi $k \in \mathbb{Z}[\omega]$ korral. Siis aga peaks kehtima $N(k) = \frac{4}{3}$, mis on jällegi vastuolu.

Järelikult arvude $0, 1$ ja 2 ekvivalentsiklassid on kõik paarikaupa erinevad ning korpuses $\mathbb{K}_{1-\omega}$ on täpselt $N(1 - \omega) = 3$ elementi. Seega teoreem on tõestatud. ■

Seega teame nüüd, et ringi $\mathbb{Z}[\omega]$ kongruentse E-algarvulise mooduli järgi võime, analoogiliselt täisarvude ringiga, uurida vastava korpuse abil. Lisaks nägime, et korpuse $\mathbb{K}_p$ elementide arv on kas algarv või algarvu ruut.

4 Kuupjäägi sümbol

Olgu p E-algarv ja $a \in \mathbb{Z}[\omega]$. Meie eesmärk on defineerida funktsioon $\left(\frac{a}{p}\right)_3$ selliselt, et $\left(\frac{a}{p}\right)_3 = 1$ parajasti siis, kui kongruents $x^3 \equiv a \pmod{p}$ on lahenduv. Sellisel juhul nimetame arvu a **kuupjäägiks** mooduli p järgi. Eelmises peatükis näitasime, et iga E-algarvu p puhul korpus $\mathbb{K}_p$ sisaldab $N(p)$ elementi. See aga tähendab, et $\mathbb{K}_p$ multiplikatiivse rühma $\mathbb{K}_p^*$ järk on $N(p) - 1$. Lagrange'i teoreemi abil saame järgmise tulemuse.

Teoreem 4.1. *Olgu $a \in \mathbb{Z}[\omega]$ ja olgu p E-algarv. Kui $p \nmid a$ ringis $\mathbb{Z}[\omega]$, siis $a^{N(p)-1} \equiv 1 \pmod{p}$.*

Märkus 4.2. Olgu p E-algarv. Näitame, et kui $N(p) \neq 3$ (ehk $p \nsim 1 - \omega$), siis $1, \omega, \omega^2$ jäägiklassid on kõik erinevad korpuses $\mathbb{K}_p$. Tõepoolest, olgu $N(p) \neq 3$.

- Kui $\omega \equiv 1 \pmod{p}$, siis $p|1 - \omega$. Kuna aga $1 - \omega$ on E-algarv, siis antud omadus tähendab, et p ja $1 - \omega$ peavad olema assotsieeritud, ehk $pu = 1 - \omega$ mingi pööratava elemendi $u \in \mathbb{Z}[\omega]$ korral. Eelnevalt näitasime, et sel juhul $N(u) = 1$, seega $N(p) = N(pu) = N(1 - \omega) = 3$, vastuolu.
- Kui $\omega \equiv \omega^2 \pmod{p}$, siis $p|\omega - \omega^2 = \omega(1 - \omega)$ ehk $p \sim 1 - \omega$, vastuolu.
- Kui $1 \equiv \omega^2 \pmod{p}$, siis $p|1 - \omega^2 = (1 + \omega)(1 - \omega) = -\omega^2(1 - \omega)$ ehk jällegi $p \sim 1 - \omega$, vastuolu.

Seega, elementidest $[1], [\omega], [\omega^2]$ koosnev multiplikatiivne rühm on suvalise $\mathbb{K}_p^*$, kus $N(p) \neq 3$, alamrühm, mille järk on kolm. Lagrange'i teoreemi tõttu kehtib järgmine tulemus.

Järeldus 4.3. *Olgu p E-algarv ja $N(p) \neq 3$. Siis multiplikatiivse rühma $\mathbb{K}_p^*$ järk jagub kolmega.*

See tulemus tähendab, et E-algarvu p puhul, mille norm ei võrdu kolmega, on suvalise $[a] \in \mathbb{K}_p$ korral $\frac{N(p)-1}{3}$ naturaalarv ja avaldis $a^{\frac{N(p)-1}{3}}$ on ringis $\mathbb{Z}[\omega]$ defineeritud.

Järgnevas tõestame, et kui $a \in \mathbb{Z}[\omega]$ ei ole p kordne, siis element $a^{\frac{N(p)-3}{3}}$ on alati kongruentne täpselt ühe kolmanda astme ühejuurega ringis $\mathbb{Z}[\omega]$.

Lause 4.4. *Olgu E-algarv p selline, et $N(p) \neq 3$, ning kehtigu $p \nmid a$, kus $a \in \mathbb{Z}[\omega]$. Siis leidub üheselt määratud täisarv $m \in \{0,1,2\}$ nii, et $a^{\frac{N(p)-1}{3}} \equiv \omega^m \pmod{p}$ ringis $\mathbb{Z}[\omega]$.*

Tõestus. Teoreemi 4.1 tõttu teame, et $a^{N(p)-1} \equiv 1 \pmod{p}$ ehk $p \mid a^{N(p)-1} - 1$ ringis $\mathbb{Z}[\omega]$. Kuna $1, \omega, \omega^2$ on polünoomi $X^3 - 1 \in \mathbb{C}[X]$ juured, siis $X^3 - 1 = (X-1)(X-\omega)(X-\omega^2)$. Järelikult

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

Eelnevalt näitasime, et $a^{\frac{N(p)-1}{3}} \in \mathbb{Z}[\omega]$, seega kõik kasutatud suurused on $\mathbb{Z}[\omega]$ elemendid ning võrdus kehtib ka ringis $\mathbb{Z}[\omega]$.

Kuna p on E-algarv, siis järelduse 2.6 tõttu ta peab jagama vähemalt ühte paarempoolsetest teguritest. Kui me oletame vastuväiteliselt, et p jagab kahte neist teguritest, siis ta jagaks ka tegurite vahet, millest märkuse 4.2 tõttu järelduks, et $N(p) = 3$, vastuolu. Seega p jagab neist täpselt ühte; olgu see tegur $a^{\frac{N(p)-1}{3}} - \omega^m$, kus $m \in \{0,1,2\}$. Siis

$$p \mid a^{\frac{N(p)-1}{3}} - \omega^m$$

ehk $a^{\frac{N(p)-1}{3}} \equiv \omega^m \pmod{p}$. ∎

Nüüd, kus me oleme veendunud, et selline ω aste alati leidub, saame defineerida kuupjäägi sümboli.

Definitsioon 4.5. Olgu p E-algarv ning $N(p) \neq 3$. Olgu $a \in \mathbb{Z}[\omega]$. **Kuupjäägi sümbol** $\left(\frac{a}{p}\right)_3$ on defineeritud järgmiselt:

$$\left(\frac{a}{p}\right)_3 = \begin{cases} 0, & \text{kui } p \mid a, \\ \omega^m, \text{ kus } \omega^m \equiv a^{\frac{N(p)-1}{3}} \pmod{p}, & \text{kui } p \nmid a, \end{cases}$$

kus $m \in \{0, 1, 2\}$.

Seega $\left(\frac{a}{p}\right)_3 \in \{0, 1, \omega, \omega^2\}$. Näitame, et kuupjäägi sümbol täidab sama rolli kuupjääkide tuvastamises kui Legendre'i sümbol ruutjääkide puhul.

Teoreem 4.6. *Olgu p E-algarv, $N(p) \neq 3$ ja olgu $a \in \mathbb{Z}[\omega]$ selline, et $p \nmid a$. Võrdus $\left(\frac{a}{p}\right)_3 = 1$ kehtib parajasti siis, kui kongruents $x^3 \equiv a \pmod{p}$ on lahenduv ringis $\mathbb{Z}[\omega]$.*

Tõestus. Kuna iga lõpliku korpuse multiplikatiivne rühm on tsükliline (teoreem 1.20), siis leidub selline $g \in \mathbb{Z}[\omega]$, et $[g]$ on multiplikatiivse rühma $\mathbb{K}_p^*$ moodustaja. See tähendab, et leidub $u \in \mathbb{N}_0$ selliselt, et $a \equiv g^u \pmod{p}$.
Piisavus. Oletame, et leidub selline $x_0 \in \mathbb{Z}[\omega]$, et $x_0^3 \equiv a \pmod{p}$. Siis leidub $v \in \mathbb{N}_0$ nii, et $x_0 \equiv g^v \pmod{p}$. Seega kongruents $x_0^3 \equiv a \pmod{p}$ tähendab, et

$$\begin{aligned} g^{3v} &\equiv g^u, && \pmod{p} \\ 3v &\equiv u && \pmod{N(p)-1}, \end{aligned}$$

kus teine kongruents on esimesega samaväärne lause 1.26 tõttu. Teoreemist 2.9 saame, et kui $N(p) \neq 3$, siis $N(p) \equiv 1 \pmod{3}$. Järelikult $(3, N(p)-1) = 3$. Teame (lause 1.25), et lineaarkongruents $3v \equiv u \pmod{N(p)-1}$ on lahenduv parajasti siis, kui $(3, N(p)-1) | u$ ehk $u = 3k$ mingi $k \in \mathbb{N}$ korral. Seega peab kehtima

$$a^{\frac{N(p)-1}{3}} \equiv g^{3k\frac{(N(p)-1)}{3}} = (g^k)^{N(p)-1} \equiv 1 \pmod{p}.$$

Tarvilikkus. Kehtigu $\left(\frac{a}{p}\right)_3 = 1$. Kui $[g]$ on $\mathbb{K}_p^*$ moodustaja, siis tema järk on $N(p)-1$, ehk $N(p)-1 =: n$ peab olema vähim naturaalarv, mille korral $g^n \equiv 1 \pmod{p}$. Nüüd

$$1 \equiv a^{\frac{N(p)-1}{3}} \equiv (g^u)^{\frac{N(p)-1}{3}} = g^{u\cdot\frac{(N(p)-1)}{3}} \pmod{p}.$$

Kuna $g^{u\cdot\frac{N(p)-1}{3}} \equiv 1 \pmod{p}$ ja moodustaja g järk on $N(p)-1$, siis $u\cdot\frac{(N(p)-1)}{3}$ peab olema $N(p)-1$ kordne. Seega $\frac{u}{3}$ peab olema täisarv ehk u peab jaguma kolmega.

Seega $a \equiv g^u = (g^{\frac{u}{3}})^3 \pmod{p}$ ehk a on kuupjääk. ■

Tõestame nüüd mõned kuupjäägi sümboli omadustest.

Lemma 4.7. *Olgu $a, b, p \in \mathbb{Z}[\omega]$. Kui $a \equiv b \pmod{p}$, siis $\overline{a} \equiv \overline{b} \pmod{\overline{p}}$.*

Tõestus. Kui $a \equiv b \pmod{p}$, siis leidub selline $k \in \mathbb{Z}[\omega]$, et $pk = b - a$. Võttes kaaskompleksarvu mõlemalt poolt saame võrduse $\overline{p}\overline{k} = \overline{b} - \overline{a}$, ehk $\overline{a} \equiv \overline{b} \pmod{\overline{p}}$.
■

Teoreem 4.8. *Olgu p E-algarv, $N(p) \neq 3$, ning $a, b \in \mathbb{Z}[\omega]$ suvalised. Siis*

1. $\left(\frac{a}{p}\right)_3 \equiv a^{\frac{N(p)-1}{3}} \pmod{p}$;
2. *kui* $a \equiv b \pmod{p}$, *siis* $\left(\frac{a}{p}\right)_3 = \left(\frac{b}{p}\right)_3$;
3. $\left(\frac{ab}{p}\right)_3 = \left(\frac{a}{p}\right)_3 \left(\frac{b}{p}\right)_3$;
4. $\overline{\left(\frac{a}{p}\right)_3} = \left(\frac{a}{p}\right)_3^2 = \left(\frac{a^2}{p}\right)_3$;
5. $\overline{\left(\frac{a}{p}\right)_3} = \left(\frac{\overline{a}}{\overline{p}}\right)_3$.

Tõestus.

1. See väide järeldub kohe definitsioonist.

2. Kui $a \equiv b \pmod{p}$, siis ka $a^k \equiv b^k \pmod{p}$ suvalise $k \in \mathbb{N}$ korral. Järelikult kehtib

$$\left(\frac{a}{p}\right)_3 \equiv a^{\frac{N(p)-1}{3}} \equiv b^{\frac{N(p)-1}{3}} \equiv \left(\frac{b}{p}\right)_3 \pmod{p},$$

ja kuna $N(p) \neq 3$, siis tänu märkusele 4.2 on $1, \omega$ ja ω^2 kõik erinevate jäägiklasside esindajad. Seega $\left(\frac{a}{p}\right)_3 = \left(\frac{b}{p}\right)_3$.

3. Näeme, et

$$\left(\frac{ab}{p}\right)_3 \equiv (ab)^{\frac{N(p)-1}{3}} = a^{\frac{N(p)-1}{3}} \cdot b^{\frac{N(p)-1}{3}} \equiv \left(\frac{a}{p}\right)_3 \left(\frac{b}{p}\right)_3 \pmod{p}.$$

4. Iga kuupjäägi sümboli väärtuse $x \in \{1, \omega, \omega^2\}$ korral kehtib, et $\overline{x} = x^2$. Lisaks saame, et

$$\left(\frac{a^2}{p}\right)_3 = \left(\frac{a}{p}\right)_3 \left(\frac{a}{p}\right)_3 = \left(\frac{a}{p}\right)_3^2.$$

5. Kuna $a^{\frac{N(p)-1}{3}} \equiv \left(\frac{a}{p}\right)_3 \pmod{p}$, siis lemma 4.7 tõttu $\overline{a}^{\frac{N(p)-1}{3}} \equiv \overline{\left(\frac{a}{p}\right)_3} \pmod{\overline{p}}$. Lisaks $N(p) = p\overline{p} = N(\overline{p})$, seega saame

$$\left(\frac{\overline{a}}{\overline{p}}\right)_3 \equiv \overline{a}^{\frac{N(\overline{p})-1}{3}} = \overline{a}^{\frac{N(p)-1}{3}} \equiv \overline{\left(\frac{a}{p}\right)_3} \pmod{\overline{p}}$$

ehk $\left(\frac{\overline{a}}{\overline{p}}\right)_3 = \overline{\left(\frac{a}{p}\right)_3}$. ■

Tuleb välja, et kui moodul p on täisarv, siis kehtivad veel mõned kasulikud omadused.

Lause 4.9. *Olgu q algarv, $q \equiv 2 \pmod 3$ (ehk q on ka E-algarv) ja $a \in \mathbb{Z}[\omega]$. Siis*

1. $\left(\frac{\overline{a}}{q}\right)_3 = \left(\frac{a^2}{q}\right)_3$;
2. *kui $n \in \mathbb{Z}$ on selline, et $(n, q) = 1$, siis $\left(\frac{n}{q}\right)_3 = 1$.*

Tõestus.

1. Kuna $\overline{q} = q$, siis $\left(\frac{\overline{a}}{q}\right)_3 = \left(\frac{\overline{a}}{\overline{q}}\right)_3 = \overline{\left(\frac{a}{q}\right)_3} = \left(\frac{a^2}{q}\right)_3$, kus teine ja kolmas võrdus järelduvad lausest 4.8.

2. Kuna $\overline{n} = n$, siis $\left(\frac{n}{q}\right)_3 = \overline{\left(\frac{n}{q}\right)_3} = \left(\frac{n}{q}\right)_3^2$, kus esimene võrdus kehtib teoreemi 4.8 viienda punkti tõttu ja teine võrdus järeldub sellest, et iga $x \in \{1, \omega, \omega^2\}$ korral kehtib $\overline{x} = x^2$. Kuna $q \nmid n$, siis $\left(\frac{n}{q}\right)_3 \neq 0$, ja kuna $\left(\frac{n}{q}\right)_3 \equiv n^{\frac{q^2-1}{3}} \pmod q$ on täisarv, siis peab kehtima $\left(\frac{n}{q}\right)_3 = 1$. ■

5 Gaussi ja Jacobi summa

Toome nüüd sisse mõned definitsioonid ja tulemused, mida läheb pärast vaja kuupvastavusseaduse tõestuses.

Definitsioon 5.1 ([2], ptk. 5.1)**.** Olgu p algarv. Kujutust $\chi : \mathbb{F}_p^* \to \mathbb{C}\backslash\{0\}$ nimetame lõpliku korpuse $\mathbb{F}_p$ **karakteriks**, kui iga $a, b \in \mathbb{F}_p^*$ korral

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

Üks selline karakter on defineeritud võrdusega $\varepsilon(a) = 1$ iga $a \in \mathbb{F}_p^*$ korral. Laiendame karakterite määramispiirkonda tervele korpusele, defineerides $\chi(0) = 0$, kui $\chi \neq \varepsilon$, ja $\chi(0) = 1$, kui $\chi = \varepsilon$.

NB! A. Ahvena töös on karakteri asemel kasutatud sõna multiplikatiivne karakteristik.

Definitsioon 5.2. Korpuse $\mathbb{F}_p$ karakterit ε nimetame **triviaalseks**, kui iga $a \in \mathbb{F}_p^*$ korral kehtib $\varepsilon(a) = 1$.

Lemma 5.3 ([2], lause 5.3)**.** *Korpuse $\mathbb{F}_p$ karakterid moodustavad rühma punktiviisi korrutamise*

$$(\chi_1 \cdot \chi_2)(x) := \chi_1(x) \cdot \chi_2(x),$$

$x \in \mathbb{F}_p^*$, suhtes.

Definitsioon 5.4. Karakteri χ **järguks** nimetame tema kui karakterite rühma elemendi järku.

Definitsioon 5.5 ([2], definitsioon 5.4)**.** Kui χ on korpuse $\mathbb{K}_p$ karakter, kus $a \in \mathbb{K}_p$ ning $\zeta = e^{\frac{2\pi i}{p}} \in \mathbb{C}$ on p. astme algjuur, siis kompleksarvu

$$g_a(\chi) := \sum_{[t] \in \mathbb{K}_p} \chi([t])\zeta^{at}$$

nimetame karakteri χ **Gaussi summaks** elemendi a järgi. Edaspidi kirjutame Gaussi summa $g_1(\chi)$ asemel ka lihtsalt $g(\chi)$.

Definitsioon 5.6 ([2], definitsioon 5.11)**.** Olgu χ ja λ korpuse $\mathbb{K}_p$ karakterid. Siis kompleksarvu

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

nimetame karakterite χ ja λ **Jacobi summaks**.

Lause 5.7 ([2], lause 5.13)**.** *Olgu $p \equiv 1 \pmod{n}$ ja χ karakter, mille järk on $n > 2$. Siis*

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

Järeldus 5.8. *Olgu algarv p selline, et $p \equiv 1 \pmod{3}$. Kui χ on kolmandat järku karakter üle korpuse $\mathbb{K}_p$, siis*

$$g(\chi)^3 = pJ(\chi, \chi).$$

Tõestus. Kuna $\chi(-1) = \chi((-1)^3) = 1$, siis antud tulemus järeldub eelmisest lausest juhul $n = 3$. ■

Lemma 5.9 ([2], lemma 5.8)**.** *Kehtib seos*

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

Lause 5.10 ([1], lause 6.1.1)**.** *Olgu algarv p selline, et $p \equiv 1 \pmod{3}$. Kui χ on kolmandat järku karakter üle korpuse $\mathbb{K}_p$ ja $J(\chi, \chi) = a + b\omega$ on tema Jacobi summa, siis $a \equiv -1 \pmod{3}$ ja $b \equiv 0 \pmod{3}$.*

Seda lauset me kahjuks siinkohal tõestada ei jõua.

Lause 5.11 ([2], lause 5.10)**.** *Kui χ on korpuse $\mathbb{K}_p$ karakter ja $\chi \neq \varepsilon$, siis $|g(\chi)| = \sqrt{p}$.*

Järeldus 5.12. *Olgu lõpliku korpuse $\mathbb{Z}_p$ kolmandat järku karakterid χ ja χ^2 mittetriviaalsed ja kehtigu $p \equiv 1 \pmod 3$. Siis kompleksarvu $J(\chi, \chi)$ moodul võrdub p ruutjuurega:*

$$|J(\chi, \chi)| = \sqrt{p}.$$

Tõestus. Eelneva lause tõttu teame, et $|g(\chi)| = \sqrt{p}$. Järeldusest 5.8 saame, et $g(\chi)^3 = pJ(\chi, \chi)$. Seega

$$|g(\chi)|^3 = (\sqrt{p})^3 = p|J(\chi, \chi)|,$$

millest saamegi võrduse $J|(\chi, \chi)| = \sqrt{p}$. ■

Lause 5.13 ([2], lause 5.7)**.** *Olgu χ korpuse $\mathbb{K}_p$ karakter. Kui $a \not\equiv 0 \pmod p$ ja $\chi \neq \varepsilon$, siis $g_a(\chi) = \chi(a^{-1})g(\chi)$.*

6 Eisensteini kuupvastavusseadus

Oleme nüüd teinud piisavalt eeltööd, et kuupvastavusseaduse vaatlemisega hakata. Selle sõnastamiseks jääb üle vaid primaarsuse mõiste defineerimine.

Definitsioon 6.1. Olgu $p = a + b\omega$ E-algarv. Ütleme, et p on **primaarne**, kui $a \equiv 2 \pmod 3$ ja $b \equiv 0 \pmod 3$.

Seega primaarne E-algarv on kujul $p = 3m - 1 + 3n\omega$, kus $m, n \in \mathbb{Z}$.

Teoreem 6.2. *Olgu E-algarv $p \in \mathbb{Z}[\omega]$ selline, et $N(p) \equiv 1 \pmod 3$ (ehk $p \neq 1-\omega$ ja $p \notin \mathbb{Z}$). Siis täpselt üks temaga assotsieeritud arvudest on primaarne.*

Tõestus. Olgu $p := a + b\omega$. E-algarvuga p assotsieeritud arvud on parajasti

1. $p = a + b\omega$,
2. $\omega p = -b + (a - b)\omega$,
3. $\omega^2 p = (b - a) - a\omega$,
4. $-p = -a - b\omega$,
5. $-\omega p = b + (b - a)\omega$,
6. $-\omega^2 p = (a - b) + a\omega$.

Soovime näidata, et nende seas leidub täpselt üks primaarne element. Kui $3|a$ ja $3|b$, siis ka $3|a^2 - ab + b^2 = N(p)$, mis on vastuolus eeldustega. Järelikult $3 \nmid a$ või $3 \nmid b$. Üldisust kitsendamata võime eeldada, et $3 \nmid a$, sest juhul $3 \nmid b$ kehtib ka $3 \nmid -b$, ehk ωp reaalosa ei jagu kolmega. Sel juhul vaatleksime p asemel edaspidi arvu ωp. Sarnaselt järeldades esimese ja neljanda võrrandi juhu puhul võime eeldada, et $a \equiv 2 \pmod 3$ — kui $3 \nmid a$, siis kas $a \equiv 2 \pmod 3$ või $-a \equiv 2 \pmod 3$. Nüüd

$$\begin{aligned} N(p) &= a^2 - ab + b^2, \\ 1 &\equiv 1 - 2b + b^2 && \pmod 3, \\ 0 &\equiv b(b-2) && \pmod 3. \end{aligned}$$

Juhul, kui $b \equiv 0 \pmod 3$, siis $p = a + b\omega$ on primaarne. Kui aga hoopis $b - 2 \equiv 0 \pmod 3$, siis $b \equiv 2 \pmod 3$ ja $-\omega p = b + (b - a)\omega$ on primaarne.

Näitame nüüd ühesust. Oletame, et $p = a+b\omega$ on primaarne. Lihtne on kontrollida, et sel juhul $\omega p, \omega^2 p, -p$ ja $-\omega p$ reaalosad ei anna kolmega jagades jääki 2. Arvu $-\omega^2 p$ puhul kehtib aga, et ω kordaja jääk modulo 3 ei ole null. Seega leidub täpselt p assotsieeritud elementide hulgas täpselt üks primaarne element. ■

Kui $p = a + b\omega$ on nii algarv kui ka E-algarv, siis ta on primaarne. Tõepoolest, sel juhul $b = 0$ ehk b jagub kolmega, ning lisaks kehtib $a = p \equiv 2 \pmod 3$ (teoreem 2.9). Kui p on aga imaginaarne, siis me just tõestasime, et leidub alati temaga assotsieeritud primaarne element. Lisaks teame kolmandast peatükist, et kui $p \sim p'$, siis nende jäägiklassikorpused on võrdsed. See tähendab, et kui asendada kuupjäägi sümboli "nimetajas" oleva E-algarvu temaga assotsieeritud primaarse E-algarvuga, siis kuupjäägi sümboli väärtus ei muutu. Seega võime nõuda E-algarvu primaarsust ilma üldisust kaotamata.

Teoreem 6.3. *(Eisensteini kuupvastavusseadus) Olgu p_1 ja p_2 primaarsed E-algarvud, $N(p_1) \neq 3$, $N(p_2) \neq 3$, $N(p_1) \neq N(p_2)$. Siis*

$$\left(\frac{p_2}{p_1}\right)_3 = \left(\frac{p_1}{p_2}\right)_3. \tag{3}$$

Selle teoreemi tõestamiseks on vajalikud mõned eelteadmised.

Märkus 6.4. (*Pööratavate elementide kuupjäägi sümboli väärtus*) Kuna $1^3 = 1$ ja $(-1)^3 = -1$, siis 1 ja -1 on kuupjäägid iga E-algarvu järgi. Kui $N(p) \neq 3$, siis $\left(\frac{\omega}{p}\right)_3 = \omega^{\frac{N(p)-1}{3}}$, ehk kuupjäägi sümboli väärtus sõltub sellest, millise jäägi annab arv $\frac{N(p)-1}{3}$ modulo 3. See on samaväärne küsimusega, mis on $N(p) - 1$ jääk modulo 9, ehk sõltuvalt sellest, kas $N(p)$ jääk on 1, 4 või 7, on $\left(\frac{\omega}{p}\right)_3$ väärtus vastavalt $1, \omega$ või ω^2. Teiste pööratavate elementide kuupjäägi sümboli väärtused saab nüüd lihtsasti järeldada kuupjäägi omaduste abil.

Märkus 6.5. Erandina peame arvestama E-algarvuga $1 - \omega$ (ja temaga assotsieeritud arvudega) — see on ainus E-algarv, mis ei täida Eisensteini kuupvastavusseaduse eeldusi.

Teoreem 6.6. *Olgu primaarne E-algarv $p = a + b\omega$ selline, et $N(p) \neq 3$. Juhul, kui p on täisarv, kirjutame $p = 3m - 1$, $m \in \mathbb{Z}$. Kui p on imaginaarne, kirjutame $a = 3m - 1$. Siis kehtib võrdus*

$$\left(\frac{1-\omega}{p}\right)_3 = \omega^{2m}. \tag{4}$$

Selle teoreemi tõestus kahjuks käesolevasse töösse ei mahu.

6.1 Gaussi ja Jacobi summad kuupjäägi sümboli korral

Olgu p selline imaginaarne E-algarv, et $N(p) \equiv 1 \pmod 3$ (ehk $p \neq 1-\omega$). Teoreemi 2.7 põhjal peab $N(p)$ olema algarv. Kuna $\mathbb{K}_p$ on lõplik korpus $N(p)$ elemendiga, siis ta on isomorfne korpusega $\mathbb{Z}_{N(p)}$. Seega uurime edaspidi korpuse $\mathbb{K}_p$ asemel korpust $\mathbb{Z}_{N(p)}$ ning samastame jäägiklassid nende esindajatega. Võime vaadata kuupjäägi funktsiooni $\chi_p := \left(\frac{\cdot}{p}\right)_3$ kolmandat järku karakterina üle korpuse $\mathbb{K}_p$. Tõepoolest, lause 4.8 tõttu see on korrektselt defineeritud ja multiplikatiivne. Lisaks see on kolmandat järku. Tõepoolest, kui näiteks $\chi(x) = \omega$, siis $\chi(x)^2 = \omega^2 \neq 1$. Lisaks suvalise $x \in \mathbb{Z}[\omega]$ korral kehtib, et $\chi(x)^3 = 1$. Seega võime kasutada Gaussi summat $g_a(\chi_p)$ ja Jacobi summat $J(\chi_p, \chi_p)$. Kuna χ_p on karakter, siis järelduse 5.8 ja lause 5.10 tõttu kehtib, et

1. $g(\chi_p)^3 = N(p)J(\chi_p, \chi_p)$;
2. $J(\chi_p, \chi_p) = a + b\omega \in \mathbb{Z}[\omega]$, kus $a \equiv -1 \pmod 3$ ja $b \equiv 0 \pmod 3$.

Paneme tähele, et nii χ kui ka χ^2 ei ole triviaalsed. Tõepoolest, nii χ kui ka χ^2 muutumispiirkond üle multiplikatiivse rühma $\mathbb{K}_|^*$ on parajasti $\{1, \omega, \omega^2\}$. Seega saame lausest 5.12, et $|J(\chi_p, \chi_p)| = \sqrt{N(p)}$. Kuna $N(z) = |z|^2$ iga $z \in \mathbb{Z}[\omega]$ korral, siis

$$N(p) = |J(\chi_p, \chi_p)|^2 = N(J(\chi_p, \chi_p)).$$

Väite 2 ja teoreemi 2.8 tõttu teame nüüd, et $J(\chi_p, \chi_p)$ on primaarne algarv ringis $\mathbb{Z}[\omega]$ normiga $N(p)$.

Lemma 6.7. *Kui $\mathbb{K}_q$ on lõplik korpus q elemendiga, kus q on algarv, ja $q-1 \nmid k$, kus $k \in \mathbb{N}$, siis $\sum_{a \in \mathbb{K}_q^*} a^k = 0$.*

Tõestus. Kuna $\mathbb{K}_q$ on lõplik korpus, siis tal leidub moodustaja g nii, et iga $\mathbb{K}_q^*$ element on väljendatav g astmena. Järelikult

$$1^k + 2^k + \cdots + (q-1)^k = g^{0k} + g^{1k} + g^{2k} + \cdots + g^{(q-2)k} =: S_k.$$

See on lõplik geomeetriline jada, mille summa avaldub kujul

$$S_k = \frac{1 - g^{(q-1)k}}{1 - g^k}.$$

Kuna $q-1 \nmid k$, siis $g^k \neq 1$, ja Fermat' väikese teoreemi tõttu $g^{(q-1)k} = (g^{q-1})^k = 1^k = 1$, järelikult $S_k = \frac{1-1}{1-g^k} = 0$. ■

Lause 6.8. *Olgu p primaarne E-algarv, mis on imaginaarne. Siis $J(\chi_p, \chi_p) = p$.*

Tõestus. Olgu $J(\chi_p, \chi_p) = p' \in \mathbb{Z}[\omega]$. Eelnevalt näitasime, et p' on primaarne E-algarv. Jacobi summa ja kuupjäägi sümboli definitsioonide kohaselt

$$J(\chi_p, \chi_p) = \sum_{x \in \mathbb{Z}_{N(p)}} \chi_p(x)\chi_p(1-x) \equiv \sum_{x \in \mathbb{Z}_{N(p)}} x^{\frac{N(p)-1}{3}} (1-x)^{\frac{N(p)-1}{3}} \pmod{p}.$$

Olgu $\frac{N(p)-1}{3} =: n$. Fikseerime suvaliselt $x \in \mathbb{Z}_{N(p)}$ ning vaatleme termi $x^n(1-x)^n$ mooduli $N(p)$ järgi. Siis

$$\begin{aligned} x^n(1-x)^n &= x^n \cdot \left(1 - \binom{n}{1}x + \binom{n}{2}x^2 - \cdots + (-1)^n x^n\right) \\ &= x^n - \binom{n}{1}x^{n+1} + \binom{n}{2}x^{n+2} - \cdots + (-1)^n x^{2n}. \end{aligned}$$

Olgu $x_1, \ldots, x_{3n}$ kõik korpuse $\mathbb{Z}_{N(p)}$ elemendid. Siis terve summa avaldub kujul

$$\sum_{x\in\mathbb{Z}_{N(p)}} x^{\frac{N(p)-1}{3}}(1-x)^{\frac{N(p)-1}{3}} = x_1^n - \binom{n}{1}x_1^{n+1} + \binom{n}{2}x_1^{n+2} - \cdots + (-1)^n x_1^{2n}$$
$$+ \ldots$$
$$+ x_{3n}^n - \binom{n}{1}x_{3n}^{n+1} + \binom{n}{2}x_{3n}^{n+2} - \cdots + (-1)^n x_{3n}^{2n}.$$

Nüüd võime termid ümber grupeerida järgmiselt: Moodustame summa esimese veeru liikmetest: $\sum_{x\in\mathbb{Z}_{N(p)}} x^n$. Lemma 6.7 tõttu see on kongruentne nulliga mooduli $N(p)$ järgi. Sama teeme ka teise veeru liikmetega, mille summa on jällegi lemma 6.7 tõttu kongruentne arvuga $\binom{n}{1}\cdot 0 = 0$ mooduli p järgi. Kuna $2n < N(p)-1$, siis võime analoogiliselt jätkata, ning saame tulemusena, et terve summa on kongruentne nulliga mooduli $N(p)$ järgi. Kuna $p|N(p)$, siis kehtib seetõttu ka

$$\sum_{x\in\mathbb{Z}_{N(p)}} x^{\frac{N(p)-1}{3}}(1-x)^{\frac{N(p)-1}{3}} \equiv 0 \pmod{p}.$$

Seega $J(\chi_p, \chi_p) \equiv 0 \pmod{p}$, järelikult $p|p'$, ehk $pk = p'$ mingi $k \in \mathbb{Z}[\omega]$ korral. Kuna

$$N(J(\chi_p, \chi_p)) = |J(\chi_p, \chi_p)|^2 = N(p) \qquad \text{(lause 6.8)}$$

ning samas ka $J(\chi_p, \chi_p) = p'$ ehk $N(J(\chi_p, \chi_p)) = N(p')$, siis võrduse $N(pk) = N(p)N(k) = N(p')$ tõttu peab kehtima, et k on pööratav ehk $p \sim p'$. Kuna omavahel assotsieeritud elementidest täpselt üks on primaarne, siis $p = p'$.

Järeldus 6.9. *Kui p on primaarne ja imaginaarne E-algarv, siis $g(\chi_p)^3 = pN(p)$.*

Tõestus. See järeldub otseselt järeldusest 5.8 ja lausest 6.8. ■

6.2 Eisensteini kuupvastavusseaduse tõestus

On kolm võimalikku juhtu p_1 ja p_2 liigituses:

a) mõlemad on täisarvud;

b) üks neist on imaginaarne;

c) mõlemad on imaginaarsed.

Järgnevas tõestame antud tulemuse iga juhu jaoks eraldi.

(a) Esimene osa on lihtne: kui p_1 ja p_2 on mõlemad täisarvud, $p_1^2 = N(p_1) \neq N(p_2) = p_2^2$. Järelikult p_1 ja p_2 ei ole omavahel assotsieeritud. Kuna nad on samas ka algarvud (teoreem 2.9), siis $(p_1, p_2) = 1$. Lause 4.9 tõttu kehtib nüüd, et $\left(\frac{p_1}{p_2}\right)_3 = 1 = \left(\frac{p_2}{p_1}\right)_3$.

(b) Vaatleme juhtu, kus $p_1 = q$ on algarv, $N(q) = q^2$, ja $p_2 = p$ on imaginaarne E-algarv normiga $N(p)$. Siis kehtib $g(\chi_p)^3 = pN(p)$ (järeldus 6.9). Tõstes mõlemad pooled astmesse $\frac{q^2-1}{3}$, saame võrduse

$$g(\chi_p)^{q^2-1} = (pN(p))^{\frac{q^2-1}{3}},$$

kusjuures paneme tähele, et kuna $q^2 \equiv 1 \pmod 3$, siis $\frac{q^2-1}{3}$ on täisarv. Kasutades kuupjäägi sümboli definitsiooni saame nüüd

$$g(\chi_p)^{q^2-1} \equiv \chi_q(pN(p)) \pmod q.$$

Kuna $q \equiv 2 \pmod 3$ ja $N(p) \equiv 1 \pmod 3$ ning mõlemad on algarvud, siis nende suurim ühistegur on 1, ehk lause 4.9 tõttu $\chi_q(N(p)) = 1$. Nüüd

$$g(\chi_p)^{q^2} \equiv \chi_q(p)g(\chi_p) \pmod q. \tag{5}$$

Gaussi summa definitsioonist saame

$$g(\chi_p)^{q^2} = \left(\sum_{[t]\in\mathbb{Z}_{N(p)}} \chi_p([t])\zeta^t\right)^{q^2} \equiv \sum_{[t]\in\mathbb{Z}_{N(p)}} \chi_p([t])^{q^2}\zeta^{q^2t}$$
$$= \sum_{[t]\in\mathbb{Z}_{N(p)}} \chi_p([t])\zeta^{q^2t} \pmod q,$$

kus kongruents kehtib lemma 1.24 ning 5.10 tõestuses analoogilise arutluskäigu tõttu: Kui avame sulud, siis iga liidetava $\chi_p(t_1)^k\zeta^{kt}\cdot\chi_p(t_2)^{q^2-k}\zeta^{(q^2-k)t}$ korral, kus $x_1 \neq x_2$, jagub vastav binoomkordaja algarvuga q, ehk muutub nulliks mooduli q järgi. Viimane võrdus kehtib seetõttu, et $\chi_p(t)^{q^2} = \chi_p(t)$, kuna $q^2 \equiv 1 \pmod 3$. Nüüd

$$g(\chi_p)^{q^2} \equiv g_{q^2}(\chi_p) \pmod q. \tag{6}$$

Kuna χ_p ei ole triviaalne ja $p \nmid q^2$, siis lause 5.13 eeldused on täidetud. Järelikult $g_{q^2}(\chi_p) = \chi_p(q^{-2})g(\chi_p) = \chi_p(q)g(\chi_p)$. Seega võrdused (5) ja (6) annavad meile

$$\chi_p(q)g(\chi_p) \equiv \chi_q(p)g(\chi_p) \pmod q. \tag{7}$$

Kehtib, et $g(\chi_p)\overline{g(\chi_p)} = N(p)$. Tõepoolest, kuna $g(\chi_p)^3 = pN(p)$, siis

$$|g(\chi_p)|^3 = |pN(p)| = |p^3| = |p|^3,$$
$$|g(\chi_p)| = |p|,$$

millest omakorda

$$g(\chi_p)\overline{g(\chi_p)} = N(g(\chi_p)) = |g(\chi_p)|^2 = |p|^2 = N(p).$$

Sellega arvestades korrutame mõlemad võrduse (7) pooled arvuga $\overline{g(\chi_p)}$, millest

saame ekvivalentsid

$$\begin{aligned}
\chi_p(q)N(p) &\equiv \chi_q(p)N(p) \pmod{q}, \\
\chi_p(q) &\equiv \chi_q(p) \pmod{q}, && (N(p) \not\equiv 0 \pmod{q}) \\
\chi_p(q) &= \chi_q(p),
\end{aligned}$$

kus viimane võrdus kehtib märkuse 4.2 tõttu.

(c) Vaatame nüüd, mis toimub kahe imaginaarse E-algarvu p_1, p_2 puhul, kus $N(p_1), N(p_2) \equiv 1 \pmod 3$. Teame, et $N(p_1) = p_1\overline{p_1} = N(\overline{p_1})$ ja $N(p_2) = p_2\overline{p_2} = N(\overline{p_2})$, kus $\overline{p_1}, \overline{p_2}$ on samuti primaarsed, kuna

$$b \equiv 0 \pmod 3 \Rightarrow -b \equiv 0 \pmod 3.$$

Analoogiliselt eelmise juhuga alustame võrdusega $g(\chi_{\overline{p_1}})^3 = N(p_1)\overline{p_1}$ ning tõstame ta astmesse $\frac{N(p_2)-1}{3}$. Siis

$$g(\chi_{\overline{p_1}})^{N(p_2)-1} = (N(p_1)\overline{p_1})^{\frac{N(p_2)-1}{3}} \equiv \chi_{p_2}(N(p_1)\overline{p_1}) \pmod{p_2}. \tag{8}$$

Samas aga kehtib

$$\begin{aligned}
g(\chi_{\overline{p_1}})^{N(p_2)} &= \left(\sum_{[t] \in \mathbb{K}_{p_1}} \chi_{\overline{p_1}}([t])\zeta^t \right)^{N(p_2)} \\
&\equiv \sum_{[t] \in \mathbb{K}_{p_1}} \chi_{\overline{p_1}}([t])^{N(p_2)} \zeta^{N(p_2)t} \pmod{N(p_2)} && \text{(lemma 1.24)} \\
&= \sum_{[t] \in \mathbb{K}_{p_1}} \chi_{\overline{p_1}}([t])\zeta^{N(p_2)t} && (N(p_2) \equiv 1 \pmod 3) \\
&= g_{N(p_2)}(\chi_{\overline{p_1}}) && \text{(Gaussi summa definitsioon)} \\
&= \chi_{\overline{p_1}}\left(N(p_2)^{-1}\right) g(\chi_{\overline{p_1}}) && \text{(lause 5.13)} \\
&= \chi_{\overline{p_1}}\left(N(p_2)^2\right) g(\chi_{\overline{p_1}}).
\end{aligned}$$

ehk lühidalt

$$g(\chi_{\overline{p_1}})^{N(p_2)} \equiv \chi_{\overline{p_1}}\left(N(p_2)^2\right) g(\chi_{\overline{p_1}}) \pmod{N(p_2)}.$$

Võrduse (8) tõttu kehtib nüüd

$$\chi_{p_2}(N(p_1)\overline{p_1}) \equiv \chi_{\overline{p_1}}\left(N(p_2)^2\right) \pmod{N(p_2)}$$

ja märkusest 4.2 saame, et kehtib

$$\chi_{p_2}(N(p_1)\overline{p_1}) = \chi_{\overline{p_1}}\left(N(p_2)^2\right). \tag{9}$$

Arendame $g(\chi_{p_2})^3 = N(p_2)p_2$ analoogiliselt, kus nüüd $\overline{p_1}$ asemel on p_2 ja p_2 asemel on p_1. Eelnevas arutluskäigus tehtud eeldused kehtivad endiselt, seega saame võrduse

$$\chi_{p_1}(N(p_2)p_2) = \chi_{p_2}\left(N(p_1)^2\right). \tag{10}$$

Viimane vajalik võrdus on

$$\chi_{\overline{p_1}}(N(p_2)^2) = \chi_{p_1}(N(p_2)), \tag{11}$$

mida me saame teoreemist 4.8: kuna $N(p_2) = \overline{N(p_2)}$, siis

$$\begin{aligned}
\chi_{\overline{p_1}}(N(p_2)^2) &= (\chi_{\overline{p_1}}(N(p_2)))^2 && \text{(omadus 4)}\\
&= \overline{\chi_{\overline{p_1}}(N(p_2))} && \text{(omadus 4)}\\
&= \chi_{p_1}(\overline{N(p_2)}) && \text{(omadus 5)}\\
&= \chi_{p_1}(N(p_2)). && \text{(norm on naturaalarv)}
\end{aligned}$$

Kombineerime nüüd võrdused (9), (10) ja (11):

$$\begin{aligned}
\chi_{p_1}(p_2)\chi_{p_2}(N(p_1)\overline{p_1}) &= \chi_{p_1}(p_2)\chi_{\overline{p_1}}(N(p_2)^2) && \text{(võrdus (9))}\\
&= \chi_{p_1}(p_2)\chi_{p_1}(N(p_2)) = \chi_{p_1}(N(p_2)p_2) && \text{(võrdus (11))}\\
&= \chi_{p_2}(N(p_1)^2) = \chi_{p_2}(N(p_1)p_1\overline{p_1}) && \text{(võrdus (10))}\\
&= \chi_{p_2}(p_1)\chi_{p_2}(N(p_1)\overline{p_1})
\end{aligned}$$

ehk lühidalt

$$\chi_{p_1}(p_2)\chi_{p_2}(N(p_1)\overline{p_1}) = \chi_{p_2}(p_1)\chi_{p_2}(N(p_1)\overline{p_1}).$$

Taandades mõlemalt poolt teguri $\chi_{p_2}(N(p_1)\overline{p_1})$ saamegi võrduse

$$\chi_{p_1}(p_2) = \chi_{p_2}(p_1).$$

■

Kasutatud kirjandus

[1] Kenneth Ireland ja Michael Rosen. *A Classical Introduction to Modern Number Theory (2nd ed)*. Springer Verlag, 1990.

[2] Anu Ahven. *Biruutvastavusseadus*. 2015. URL: https://dspace.ut.ee/server/api/core/bitstreams/38e74177-e086-4913-bbe4-6a3ff7194ddd/content. Viimati vaadatud 29.05.2025.

[3] Valdis Laan ja Lauri Tart. *Arvuteooria*. 2024. URL: https://courses.ms.ut.ee/MTMM.00.012/2024_spring/uploads/Main/kon_2024.pdf. Viimati vaadatud 29.05.2025.

[4] Valdis Laan. *Algebra I*. 2024. URL: https://courses.ms.ut.ee/MTMM.00.038/2024_fall/uploads/Main/kon2024.pdf. Viimati vaadatud 12.04.2025.

[5] Valdis Laan ja Kristo Väljako. *Algebra II*. 2024. URL: https://courses.ms.ut.ee/MTMM.00.040/2024_fall/uploads/Main/kon.pdf. Viimati vaadatud 24.05.2025.

[6] Valdis Laan. *Sissejuhatus algebra struktuuridesse*. 2024. URL: https://courses.ms.ut.ee/MTMM.00.013/2024_fall/uploads/Main/kon.pdf. Viimati vaadatud 18.04.2025.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Johanna Charlotte Jeltsch (sünnikuupäev 27.05.2002),

1. annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose "Eisensteini kuupvastavusseadus", mille juhendajad on Lauri Tart ja Valdis Laan, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada Tartu Ülikooli digitaalarhiivi kuni autoriõiguse kehtivuse lõppemiseni;

2. annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi kaudu Creative Commonsi litsentsiga CC BY NC ND 4.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni;

3. olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile;

4. kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.