Kompleksilukujen lukuteoriaa ja lukuteoriaa kompleksiluvuilla

Ellinoora Lindqvist

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kesä 2019

Tiivistelmä: Ellinoora Lindqvist, *Kompleksilukujen lukuteoriaa ja lukuteoriaa kompleksiluvuilla* (engl. *Number Theory of Complex Numbers and Number Theory with Complex Numbers*), matematiikan pro gradu -tutkielma, 45 s., Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, kesä 2019.

Tämän tutkielman tarkoituksena on näyttää, kuinka kokonaislukujen lukuteoriaa voidaan yleistää kokonaislukujen kompleksisille laajennuksille. Lisäksi halutaan osoittaa, että tilannetta voidaan tarkastella toisestakin suunnasta eli siitä, kuinka kokonaislukujen lukuteorian tuloksia voidaan todistaa kompleksilukujen avulla. Kokonaislukujen kompleksisista laajennuksista erityisen kiinnostuneita tutkielmassa ollaan Gaussin, Hurwitzin ja Eisensteinin kokonaisluvuista.

Tutkielman alussa esitellään perusteellisesti Gaussin kokonaisluvut, jotka ovat tärkein tutkielmassa käytettävistä kokonaislukujen laajennuksista. Gaussin kokonaisluvuille näytetään ensin niiden algebrallisia ominaisuuksia, minkä jälkeen siirrytään lukuteoreettisiin ominaisuuksiin. Osoittautuu, että monet kokonaislukujen lukuteorian käsitteet ja tulokset, kuten alkuluvut, Eukleideen algoritmi, aritmetiikan peruslause ja Bézout'n lemma, voidaan yleistää Gaussin kokonaisluvuille.

Tämän jälkeen vaihdetaan tarkastelusuuntaa. Tutustutaan kokonaislukujen lukuteorian tuloksiin ja niiden todistamiseen kokonaislukujen kompleksilaajennusten avulla. Ensimmäisenä annetaan tulos luonnollisen luvun esittämisestä kahden neliön summana. Tuloksen todistuksessa hyödynnetään Gaussin kokonaislukuja. Tämän jälkeen esitellään toinen kokonaislukujen kompleksisista laajennuksista, Hurwitzin kokonaisluvut. Niiden avulla todistetaan tulos luonnollisen luvun esittämisestä neljän neliön summana. Kolmantena todistettavana lukuteorian tuloksena esitellään eräs tapaus Fermat'n suuresta lauseesta. Todistusta varten perehdytään Eisensteinin kokonaislukuihin, jotka ovat viimeinen tutkielmassa esiteltävistä kokonaislukujen laajennuksista.

Lopuksi kootaan yhteen tutkielmassa käytetyt kokonaislukujen laajennukset niiden geometrisen tulkinnan kautta. Samalla käsitellään lyhyesti tavallisten kokonaislukujen ja niiden kompleksisten laajennusten ulottuvuuksien määrää ja esitellään eräs siihen liittyvä toistaiseksi ratkaisematon ongelma.

Sisältö

Johdanto

Tässä tutkielmassa tarkastellaan sekä kompleksilukujen lukuteoriaa että kokonaislukujen lukuteoriaa kompleksilukuja apuna käyttäen. Tutkielman yhtenä tavoitteena on näyttää useiden lukuteorian tulosten yleistyminen tavallisten kokonaislukujen kompleksisille laajennuksille. Toisena tavoitteena on näyttää lukijalle, kuinka lukuteorian tuloksia voidaan todistaa suhteellisen yksinkertaisesti kokonaislukujen kompleksisten laajennusten avulla.

Kokonaislukujen laajennuksia tunnetaan useita, mutta tässä tutkielmassa keskitytään Gaussin, Hurwitzin ja Eisensteinin kokonaislukuina tunnettuihin kompleksisiin laajennuksiin. Näistä eniten syvennytään Gaussin kokonaislukuihin, jotka ovat muotoa $z = a + ib$ olevia kompleksilukuja, missä a ja b ovat kokonaislukuja ja i imaginääriyksikkö. Gaussin kokonaislukuihin liittyviin käsitteisiin annetaan tarkat määritelmät ja tuloksiin huolelliset perustelut. Oleellisesti samoin voitaisiin tehdä myös Hurwitzin ja Eisensteinin kokonaisluvuille, joten toiston välttämiseksi näiden perustulosten todistukset sivuutetaan tutkielmassa. Päätulosten todistusten kannalta tärkeimmät määritelmät, tulokset tai mahdolliset eroavaisuudet kuitenkin esitellään niillekin.

Ensimmäisessä luvussa tutustutaan Gaussin kokonaislukuihin ja tarkastellaan niitä erityisesti algebran näkökulmasta. Aluksi näytetään niiden perusominaisuuksia, kuten hyvin määritellyt laskutoimitukset $+$ ja $\times$. Tämän jälkeen näytetään, että Gaussin kokonaisluvut muodostavat vaihdannaisen renkaan ja kokonaisalueen. Lisäksi esitellään tutkielman kannalta hyvin tärkeä kuvaus, normi N, ja sille näytetään muutamia hyödyllisiä ominaisuuksia. Normin N avulla perustellaan luvun lopuksi Gaussin kokonaislukujen renkaan Euklidisuus.

Toisessa luvussa keskitytään tarkastelemaan Gaussin kokonaislukujen lukuteoriaa. Aluksi määritellään Gaussin kokonaisluvuille lukuteorian peruskäsitteet, kuten jaollisuus ja yksiköt. Tämän jälkeen annetaan määritelmät liittolaisille, Gaussin alkuluvuille ja Gaussin alkutekijäesitykselle. Luvussa esitellään Eukleideen algoritmi ja kuinka suurin yhteinen tekijä löydetään sen avulla. Lisäksi näytetään lukuteoriasta tuttujen tulosten yleistyminen esimerkiksi Eukleideen lemmalle, aritmetiikan peruslauseelle ja Bézout'n lemmalle. Normi N osoittautuu tässäkin luvussa hyödylliseksi, sillä monissa luvun todistuksissa hyödynnetään sitä.

Kolmannessa luvussa tehdään tarkastelunäkökulman muutos eli tutkitaan, kuinka tavallisen lukuteorian tuloksia voidaan todistaa kompleksiluvuilla. Luvussa keskitytään neliösummiin liittyviin tuloksiin ja annetaan tarkat todistukset luonnollisen

luvun esittämisestä kahden neliön summana sekä neljän neliön summana. Näistä ensimmäisenä mainitussa todistuksessa hyödynnetään tutuksi tulleita Gaussin kokonaislukuja. Tämän jälkeen annetaan Gaussin alkulukujen karakterisointi, jonka todistuksessa apuna käytetään kahden neliön summaan liittyvää tulosta. Seuraavaksi esitellään Hurwitzin kokonaisluvut, jotka ovat kokonaislukujen neliulotteinen laajennus kvaternioiden avulla. Hurwitzin kokonaislukuja hyödennetään neljän neliön summaan liittyvän tuloksen todistuksessa. Kyseinen tulos tunnetaan myös Lagrangen neljän neliön lauseena.

Neljännessä luvussa esitellään Fermat'n suuri lause, jota voidaan pitää yhtenä kuuluisimmista tuloksista koko matematiikan historiassa. Lauseen mukaan yhtälöllä

$$x^n + y^n = z^n$$

ei ole positiivisia kokonaislukuratkaisuja, kun n on suurempaa kuin 2. Lauseen muotoilu on yksinkertainen, mutta sen todistaminen kesti yli 300 vuotta, kunnes se 1990-luvulla lopulta ratkaistiin. Luvussa esitellään Eisensteinin kokonaisluvut, jotka ovat kokonaislukujen kaksiulotteinen kompleksinen laajennus. Eisensteinin kokonaislukujen avulla annetaan todistus Fermat'n suuren lauseen tapauksessa, jossa $n = 3$.

Viidennessä ja tutkielman päättävässä luvussa kuvataan käytettyjen kokonaislukujen laajennuksien geometrista puolta. Ne on koottu yhteen paikkaan, jotta niiden toisiinsa vertaaminen olisi helpompaa. Suositeltavaa on kuitenkin vilkaista alalukuja sitä mukaa, kun jokin kokonaislukujen laajennuksista esitellään. Luvussa tarkastellaan, kuinka Eisensteinin, Hurwitzin ja Gaussin kokonaisluvut voidaan järjestää normin N avulla osittaiseen suuruusjärjestykseen. Lisäksi Gaussin kokonaislukujen yhteydessä käsitellään lyhyesti Gaussin vallihautaongelmaa, joka on kiintoisa Gaussin alkulukuihin liittyvä pulma ja toistaiseksi ratkaisematon.

Tutkielman lukijalle oletetaan olevan tuttuja tavallisten kokonaislukujen ja kompleksilukujen ominaisuudet ja laskusäännöt. Lukuteorian perusteiden ja yleisimpien tulosten tunteminen on myös eduksi. Algebran määritelmistä ja tuloksista on hyvä olla pohjatietoa, mutta niistä tutkielman kannalta tärkeimmät kerrataan. Lisäksi kongruenssit ja niiden laskusäännöt oletetaan tutuiksi.

Merkinnöissä, määritelmissä ja tulosten nimityksissä pyritään käyttämään kompleksilukujen ja tavallisten kokonaislukujen puolelta tuttuja vastineita. Esimerkiksi Gaussin kokonaislukuja merkitään kirjaimilla z ja w. Tavalliselle alkuluvulle käytetään merkintää p ja Gaussin alkuluvulle merkintää ρ. Lisäksi lukijan on syytä kiinnittää huomio siihen, että Eisensteinin kokonaislukujen yhteydessä kirjaimella ρ on täysin eri merkitys. Pelkällä kokonaisluvulla tai alkuluvulla viitataan aina joukon $\mathbb{Z}$ alkioon, mutta joissakin tilanteissa sekaannusten välttämiseksi saatetaan käyttää samasta asiasta myös ilmaisua tavallinen kokonaisluku tai tavallinen alkuluku. Muut merkinnät ja ilmaisut esitellään tutkielman aikana.

Tutkielman päälähteinä on hyödynnetty W. A. Coppelin teosta Number Theory: An Introduction to Mathematics [**2**], G. H. Hardyn ja E. M. Wrightin teosta An Introduction to the Theory of Numbers [**6**] ja G. Everestin ja T. Wardin teosta An Introduction to Number Theory [**4**]. Lisäksi ensimmäisessä luvussa on käytetty apuna P. Koskelan luentomonistetta Algebra 1: Renkaat ja kunnat [**8**]. Matematiikan historiasta kiinnostuneelle lukijalle voi lämpimästi suositella tutustumista J. Stillwellin

teokseen Mathematics and its History [**11**] ja erityisesti Fermat'n suuresta lauseesta kiinnostuneelle A. D. Aczelin teosta Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem [**1**].

LUKU 1

Algebraa Gaussin kokonaisluvuille

Tässä luvussa tutustutaan Gaussin kokonaislukuihin ja tarkastellaan niitä algebran näkökulmasta. Gaussin kokonaisluvut ovat saaneet nimensä saksalaisen Carl Friedrich Gaussin (1777–1855) mukaan. Hän oli ensimmäinen matemaatikko, joka tutki kyseisiä lukuja ja todisti niiden perusominaisuuksia.

1.1. Gaussin kokonaislukujen perusominaisuuksia

Annetaan ensin Gaussin kokonaislukujen tarkka määritelmä ja tarkastellaan sitten, millaisia perusominaisuuksia ne toteuttavat.

MÄÄRITELMÄ 1.1. Kompleksilukua z, joka on muotoa $z = a + ib$, missä $a, b \in \mathbb{Z}$, kutsutaan *Gaussin kokonaisluvuksi*. Kaikkien Gaussin kokonaislukujen muodostamaa joukkoa merkitään symbolilla $\mathbb{Z}[i]$.

HUOMAUTUS 1.2. Määritelmän 1.1 pohjalta on syytä huomata, että kaikki Gaussin kokonaisluvut ovat kompleksilukuja, mutta kaikki kompleksiluvut eivät ole Gaussin kokonaislukuja (vertaa $\mathbb{Z}[i] = \{a + ib \mid a, b \in \mathbb{Z}\}$ ja $\mathbb{C} = \{a + ib \mid a, b \in \mathbb{R}\}$). Lisäksi havaitaan, että ne Gaussin kokonaisluvut, joissa $b = 0$, ovat itse asiassa tavallisia kokonaislukuja.

Myöhemmin tässä luvussa tullaan käyttämään Gaussin kokonaisluvun kompleksikonjugaattia. Tässä vaiheessa esitellään vain lyhyesti eräs siihen liittyvä tulos.

LAUSE 1.3. *Jos $z = a + ib$ on Gaussin kokonaisluku, niin myös sen kompleksikonjugaatti $\bar{z} = a - ib$ on Gaussin kokonaisluku.*

TODISTUS. Olkoon $z = a + ib$ mikä tahansa Gaussin kokonaisluku. Sen kompleksikonjugaatti on $\bar{z} = a - ib$ ja nyt

$$\bar{z} = a - ib = a + (-1)ib = a + i(-1)b = a + i(-b).$$

Koska b on kokonaisluku, niin myös $-b$ on kokonaisluku. Siten kompleksikonjugaatti $\bar{z}$ on Gaussin kokonaisluku.

□

Huomautuksen 1.2 perusteella lienee selvää, että tavalliset kokonaisluvut ovat Gaussin kokonaislukujen osajoukko. Gaussin kokonaislukujen joukko on siis yksi esimerkki tavallisten kokonaislukujen laajennuksista. Kyseisen tiedon pohjalta on houkuttelevaa ajatella, että tavallisiin kokonaislukuihin liittyviä tuloksia ja perusominaisuuksia voitaisiin laajentaa koskemaan kaikkia Gaussin kokonaislukuja. Näin voidaan todella tehdä, esimerkkeinä mainittakoon tässä vaiheessa algebran puolelta laskutoimitukset

$+$ ja $\times$, sekä lukuteorian puolelta alkulukujen ja yksikäsitteisen alkutekijäesityksen olemassaolo. Perustellaan tässä vaiheessa vain äsken mainitut laskutoimitukset. Lukuteoreettisiin ominaisuuksiin syvennytään tarkemmin seuraavassa luvussa.

LAUSE 1.4. *Olkoot z_1, z_2 Gaussin kokonaislukuja. Tällöin myös niiden summa $z_1 + z_2$ ja tulo $z_1 \times z_2$ ovat Gaussin kokonaislukuja.*

TODISTUS. Olkoot $z_1 = a_1 + ib_1$ ja $z_2 = a_1 + ib_2$ mitä tahansa Gaussin kokonaislukuja. Koska z_1, z_2 ovat Gaussin kokonaislukuja, niin tiedetään, että $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Nyt

$$\begin{aligned} z_1 + z_2 &= (a_1 + ib_1) + (a_2 + ib_2) = a_1 + a_2 + ib_1 + ib_2 \\ &= (a_1 + a_2) + i(b_1 + b_2) \end{aligned}$$

ja

$$\begin{aligned} z_1 z_2 &= (a_1 + ib_1)(a_2 + ib_2) = a_1 a_2 + a_1 ib_2 + ib_1 a_2 + ib_1 ib_2 \\ &= (a_1 a_2 - b_1 b_2) + i(a_1 b_2 + b_1 a_2). \end{aligned}$$

Koska a_1, a_2, b_1, b_2 ovat kokonaislukuja, niin myös $a_1 + a_2$, $b_1 + b_2$, ja $a_1 a_2 - b_1 b_2$ ja $a_1 b_2 + b_1 a_2$ ovat kokonaislukuja. Siten luvut $z_1 + z_2$ ja $z_1 z_2$ todella ovat Gaussin kokonaislukuja.

□

Laskutoimitukset $+$ ja $\times$ ovat hyvin määriteltyjä Lauseen 1.4 perusteella. Se luo perustan sille, miksi Gaussin kokonaisluvuista puhuttaessa on luontevaa ajatella Gaussin kokonaislukujen muodostamaa joukkoa renkaana. Palautetaan kuitenkin ensin mieleen, mitä renkaalla tarkoitetaan.

MÄÄRITELMÄ 1.5. Epätyhjä joukko R on *rengas*, jos se on varustettu kahdella laskutoimituksella (merk. $+, \times$), jotka toteuttavat seuraavat ehdot kaikilla $a, b, c \in R$:

(1) $a + (b + c) = (a + b) + c$ (liitännäisyys)

(2) $a + b = b + a$ (vaihdannaisuus)

(3) On olemassa 0_R siten, että $a + 0_R = a = 0_R + a$ kaikilla $a \in R$. (neutraalialkio)

(4) Jokaisella $a \in R$ yhtälöllä $a + x = 0_R$ on ratkaisu $x \in R$. (vastaluku)

(5) $a \times (b \times c) = (a \times b) \times c$ (liitännäisyys)

(6) $a \times (b + c) = a \times b + a \times c$ (osittelulaki)

(7) On olemassa 1_R siten, että $a \times 1_R = a = 1_R \times a$ kaikilla $a \in R$. (neutraalialkio)

Perustellaan seuraavaksi, miksi Gaussin kokonaislukujen joukko todella muodostaa renkaan. Näytetään siis, että Gaussin kokonaislukujen joukko toteuttaa Määritelmän 1.5. Merkitään kyseistä rengasta jatkossa entuudestaan tutulla symbolilla $\mathbb{Z}[i]$.

LAUSE 1.6. *Gaussin kokonaislukujen joukko on rengas.*

TODISTUS. Gaussin kokonaislukujen joukko on selvästi epätyhjä ja Lauseen 1.4 perusteella se on varustettu laskutoimituksilla + ja $\times$. Riittää siis näyttää, että ehdot (1) – (7) ovat voimassa. Olkoot $z_1 = a_1 + ib_1, z_2 = a_2 + ib_2, z_3 = a_3 + ib_3$ Gaussin kokonaislukuja.

(1) Näytetään ensin yhteenlaskun liitännäisyys:

$$\begin{aligned} &z_1 + (z_2 + z_3) = a_1 + ib_1 + (a_2 + a_3 + i(b_2 + b_3)) \\ &= a_1 + ib_1 + a_2 + ib_2 + a_3 + ib_3 = (a_1 + a_2 + i(b_1 + b_2)) + a_3 + ib_3 \\ &= (z_1 + z_2) + z_3 \end{aligned}$$

(2) Näytetään seuraavaksi yhteenlaskun vaihdannaisuus:

$$z_1 + z_2 = a_1 + a_2 + i(b_1 + b_2) = a_2 + a_1 + i(b_2 + b_1) = z_2 + z_1$$

(3) Gaussin kokonaisluvuissa nolla on luku $0_{\mathbb{Z}[i]} = 0 + i0$, koska sille pätee, että

$$z_1 + 0_{\mathbb{Z}[i]} = a_1 + 0 + i(b_1 + 0) = a_1 + ib_1 = z_1$$

ja

$$z_1 = a_1 + ib_1 = 0 + a_1 + i(0 + b_1) = 0_{\mathbb{Z}[i]} + z_1$$

kaikilla $z_1 \in \mathbb{Z}[i]$.

(4) Jokaisella $z_1 \in \mathbb{Z}$ yhtälöllä $z_1 + x = 0_{\mathbb{Z}[i]}$ on ratkaisu $x \in \mathbb{Z}[i]$. Tämä ratkaisu on $x = -a_1 + i(-b_1)$, sillä

$$z_1 + x = a_1 + (-a_1) + i(b_1 + (-b_1)) = 0 + i0 = 0_{\mathbb{Z}[i]}.$$

(5) Osoitetaan kertolaskun liitännäisyys:

$$\begin{aligned} &z_1 \times (z_2 \times z_3) = (a_1 + ib_1)((a_2a_3 - b_2b_3) + i(a_2b_3 + b_2a_3)) \\ &= a_1(a_2a_3 - b_2b_3) + a_1i(a_2b_3 + b_2a_3) + ib_1(a_2a_3 - b_2b_3) + ib_1i(a_2b_3 + b_2a_3) \\ &= a_1a_2a_3 - a_1b_2b_3 + i(a_1a_2b_3 + a_1b_2a_3) + i(a_2a_3b_1 - b_1b_2b_3) + i^2a_2b_1b_3 + i^2b_1b_2a_3 \\ &= a_1a_2a_3 - a_1b_2b_3 + i^2a_2b_1b_3 + i^2b_1b_2a_3 + i(a_1a_2b_3 + a_1a_3b_2 + a_2a_3b_1 - b_1b_2b_3) \\ &= a_1a_2a_3 - a_3b_1b_2 + i^2a_1b_2b_3 + i^2a_2b_1b_3 + i(a_1a_3b_2 + a_2a_3b_1 + a_1a_2b_3 - b_1b_2b_3) \\ &= a_1a_2a_3 - b_1b_2a_3 + i(a_1a_3b_2 + a_2a_3b_1) + i(a_1a_2b_3 - b_1b_2b_3) + i^2a_1b_2b_3 + i^2a_2b_1b_3 \\ &= (a_1a_2 - b_1b_2)a_3 + i(a_1b_2 + a_2b_1)a_3 + (a_1a_2 - b_1b_2)ib_3 + i(a_1b_2 + a_2b_1))ib_3) \\ &= ((a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2))(a_3 + ib_3) = (z_1 \times z_2) \times z_3 \end{aligned}$$

(6) Perustellaan sitten osittelulaki:

$$\begin{aligned} &z_1 \times (z_2 + z_3) = (a_1 + ib_1)(a_2 + a_3 + i(b_2 + b_3)) \\ &= (a_1(a_2 + a_3 + i(b_2 + b_3)) + ib_1(a_2 + a_3 + i(b_2 + b_3)) \\ &= (a_1a_2 + a_1a_3 + i(a_1b_2 + a_1b_3)) + ib_1a_2 + ib_1a_3 + i^2(b_1b_2 + b_1b_3) \\ &= a_1a_2 + a_1a_3 + ia_1b_2 + ia_1b_3) + ib_1a_2 + ib_1a_3 - b_1b_2 - b_1b_3 \\ &= (a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2) + (a_1a_3 - b_1b_3) + i(a_1b_3 + b_1a_3) \\ &= z_1 \times z_2 + z_1 \times z_3 \end{aligned}$$

(7) Gaussin kokonaisluvuissa ykkönen on luku $1_{\mathbb{Z}[i]} = 1 + 0i$, koska sille pätee, että

$$z_1 \times 1_{\mathbb{Z}[i]} = (a_1 \cdot 1 - b_1 \cdot 0) + i(a_1 \cdot 0 + b_1 \cdot 1) = a_1 + ib_1 = z_1$$

ja

$$z_1 = a_1 + ib_1 = (1 \cdot a_1 - 0 \cdot b_1) + i(0 \cdot a_1 + 1 \cdot b_1) = 1_{\mathbb{Z}[i]} \times z_1$$

kaikilla $z_1 \in \mathbb{Z}[i]$.

Ehdot (1)-(7) ovat siten voimassa Gaussin kokonaisluvuille. Siispä Gaussin kokonaisluvut todella muodostavat renkaan.

□

Kokonaislukujen joukossa merkitään usein $a \times b = ab$. Käytetään jatkossa samaa lyhennystä $z_1 \times z_2 = z_1 z_2$ myös Gaussin kokonaisluvuille. Renkaan Määritelmässä 1.5 vaaditaan yhteenlaskun vaihdannaisuus, mutta sitä ei vaadita kertolaskulta. Vaihdannaisuus voi olla voimassa myös kertolaskulle. Tällöin puhutaan vaihdannaisesta renkaasta.

MÄÄRITELMÄ 1.7. Rengas R on *vaihdannainen*, jos laskutoimitus $\times$ on vaihdannainen, toisin sanoen jos kaikille $a, b \in R$ pätee, että

$$ab = ba.$$

Esimerkiksi tavallisten kokonaislukujen rengas $\mathbb{Z}$ on vaihdannainen rengas. Näytetään seuraavaksi, että myös Gaussin kokonaisluvut muodostavat vaihdannaisen renkaan.

LAUSE 1.8. *Gaussin kokonaislukujen rengas on vaihdannainen.*

TODISTUS. Olkoot $z, w \in \mathbb{Z}[i]$ ja osoitetaan, että tällöin $zw = wz$. Koska luvut z, w ovat Gaussin kokonaislukuja, niin tiedetään, että ne ovat muotoa

$$z = a_1 + ib_1 \qquad \text{ja} \qquad w = a_2 + ib_2,$$

missä $a_1, a_2, b_1, b_2 \in \mathbb{Z}$. Nyt hyödyntämällä kokonaislukujen laskusääntöjä saadaan

$$zw = (a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2) = (a_2a_1 - b_2b_1) + i(a_2b_1 + b_2a_1) = wz.$$

□

Gaussin kokonaislukujen rengas muodostaa itse asiassa kokonaisalueen. Ennen tämän perustelua palautellaan mieleen, mitä kokonaisalueella ylipäätään tarkoitetaan.

MÄÄRITELMÄ 1.9. Vaihdannainen rengas R, jossa $0_R \neq 1_R$, on *kokonaisalue*, jos kaikilla $a, b \in R$ ehdosta $ab = 0_R$ seuraa, että $a = 0_R$ tai $b = 0_R$.

LAUSE 1.10. *Gaussin kokonaislukujen rengas on kokonaisalue.*

TODISTUS. Rengas $\mathbb{Z}[i]$ on jo näytetty vaihdannaiseksi. Lisäksi

$$0_{\mathbb{Z}[i]} = 0 + i0 \neq 1 + i0 = 1_{\mathbb{Z}[i]}.$$

Nyt täytyy näyttää, että jos Gaussin kokonaisluvuille $z = a_1 + ib_1$ ja $w = a_2 + ib_2$ on voimassa, että $zw = 0_{\mathbb{Z}[i]}$, niin tällöin $z = 0_{\mathbb{Z}[i]}$ tai $w = 0_{\mathbb{Z}[i]}$.

Tiedetään, että $zw = (a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2) = 0 + i0 = 0_{\mathbb{Z}[i]}$. Tämän perusteella saadaan yhtälöt

$$a_1a_2 - b_1b_2 = 0 \qquad \text{ja} \qquad a_1b_2 + b_1a_2 = 0.$$

Oletetaan ensin, että $a_1 \neq 0$. Tällöin ensimmäinen yhtälö saadaan muotoon

$$a_2 = \frac{b_1b_2}{a_1}$$

ja sijoittamalla se jälkimmäiseen yhtälöön saadaan

$$a_1b_2 + b_1\frac{b_1b_2}{a_1} = 0.$$

Kertomalla tätä puolittain luvulla a_1 ja ottamalla yhteiseksi tekijäksi luku b_2 saadaan

$$(a_1^2 + b_1^2)b_2 = 0.$$

Tulon nollasäännön nojalla $a_1^2 + b_1^2 = 0$ tai $b_2 = 0$. Koska alussa oletettiin, että $a_1 \neq 0$, niin $a_1^2 + b_1^2 > 0$ kaikilla $a_1, b_1 \in \mathbb{Z}$. Näin ollen $b_2 = 0$ ja koska $a_2 = \frac{b_1b_2}{a_1}$, niin myös $a_2 = 0$. Tämä tarkoittaa, että $w = 0_{\mathbb{Z}[i]}$.

Tutkitaan vielä tilanne, jossa $a_1 = 0$. Tällöin yhtälöiksi saadaan

$$-b_1b_2 = 0 \qquad \text{ja} \qquad b_1a_2 = 0.$$

Tulon nollasäännöllä ensimmäisestä yhtälöstä saadaan $b_1 = 0$ tai $b_2 = 0$ ja jälkimmäisestä puolestaan $b_1 = 0$ tai $a_2 = 0$. Jos nyt $b_1 = 0$, niin $z = 0_{\mathbb{Z}[i]}$.
Jos taas $b_1 \neq 0$, niin on oltava $b_2 = 0$ ja $a_2 = 0$, eli $w = 0_{\mathbb{Z}[i]}$.

Siispä kaikille Gaussin kokonaisluvuille ehdosta $zw = 0_{\mathbb{Z}[i]}$ todella seuraa, että $z = 0_{\mathbb{Z}[i]}$ tai $w = 0_{\mathbb{Z}[i]}$.

□

Mikäli oletetaan kunnan ja alirenkaan käsitteet tunnetuiksi, Gaussin kokonaislukujen rengas voitaisiin perustella kokonaisalueeksi myös seuraavalla päättelyllä. Muistetaan aluksi, että kompleksilukujen rengas $\mathbb{C}$ on kunta ja että kunnat ovat aina kokonaisalueita. Tiedetään myös, että Gaussin kokonaislukujen rengas on renkaan $\mathbb{C}$ alirengas. Koska kokonaisalueen alirenkaat ovat kokonaisalueita, niin renkaan $\mathbb{Z}[i]$ on oltava kokonaisalue.

Tässä vaiheessa on myös hyvä tarkastella sitä, onko rengas $\mathbb{Z}[i]$ kunta. Jotta se olisi, jokaiselle nollasta eroavalle Gaussin kokonaisluvulle z yhtälöllä

$$zx = 1_{\mathbb{Z}[i]}$$

olisi olemassa ratkaisu renkaassa $\mathbb{Z}[i]$. Kyseisestä ratkaisusta käytetään yleisesti nimitystä käänteisluku ja sitä merkitään symbolilla z^{-1}. Käänteisluku on olemassa renkaassa $\mathbb{Z}[i]$ kuitenkin vain luvuille $1, -1, i$ ja $-i$, joten rengas $\mathbb{Z}[i]$ ei ole kunta.

1.2. Euklidisuus ja normi N

Gaussin kokonaislukujen renkaassa on voimassa tavallisten kokonaislukujen lukuteorian puolelta tuttu Eukleideen algoritmi. Tämä luo perustan monille muille lukuteoriasta tutuille ominaisuuksille ja tuloksille, minkä vuoksi Eukleideen algoritmin olemassaolo on syytä perustella tarkasti. Halutaan siis näyttää, että rengas $\mathbb{Z}[i]$ on Euklidinen.

MÄÄRITELMÄ 1.11. Kokonaisalue R on *Euklidinen*, jos on olemassa kuvaus $\delta : R \to \mathbb{N} \cup \{0\}$ niin, että mille tahansa $a, b \in R$, $a \neq 0$, on olemassa $q, r \in R$ siten, että

$$b = qa + r \quad \text{ja} \quad \delta(r) < \delta(a).$$

Gaussin kokonaisluvuille Määritelmän 1.11 mukainen kuvaus tunnetaan normina N. Tutustutaan seuraavaksi siihen lähemmin ja todistetaan renkaan $\mathbb{Z}[i]$ Euklidisuus vasta sen jälkeen.

MÄÄRITELMÄ 1.12. Gaussin kokonaisluvuille $z = a+ib$ *normiksi* kutsutaan kuvausta $N : \mathbb{Z}[i] \to \mathbb{N} \cup \{0\}$,

$$N(z) = z\bar{z} = a^2 + b^2.$$

Normi N määritellään siis Gaussin kokonaisluvun ja sen kompleksikonjugaatin tulona. Gaussin kokonaisluvun kompleksikonjugaatin tiedetään Lauseen 1.3 perusteella olevan Gaussin kokonaisluku, joten edelleen Lauseen 1.4 perusteella normi N on Gaussin kokonaisluku. Kyseinen havainto ei ole kuitenkaan jatkon kannalta merkittävä. Merkittävä ominaisuus sen sijaan on se, että normi N kiinnittää jokaiseen Gaussin kokonaislukuun ei-negatiivisen kokonaisluvun.

LEMMA 1.13. *Olkoon kuvaus N normi ja $z \in \mathbb{Z}[i]$. Tällöin*

(i) $N(z) \in \mathbb{Z}$ kaikilla $z \in \mathbb{Z}[i]$.

(ii) $N(z) \geq 0$ kaikilla $z \in \mathbb{Z}[i]$. Erityisesti $N(z) = 0$ jos ja vain jos $z = 0_{\mathbb{Z}[i]}$.

TODISTUS. Olkoon $z = a+ib$, missä $a, b \in \mathbb{Z}$, mikä tahansa Gaussin kokonaisluku.

(i) Koska $a, b \in \mathbb{Z}$, niin $a^2, b^2 \in \mathbb{Z}$, ja edelleen $a^2 + b^2 \in \mathbb{Z}$. Koska $a^2 + b^2 = N(z)$, niin $N(z) \in \mathbb{Z}$ kaikilla $z \in \mathbb{Z}[i]$.

(ii) Tiedetään, ettei minkään kokonaisluvun neliö ole negatiivinen eli $a^2 \geq 0$ ja $b^2 \geq 0$. Siten $N(z) = a^2 + b^2 \geq 0 + 0 = 0$ kaikilla $z \in \mathbb{Z}[i]$.

Näytetään vielä, että $N(z) = 0$ jos ja vain jos $z = 0_{\mathbb{Z}[i]}$. Oletetaan ensin, että $N(z) = 0$. Toisaalta tiedetään, että $N(z) = a^2 + b^2$. Siispä $a^2 + b^2 = 0$ eli $a^2 = -b^2$. Yhtälö on totta vain silloin kun $a = 0$ ja $b = 0$. Siten $z = a + ib = 0 + i0 = 0_{\mathbb{Z}[i]}$.
Oletaan sitten, että $z = 0_{\mathbb{Z}[i]}$. Tällöin $N(z) = 0^2 + 0^2 = 0$.

□

Jatkossa tullaan huomaamaan, että normi N toteuttaa monia hyödyllisiä tuloksia. Tämän vuoksi se onkin tärkeä apuväline monissa sovelluksissa ja tutkielman edetessä sitä hyödynnetään useita kertoja. Esitellään seuraavaksi yksi aputulos, jota tarvitaan, kun näytetään, että Gaussin kokonaislukujen rengas on Euklidinen.

LEMMA 1.14. *Olkoot kuvaus N normi ja $z, w \in \mathbb{Z}[i]$. Tällöin*

$$N(zw) = N(z)N(w).$$

TODISTUS. Olkoot $z = a_1 + ib_1$ ja $w = a_2 + ib_2$. Nyt

$$\begin{aligned} N(zw) &= N((a_1a_2 - b_1b_2) + i(a_1b_2 + b_1a_2)) = (a_1a_2 - b_1b_2)^2 + (a_1b_2 + b_1a_2)^2 \\ &= (a_1a_2)^2 - 2a_1a_2b_1b_2 + (b_1b_2)^2 + (a_1b_2)^2 + 2a_1a_2b_1b_2 + (a_2b_1)^2 \\ &= {a_1}^2{a_2}^2 + {b_1}^2{b_2}^2 + {a_1}^2{b_2}^2 + {a_2}^2{b_1}^2 = {a_1}^2({a_2}^2 + {b_2}^2) + {b_1}^2({a_2}^2 + {b_2}^2) \\ &= ({a_1}^2 + {b_1}^2)({a_2}^2 + {b_2}^2) = N(z)N(w). \end{aligned}$$

□

Nyt voidaan näyttää, että normi N toteuttaa Määritelmän 1.11 ehdot eli todistaa, että rengas $\mathbb{Z}[i]$ on Euklidinen.

LAUSE 1.15. *Gaussin kokonaislukujen rengas on Euklidinen.*

TODISTUS. Gaussin kokonaislukujen rengas on jo perusteltu kokonaisalueeksi. Riittää näyttää, että mille tahansa $a, b \in \mathbb{Z}[i]$, $a \neq 0$, on olemassa $\tilde{q}, \tilde{r} \in \mathbb{Z}[i]$ niin, että

$$b = \tilde{q}a + \tilde{r} \qquad \text{ja} \qquad N(\tilde{r}) < N(a).$$

Hyödynnetään lukua $ba^{-1} = p + si$, missä $p, s \in \mathbb{Q}$. Useimmissa tapauksissa tämä ei ole Gaussin kokonaisluku, sillä käänteisluku a^{-1} on harvoin Gaussin kokonaisluku. Sopivalla valinnalla luvun $ba^{-1} = p + si$ avulla voidaan kuitenkin löytää luku, joka on varmasti Gaussin kokonaisluku. Tämä onnistuu ottamalla luvun ba^{-1} kertoimien p ja s läheltä kokonaisluvut ja valitsemalla nämä halutun luvun kertoimiksi. Valitaan siis luvut $\alpha, \beta \in \mathbb{Z}$ siten, että

$$|p - \alpha| \leq \frac{1}{2} \qquad \text{ja} \qquad |s - \beta| \leq \frac{1}{2}.$$

Olkoon nyt $\tilde{q} = \alpha + \beta i$ kyseinen Gaussin kokonaisluku ja valitaan tarvittava toinen luku niin, että $\tilde{r} = b - (\alpha + \beta i)a$. Koska $\alpha, \beta \in \mathbb{Z}$ ja $a, b \in \mathbb{Z}[i]$, niin myös luku $\tilde{r}$ on Gaussin kokonaisluku, kuten halutaan. Pienellä muokkauksella luvun $\tilde{r}$ valinnasta nähdään helposti, että ensimmäinen ehto

$$b = \tilde{q}a + \tilde{r}$$

todella pätee. Täytyy siis enää osoittaa, että myös jälkimmäinen ehto

$$N(\tilde{r}) < N(a)$$

on voimassa äsken tehdyillä valinnoilla. Tämä onnistuu mekaanisella pyörittelyllä Lemmaa 1.14 hyödyntäen:

$$\begin{aligned}
N(\tilde{r}) &= N(b-(\alpha+\beta i)a) = N(b-\alpha a-\beta i a)\\
&= N(ba^{-1}a-\alpha a-\beta i a) = N((ba^{-1}-\alpha-\beta i)a)\\
&= N((ba^{-1}-\alpha-\beta i))N(a) = N((p+si-\alpha-\beta i))N(a)\\
&= N((p-\alpha+(s-\beta)i))N(a) = ((p-\alpha)^2+(s-\beta)^2)N(a)\\
&= (|p-\alpha|^2+|s-\beta|^2)N(a) \leq \left(\frac{1}{4}+\frac{1}{4}\right)N(a)\\
&= \frac{1}{2}N(a) < N(a).
\end{aligned}$$

Siispä myös jälkimmäinen ehto pätee.

□

Nyt on näytetty, että rengas $\mathbb{Z}[i]$ on Euklidinen. Seuraavassa luvussa tarkastellaan lähemmin Eukleideen algoritmia ja muita lukuteorian tuloksia Gaussin kokonaisluvuille.

LUKU 2

Lukuteoriaa Gaussin kokonaisluvuille

Tässä luvussa tarkastellaan Gaussin kokonaislukujen lukuteoreettisia ominaisuuksia. Lähdetään liikkeelle lukuteorian perusteista Gaussin kokonaisluvuille ja syvennytään sitten Eukleideen algoritmiin ja lukuteorian tuloksiin, jotka se mahdollistaa Gaussin kokonaisluvuille. Tällaisia ovat esimerkiksi suurimman yhteisen tekijän löytäminen, Bézout'n lemma ja aritmetiikan peruslause.

2.1. Gaussin kokonaislukujen jaollisuus, yksiköt ja liittolaiset

Aloitetaan lukuteorian perusominaisuuksista ja siitä, miltä ne näyttävät Gaussin kokonaisluvuille.

MÄÄRITELMÄ 2.1. Gaussin kokonaisluku z on *jaollinen* Gaussin kokonaisluvulla w, $w \neq 0$, jos on olemassa Gaussin kokonaisluku k siten, että $z = kw$. Tällöin lukua w kutsutaan luvun z *jakajaksi*.

Jaollisuudella tarkoitetaan siis Gaussin kokonaislukujen joukossa samaa kuin tavallisten kokonaislukujen joukossa. Siten on luontevaa käyttää samaa merkintää: jos luku w jakaa luvun z, niin se voidaan lyhentää kirjoittamalla $w \mid z$. Myös seuraava tavallisille kokonaisluvuille tuttu jaollisuusominaisuus yleistyy koskemaan kaikkia Gaussin kokonaislukuja.

LAUSE 2.2. *Olkoot* $z_1, z_2, z_3 \in \mathbb{Z}[i]$. *Jos* $z_1 \mid z_2$ *ja* $z_2 \mid z_3$, *niin* $z_1 \mid z_3$.

TODISTUS. Koska $z_1 \mid z_2$, niin on olemassa $k \in \mathbb{Z}[i]$ siten, että $z_2 = kz_1$. Vastaavasti tiedetään, että on olemassa $l \in \mathbb{Z}[i]$ siten, että $z_3 = lz_2$. Nyt

$$z_3 = lz_2 = lkz_1 = mz_1,$$

missä $m = lk$. Luvut l ja k ovat Gaussin kokonaislukuja, joten Lauseen 1.4 nojalla myös luku m on Gaussin kokonaisluku. Siispä $z_1 \mid z_3$.

□

Renkaan $\mathbb{Z}[i]$ Euklidiseksi perustelussa näytettiin, että mille tahansa $a, b \in \mathbb{Z}[i]$, $a \neq 0$, on olemassa $\tilde{q}, \tilde{r} \in \mathbb{Z}[i]$ niin, että

$$b = \tilde{q}a + \tilde{r} \qquad \text{ja} \qquad N(\tilde{r}) < N(a).$$

Tämä voidaan nyt purkaa auki sanalliseen muotoon esimerkiksi seuraavalla tavalla. Kun luku b jaetaan luvulla a, saadaan $\tilde{q}$ kokonaista ja jakojäännös $\tilde{r}$. Kuten kokonaislukujen joukossakin, myös Gaussin kokonaislukujen joukossa Eukleideen algoritmissa jakojäännöksen $\tilde{r}$ tulee olla pienempi kuin luku a. Tästä normi N pitää huolen, sillä

sen avulla voidaan kuvata Gaussin kokonaislukujen suuruutta, mitä käsitellään tarkemmin luvussa 5. Algoritmia on siten luontevaa jatkaa eli seuraavaksi jaettaisiin luku a jakojäännöksellä $\tilde{r}$. Tähän palataan edempänä.

Edellisessä luvussa todettiin jo, että alkulukujen määritelmä yleistyy Gaussin kokonaisluvuille. Ennen alkulukujen luontevaa määrittelyä tutustaan kuitenkin vielä Gaussin kokonaislukujen yksiköihin ja liittolaisiin.

MÄÄRITELMÄ 2.3. Gaussin kokonaisluku on *yksikkö*, jos se jakaa luvun 1.

Lauseessa 2.5 osoitetaan, että Määritelmän 2.3 toteuttavia lukuja ovat luvut -1, 1, i ja $-i$. Gaussin kokonaislukujen joukossa on siten neljä yksikköä. Tavallisten kokonaislukujen joukossa yksiköitä ovat vain luvut -1 ja 1. Tarkastellaan seuraavaksi Gaussin kokonaislukujen yksiköiden ja normin N välistä yhteyttä.

LAUSE 2.4. *Gaussin kokonaisluku μ on yksikkö renkaassa $\mathbb{Z}[i]$ jos ja vain jos*

$$N(\mu) = 1.$$

TODISTUS. Olkoon Gaussin kokonaisluku μ yksikkö. Siispä luku μ jakaa luvun 1 eli $\mu \mid 1$. On siis olemassa $k \in \mathbb{Z}[i]$ niin, että $1 = k\mu$. Nyt

$$N(1) = N(k\mu) = N(k)N(\mu).$$

Toisaalta $N(1) = 1^2 + 0^2 = 1$, joten

$$N(k)N(\mu) = 1.$$

Luvut $N(k)$ ja $N(\mu)$ ovat kokonaislukuja, joten ne ovat myös Gaussin kokonaislukuja. Näin ollen $N(\mu) \mid 1$. Toisaalta Lemman 1.13 perusteella tiedetään, että normin N arvot ovat positiivisia kokonaislukuja. Luku 1 on ainut positiivinen kokonaisluku, joka jakaa luvun 1, joten on oltava $N(\mu) = 1$.

Näytetään vielä väitteen toinen suunta. Olkoon $N(\mu) = 1$ ja merkitään $\mu = a + ib$. Tällöin saadaan

$$1 = N(\mu) = a^2 + b^2 = a^2 - (-1)b^2 = a^2 - i^2b^2 = a^2 - (ib)^2 = (a - ib)(a + ib).$$

Luvut $a - ib$ ja $a + ib$ ovat Gaussin kokonaislukuja, joten nähdään, että $a + ib \mid 1$ eli $\mu \mid 1$. Siispä μ on yksikkö.

□

Nyt voidaan helposti perustella, miksi jo mainitut luvut -1, 1, i ja $-i$ todella ovat Gaussin kokonaislukujen joukon yksiköt.

LAUSE 2.5. *Renkaassa $\mathbb{Z}[i]$ yksiköitä ovat luvut -1, 1, i ja $-i$.*

TODISTUS. Olkoon Gaussin kokonaisluku $\mu = a + ib$ yksikkö. Siispä Lauseen 2.4 perusteella $N(\mu) = 1$. Kun yhdistetään tämä tieto normin N Määritelmään 1.12, saadaan yhtälö

$$a^2 + b^2 = 1,$$

missä luvut a ja b ovat kokonaislukuja. Yhtälön mahdolliset kokonaislukuratkaisut ovat joko

$$a = \pm 1 \quad \text{ja} \quad b = 0 \qquad \text{tai} \qquad a = 0 \quad \text{ja} \quad b = \pm 1.$$

Ratkaisuja on siten neljä ja ne ovat luvut -1, 1, i ja $-i$.

□

Yksiköiden avulla voidaan määritellä aikaisemmin mainitut liittolaiset Gaussin kokonaisluvuille.

MÄÄRITELMÄ 2.6. Olkoot $z \in \mathbb{Z}[i]$ mikä tahansa ja $\mu \in \mathbb{Z}[i]$ jokin yksiköistä. Tällöin sanotaan, että luku μz on *liittoutunut* luvun z kanssa. Luvun z *liittolaisia* ovat luvut z, iz, $-z$ ja $-iz$.

Yksiköt ja liittolaiset ovat Gaussin kokonaislukujen triviaaleja jakajia. Jokaisella Gaussin kokonaisluvulla z, joka ei ole yksikkö, on siis yhteensä kahdeksan triviaalia jakajaa, luvut -1, 1, i, $-i$, z, $-z$, iz ja $-iz$. Tavallisella kokonaisluvulla k triviaaleja jakajia on vain neljä, luvut -1, 1, k ja $-k$.

LAUSE 2.7. *Olkoot $z_1, z_2 \in \mathbb{Z}[i]$, ja $\mu_1, \mu_2 \in \mathbb{Z}[i]$ mitkä tahansa yksiköt. Jos $z_1 \mid z_2$, niin $z_1\mu_1 \mid z_2\mu_2$.*

TODISTUS. Koska $z_1 \mid z_2$, niin on olemassa $k \in \mathbb{Z}[i]$ siten, että $z_2 = kz_1$. Lisäksi tiedetään, että on olemassa $l, m \in \mathbb{Z}[i]$, niin että $1 = l\mu_1$ ja $1 = m\mu_2$. Nyt

$$z_2 = kz_1 = 1kz_1 = l\mu_1 kz_1 = 1lk\mu_1 z_1 = m\mu_2 lk\mu_1 z_1.$$

Toisaalta $z_2 = 1z_2 = m\mu_2 z_2$, joten saadaan yhtälö

$$m\mu_2 z_2 = m\mu_2 lk\mu_1 z_1.$$

Tämä voidaan kirjoittaa yhtäpitävästi muodossa

$$m(\mu_2 z_2 - \mu_2 lk\mu_1 z_1) = 0_{\mathbb{Z}[i]}.$$

Rengas $\mathbb{Z}[i]$ on kokonaisalue, joten nyt

$$m = 0_{\mathbb{Z}[i]} \qquad \text{tai} \qquad \mu_2 z_2 - \mu_2 lk\mu_1 z_1 = 0_{\mathbb{Z}[i]}.$$

Vaihtoehto $m = 0_{\mathbb{Z}[i]}$ ei ole mahdollinen, koska tällöin luku μ_2 ei olisi yksikkö. Siten on oltava $\mu_2 z_2 - \mu_2 lk\mu_1 z_1 = 0_{\mathbb{Z}[i]}$ ja tästä saadaan yhtälö

$$\mu_2 z_2 = \mu_2 lk\mu_1 z_1.$$

Gaussin kokonaislukujen tulona $\mu_2 lk \in \mathbb{Z}[i]$, joten $\mu_1 z_1 \mid \mu_2 z_2$.

□

Tiedetään siis, että mikäli Gaussin kokonaisluku z_1 jakaa Gaussin kokonaisluvun z_2, niin tällöin luvun z_1 mikä tahansa liittolainen jakaa minkä tahansa luvun z_2 liittolaisen.

2.2. Gaussin alkuluvut ja alkutekijäesitys

Määritellään seuraavaksi alkuluvut Gaussin kokonaislukujen joukossa. Käytetään näistä jatkossa nimitystä Gaussin alkuluvut. Määritelmä poikkeaa hieman siitä, mihin tavallisten kokonaislukujen keskuudessa ollaan totuttu.

MÄÄRITELMÄ 2.8. Olkoon $\rho \in \mathbb{Z}[i]$, $\rho \neq 0, \rho \neq 1$. Luku ρ on *Gaussin alkuluku*, jos se on jaollinen vain liittolaisillaan ja yksiköillä.

HUOMAUTUS 2.9. Myös Gaussin alkuluvun liittolaiset ovat selvästi Gaussin alkulukuja.

Vastaavalla tavalla voidaan määritellä myös tavallisten kokonaislukujen alkuluvut. Joukon $\mathbb{Z}$ alkulukujen tuntemuksella saadaan hyvä pohja joukon $\mathbb{Z}[i]$ alkuluvuille. Seuraava lause on tärkeä, sillä se luo normin N avulla yhteyden joukkojen $\mathbb{Z}$ ja $\mathbb{Z}[i]$ alkulukujen välille. Sen avulla voidaan esimerkiksi helposti näyttää tietyissä tapauksissa, onko jokin luku Gaussin alkuluku.

LAUSE 2.10. *Jos normi N kuvaa Gaussin kokonaisluvun z alkuluvuksi, niin luku z on Gaussin alkuluku.*

TODISTUS. Oletetaan, että $N(z) = p$, missä $z \in \mathbb{Z}[i]$ ja $p \in \mathbb{Z}$ on alkuluku joukossa $\mathbb{Z}$. Oletetaan lisäksi, että $z = z_1 z_2$. Nyt Lemman 1.14 avulla

$$p = N(z) = N(z_1 z_2) = N(z_1)N(z_2).$$

Koska p on alkuluku, niin joko

$$N(z_1) = 1 \qquad \text{tai} \qquad N(z_2) = 1.$$

Siten Lauseen 2.4 nojalla jompi kumpi luvuista z_1 ja z_2 on yksikkö. Lisäksi nähdään, että luvuista z_1 ja z_2 se, joka ei ole yksikkö, on liittolainen luvulle $z = z_1 z_2$. Siispä luku z on Gaussin alkuluku.

□

Katsotaan seuraavaksi esimerkkejä, joissa näytetään Lauseen 2.10 avulla, että Gaussin kokonaisluku on Gaussin alkuluku.

ESIMERKKI 2.11. (a) Tarkastellaan lukua $z = 2 + i \in \mathbb{Z}[i]$. Tällöin

$$N(z) = N(2 + i) = 2^2 + 1^2 = 5.$$

Koska luku 5 on alkuluku joukossa $\mathbb{Z}$, Lauseen 2.10 nojalla luku $2 + i$ on Gaussin alkuluku.

(b) Näytetään, että luku $z = 3 + 2i \in \mathbb{Z}[i]$ on Gaussin alkuluku. Nyt

$$N(z) = N(3 + 2i) = 3^2 + 2^2 = 9 + 4 = 13.$$

Koska luku 13 on alkuluku joukossa $\mathbb{Z}$, Lauseen 2.10 perusteella luku $3+2i$ on Gaussin alkuluku.

Matemaattisesti mielenkiintoista on se, kuinka alkuluvut vastaavat toisiaan joukoissa $\mathbb{Z}$ ja $\mathbb{Z}[i]$. Jos jokin tavallinen kokonaisluku on alkuluku joukossa $\mathbb{Z}[i]$, niin se on alkuluku myös joukossa $\mathbb{Z}$. Joukon $\mathbb{Z}$ alkuluvut sen sijaan eivät välttämättä ole alkulukuja joukossa $\mathbb{Z}[i]$. Esimerkiksi luku 5 on alkuluku joukossa $\mathbb{Z}$, mutta $5 = (2+i)(2-i)$, joten se ei ole Gaussin alkuluku. Vastaavasti luku 2 on alkuluku joukossa $\mathbb{Z}$, mutta $2 = (1+i)(1-i)$, joten se ei ole alkuluku joukossa $\mathbb{Z}[i]$.

Erityisen mielenkiintoisen normista N tekisi se, että se kuvaisi alkuluvun alkuluvuksi. Jotta näin olisi, tulisi Lauseen 2.10 olla voimassa käänteiseen suuntaan. Tiedosta, että luku $\rho \in \mathbb{Z}[i]$ on alkuluku joukossa $\mathbb{Z}[i]$, tulisi siis seurata, että luku $N(\rho) \in \mathbb{Z}$ on alkuluku joukossa $\mathbb{Z}$. Näin ei kuitenkaan aina ole, sillä esimerkiksi luku 3 on Gaussin alkuluku ja $N(3) = 3^2 + 0^2 = 9$, mutta luku 9 ei ole alkuluku. Luku 3 perustellaan Gaussin alkuluvuksi Esimerkissä 3.1. Lisäksi tarkka karakterisointi kaikille Gaussin alkuluvuille annetaan Lauseessa 3.12.

Tutustutaan vielä erääseen aputulokseen ennen kuin määritellään alkutekijäesitys Gaussin kokonaisluvuille.

LEMMA 2.12. *Mikä tahansa Gaussin kokonaisluku, joka ei ole nolla tai yksikkö, on jaollinen jollain Gaussin alkuluvulla.*

TODISTUS. Olkoon Gaussin kokonaisluku z mikä tahansa siten, että $z \neq 0_{\mathbb{Z}[i]}$ ja z ei ole yksikkö. Jos luku z on Gaussin alkuluku, niin väite on selvä.

Oletaan sitten, että luku z ei ole Gaussin alkuluku. Tällöin se voidaan kirjoittaa muodossa

$$z = y_1 w_1,$$

missä luvut y_1 ja w_1 ovat nollasta eroavia Gaussin kokonaislukuja niin, ettei kumpikaan ole yksikkö tai luvun z liittolainen. Lemman 1.13 ja Lauseen 2.4 perusteella tiedetään, että tällöin

$$N(y_1) > 1 \qquad \text{ja} \qquad N(w_1) > 1.$$

Lisäksi Lemman 1.14 perusteella

$$N(z) = N(y_1 w_1) = N(y_1)N(w_1),$$

joten voidaan kirjoittaa seuraavasti

$$1 < N(y_1) < N(y_1)N(w_1) = N(z).$$

Jos luku y_1 on Gaussin alkuluku, niin väite on selvä. Oletetaan siis, että y_1 ei ole Gaussin alkuluku, jolloin se voidaan edelleen kirjoittaa muodossa

$$y_1 = y_2 w_2,$$

missä $y_2, w_2 \in \mathbb{Z}[i]$ ja $y_2, w_2 \neq 0_{\mathbb{Z}[i]}$. Lisäksi voidaan olettaa, ettei kumpikaan luvuista y_2 ja w_2 ole yksikkö tai luvun y_1 liittolainen. Nyt siis

$$N(y_2) > 1 \qquad \text{ja} \qquad N(w_2) > 1$$

ja edelleen saadaan

$$1 < N(y_2) < N(y_2)N(w_2) = N(y_2 w_2) = N(y_1).$$

Oletetaan taas, että luku y_2 ei ole Gaussin alkuluku ja jatketaan prosessia samalla tavalla kuin edellä. Tällöin saadaan Gaussin kokonaisluvut $y_3, y_4, \ldots$ ja näille pätee

$$N(z) > N(y_1) > N(y_2) > N(y_3) > N(y_4) > \ldots > 1.$$

Lukujono $N(z), N(y_1), N(y_2), N(y_3), N(y_4), \ldots$ on siten aidosti vähenevä ja lisäksi se koostuu positiivisista kokonaisluvuista. Se ei siis voi pienentyä rajatta ja väistämättä nyt jollain $n \in \mathbb{N}$ luku $N(y_n)$ on alkuluku ja tällöin Lauseen 2.10 nojalla luku y_n Gaussin alkuluku. Koska nyt

$$z = y_1 w_1 = y_2 w_2 w_1 = \cdots = y_n w_n \cdots w_2 w_1,$$

on luku z jaollinen Gaussin alkuluvulla.

□

Esimerkki 2.13. Tutkitaan Gaussin kokonaislukua $-2+24i$ ja annetaan jokin Gaussin alkuluku z siten, että $z \mid (-2+24i)$. Olkoon $z = 2+5i \in \mathbb{Z}[i]$. Luku z jakaa luvun $-2+24i$, sillä

$$-2 + 24i = (4 + 2i)(2 + 5i),$$

missä $4 + 2i \in \mathbb{Z}[i]$. Lisäksi voidaan huomata, että

$$N(2 + 5i) = 2^2 + 5^2 = 4 + 25 = 29.$$

Tiedetään, että luku 29 on alkuluku, joten Lauseen 2.10 nojalla luku $z = 2 + 5i$ on Gaussin alkuluku.

Äskeisessä esimerkissä Gaussin kokonaisluku kirjoitettiin tulomuodossa, jossa on ainakin yksi Gaussin alkuluku. Kun Gaussin kokonaisluku kirjoitetaan pelkästään Gaussin alkulukujen tulona, saadaan Gaussin kokonaisluvun alkutekijäesitys. Kyseinen alkutekijäesitys vastaa oleellisesti kokonaisluvuille tuttua alkutekijäesitystä.

Lause 2.14. *Jokainen Gaussin kokonaisluku, joka ei ole nolla tai yksikkö, voidaan kirjoittaa Gaussin alkulukujen tulona.*

Todistus. Olkoon luku z jokin Gaussin kokonaisluku siten, ettei se ole nolla tai yksikkö. Nyt Lemman 2.12 perusteella on olemassa Gaussin alkuluku ρ_1 niin, että

$$z = \rho_1 z_1,$$

missä $z_1 \in \mathbb{Z}[i]$ ja nyt $N(z_1) < N(z)$. Jos luku z_1 on yksikkö, niin väite on selvä.

Jos luku z_1 ei ole yksikkö, voidaan edelleen Lemman 2.12 perusteella kirjoittaa

$$z_1 = \rho_2 z_2,$$

missä ρ_2 on Gaussin alkuluku ja $z_2 \in \mathbb{Z}[i]$. Lisäksi $N(z_2) < N(z_1)$. Jos nyt luku z_2 on yksikkö, niin väite on selvä, koska tällöin $z = \rho_1 \rho_2 z_2$.

Mikäli luku z_2 ei ole yksikkö, jatketaan prosessia vastaavalla tavalla. Saadaan luvut $z_3, z_4, \ldots$, joille

$$N(z) > N(z_1) > N(z_2) > N(z_3) > N(z_4) > \ldots.$$

Tällöin lukujono $N(z), N(z_1), N(z_2), N(z_3), N(z_4), \ldots$ on aidosti vähenevä ja se koostuu positiivisista kokonaisluvuista. Sille on siis olemassa jokin alaraja ja siten myös jollekin $n \in \mathbb{N}$ pätee

$$N(z_n) = 1.$$

Lauseen 2.4 perusteella luku z_n on yksikkö ja tällöin luku z voidaan kirjoittaa alkulukujen tulona seuraavasti

$$z = \rho_1 \rho_2 \cdots \rho_n z_n.$$

□

ESIMERKKI 2.15. Tutkitaan taas Gaussin kokonaislukua $-2 + 24i = (4 + 2i)(2 + 5i)$ ja esitetään se tällä kertaa pelkästään Gaussin alkulukujen tulona.

Lauseen 2.10 perusteella ei tiedetä, onko luku $4 + 2i$ Gaussin alkuluku, sillä

$$N(4 + 2i) = 4^2 + 2^2 = 16 + 4 = 20$$

eikä luku 20 ole alkuluku. Huomataan kuitenkin, että

$$4 + 2i = 2(2 + i) = (1 + i)(1 - i)(2 + i).$$

Näytetään vielä, että saatu muoto koostuu Gaussin alkuluvuista. Nyt

$$N(1 \pm i) = 1^2 + (\pm 1)^2 = 2 \qquad \text{ja} \qquad N(2 + i) = 2^2 + 1^2 = 5.$$

Koska luvut 2 ja 5 ovat alkulukuja, niin luvut $1 + i$, $1 - i$ ja $2 + i$ ovat Gaussin alkulukuja. Siispä luvun $-2 + 24i$ alkutekijäesitys on

$$-2 + 24i = (1 + i)(1 - i)(2 + i)(2 + 5i).$$

2.3. Suurin yhteinen tekijä, aritmetiikan peruslause ja Bézout'n lemma

Vastaavasti kuin kokonaisluvuille, alkutekijäesitys on oleellisesti yksikäsitteinen myös Gaussin kokonaisluvuille. Kyseinen tulos on aritmetiikan peruslause Gaussin kokonaisluvuille ja se vastaa kokonaisluvuille tuttua aritmetiikan peruslausetta. Ennen sen todistamista tarvitaan muutama aputulos. Tarkastellaan ensin, mitä Gaussin kokonaislukujen suurimmalla yhteisellä tekijällä tarkoitetaan.

MÄÄRITELMÄ 2.16. Jos Gaussin kokonaisluku ζ on yhteinen jakaja luvuille $z, w \in \mathbb{Z}[i]$ ja jokainen lukujen z ja w yhteinen jakaja on jakaja myös luvulle ζ, niin lukua ζ kutsutaan lukujen z ja w *suurimmaksi yhteiseksi tekijäksi* ja tällöin merkitään $(z, w) = \zeta$.

Gaussin kokonaislukujen z ja w, $z, w \neq 0_{\mathbb{Z}[i]}$, suurin yhteinen tekijä löydetään Eukleideen algoritmin avulla seuraavasti. Tiedetään, että on olemassa $q_1, r_1 \in \mathbb{Z}[i]$ siten, että

$$z = q_1 w + r_1 \qquad \text{ja} \qquad N(r_1) < N(w).$$

Jos nyt $r_1 \neq 0_{\mathbb{Z}[i]}$, niin jatketaan edelleen, jolloin on olemassa $q_2, r_2 \in \mathbb{Z}[i]$ siten, että

$$w = q_2 r_1 + r_2 \qquad \text{ja} \qquad N(r_2) < N(r_1).$$

Oletaan taas, että $r_2 \neq 0_{\mathbb{Z}[i]}$, jolloin saadaan luvut $q_3, r_3 \in \mathbb{Z}[i]$ siten, että

$$r_1 = q_3 r_2 + r_3 \qquad \text{ja} \qquad N(r_3) < N(r_2).$$

Jos edelleen luku $r_3 \neq 0_{\mathbb{Z}[i]}$, jatketaan vastaavalla tavalla. Saadaan aidosti vähenevä lukujono $N(w), N(r_1), N(r_2), N(r_3) \ldots$, joka koostuu ei-negatiivisista kokonaisluvuista. Siten on olemassa $n \in \mathbb{N}$, jolle

$$N(r_{n+1}) = 0.$$

Lemman 1.13 perusteella $r_{n+1} = 0_{\mathbb{Z}[i]}$. Tällöin Eukleideen algoritmin viimeiset vaiheet ovat seuraavat

$$r_{n-2} = q_n r_{n-1} + r_n$$

ja

$$r_{n-1} = q_{n+1} r_n + r_{n+1} = q_{n+1} r_n.$$

Näytetään vielä, että Eukleideen algoritmin viimeisessä vaiheessa saatu luku r_n on lukujen z ja w suurin yhteinen tekijä. Olkoon luku ζ lukujen z ja w yhteinen jakaja. Koska nyt $\zeta \mid z$ ja $\zeta \mid w$, saadaan algoritmin ensimmäisen vaiheen perusteella, että $\zeta \mid r_1$. Tällöin toisesta vaiheesta saadaan $\zeta \mid r_2$, jolloin edelleen kolmannesta vaiheesta saadaan $\zeta \mid r_3$. Jatkamalla vastaavasti, saadaan lopulta, että $\zeta \mid r_n$.

Toisaalta, kun lähdetään liikkeelle algoritmin viimeisestä rivistä, nähdään, että $r_n \mid r_{n-1}$. Siten toiseksi viimeisen rivin perusteella $r_n \mid r_{n-2}$ ja edelleen $r_n \mid r_{n-3}$. Näin jatkamalla algoritmin toisen ja ensimmäisen rivin perusteella nähdään, että $r_n \mid w$ ja $r_n \mid z$. Siispä luku r_n on lukujen z ja w yhteinen jakaja. Siten luku r_n todella on suurin yhteinen tekijä luvuille z ja w. Lisäksi voidaan huomata, että myös luvun r_n liittolaiset ovat suurimpia yhteisiä tekijöitä luvuille z ja w. Suurin yhteinen tekijä ei siten ole täysin yksikäsitteinen, mutta liittolaisia lukuunottamatta se on. Lisäksi suurimmalle yhteiselle tekijälle pätevät seuraavat tulokset.

LEMMA 2.17. *Olkoot $\gamma, z, w \in \mathbb{Z}[i]$. Jos $\gamma \mid z$ ja $\gamma \mid w$, niin $\gamma \mid (z, w)$.*

TODISTUS. Oletusten nojalla nähdään helposti, että γ on lukujen z ja w yhteinen jakaja. Jos nyt $\gamma = (z, w)$, niin väite on selvä.

Jos $\gamma \neq (z, w)$, niin merkitään lukujen z ja w suurinta yhteistä tekijää luvulla ζ. Nyt suurimman yhteisen tekijän määritelmän nojalla $\gamma \mid \zeta$, joten tällöinkin väite pätee.

□

LEMMA 2.18. *Olkoot $z, v, w \in \mathbb{Z}[i]$. Jos $(z, v) = 1$ ja $v \mid zw$, niin $v \mid w$.*

TODISTUS. Käytetään todistuksessa apuna Eukleideen algoritmia luvuille z ja w. Oletuksen nojalla $r_n = 1$. Kerrotaan jokainen algoritmin rivi luvulla w.

$$zw = q_1 vw + r_1 w$$
$$vw = q_2 r_1 w + r_2 w$$
$$r_1 w = q_3 r_2 w + r_3 w$$
$$\dots$$
$$r_{n-2} w = q_n r_{n-1} w + w$$
$$r_{n-1} w = q_{n+1} w$$

Tällöin saadaan Eukleideen algoritmi luvuille zw ja vw. Tästä nähdään, että

$$(zw, vw) = w.$$

Oletuksen nojalla tiedetään, että $v \mid zw$. Lisäksi selvästi pätee, että $v \mid vw$. Nyt Lemman 2.17 nojalla $v \mid (zw, vw)$. Siten todella $v \mid w$.

□

Eukleideen lemmana tunnettu lukuteorian tulos yleistyy Gaussin kokonaisluvuille.

LAUSE 2.19. *Jos ρ on Gaussin alkuluku, joka jakaa luvun $\alpha\beta \in \mathbb{Z}[i]$, niin luku ρ jakaa luvun α tai β.*

TODISTUS. Oletuksen nojalla $\rho \mid \alpha\beta$. Jos $\rho \mid \alpha$, niin väite on selvä.

Jos taas $\rho \nmid \alpha$, niin $(\rho, \alpha) = 1$. Koska nyt $\rho \mid \alpha\beta$ ja $(\rho, \alpha) = 1$, Lemman 2.18 nojalla $\rho \mid \beta$. Siten väite pätee tässäkin tapauksessa.

□

Nyt voidaan viimein todistaa aritmetiikan peruslause Gaussin kokonaisluvuille.

LAUSE 2.20. *Gaussin kokonaisluvun alkutekijäesitys $z = \rho_1^{a_1}\rho_2^{a_2}\cdots\rho_n^{a_n}$ Gaussin alkulukujen $\rho_1, \rho_2, \ldots \rho_n$ tulona on yksikäsitteinen lukuun ottamatta Gaussin alkulukujen järjestystä, yksiköitä ja liittolaisia.*

TODISTUS. Näytetään alkutekijäesityksen yksikäsitteisyys. Olkoot

$$z = \rho_1^{a_1}\rho_2^{a_2}\cdots\rho_n^{a_n} = \beta_1^{b_1}\beta_2^{b_2}\cdots\beta_k^{b_k}$$

Gaussin kokonaisluvun z alkutekijäesityksiä. Nähdään, että kaikille $i = 1, \ldots, n$ on voimassa, että

$$\rho_i \mid \beta_1^{b_1}\beta_2^{b_2}\cdots\beta_k^{b_k}.$$

Eukleideen lemmasta eli Lauseesta 2.19 seuraa, että kaikille luvuille ρ_i, missä siis $i = 1, \ldots, n$, pätee, että luku ρ_i jakaa luvun $\beta_j^{b_j}$ tai jonkun sen liittolaisen jollain $j = 1, \ldots, k$. Käyttämällä Eukleideen lemmaa uudelleen saadaan, että luku ρ_i jakaa luvun β_j tai sen liittolaisen. Aritmetiikan peruslauseen muotoilun perusteella voidaan yksinkertaisuuden vuoksi olettaa, että $\rho_i \mid \beta_j$. Koska luvut ρ_i ja β_j ovat Gaussin alkulukuja, niin nyt saadaan, että kaikille $i = 1, \ldots, n$ on olemassa β_j siten, että $\rho_i = \beta_j$, missä $j = 1, \ldots, k$.

Vastaavasti nähdään, että kaikille $j = 1, \ldots, k$ pätee,

$$\beta_j \mid \rho_1^{a_1}\rho_2^{a_2}\cdots\rho_n^{a_n},$$

joten luku β_j jakaa luvun $\rho_i^{a_i}$ tai jonkun sen liittolaisen jollain $i = 1, \ldots, n$. Edelleen β_j jakaa luvun ρ_i tai sen liittolaisen jollain $i = 1, \ldots, n$. Tehdään jälleen yksinkertaisuuden vuoksi oletus, että $\beta_j \mid \rho_i$. Nähdään taas, että kaikille $j = 1, \ldots, k$ täytyy olla olemassa ρ_i siten, että $\beta_j = \rho_i$, missä $i = 1, \ldots, n$.

Siten täytyy olla $n = k$, joten järjestystä vaihtamalla voidaan olettaa, että $\rho_i = \beta_i$ kaikilla $i = 1, \ldots, n$. Alkutekijäesitykset näyttävät nyt seuraavalta

$$\rho_1^{a_1}\rho_2^{a_2}\cdots\rho_n^{a_n} = \rho_1^{b_1}\rho_2^{b_2}\cdots\rho_n^{b_n}.$$

Täytyy vielä näyttää, että kaikille $i = 1, \ldots, n$ pätee, että $a_i = b_i$, jotta alkutekijäesitys olisi yksikäsittäinen. Oletetaan, että näin ei ole, eli nyt joko $a_i < b_i$ tai $b_i > a_i$ jollakin $i = 1, \ldots, n$.

Jos $a_i > b_i$, niin alkutekijäesitykset voidaan jakaa luvulla $\rho_i^{b_i}$. Tällöin saadaan

$$\rho_1^{a_1}\rho_2^{a_2}\cdots\rho_i^{a_i-b_i}\cdots\rho_n^{a_n} = \rho_1^{b_1}\rho_2^{b_2}\cdots\rho_{i-1}^{b_{i-1}}\rho_{i+1}^{b_{i+1}}\cdots\rho_n^{b_n}.$$

Nyt saadusta yhtälöstä nähdään, että vasen puoli on jaollinen luvulla ρ_i, mutta yhtälön oikea puoli ei ole. Tämä on mahdotonta. Vastaavaan ristiriitaan päädytään

myös kun $b_i > a_i$, mutta tällöin yhtälö jaetaan puolittain luvulla $\rho_i^{a_i}$. Siispä täytyy olla $a_i = b_i$ kaikille $i = 1, \ldots, n$. Siten alkutekijäesitys todella on yksikäsitteinen.

□

Eukleideen algoritmin avulla voidaan näyttää, että Bézout'n lemmana tunnettu tulos pätee myös Gaussin kokonaisluvuille. Siinä esiintyvä yhtälö, jossa kahden Gaussin kokonaisluvun yhteinen tekijä on ilmoitettu kahden Gaussin kokonaisluvun lineaarikombinaationa, tunnetaan Bézout'n yhtälönä.

LAUSE 2.21. *Olkoot $z, w \in \mathbb{Z}[i]$ siten, että $(z, w) = \zeta$. Tällöin olemassa $\alpha, \beta \in \mathbb{Z}[i]$ niin, että $\zeta = \alpha z + \beta w$.*

TODISTUS. Käytetään apuna Eukleideen algoritmia ja lähdetään liikkeelle toiseksi viimeisestä vaiheesta. Nyt siis $\zeta = r_n$, joten

$$r_{n-2} = q_n r_{n-1} + \zeta.$$

Toisaalta tämä voidaan kirjoittaa yhtäpitävästi muodossa

$$\zeta = r_{n-2} - q_n r_{n-1}.$$

Pidetään tätä yhtälöä pohjana, kun hyödynnetään Eukleideen algoritmia takaisinpäin. Otetaan siis seuraavaksi avuksi algoritmin kolmanneksi viimeinen rivi

$$r_{n-3} = q_{n-1} r_{n-2} + r_{n-1}.$$

Ratkaistaan siitä luku r_{n-1} eli

$$r_{n-1} = r_{n-3} - q_{n-1} r_{n-2}$$

ja sijoitetaan tämä aikaisempaan yhtälöön. Saadaan

$$\zeta = r_{n-2} - q_n(r_{n-3} - q_{n-1} r_{n-2}).$$

Järjestelemällä tätä uudelleen, saadaan yhtälö muotoon

$$\zeta = (1 + q_n q_{n-1}) r_{n-2} - q_n r_{n-3}.$$

Merkitään nyt $\alpha_1 = 1 + q_n q_{n-1}$ ja $\beta_1 = -q_n$. Tällöin siis

$$\zeta = \alpha_1 r_{n-2} + \beta_1 r_{n-3}.$$

Tästä voidaan nyt nähdä, että hyödyntämällä Eukleideen algoritmin edellistä riviä ja järjestelemällä termejä uudelleen, saadaan i:nnen rivin yhtälöstä eliminoitua luku r_i. Tällöin yhtälö koostuu luvuista r_{i-2} ja r_{i-1} ja sama prosessi voidaan toistaa luvulle r_{i-1}.

Koska indeksi i ei pienene rajatta, päästään toistojen jälkeen lopulta tilanteeseen, jossa tehdään viimeinen sijoitus $r_1 = z - q_1 w$. Ottamalla yhteiseksi tekijäksi luvut z ja w sekä merkitsemällä niille saadut kokonaislukukertoimet luvuilla α ja β saadaan yhtälö muotoon

$$\zeta = \alpha z + \beta w.$$

Nyt ollaan siis löydetty Gaussin kokonaisluvut α ja β, joille Bézout'n yhtälö todella pätee.

□

LUKU 3

Neliöiden summat

Tässä luvussa tarkastellaan luonnollisten lukujen esittämistä neliöiden summina. Vaihdetaan siis tarkastelunäkökulmaa eli lähdetään tutkimaan lukuteorian tuloksia tavallisille luvuille ja hyödynnetään todistuksissa kokonaislukujen kompleksisia laajennuksia. Aluksi käytetään jo tutuksi tulleita Gaussin kokonaislukuja ja sen jälkeen hyödynnetään Hurwitzin kokonaislukuja.

3.1. Yleistä neliöiden summista

Edellisessä luvussa esiteltiin Gaussin alkuluvuksi todistamiselle helppo keino Lauseen 2.10 avulla. Luku 3 on kuitenkin hyvä esimerkki Gaussin kokonaisluvusta, jota ei voida perustella Gaussin alkuluvuksi kyseisellä tavalla. Esitellään seuraavaksi toinen tapa, miten jokin Gaussin kokonaisluku voidaan näyttää Gaussin alkuluvuksi.

Esimerkki 3.1. Halutaan näyttää, että luku 3 on Gaussin alkuluku. Koska $N(3) = 9$ ja luku 9 ei ole alkuluku joukossa $\mathbb{Z}$, niin Lausetta 2.10 ei voida käyttää. Kirjoitetaan aluksi luku 3 kahden Gaussin kokonaisluvun tulona eli olkoot $a, b, c, d \in \mathbb{Z}$ siten, että

$$3 = (a + ib)(c + id).$$

Jos nyt tarkastellaan luvun 3 normia, niin

$$9 = N(3) = N((a + ib)(c + id)) = N(a + ib)N(c + id) = (a^2 + b^2)(c^2 + d^2).$$

Kun luku 9 esitetään positiivisten kokonaislukujen avulla vaihtoehtoja on kaksi: $9 = 3 \times 3 = 1 \times 9$. Ensimmäisen vaihtoehdon perusteella

$$a^2 + b^2 = 3 \qquad \text{ja} \qquad c^2 + d^2 = 3.$$

Koska lukua 3 ei voida esittää kahden kokonaisluvun neliön summana, ensimmäinen vaihtoehto ei ole mahdollinen. Siten jälkimmäisen vaihtoehdon on oltava voimassa. Tästä saadaan, että luvuista $a + ib$ ja $c + id$ toisen on oltava yksikkö ja toisen luvun 3 liittolainen. Siten luku 3 todella on Gaussin alkuluku.

Äskeisessä esimerkissä tyydyttiin vain toteamaan, ettei lukua 3 voida esittää kahden kokonaisluvun neliön summana. Joissakin tapauksissa tämä kuitenkin on mahdollista, kuten seuraavassa esimerkissä nähdään.

Esimerkki 3.2. (a) Luku 5 voidaan esittää kahden neliön summana, sillä

$$5 = 1 + 4 = 1^2 + 2^2.$$

(b) Vastaavasti luku 4050 voidaan esittää kahden neliön summana, sillä

$$4050 = 81 + 3969 = 9^2 + 63^2.$$

Seuraavassa alaluvussa tarkastellaan asiaa lähemmin. Halutaan siis selvittää, milloin jokin luonnollinen luku voidaan esittää kahden neliön summana. Tämän jälkeen tutustutaan siihen, milloin luonnollinen luku voidaan esittää neljän neliön summana. Myös kolmen neliön summalle on olemassa oma tuloksensa, mikä tunnetaan nimellä Legendren kolmen neliön lause ranskalaisen matemaatikon Adrien-Marie Legendren (1752–1833) mukaan. Tässä tutkielmassa kyseinen tulos ja sen todistus ohitetaan [**2**, VII: Proposition 41].

3.2. Luonnollinen luku kahden neliön summana

Tuloksen luonnollisen luvun esittämisestä kahden neliön summana esitti ensimmäisen kerran ranskalaissyntyinen Albert Girard (1595–1632) vuonna 1625. Ranskalainen Pierre de Fermat (1601–1665) väitti todistaneensa sen, mutta ensimmäinen julkaistu todistus on sveitsiläiseltä matemaatikolta Leonhard Eulerilta (1707–1783) vuodelta 1754. Ennen kyseisen tuloksen esittelyä ja todistusta tutustutaan hieman neliönjäännöksiin ja neliönepäjäännöksiin.

MÄÄRITELMÄ 3.3. Olkoot p alkuluku ja a kokonaisluku, joka ei ole jaollinen luvulla p. Luku a on *neliönjäännös* luvulle p, jos on olemassa kokonaisluku c siten, että

$$c^2 \equiv a \pmod{p}.$$

Muussa tapauksessa sanotaan, että luku a on *neliönepäjäännös* luvulle p.

Määritelmän 3.3 mukaan siis luku a on neliönjäännös luvulle p jos ja vain jos se on neliö kunnassa $\mathbb{Z}_p$. Katsotaan tästä muutama esimerkki.

ESIMERKKI 3.4. (a) Luku 2 on neliönjäännös luvulle 7, koska $3^2 = 9 \equiv 2 \pmod{7}$. Luku 2 on siis neliö kunnassa $\mathbb{Z}_7$.

(b) Luku 3 on neliö kunnassa $\mathbb{Z}_{11}$ ja siten neliönjäännös luvulle 11, sillä

$$5^2 = 25 \equiv 3 \pmod{11}.$$

(c) Luku 3 on neliönepäjäännös luvulle 5, koska ei ole olemassa lukua c siten, että kongruenssi $c^2 \equiv 3 \pmod{5}$ olisi tosi. Koska tarkastellaan rengasta $\mathbb{Z}_5$, riittää tarkastella tilanteet luvuille 0, 1, 2, 3 ja 4.

$$0^2 = 0 \not\equiv 3 \pmod{5}$$
$$1^2 = 1 \not\equiv 3 \pmod{5}$$
$$2^2 = 4 \not\equiv 3 \pmod{5}$$
$$3^2 = 9 \equiv 4 \not\equiv 3 \pmod{5}$$
$$4^2 = 16 \equiv 1 \not\equiv 3 \pmod{5}$$

Jos luku p on suuri, niin äskeisen kaltainen kaikkien vaihtoehtojen kokeilu ei ole kovin mielekestä. Suurena apuna voidaan hyödyntää Eulerin kriteerinä tunnettua tulosta. Eulerin kriteerin todistuksessa hyödynnetään Fermat'n pientä lausetta, joka näyttää seuraavalta.

LAUSE 3.5. *Olkoon p alkuluku ja olkoon $a \in \mathbb{N}$ mikä tahansa luku, jolle $a \not\equiv 0 \pmod{p}$. Tällöin*

$$a^{p-1} \equiv 1 \pmod{p}.$$

Fermat'n pieni lause oletetaan tunnetuksi, joten sen todistus ohitetaan, katso esimerkiksi [**2**, II: Corollary 26]. Siirrytään suoraan Eulerin kriteeriin, joka on peräisin Eulerin omista papereista vuodelta 1748.

LAUSE 3.6. *Olkoot p pariton alkuluku ja a kokonaisluku, joka ei ole jaollinen luvulla p. Jos luku a on neliönjäännös luvulle p, niin*

$$a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Jos luku a on neliönepäjäännös luvulle p, niin

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

TODISTUS. Jos a on neliönjäännös luvulle p, niin $a \equiv c^2 \pmod{p}$ jollekin kokonaisluvulle c. Fermat'n pientä lausetta hyödyntämällä saadaan

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

Jos nyt a ei ole neliöjäännös luvulle p, niin $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$ (ks. [**2**, II: Proposition 28]). Fermat'n pienen lauseen mukaan $a^{p-1} \equiv 1 \pmod{p}$ eli $a^{p-1} - 1 = kp$ jollakin $k \in \mathbb{Z}$. Toisaalta tiedetään, että

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

Nyt siis ainakin toinen tulontekijöistä on jaollinen luvulla p. Koska $a^{\frac{p-1}{2}} \not\equiv 1 \pmod{p}$, on luvun $a^{\frac{p-1}{2}} + 1$ oltava jaollinen luvulla p. Siispä todella

$$a^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

□

Eulerin kriteeri antaa yksinkertaisen tavan tutkia, onko annettu luku neliönjäännös jollekin tietylle luvulle.

ESIMERKKI 3.7. Tutkitaan Eulerin kriteerin avulla Esimerkin 3.4 tilanteita.

(a) Koska $2^{\frac{7-1}{2}} = 2^3 = 8 \equiv 1 \pmod{7}$, luku 2 on neliönjäännös luvulle 7.

(b) Vastaavasti nähdään luvun 3 olevan neliönjäännös luvulle 11, sillä

$$3^{\frac{11-1}{2}} = 3^5 = 243 \equiv 1 \pmod{11}.$$

(c) Luku 3 on epäneliönjäännös luvulle 5, koska $3^{\frac{5-1}{2}} = 9 \equiv -1 \pmod{5}$.

Eulerin kriteeristä seuraa oheinen hyödyllinen tulos.

SEURAUS 3.8. *Jos luku p on pariton alkuluku, niin luku -1 on*

(i) neliönjäännös luvulle p, jos $p \equiv 1 \pmod{4}$.

(ii) neliönepäjäännös luvulle p, jos $p \equiv 3 \pmod{4}$.

TODISTUS. (i) Koska $p \equiv 1 \pmod 4$, on olemassa $k \in \mathbb{Z}$ siten, että $p - 1 = 4k$. Nyt

$$(-1)^{\frac{p-1}{2}} = (-1)^{2k} \equiv 1 \pmod p$$

eli luku -1 todella on neliönjäännös luvulle p.

(ii) Tiedetään, että on olemassa $l \in \mathbb{Z}$ siten, että $p - 3 = 4l$. Tällöin saadaan

$$(-1)^{\frac{p-1}{2}} = (-1)^{\frac{p-3+2}{2}} = (-1)^{\frac{p-3}{2}+1} = (-1)^{\frac{4l}{2}+1} \equiv -1 \pmod p.$$

Siispä luku -1 on neliönepäjäännös luvulle p.

□

Nyt voidaan antaa täsmällinen tulos luonnollisen luvun esittämiselle kahden neliön summana. Tuloksen todistuksen lopussa hyödynnetään Gaussin kokonaislukuja.

LAUSE 3.9. *Luonnollinen luku n voidaan esittää kahden neliön summana jos ja vain jos sen alkutekijäesityksessä ei ole alkulukua $p \equiv 3 \pmod 4$ korotettuna parittomaan potenssiin.*

TODISTUS. Näytetään aluksi väitteen ensimmäinen suunta. Oletetaan, että luku n voidaan esittää kahden neliön summana eli $n = x^2 + y^2$ joillekin kokonaisluvuille x ja y. Olkoon lisäksi luku p luvun n alkutekijäesityksessä esiintyvä alkuluku siten, että se on muotoa $p \equiv 3 \pmod 4$. Täytyy siis näyttää, että alkutekijäesityksessä luvun p potenssi on parillinen. Luku $n = x^2 + y^2$ on jaollinen luvulla p, joten tiedetään, että seuraava kongruenssi pätee

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

Seurauksen 3.8 perusteella tiedetään, että luku -1 on neliönepäjäännös luvulle p eli se ei ole neliö kunnassa $\mathbb{Z}_p$. Jos nyt oletetaan, että $y \neq 0_{\mathbb{Z}_p}$, niin sille on olemassa käänteisluku $y^{-1} \in \mathbb{Z}_p$. Kertomalla nyt luvulla $(y^{-1})^2$ äskeistä kongruenssia, saadaan

$$(xy^{-1})^2 \equiv -1 \pmod p,$$

eli luku -1 olisi neliö, mikä on ristiriita. Vastaava päättely voidaan toteuttaa luvulle x, kun kerrotaan kongruenssi ensin luvulla -1

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

ja sitten luvulla $(x^{-1})^2$, kun oletetaan, että $x \neq 0_{\mathbb{Z}_p}$. Saadaan siis

$$-1 \equiv (yx^{-1})^2 \pmod p,$$

mikä aiheuttaa ristiriidan. Kun yhdistetään äskeiset, saadaan kongruenssi

$$y^2 \equiv x^2 \equiv 0 \pmod p.$$

Tästä nähdään, että luku p jakaa molemmat luvut x ja y, kun muistetaan, että p on alkuluku. Edelleen luvut x^2 ja y^2 ovat jaollisia luvulla p^2. Siispä p^2 jakaa myös luvun $n = x^2 + y^2$. Nyt $\frac{n}{p^2}, \frac{x}{p}, \frac{y}{p} \in \mathbb{Z}$ ja

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

Nyt ollaan siis näytetty, että kun luku $n = x^2 + y^2$ on jaollinen luvulla p, niin tästä seuraa, että n on jaollinen myös luvulla p^2. Kun äskeistä päättelyä toistetaan tarvittava määrä, induktiolla seuraa, että luvun p potenssi on parillinen luvun n alkutekijäesityksessä.

Perustellaan sitten väitteen toinen suunta eli halutaan näyttää, että luku n voidaan esittää kahden neliön summana. Kirjoitetaan luku n muodossa

$$n = qm^2,$$

missä luku q on neliövapaa eli sen alkutekijäesityksessä ei ole mitään tekijää enempää kuin yksi. Alkuluvut muotoa $p \equiv 3 \pmod 4$ ovat tekijöitä luvulle m^2. Luvun q ainoat mahdolliset tekijät ovat luku 2 ja alkuluvut muotoa $p \equiv 1 \pmod 4$.

Tehdään seuraava huomio olettaen, että luvut a, b, c, d ovat kokonaislukuja:

$$\begin{aligned}(a^2 + b^2)(c^2 + d^2) &= a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \\ &= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 \\ &= (ac)^2 + 2abcd + (bd)^2 + (ad)^2 - 2abcd + (bc)^2 \\ &= (ac + bd)^2 + (ad - bc)^2.\end{aligned}$$

Saadusta yhtälöstä

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 \tag{3.1}$$

nähdään, että jokainen tulo, jonka tekijät koostuvat kahden neliön summista, voidaan esittää uudelleen järjestelemällä kahden neliön summana. Tämän huomion ansiosta riittää todistuksessa alkulukuihin keskittyminen, sillä jos luku n on yhdistetty luku, niin alkutekijäesityksen avulla se saadaan uudelleen järjestelemällä muunnettua kahden neliön summaksi. Lisäksi, koska

$$m^2 = 0^2 + m^2 \qquad \text{ja} \qquad 2 = 1^2 + 1^2,$$

äskeisestä huomiosta seuraa, että luku n on esitettävissä kahden neliön summana, jos jokainen alkuluku $p \equiv 1 \pmod 4$ on esitettävissä kahden neliön summa. Tämän näyttäminen onnistuu hyödyntämällä sopivasti Gaussin kokonaislukuja ja normia N.

Olkoon siis luku p mikä tahansa alkuluku muotoa $p \equiv 1 \pmod 4$. Näytetään, että p on esitettävissä kahden neliön summana valitsemalla Gaussin kokonaisluku $z = a + ib$ niin, että $N(z) = p$. Seurauksen 3.8 perusteella on olemassa $c \in \mathbb{Z}$ siten, että

$$c^2 \equiv -1 \pmod p.$$

Valitaan nyt $\alpha = c + i \in \mathbb{Z}[i]$ ja lasketaan sille normi. Saadaan

$$N(\alpha) = \alpha\bar{\alpha} = c^2 + 1^2 = c^2 + 1.$$

Luku p jakaa luvun $N(\alpha)$ tavallisten kokonaislukujen joukossa ja siten myös Gaussin kokonaislukujen joukossa. Sen sijaan α ja $\bar{\alpha}$ eivät ole jaollisia luvulla p renkaassa $\mathbb{Z}[i]$. Jos näin olisi, niin luvut $\alpha p^{-1} = \frac{c}{p} + \frac{1}{p}i$ ja $\bar{\alpha}p^{-1} = \frac{c}{p} - \frac{1}{p}i$ kuuluisivat Gaussin kokonaislukuihin. Tämä olisi mahdollista vain jos p^{-1} olisi yksikkö, ja näin ei ole. Luku p ei voi olla Gaussin alkuluku, sillä muutoin Eukleideen lemman nojalla p jakaa

ainakin toisen luvuista α tai $\bar{\alpha}$. Luku p voidaan siis kirjoittaa muodossa $p = zy$, missä kumpikaan luvuista z ja y ei ole yksikkö. Siten $N(z) > 1$ ja $N(z) > 1$. Nyt

$$N(z)N(y) = N(p) = p^2 + 0^2 = p^2,$$

joten $N(z) = p = N(y)$. Jos $z = a + ib$, niin

$$p = N(z) = a^2 + b^2.$$

Luku p voidaan siten esittää kahden neliön summana. Siispä myös luku n voidaan esittää kahden neliön summana.

□

Nyt kun tiedetään sääntö, milloin luonnollinen luku voidaan esittää kahden neliön summana, palataan tarkastelemaan aikaisempia esimerkkejä äskeisen tuloksen näkökulmasta.

Esimerkki 3.10. (a) Lukua 3 ei voida esittää kahden neliön summana. Tämä johtuu siitä, että luku 3 on alkuluku, joka on muotoa $p \equiv 3 \pmod 4$.

(b) Luku 5 voidaan esittää kahden neliön summana, koska se on alkuluku, joka on muotoa $p \equiv 1 \pmod 4$ eikä siten sisällä ollenkaan $p \equiv 3 \pmod 4$ muotoa olevaa tekijää.

(c) Luvun 4050 alkutekijäesitys on $4050 = 2 \cdot 5^2 \cdot 3^4$. Huomataan, että luku 3 on ainut tekijä muotoa $p \equiv 3 \pmod 4$. Lisäksi se on korotettu parilliseen potenssiin, joten luku 4050 voidaan esittää kahden neliön summana.

Jos luonnollinen luku on pieni, on usein helppo päätellä, kuinka se esitetään kahden neliön summana. Jos suora päättely ei onnistu, voidaan summaesitys johtaa alkutekijäesityksestä seuraavalla tavalla.

Esimerkki 3.11. Tutkitaan lukua 39 690. Sen alkutekijäesitys on

$$39\,690 = 2 \cdot 3^4 \cdot 5 \cdot 7^2.$$

Lauseen 3.9 perusteella tiedetään, että se on mahdollista esittää kahden neliön summana. Muokataan alkutekijäesitystä niin, että esitetään kahden neliön summana ne tekijät, jotka pystytään. Saadaan

$$2 \cdot 3^4 \cdot 5 \cdot 7^2 = (1^2 + 1^2) \cdot 3^4 \cdot (1 + 2^2) \cdot 7^2.$$

Järjestellään seuraavaksi termejä ja hyödynnetään Lauseen 3.9 todistuksessa saatua yhtälöä (3.1) jolloin

$$\begin{aligned}(1^2 + 1^2) \cdot 3^4 \cdot (1 + 2^2) \cdot 7^2 &= 3^4 \cdot 7^2 \cdot (1^2 + 1^2) \cdot (1 + 2^2) \\ &= (3^2 \cdot 7)^2 \cdot ((1 \cdot 1 + 1 \cdot 2)^2 + (1 \cdot 2 - 1 \cdot 1)^2).\end{aligned}$$

Lopuksi sievennetään äsken saatua lauseketta, kunnes päädytään haluttuun muotoon

$$(3^2 \cdot 7)^2 \cdot ((1 \cdot 1 + 1 \cdot 2)^2 + (1 \cdot 2 - 1 \cdot 1)^2) = 63^2 \cdot (3^2 + 1^2) = 189^2 + 63^2.$$

Näin ollen luku 39 690 voidaan esittää kahden neliön summana seuraavasti

$$39\,690 = 63^2 + 189^2.$$

Lauseen 3.9 todistuksessa hyödynnettiin tavallisten kokonaislukujen puolelta tuttua tulosta alkulukujen karakterisoinnista. Vastaavan kaltainen karakterisointi voidaan antaa nyt myös Gaussin alkuluvuille.

LAUSE 3.12. *Gaussin alkulukuja ρ on kolmea eri muotoa:*

(i) $\rho = 1 + i$

(ii) $\rho = a + ib$ *ja* $\rho' = a - ib$, *missä* $p = a^2 + b^2$ *on alkuluku ja* $p \equiv 1 \pmod 4$

(iii) $\rho = p$, *missä* p *on alkuluku ja* $p \equiv 3 \pmod 4$

ja kaikki näiden liittolaiset.

TODISTUS. Olkoon z mikä tahansa Gaussin alkuluku. Tällöin

$$N(z) = z\bar{z} = n,$$

missä luku n on tavallinen positiivinen kokonaisluku. Koska $n = z\bar{z}$, luku z jakaa luvun n. Tästä seuraa, että z jakaa jonkun luvun n alkutekijöistä $p \in \mathbb{Z}$. Tämän huomion perusteella tiedetään siis, että jokaiselle Gaussin alkuluvulle z voidaan löytää alkuluku p siten, että $z \mid p$.

Jokainen Gaussin alkuluku on siis jonkun tavallisen alkuluvun tekijä Gaussin kokonaislukujen joukossa. Kun tiedetään kaikki alkulukujen tekijät Gaussin kokonaislukujen joukossa, tiedetään myös kaikki Gaussin alkuluvut. Lähdetään etsimään alkutekijöitä kahdessa osassa riippuen siitä, voidaanko alkuluku p esittää kahden neliön summana vai ei.

Jos alkuluku p on kahden neliön summa eli $p = a^2 + b^2$, niin $p = (a+ib)(a-ib)$. Tästä muodosta nähdään, että p ei voi olla Gaussin alkuluku. Voidaan kuitenkin huomata, että

$$N(a \pm ib) = a^2 + b^2 = p,$$

joten Lauseen 2.10 nojalla luvut $a + ib$ ja $a - ib$ ovat Gaussin alkulukuja. Koska $p = a^2 + b^2$ on alkuluku, tiedetään Lauseen 3.9 perusteella, että joko

$$p = 2 \qquad \text{tai} \qquad p \equiv 1 \pmod 4.$$

Jos $p = 2 = 1^2 + 1^2 = (1 + i)(1 - i)$, niin luvut $1 + i$ ja $1 - i$ ovat Gaussin alkulukuja. Koska luku $1-i$ on liittolainen luvulle $1+i$, saadaan molemmat vaihtoehdot muodosta $1 + i$ eli kohdasta (i).

Kun $p \equiv 1 \pmod 4$ ja $p = a^2 + b^2$, luvut muotoa $a + ib$ ja $a - ib$ sekä kaikki niiden liittolaiset ovat Gaussin alkulukuja. Tämä vastaa kohtaa (ii).

Nyt aritmetiikan peruslause Gaussin kokonaisluvuille sanoo, että kummassakin tapauksessa saadut alkutekijäesitykset ovat yksikäsitteisiä. Siispä olemme nyt löytäneet kaikki alkulukutekijät Gaussin kokonaislukujen joukossa niille alkuluvuille p, jotka voidaan esittää kahden neliön summana.

Jos taas p on alkuluku, jota ei voida esittää kahden neliön summana, niin Lauseen 3.9 perusteella sen on oltava muotoa $p \equiv 3 \pmod 4$. Tällöin luvun p on oltava Gaussin alkuluku. Tämä voidaan perusteella antiteesin kautta. Oletetaan siis, että p ei ole

Gaussin alkuluku. Siispä se voidaan kirjoittaa muodossa $p = zw$, missä kumpikaan tekijöistä z ja w ei ole yksikkö. Nyt siis

$$p^2 = N(p) = N(zw) = N(z)N(w).$$

Koska $N(z) > 1$ ja $N(w) > 1$, saadaan $N(z) = p$. Jos nyt $z = a + ib$, niin

$$p = N(z) = a^2 + b^2$$

eli alkuluku p olisikin kahden neliön summa. Tämä on kuitenkin ristiriita alkuoletuksen kanssa. Siispä p on Gaussin alkuluku eikä sillä siten ole muita alkutekijöitä kuin itsensä ja liittolaisensa. Tämä vastaa kohtaa (iii).

Nyt ollaan löydetty kaikki alkulukujen tekijät Gaussin kokonaislukujen joukossa. Siten ollaan käyty läpi myös kaikki Gaussin alkuluvut ja todettu niiden vastaavan aina jotain kohtien (i)-(iii) muotoiluista tai niiden liittolaisista.

□

Gaussin alkulukujen karakterisoinnin perusteella nähdään, että tavallisista alkuluvuista Gaussin alkulukuja ovat vain ne, jotka ovat muotoa $p \equiv 3 \pmod 4$. Alkuluvut $p = 2$ ja $p \equiv 1 \pmod 4$ eivät siis ole Gaussin alkulukuja, mutta niille voidaan löytää alkutekijäesitys normin N avulla.

3.3. Luonnollinen luku neljän neliön summana

Keskitytään seuraavaksi tapaukseen, jossa halutaan esittää luonnollinen luku neljän neliön summana. Ilmenee, että tämä on mahdollista itse asiassa kaikille luonnollisille luvuille. Tuloksen luonnollisen luvun esittämisestä neljän neliön summana on alunperin esittänyt ranskalainen matemaatikko Claude Gaspard Bachet (1581–1638) vuonna 1621. Ensimmäinen todistus kyseiselle tulokselle on kuitenkin vasta vuodelta 1770 italialaiselta matemaatikolta Joseph-Louis Lagrangelta, minkä vuoksi tulos tunnetaan myös nimellä Lagrangen neljän neliön lause. Tiedetään, että Eulerkin oli yrittänyt todistaa sitä useita vuosia siinä kuitenkaan onnistumatta. Lagrangen antamassa todistuksessa on kuitenkin näkyvissä Eulerin ideoita.

Ennen varsinaista tuloksen esittelyä ja sen todistusta tutustutaan hieman kvaternioihin ja Hurwitzin kokonaislukuihin. Kvaternioiden avulla voidaan määritellä Hurwitzin kokonaisluvut, joita hyödynnetään Lagrangen neljän neliön lauseen todistuksessa.

MÄÄRITELMÄ 3.13. Olkoot a_0, a_1, a_2 ja a_3 reaalilukuja. Lisäksi olkoot i, j ja k imaginäärisiä siten, että

$$i^2 = j^2 = k^2 = -1, \qquad ij = k = -ji, \qquad jk = i = -kj \qquad \text{ja} \qquad ki = j = -ik.$$

Tällöin a on *kvaternio*, jos se on muotoa $a = a_0 + a_1 i + a_2 j + a_3 k$.

Kvaterniot keksi irlantilainen matemaatikko William Rowan Hamilton (1805–1865) vuonna 1843. Ne vastaavat oleellisesti kompleksilukuja, mutta ulottuvuuksien määrä kasvaa. Kaikkien kvaternioiden joukkoa merkitään Hamiltonin kunniaksi tunnuksella $\mathbb{H}$. Monet laskutoimitukset ja ominaisuudet, jotka on määritelty kompleksiluvuille, toteutuvat myös kvaternioille. Tällaisia ovat esimerkiksi yhteenlasku ja kertolasku sekä konjugaatti $\bar{a} = a_0 - a_1 i - a_2 j - a_3 k \in \mathbb{H}$. Yhteenlaskulla on samat ominaisuudet

kuin kompleksiluvuillakin, mutta kvaternioiden kertolaskulle vaihdannaisuus ei päde yleisesti.

Kompleksilukujen joukosta voitiin erottaa tavallisia kokonaislukuja vastaavat Gaussin kokonaisluvut. Vastaavasti voidaan kvaternioiden joukosta erottaa Hurwitzin kokonaisluvut, joiden määritelmässä hyödynnetään tavallisten kokonaislukujen lisäksi puolikokonaislukuja.

MÄÄRITELMÄ 3.14. Olkoon n kokonaisluku. Jos $m = n + \frac{1}{2}$, eli luku m on parittoman kokonaisluvun puolikas, niin sanotaan, luku m on *puolikokonaisluku*.

MÄÄRITELMÄ 3.15. Kvaterniota α, joka on muotoa $\alpha = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k$, missä kaikki luvut α_0, α_1, α_2 ja α_3 ovat joko kokonaislukuja tai puolikokonaislukuja, kutsutaan *Hurwitzin kokonaisluvuksi*. Kaikkien Hurwitzin kokonaislukujen muodostamaa joukkoa merkitään symbolilla $\mathcal{H}$.

Hurwitzin kokonaisluvut ovat saaneet nimensä saksalaiselta matemaatikolta Adolf Hurwitzilta (1859–1919). Niistä käytetään usein myös nimitystä Hurwitzin kvaterniot. Monet Gaussin kokonaisluvuille tutut ominaisuudet toteutuvat Hurwitzin kokonaisluvuille. Esimerkiksi jos α ja β ovat Hurwitzin kokonaislukuja, niin

$$\bar{\alpha} \in \mathcal{H}, \qquad \alpha \pm \beta \in \mathcal{H} \qquad \text{ja} \qquad \alpha\beta \in \mathcal{H}.$$

Kuten Gaussin kokonaisluvut, myös Hurwitzin kokonaisluvut muodostavat renkaan. Toisin kuin Gaussin kokonaislukujen rengas, Hurwitzin kokonaislukujen rengas ei ole vaihdannainen. Tämä johtuu siitä, että kertolasku ei ole yleisesti vaihdannainen kvaternioille eikä siten myöskään Hurwitzin kokonaisluvuille. Gaussin kokonaislukujen tavoin Hurwitzin kokonaisluvuille voidaan määritellä normi N.

MÄÄRITELMÄ 3.16. Hurwitzin kokonaisluvuille *normiksi* kutsutaan kuvausta $N : \mathcal{H} \to \mathbb{N} \cup \{0\}$,

$$N(\alpha) = \alpha\bar{\alpha} = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2.$$

Gaussin kokonaislukujen puolelta tutut normin N ominaisuudet pätevät Hurwitzin kokonaisluvuille. Jos $\alpha, \beta \in \mathcal{H}$, niin $N(\alpha\beta) = N(\alpha)N(\beta)$. Lisäksi $N(\alpha) \geq 0$ pätee kaikille Hurwitzin kokonaisluvuille ja $N(\alpha) = 0$ jos ja vain jos $\alpha = 0_{\mathcal{H}}$.

Monet Gaussin kokonaisluvuille näytetyt lukuteorian tulokset ovat voimassa Hurwitzin kokonaisluvuille. Yksiköt määritellään Hurwitzin kokonaisluvuille oleellisesti samoin ja niiden yhteys normiin N on sama: Hurwitzin kokonaisluku α on yksikkö jos ja vain jos $N(\alpha) = 1$. Lisäksi voidaan näyttää, että Eukleideen algoritmi on määritelty Hurwitzin kokonaisluvuille, ja kuten Gaussin kokonaisluvuillekin, sen avulla voidaan määrittää suurin yhteinen tekijä. Perustelut sivuutetaan, koska ne noudattavat oleellisesti samaa kaavaa kuin Gaussin kokonaisluvuille. Tärkeää on kuitenkin huomata, että koska kertolasku ei ole yleisesti vaihdannainen, niin esimerkiksi jakajan ja siten myös suurimman yhteisen tekijän määritelmät poikkeavat hieman aikaisemmasta.

MÄÄRITELMÄ 3.17. Olkoot $\alpha, \beta, \gamma \in \mathcal{H}$. Jos $\gamma = \alpha\beta$, niin

(a) luku α on *vasemmanpuoleinen jakaja* luvulle γ.

(b) luku β on *oikeanpuoleinen jakaja* luvulle γ.

Nyt voidaan siirtyä Lagrangen neljän neliön lauseeseen ja sen todistamiseen.

LAUSE 3.18. *Jokainen luonnollinen luku n voidaan esittää neljän neliön summana.*

TODISTUS. Olkoon positiivinen kokonaisluku n neljän neliön summa eli

$$n = \alpha_0^2 + \alpha_1^2 + \alpha_2^2 + \alpha_3^2,$$

missä $\alpha_0, \alpha_1, \alpha_2, \alpha_3 \in \mathbb{Z}$. Tällöin $n = \alpha\bar{\alpha}$, missä $\alpha = \alpha_0 + \alpha_1 i + \alpha_2 j + \alpha_3 k \in \mathcal{H}$. Koska Hurwitzin kokonaisluvuille pätee, että tulon normi on yhtä suurta kuin normien tulo, mikä tahansa neljän neliön summista koostuva tulo on edelleen neljän neliön summa. Lauseen todistamiseksi riittää siis näyttää, että mikä tahansa alkuluku p on neljän neliön summa.

Aloitetaan näyttämällä, että on olemassa kokonaisluvut a ja b niin, että

$$a^2 + b^2 \equiv -1 \pmod{p}.$$

Jos $p = 2$, niin kongruenssi pätee, kun valitaan $a = 1$ ja $b = 0$.

Jos $p \equiv 1 \pmod 4$, niin Seurauksen 3.8 perusteella tiedetään, että luku -1 on neliönjäännös luvulle p. On siis olemassa kokonaisluku a siten, että $a^2 \equiv -1 \pmod p$ ja nyt voidaan taas valita, että $b = 0$.

Jos p on muotoa $p \equiv 3 \pmod 4$, niin olkoon c pienin positiivinen neliönepäjäännös luvulle p. Tällöin $c \geq 2$ ja $c - 1$ on neliönjäännös luvulle luvulle p eli on olemassa $a \in \mathbb{Z}$ siten, että

$$a^2 \equiv c - 1 \pmod{p}.$$

Seurauksen 3.8 nojalla luku -1 on neliönepäjäännös. Nyt Eulerin kriteerin pohjalta tiedetään, että

$$c^{\frac{p-1}{2}} \equiv -1 \pmod{p} \qquad \text{ja} \qquad (-1)^{\frac{p-1}{2}} \equiv -1 \pmod{p}.$$

Edelleen Eulerin kriteeriä hyödyntämällä saadaan, että luvun $-c$ on oltava neliönjäännös, sillä

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

On siis olemassa kokonaisluku b siten, että

$$b^2 \equiv -c \pmod{p}.$$

Nyt kongruenssien laskusääntöjä käyttämällä nähdään, että tässäkin tapauksessa on löydetty kokonaisluvut a ja b siten, että

$$a^2 + b^2 \equiv c - 1 + (-c) \equiv -1 \pmod{p}.$$

Olkoon nyt $\alpha = 1 + ai + bj \in \mathcal{H}$. Tällöin

$$N(\alpha) = \alpha\bar{\alpha} = 1 + a^2 + b^2.$$

Koska $a^2 + b^2 \equiv -1 \pmod p$, luku p jakaa luvun $N(\alpha)$ tavallisten kokonaislukujen joukossa ja siten myös Hurwitzin kokonaislukujen joukossa. Luku p ei ole yksikkö, joten $\alpha p^{-1} \notin \mathcal{H}$ ja $\bar{\alpha} p^{-1} \notin \mathcal{H}$. Siispä luku p ei jaa kumpaakaan luvuista α tai $\bar{\alpha}$.

Olkoon nyt $\gamma = (p, \alpha)_r$ eli luku γ on suurin yhteinen oikeanpuoleinen tekijä luvuille p ja α. Tällöin on siis olemassa $\beta \in \mathcal{H}$ siten, että

$$p = \beta\gamma.$$

Jos nyt luku β on yksikkö, niin luku p olisi oikeanpuoleinen jakaja luvulle γ ja siten myös luvulle α, mikä ei pidä paikkaansa. Siispä luku β ei ole yksikkö ja siten $N(\beta) > 1$.

Selvästi nähdään, että luku $\gamma\bar{\alpha}$ on yhteinen oikea jakaja luvuille $p\bar{\alpha}$ ja $\alpha\bar{\alpha}$. Bézout'n yhtälöstä luvulle γ nähdään, että itse asiassa

$$\gamma\bar{\alpha} = (p\bar{\alpha}, \alpha\bar{\alpha})_r.$$

Koska p on tavallinen kokonaisluku, on sillä kerrottaessa kertolasku vaihdannainen eli

$$p\bar{\alpha} = \bar{\alpha}p.$$

Lisäksi tiedetään, että luku p jakaa luvun $\alpha\bar{\alpha}$. Siispä luku p on oikea jakaja luvulle $\gamma\bar{\alpha}$. Luku p ei jaa lukua $\bar{\alpha}$, joten luku γ ei voi olla yksikkö ja siten $N(\gamma) > 1$. Nyt siis

$$N(\beta)N(\gamma) = N(p) = p^2,$$

joten täytyy olla, että $N(\beta) = N(\gamma) = p$.

Olkoon luku γ muotoa $\gamma = c_0 + c_1 i + c_2 j + c_3 k \in \mathcal{H}$. Tällöin

$$c_0^2 + c_1^2 + c_2^2 + c_3^2 = N(\gamma) = p.$$

Jos nyt luvut c_0, c_1, c_2 ja c_3 ovat kokonaislukuja, niin luku p todella voidaan esittää neljän neliön summana. Jos ne taas eivät ole kokonaislukuja, täytyy niiden kaikkien olla puolikokonaislukuja Hurwitzin kokonaislukujen määritelmän nojalla. Ne voidaan siis kirjoittaa muodossa

$$c_i = 2d_i + e_i,$$

missä $d_i \in \mathbb{Z}$ ja $e_i = \pm\frac{1}{2}$, kun $i = 0, 1, 2, 3$. Olkoot tällöin luvut δ ja ε Hurwitzin kokonaislukuja siten, että

$$\delta = d_0 + d_1 i + d_2 j + d_3 k \qquad \text{ja} \qquad \varepsilon = e_0 + e_1 i + e_2 j + e_3 k.$$

Nyt $\gamma = 2\delta + \varepsilon$ ja $N(\varepsilon) = (\pm\frac{1}{2})^2 + (\pm\frac{1}{2})^2 + (\pm\frac{1}{2})^2 + (\pm\frac{1}{2})^2 = 1$. Valitaan seuraavaksi luku θ siten, että

$$\theta = \gamma\bar{\varepsilon} = (2\delta + \varepsilon)\bar{\varepsilon} = 2\delta\bar{\varepsilon} + 1 \in \mathcal{H}.$$

Tällöin luku θ voidaan kirjoittaa muodossa $\theta = t_0 + t_1 i + t_2 j + t_3 k$, missä luvut t_0, t_1, t_2 ja t_3 ovat kokonaislukuja. Nyt siis

$$t_0^2 + t_1^2 + t_2^2 + t_3^2 = N(\theta) = N(\gamma\bar{\varepsilon}) = N(\gamma)N(\bar{\varepsilon}) = N(\gamma) = p$$

eli luku p voidaan todella esittää neljän neliön summana. Siispä jokainen luonnollinen luku voidaan esittää neljän neliön summana.

□

Katsotaan seuraavaksi muutama esimerkki luonnollisen luvun esittämisestä neljän neliön summana.

Esimerkki 3.19. (a) Luku 15 neljän neliön summana näyttää seuraavalta

$$15 = 1 + 1 + 4 + 9 = 1^2 + 1^2 + 2^2 + 3^2.$$

(b) Luku 290 voidaan esittää neljän neliön summana esimerkiksi seuraavasti

$$290 = 9 + 36 + 49 + 196 = 3^2 + 6^2 + 7^2 + 14^2.$$

LUKU 4

Fermat'n suuri lause

Fermat'n suuresta lauseesta on tullut kenties yksi matematiikan kuuluisimmista lauseista. Lauseen mukaan ei ole olemassa positiivisia kokonaislukuja x, y ja z, jotka toteuttaisivat yhtälön

$$x^n + y^n = z^n,$$

missä n on lukua 2 suurempi luonnollinen luku. Lause on peräisin Fermat'lta itseltään, kun hän sen vuonna 1637 kirjoitti Diofantoksen Arithmetica-teoksen marginaaliin. Hän kirjoitti latinaksi sen yhteyteen myös kuuluisaksi tulleen lauseen "Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet"eli suomennettuna "Olen keksinyt väittämälle ihmeellisen todistuksen, mutta marginaalissa ei riitä sille tilaa". Erityistä tästä tekee, että lause on pystytty todistamaan kovista yrityksistä huolimatta kaikille luonnollisille luvuille n vasta yli 300 vuoden päästä.

Kyseinen todistus on brittiläiseltä matemaatikolta Andrew Wilesilta (1953–). Hän esitti sen ensimmäisen kerran vuonna 1993, mutta sitä tarkastaessa löydettiin yksi virhe. Wiles sai virheen korjattua vuotta myöhemmin eli vuonna 1994, mikä ratkaisi viimein yli 350-vuotisen ongelman. Wilesin todistus [**13**] on hyvin vaativa ja yli sata sivua pitkä, minkä vuoksi Fermat'n suuren lauseen täydellinen todistus ohitetaan tässä tutkielmassa. Todistuksen synnystä ja sen vaiheista voi lukea Aczelin teoksesta Fermat's Last Theorem: Unlocking the Secret of an Ancient Mathematical Problem [**1**].

Yksittäisiä osia lauseesta on kuitenkin onnistuttu todistamaan jo paljon aikaisemmin. Esimerkiksi Fermat itse osasi todistaa ainakin tapaukset, joissa $n = 3$ ja $n = 4$. Lisäksi hän oli tehnyt havainnon, että mikäli ratkaisu löytyisi jollekin luvulle $n > 2$, niin ratkaisu löytyisi myös luvun n monikerroille. Huomion ansiosta lauseesta riitti enää tarkastella tapauksia, joissa n on pariton alkuluku. Eulerinkin tiedetään osanneen perustella tapaukset $n = 3$ ja $n = 4$. Kun Fermat'n kuuluisasta marginaalikirjoituksesta oli kulunut 200 vuotta, parittomista alkulukueksponenteista oli todistettu vasta tapaukset, joissa $n = 3$, $n = 5$ ja $n = 7$ [**1**, s. 44–45].

Tämän luvun päälause on Fermat'n suuren lauseen tapaus, jossa $n = 3$. Sille annetaan todistus kokonaislukujen kompleksisen laajennuksen kautta, kuten edellisessäkin luvussa tehtiin.

4.1. Yleistä Eisensteinin kokonaisluvuista

Tämän luvun päälauseen todistuksessa hyödynnetään Eisensteinin kokonaislukuja. Ne ovat saaneet nimensä saksalaiselta matemaatikolta Gotthold Eisensteinilta (1823–1852).

MÄÄRITELMÄ 4.1. Kompleksilukua z, joka on muotoa $z = (a - \frac{b}{2}) + \frac{b}{2}\sqrt{-3} = a + \rho b$, missä $a, b \in \mathbb{Z}$ ja

$$\rho = \frac{i\sqrt{3} - 1}{2} \quad \text{on ykkösen kuutiojuuri,}$$

kutsutaan *Eisensteinin kokonaisluvuksi*. Kaikkien Eisensteinin kokonaislukujen muodostamaa joukkoa merkitään symbolilla $\mathcal{E}$.

Monet Gaussin kokonaislukujen ominaisuudet pätevät Eisensteinin kokonaisluvuille. Tällaisia ovat muun muassa normi N ja Eukleideen algoritmi sekä useat jaollisuuteen liittyvät tulokset, kuten tekijöihin jako ja Bézout'n lemma. Tulokset näytetään oleellisesti samalla tavalla kuin Gaussin kokonaisluvuille, joten ne sivuutetaan. Tässä vaiheessa on kuitenkin hyvä huomata, että Eisensteinin kokonaislukujen normi N näyttää hieman erilaiselta eivätkä yksiköt kään ole täysin samat kuin Gaussin kokonaisluvuilla.

MÄÄRITELMÄ 4.2. Eisensteinin kokonaisluvuille $\alpha = a + \rho b$ *normiksi* kutsutaan kuvausta $N : \mathcal{E} \to \mathbb{N} \cup \{0\}$,

$$N(\alpha) = \alpha\bar{\alpha} = \left(a - \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2 = a^2 - ab + b^2.$$

LEMMA 4.3. *Eisensteinin kokonaisluvuille yksiköitä ovat luvut* ± 1, $\pm\rho$ *ja* $\pm\rho^2$.

TODISTUS. Tiedetään, että $\mu = a + \rho b \in \mathcal{E}$, missä $\rho = \frac{i\sqrt{3}-1}{2}$, on yksikkö jos ja vain jos $N(\mu) = 1$. Näin ollen tiedetään, että

$$1 = N(\mu) = N(a + \rho b) = \left(a - \frac{b}{2}\right)^2 + 3\left(\frac{b}{2}\right)^2.$$

Tätä sieventämällä saadaan

$$(2a - b)^2 + 3b^2 = 4.$$

Saadun yhtälön ratkaisemiseksi ratkaistaan ensin Diofantoksen yhtälö

$$x^2 + 3y^2 = 4.$$

Mahdolliset kokonaislukuratkaisut tälle ovat

$$y = 0 \quad \text{ja} \quad x = \pm 2 \qquad \text{tai} \qquad y = \pm 1 \quad \text{ja} \quad x = \pm 1.$$

Jos $y = 0$ ja $x = \pm 2$, niin $b = 0$ ja $a = \pm 1$. Yksiköksi saadaan tällöin luvut -1 ja 1.

Jos $y = \pm 1$, niin $b = \pm 1$. Jos $b = -1$, niin $a = -1$ tai $a = 0$. Yksiköiksi saadaan siis luvut $-1 - \rho$ ja $-\rho$.

Jos taas $b = 1$, niin $a = 0$ tai $a = 1$. Yksiköiksi saadaan tällöin ρ ja $1 + \rho$.

Toisaalta nyt $-1-\rho=\rho^2$ ja $1+\rho=-\rho^2$, sillä

$$\begin{aligned}\rho^2 &= \left(\frac{i\sqrt{3}-1}{2}\right)^2 = \frac{3i^2-2i\sqrt{3}+1}{4} = \frac{-2(1+i\sqrt{3})}{4} = \frac{-1-i\sqrt{3}}{2}\\ &= \frac{-2-i\sqrt{3}+1}{2} = \frac{-(2+i\sqrt{3}-1)}{2} = -\left(\frac{2}{2}+\frac{i\sqrt{3}-1}{2}\right)\\ &= -\rho-1.\end{aligned}$$

Siispä Eisensteinin kokonaislukujen yksiköt todella ovat ±1, $\pm\rho$ ja $\pm\rho^2$. □

4.2. Eräs tapaus Fermat'n suuresta lauseesta

Siirrytään nyt luvun päätulokseen eli Fermat'n suuren lauseeseen ja sen todistukseen, kun $n=3$.

LAUSE 4.4. *Luonnollisten lukujen joukossa ei ole ratkaisua yhtälölle*

$$x^3+y^3=z^3.$$

TODISTUS. Todistetaan väite antiteesin avulla eli tehdään oletus, että kyseiselle yhtälölle on ainakin yksi ratkaisu luonnollisille luvuille x, y ja z. Valitaan mahdollisista ratkaisuista se, joille $|xyz|$ on pienin. Siispä luvuilla x, y ja z ei ole yhteisiä tekijöitä keskenään eli

$$(x,y)=(x,z)=(y,z)=1.$$

Jos luku 3 ei jaa tuloa xyz, niin se ei jaa mitään luvuista x, y ja z. Siten

$$x\equiv\pm1, \qquad y\equiv\pm1, \qquad z\equiv\pm1 \qquad (\mathrm{mod}\ 3).$$

Kongruenssin määritelmän mukaan on olemassa $k\in\mathbb{Z}$ siten, että $x\pm1=3k$. Tällöin

$$(x\pm1)^3=(3k)^3,$$

joten edelleen

$$x^3\pm3x^2+3x\pm1=(3k)^3.$$

Ottamalla yhteinen tekijä saadaan

$$x^3\pm3x(x\pm1)\pm1=9(3k^3).$$

Tehdään sitten sijoitus $x\pm1=3k$, jolloin

$$x^3\pm3x(3k)\pm1=9(3k^3).$$

Kun nyt järjestetään termit uudelleen ja otetaan luku 9 yhteiseksi tekijäksi yhtälön oikealle puolelle, saadaan

$$x^3=\pm1 \quad (\mathrm{mod}\ 9).$$

Samat vaiheet voidaan tehdä luvuille y ja z, joten

$$x^3\equiv\pm1, \qquad y^3\equiv\pm1, \qquad z^3\equiv\pm1 \qquad (\mathrm{mod}\ 9).$$

Tämä taas aiheuttaa ristiriidan alkuperäisen yhtälön $x^3+y^3=z^3$ kanssa, koska tällöin

$$\pm2\equiv x^3+y^3=z^3\equiv\pm1 \quad (\mathrm{mod}\ 9) \qquad \text{tai} \qquad 0\equiv x^3+y^3=z^3\equiv\pm1 \quad (\mathrm{mod}\ 9).$$

Siispä voidaan olettaa, että luku 3 jakaa tulon xyz. Tästä seuraa, että luku 3 jakaa jonkun luvuista x, y tai z. Yhtälö $x^3 + y^3 = z^3$ on oleellisesti sama kuin yhtälö

$$x^3 + y^3 + z^3 = 0,$$

mistä nähdään yhtälön symmetrisyys. Yksinkertaisuuden vuoksi voidaan nyt olettaa, että luku 3 jakaa luvun z eli

$$z \equiv 0 \pmod 3.$$

Tästä seuraa, että $x^3 + y^3 \equiv 0 \pmod 3$, sillä muuten alkuperäinen yhtälö ei olisi voimassa. Koska $x \not\equiv 0 \pmod 3$ ja $y \not\equiv 0 \pmod 3$ ja x sekä y ovat keskenään jaottomat, voidaan olettaa lisäksi, että

$$x \equiv 1 \pmod 3 \qquad \text{ja} \qquad y \equiv -1 \pmod 3.$$

On siis olemassa $k, l \in \mathbb{Z}$ siten, että $x = 3k + 1$ ja $y = 3l - 1$ Näin ollen

$$\begin{aligned} x^2 - xy + y^2 &= (3k+1)^2 - (3k+1)(3l-1) + (3l-1)^2 \\ &= 9k^2 + 6k + 1 - 9kl + 3k - 3l + 1 + 9l^2 - 6l + 1 \\ &= 9(k^2 + k - kl - l + l^2) + 3. \end{aligned}$$

Tästä nähdään, että $x^2 - xy + y^2 \equiv 3 \pmod 9$.

Jos luvuilla $x + y$ ja $x^2 - xy + y^2$ on yhteinen jakaja p, niin luku p jakaa myös luvun $3xy$, sillä

$$(x+y)^2 - (x^2 - xy + y^2) = x^2 + 2xy + y^2 - x^2 + xy - y^2 = 3xy.$$

Kumpikaan luvuista x ja y ei ole kolmella jaollinen, joten tiedosta $3 \mid 3xy$ voidaan päätellä, että tällöin $p = 3$. Tämä on helppo varmistaa aikaisempien kohtien perusteella, sillä

$$x + y = 3k + 1 + 3l - 1 = 3(k + l)$$

ja

$$x^2 - xy + y^2 = 9(k^2 + k - kl - l + l^2) + 3 = 3(3(k^2 + k - kl - l + l^2) + 1).$$

Tiedetään, että $z \equiv 0 \pmod 3$, joten on olemassa $m \in \mathbb{Z}$ niin, että $z = 3m$. Tästä saadaan, että

$$z^3 = (3m)^3 = 27m^3.$$

Siispä $z^3 \equiv 0 \pmod{27}$. Toisaalta

$$\begin{aligned} (x+y)(x^2 - xy + y^2) &= x^3 - x^2y + xy^2 + x^2y - xy^2 + y^3 \\ &= x^3 + y^3 = z^3, \end{aligned}$$

joten

$$(x+y)(x^2 - xy + y^2) = z^3 \equiv 0 \pmod{27}.$$

Tästä nähdään, että luku $(x + y)(x^2 - xy + y^2)$ on muotoa

$$(x+y)(x^2 - xy + y^2) = 27n = 3^3 n,$$

missä $n \in \mathbb{Z}$. Toisaalta aikaisemman perusteella tiedetään, että

$$3 \mid (x+y) \qquad 3 \mid (x^2 - xy + y^2) \qquad \text{ja} \qquad 9 \nmid x^2 - xy + y^2.$$

Luvut $x + y$ ja $x^2 - xy + y^2$ voidaan siis kirjoittaa muodossa

$$x + y = 9a^3 \qquad \text{ja} \qquad x^2 - xy + y^2 = 3b^3,$$

missä $a, b \in \mathbb{Z}$ ja luku b ei ole jaollinen luvulla 3. Nyt siis

$$z^3 = (x+y)(x^2 - xy + y^2) = 9a^3 \cdot 3b^3 = 27a^3b^3 = (3ab)^3.$$

Siispä $z = 3ab$ eli $a = \frac{z}{3b}$.

Tarkastellaan seuraavaksi lukua $x^2 - xy + y^2$. Se voidaan kirjoittaa Eisenteinin kokonaislukujen avulla muodossa $x^2 - xy + y^2 = (x + y\rho)(x + y\rho^2)$, missä $\rho = \frac{i\sqrt{3}-1}{2}$ on ykkösen kuutiojuuri, sillä

$$\begin{aligned}(x + y\rho)(x + y\rho^2) &= (x + y\rho)(x + y(-\rho - 1)) = (x + y\rho)(x - y\rho - y)\\ &= x^2 - xy\rho - xy + xy\rho - y^2\rho^2 - y^2\rho\\ &= x^2 - xy + y^2(-\rho^2 - \rho) = x^2 - xy + y^2(1 + \rho - \rho)\\ &= x^2 - xy + y^2.\end{aligned}$$

Valitaan $\lambda = 1 - \rho \in \mathcal{E}$. Tällöin $(1 + \rho)\lambda^2 = 3$, sillä

$$\begin{aligned}(1 + \rho)\lambda^2 &= (1 + \rho)(1 - \rho)^2 = (1 + \rho)(1 - \rho)(1 - \rho)\\ &= (1 - \rho^2)(1 - \rho) = (1 + \rho + 1)(1 - \rho)\\ &= (2 + \rho)(1 - \rho) = 2 - 2\rho + \rho - \rho^2\\ &= 2 - \rho + \rho + 1 = 3.\end{aligned}$$

Nyt siis luku λ jakaa luvun 3, sillä $(1 + \rho)\lambda^2 = 3$ ja $\rho + 1 \in \mathcal{E}$.

Tiedetään, että $x \equiv 1 \pmod 3$ ja $y \equiv -1 \pmod 3$, joten saadaan

$$x + y \equiv 1 - 1 \equiv 0 \pmod 3 \quad \text{ja} \quad x - 2y \equiv 1 - 2 \cdot (-1) \equiv 0 \pmod 3.$$

Koska $\lambda \mid 3$, luku λ jakaa myös luvut $x + y$ ja $x - 2y$. Lisäksi

$$x + y\rho = x + y(1 - \lambda) = x + y - y\lambda$$

ja

$$\begin{aligned}x + y\rho^2 &= x + y(-\rho - 1) = x - y(\rho + 1) = x - y(1 - \lambda + 1)\\ &= x - y(2 - \lambda) = x - 2y + y\lambda,\end{aligned}$$

joten nyt nähdään, että luku λ on yhteinen tekijä luvuille $x + y\rho$ ja $x + y\rho^2$. Itse asiassa voidaan näyttää, että luku λ on suurin yhteinen tekijä luvuille $x + y\rho$ ja $x + y\rho^2$. Kaikille kokonaisluvuille m ja n pätee, että

$$\begin{aligned}&(m + n + n\rho)(x + y\rho^2) - (n + m\rho + n\rho)(x + y\rho)\\ &= mx + my\rho^2 + nx + ny\rho^2 + nx\rho + ny - nx - ny\rho - mx\rho - my\rho^2 - nx\rho - ny\rho^2\\ &= mx(1 - \rho) + ny(1 - \rho) = (mx + ny)\lambda.\end{aligned}$$

Koska $(x, y) = 1$, voidaan Bézout'n lemman nojalla valita luvut m ja n siten, että $mx + ny = 1$. Siispä luku λ todella on suurin yhteinen tekijä luvuille $x + y\rho$ ja $x + y\rho^2$.

Tiedetään, että $(1+\rho)\lambda^2 = 3$. Koska $-\rho^2 = 1+\rho$, voidaan yhtälö kirjoittaa muodossa $(-\rho^2)\lambda^2 = 3$. Kertomalla tätä luvulla $-\rho$ ja muistamalla, että luku ρ on ykkösen kuutiojuuri, nähdään, että $\lambda^2 = -3\rho$. Lisäksi tiedetään Lemmasta 4.3, että luku ρ on Eisensteinin kokonaislukujen yksikkö. Siten yhtälöstä

$$(x + y\rho)(x + y\rho^2) = x^2 - xy + y^2 = 3b^3$$

ja luvun b yksikäsitteisestä Eisensteinin alkutekijäesityksestä, saadaan yhtälö

$$x + y\rho = \varepsilon\lambda(c + d\rho)^3,$$

missä luvut c ja d ovat kokonaislukuja ja ε on yksikkö. Tiedetään, että λ jakaa luvun $x + y\rho$ ja sieventämällä saadaan

$$\begin{aligned}\frac{x+y\rho}{\lambda} &= \frac{x - x\rho + x\rho + y\rho}{\lambda} = \frac{x(1-\rho)+\rho(x+y)}{\lambda} = \frac{x\lambda}{\lambda} - \frac{-3\rho(x+y)}{3\lambda} \\ &= x + \frac{\lambda^2(x+y)}{3\lambda} = x - \frac{\lambda(x+y)}{3} = x - \lambda\frac{9a^3}{3} = x - 3a^3\lambda.\end{aligned}$$

Lisäksi

$$\begin{aligned}(c+d\rho)^3 &= c^3 + 3c^2d\rho + 3c(d\rho)^2 + (d\rho)^3 = c^3 + 3c^2d\rho + 3cd^2(-\rho - 1) + d^3 \\ &= c^3 + 3c^2d\rho - 3cd^2\rho - 3cd^2 + d^3 = c^3 + 3cd(c-d)\rho - 3cd^2 + d^3 \\ &= c^3 - 3cd^2 + d^3 + 3cd(c-d)\rho.\end{aligned}$$

Näiden avulla yhtälö $x + y\rho = \varepsilon\lambda(c + d\rho)^3$ saadaan muotoon

$$x - 3a^3\lambda = \varepsilon(c^3 - 3cd^2 + d^3 + 3cd(c-d)\rho).$$

Järjestetään nyt yhtälö siten, että oikealla puolella on kaikki termit, joista löytyy kertoimena luku 3, ja vasemmalla puolella on termit, joissa sitä ei ole. Näin saadaan yhtälö muotoon

$$x - \varepsilon(c^3 + d^3) = 3(a^3\lambda + \varepsilon(cd(c-d)\rho - cd^2)).$$

Koska $x \equiv 1 \pmod 3$, nähdään tästä, että

$$\varepsilon(c^3 + d^3) \equiv 1 \pmod 3.$$

Lemman 4.3 nojalla Eisensteinin kokonaislukujen joukossa yksiköitä ovat luvut ± 1, $\pm\rho$ ja $\pm\rho^2$. Siten saadusta yhtälöstä nähdään, että $\varepsilon = \pm 1$. Vaihtamalla tarvittaessa lukujen c ja d merkit, voidaan olettaa, että $\varepsilon = 1$. Nyt saadaan siis, että

$$x - (c^3 + d^3) = 3(a^3\lambda + (cd(c-d)\rho - cd^2)).$$

Koska $x, c, d \in \mathbb{Z}$, luku $x - (c^3 + d^3)$ on kokonaisluku. Siispä myös luvun

$$a^3\lambda + (cd(c-d)\rho - cd^2) = a^3 - a^3\rho + cd(c-d)\rho - cd^2$$

on oltava kokonaisluku. Huomataan, että tämä on totta vain, kun

$$a^3 = cd(c-d).$$

Jos luvuilla c ja d on yhteinen tekijä, niin siitä seuraisi, että myös luvuilla x ja y olisi yhteinen tekijä. Tämä on kuitenkin ristiriita, joten $(c, d) = 1$. Tästä taas seuraa, että

$$(c, c-d) = (d, c-d) = 1.$$

On siis oltava kokonaisluvut x_1, y_1 ja z_1 siten, että

$$c = z_1^3, \qquad d = y_1^3 \qquad \text{ja} \qquad c - d = x_1^3.$$

Nyt $x_1^3 + y_1^3 = c - d + d = c = z_1^3$ ja

$$|x_1y_1z_1| = \left|((c-d)cd)^{\frac{1}{3}}\right| = \left|(a^3)^{\frac{1}{3}}\right| = |a| = \left|\frac{z}{3b}\right| < |zxy|.$$

Tämä on kuitenkin ristiriita, sillä kokonaisluvut x, y ja z valittiin todistuksen alussa siten, että yhtälö $x^3 + y^3 = z^3$ on voimassa ja $|zxy|$ on pienin mahdollinen.

□

Äsken nähty todistus ja kolmannessa luvussa nähtyjen neliöiden summiin liittyvien lauseiden (Lause 3.9 ja Lause 3.18) todistukset ovat hyviä esimerkkejä siitä, kuinka luonnollisille luvuille pystytään näyttämään jokin ominaisuus, kun laajennetaan tavallisten kokonaislukujen joukkoa. Seuraavassa luvussa tarkastellaan lyhyesti tutkielmassa käytettyjä laajennuksia niiden geometrisen tulkinnan kautta.

LUKU 5

Kokonaislukujen laajennusten geometrista tulkintaa

Tässä luvussa tarkastellaan lähemmin Gaussin, Eisensteinin ja Hurwitzin kokonaislukujen geometrista tulkintaa. Kuten aikaisemmin on jo huomattu, kokonaislukujen laajennukset tarjoavat kätevän apuvälineen lukuteorian tulosten todistamisessa. Niiden käyttöön liittyy kuitenkin ongelmia, joita pelkillä kokonaisluvuilla ei esiinny. Tästä esimerkkinä mainittakoon lukujen asettaminen suuruusjärjestykseen. Kuten aikaisemmin on mainittu, tämä voidaan ratkaista normin N avulla.

Kerrataan kuitenkin ensin hieman tavallisten kokonaislukujen ominaisuuksia. Kuvassa 5.1 on esitetty itseisarvoltaan pienimmät kokonaisluvut ja siitä voidaan nähdä, että kokonaisluvut ovat pisteitä reaalilukusuoralla. Luku 0 on esitetty kuvassa keltaisella, yksiköt punaisella ja loput sinisellä.

Kuva 5.1. Kokonaisluvut ovat pisteitä reaalilukusuoralla.

Kokonaislukujen joukko on hyvinjärjestetty eli esimerkiksi kahden eri luvun suuruutta voidaan helposti verrata. Jos esimerkiksi tarkastellaan lukuja -6 ja 4, niin nähdään, että

$$-6 < 4.$$

Jos taas halutaan verrata niiden etäisyyttä luvusta 0, onnistuu tämä itseisarvon avulla. Tällöin

$$|-6| = 6 \qquad \text{ja} \qquad |4| = 4$$

ja koska $4 < 6$, nähdään, että luku 4 on lähempänä lukua 0. Suuruusjärjestys antaa mahdollisuuden esimerkiksi siihen, että kokonaisluvun alkutekijäesityksessä tekijät voidaan helposti järjestää.

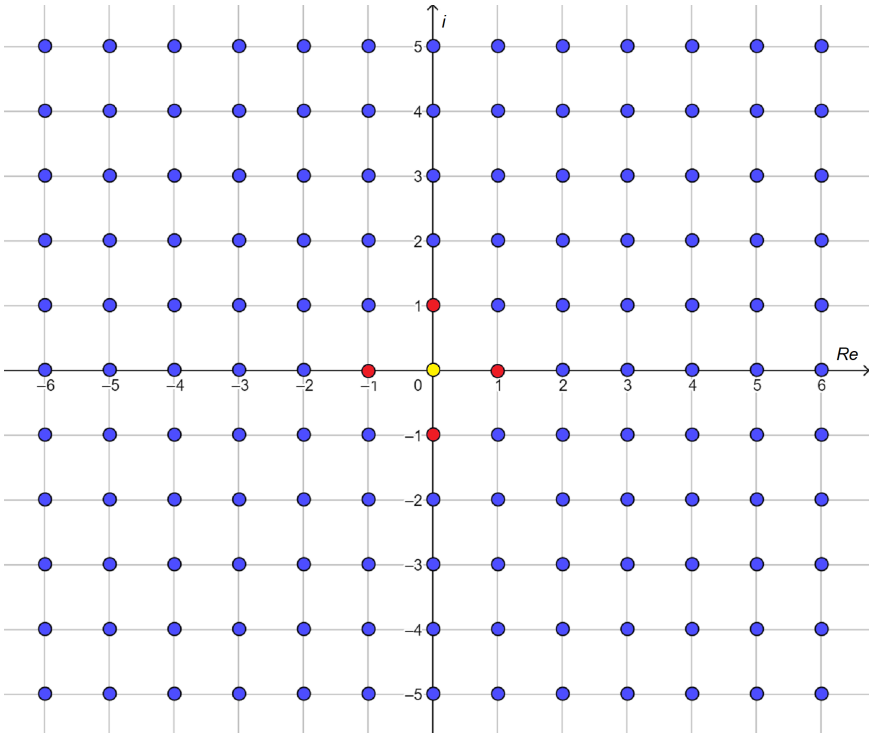
Lisäksi on syytä huomioida, että tavallisia kokonaislukuja tarkasteltaessa liikutaan yhdessä ulottuvuudessa. Tämän ansiosta esimerkiksi kokonaislukujen alkuluvuille voidaan näyttää melko vaivatta eräs alkulukuihin liittyvä tulos. Jos reaalilukusuoraa pitkin lähdetään kävelemään kuvittelemalla alkuluvut askelkiviksi ja ottamalla askelmitalle jokin tietty yläraja, niin huomattaisiin, että kävely tulisi päätökseen jossain

vaiheessa, kun kiellettäisiin samalle askelkivelle uudelleen astuminen. Äskeinen alkulukukävely tarkoittaa siis sitä, että alkulukujen välissä on olemassa mielivaltaisen suuria välejä.

Lähdetään seuraavaksi tarkastelemaan kokonaislukujen laajennuksia ja aloitetaan Gaussin kokonaisluvuista.

5.1. Gaussin kokonaislukujen geometrista tulkintaa

Gaussin kokonaisluvut ovat esimerkki kokonaislukujen kaksiulotteisesta laajennuksesta. Kuvasta 5.2 nähdään, että Gaussin kokonaisluvut ovat pisteitä reaaliakselin ja imaginääriakselin määräämässä tasossa. Luku $0_{\mathbb{Z}[i]}$ on merkitty keltaisella, yksiköt punaisella ja loput sinisellä. Gaussin kokonaislukuja edustavat pisteet ovat kokonaislukujen määräämien suorien leikkauspisteitä.



Kuva 5.2. Gaussin kokonaisluvut ovat pisteitä kompleksitasossa.

Kuvassa 5.2 näkyvät Gaussin kokonaislukujen pisteet ovat itse asiassa "pienimmät" joukosta $\mathbb{Z}[i]$. Tarkastellaan seuraavaksi, mitä Gaussin kokonaislukujen pienuudella tai suuruudella oikeastaan tarkoitetaankaan. Jos esimerkiksi tarkasteltaisiin Gaussin kokonaislukuja $5+3i$ ja $-4-4i$, niin suoraan lukuja vertaamalla on niitä hankala asettaa suuruusjärjestykseen kuten äsken kokonaisluvuille helposti tehtiin.

Näytetään seuraavaksi, että Gaussin kokonaislukujen normi N antaa ratkaisun tälle ongelmalle. Aluksi voidaan huomata normin N vastaavan tason $\mathbb{R}^2$ normin neliötä. On siten luontevaa ajatella normin N kertovan Gaussin kokonaisluvun etäisyydestä

lukuun $0_{\mathbb{Z}[i]}$. Lisäksi tiedetään, että normi N liittää jokaiseen Gaussin kokonaislukuun jonkin ei-negatiivisen kokonaisluvun. Kokonaislukujen joukko taas on hyvinjärjestetty, joten normin N avulla voidaan Gaussin kokonaisluvut järjestää eräänlaiseen suuruusjärjestykseen. Esimerkiksi äskeisille luvuille

$$N(5+3i) = 5^2 + 3^2 = 25 + 9 = 34$$

ja

$$N(-4-4i) = (-4)^4 + (-4)^2 = 16 + 16 = 32.$$

Koska nyt $32 < 34$, voidaan luvut $5+3i$ ja $-4-4i$ järjestää seuraavasti:

$$-4-4i < 5+3i,$$

missä merkillä $<$ tarkoitetaan nyt oleellisesti samaa kuin kokonaislukujen joukossa. Äsken esitetyllä tavalla Gaussin alkuluvut voidaan järjestää Gaussin alkutekijäesityksessä. On kuitenkin syytä huomioida, ettei normin N arvot ole yksikäsitteiset eli Gaussin kokonaislukujen normit voivat olla yhtä suuret. Esimerkissä 2.15 saatiin luvun $-2+24i$ Gaussin alkutekijäesitykseksi

$$-2+24i = (1+i)(1-i)(2+i)(2+5i).$$

Tässä tekijöiden $1+i$ ja $1-i$ normin arvot ovat yhtä suuret, sillä

$$N(1+i) = 1^2 + 1^2 = 2 \qquad \text{ja} \qquad N(1-i) = 1^2 + (-1)^2 = 2.$$

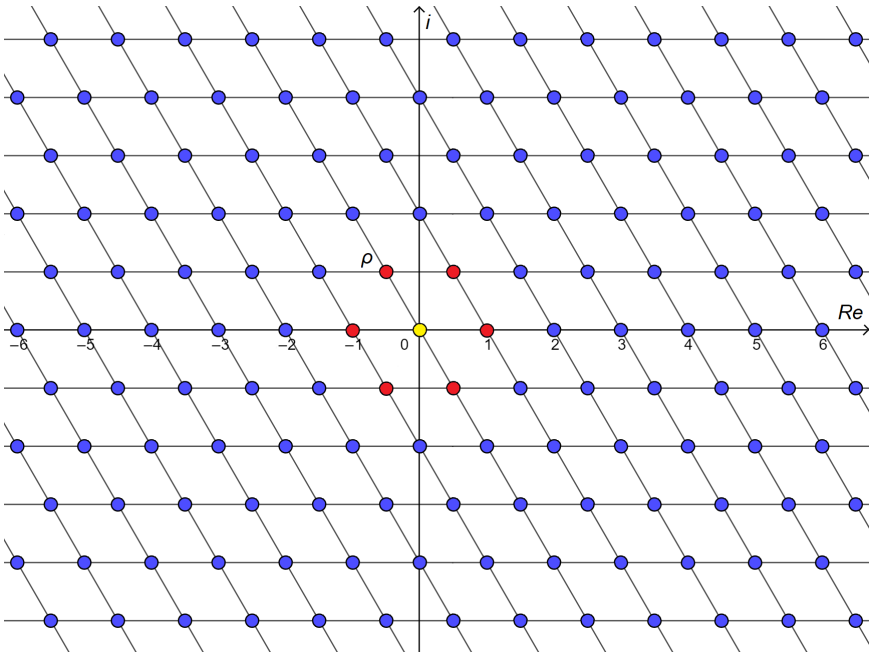
Aikaisemmin todettiin ikuisesti jatkuvan alkulukukävelyn olevan mahdoton kokonaislukujen alkuluvuille, kun valitaan jokin kiinteä yläraja askelpituudelle. Gaussin alkuluvuille vastaava tilanne on toistaiseksi ratkaisematon ongelma. Sen esitti ensimmäisenä yhdysvaltalainen matemaatikko Basil Gordon (1931–2012) vuonna 1962. Kokonaisluvuille yhdessä ulottuvuudessa liikkuminen teki ongelmasta helpon ratkaista. Gaussin kokonaisluvuilla sen sijaan liikutaan kahdessa ulottuvuudessa, mikä tekee ongelmasta huomattavasti haastavamman.

Tähän mennessä on pystytty näyttämään, että Gaussin kokonaislukujen tasossa on olemassa mielivaltaisen suuria kiekkoja, joissa ei esiinny Gaussin alkulukuja. Tämä ei kuitenkaan ole este alkulukukävelylle, sillä este voi olla mahdollista kiertää. Ongelman yksi ratkaisutapa on osoittaa, että on olemassa mielivaltaisen leveä rinki, joka ympäröi kävelyn lähtöpistettä ja jossa ei ole Gaussin alkulukuja. Jos tällainen rinki on olemassa, niin askelkivien määrä on rajallinen ja tällöin alkulukukävelyä ei voida jatkaa ikuisesti. Rinki voidaan ajatella eräänlaisena vallihautana, minkä vuoksi ongelma tunnetaan myös Gaussin vallihautaongelmana. Aiheesta voi lukea lisää Gethnerin ja kumppaneiden artikkelista A Stroll Through Gaussian primes [**5**].

5.2. Eisensteinin kokonaislukujen geometrista tulkintaa

Tarkastellaan seuraavaksi Eisensteinin kokonaislukuja. Ne ovat toinen hyvä esimerkki kokonaislukujen kaksiulotteisesta laajennuksesta. Kuvasta 5.3 nähdään, että myös Eisensteinin kokonaisluvut ovat pisteitä tasossa, jonka muodostavat reaaliakseli ja imaginääriakseli. Kuvassa luku $0_{\mathcal{E}}$ on esitetty keltaisella, yksiköt punaisella ja loput sinisellä. Tärkeä ero Gaussin kokonaislukuihin on hilassa, joka molemmille lukujoukoille

rakentuu hieman eri tavalla. Gaussin kokonaisluvut muodostavat neliöhilan, mutta Eisensteinin kokonaisluvut muodostavat heksagonaalisen hilan, mistä käytetään myös nimitystä kolmiohila.



KUVA 5.3. Eisensteinin kokonaisluvut ovat pisteitä kompleksitasossa.

Ero hilarakenteessa johtuu Gaussin ja Eisensteinin kokonaislukujen määrittelystä. Gaussin kokonaisluvut määriteltiin kompleksilukuina z, jotka ovat muotoa

$$z = a + ib,$$

missä $a, b \in \mathbb{Z}$. Reaaliakseli ja imaginääriakseli leikkaavat toisensa 90 asteen kulmassa, minkä vuoksi hilarakenteeseenkin muodostuu 90 asteen kulmat. Eisensteinin kokonaisluvut taas määriteltiin kompleksilukuina z, jotka ovat muotoa

$$z = a + \rho b,$$

missä $a, b \in \mathbb{Z}$ ja $\rho = \frac{i\sqrt{3}-1}{2}$. Nyt luvun ρ määrittelystä voidaan huomata, että se muodostaa 120 asteen kulman reaaliakselin kanssa. Siten hilarakennekin koostuu 120 asteen kulmista.

Eisensteinin kokonaisluvut voidaan järjestää samaan tapaan suuruusjärjestykseen kuin Gaussin kokonaisluvut, sillä myös jokaiselle Eisensteinin kokonaisluvuille normi N kiinnittää jonkin ei-negatiisen kokonaisluvun, jolle suuruuden vertailu onnistuu helposti.

5.3. Hurwitzin kokonaislukujen geometrista tulkintaa

Hurwitzin kokonaisluvut ovat esimerkki kokonaislukujen neliulotteisesta laajennuksesta, minkä vuoksi niiden esittäminen kuvana on hankalaa. Neliulotteisen avaruuden

niille muodostavat reaaliakseli ja imaginääriakselit i, j ja k. Näiden akselien kokonaislukujen ja puolikokonaislukujen määrämien suorien leikkauspisteet ovat Hurwitzin kokonaislukuja.

Hurwitzin kokonaislukujen normi N kiinnittää jokaiseen Hurwitzin kokonaislukuun ei-negatiivisen kokonaisluvun, joten myös Hurwitzin kokonaisluvuilla osittaiseen suuruusjärjestykseen asettaminen on mahdollista.

Lähteet

[1] A. D. Aczel: *Fermat's Last Theorem: Unlocking the Secret of Ancient Mathematical Problem.* First Edition, Four Walls Eight Windows, 1996.

[2] W. A. Coppel: *Number Theory: An Introduction to Mathematics.* Second Edition, Clarendon Press: Oxford University Press, 2009.

[3] G. Dresden ja W. Dymàček : *Finding Factors of Factor Rings over the Gaussian Integers.* The American Mathematical Monthly. 112 (2005), no. 7, 602–611.

[4] G. Everest ja T. Ward: *An Introduction to Number Theory.* First Edition, Springer, 2005.

[5] E. Gethner, S. Wagon ja B. Wick : *A Stroll Through the Gaussian Primes.* The American Mathematical Monthly. 105 (1998), no. 4, 327–337.

[6] G. H. Hardy ja E. M. Wright: *An Introduction to the Theory of Numbers.* Fourth Edition, Springer, 1960.

[7] G.A. Jones ja J. M. Jones: *Elementary Number Theory.* First Edition, Springer, 1998.

[8] P. Koskela: *Algebra 1: Renkaat ja kunnat, luentomoniste.* Jyväskylän yliopisto, kevät 2017.

[9] F. Lemmermeyer: *Reciprocity Laws: from Euler to Eisenstein.* First Edition, Springer, 2000.

[10] J. H. Silverman: *A Friendly Introduction to Number Theory.* Third Edition, Pearson, 2006.

[11] J. Stillwell: *Mathematics and its History.* Third Edition, Springer, 2010.

[12] D. Underwood: *A Guide to Elementary Number Theory.* First Edition, Cambridge University Press, 2012.

[13] A. Wiles: *Modular Elliptic Curves and Fermat's Last Theorem.* Ann. of Math. (2) 141 (1995), no. 3, 443–551.