TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Elina Holopainen

Gaussin kokonaisluvuista

Matematiikan ja tilastotieteen laitos
Matematiikka
Maaliskuu 2009

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

HOLOPAINEN, ELINA: Gaussin kokonaisluvuista

Pro gradu -tutkielma, 30 s.

Matematiikka

Maaliskuu 2009

Tiivistelmä

Tässä tutkielmassa käsitellään Gaussin kokonaislukuja ja niiden ominaisuuksia. Gaussin kokonaisluvuiksi kutsutaan kompleksilukuja, joissa sekä reaaliosa että imaginaariosa ovat kokonaislukuja. Luvussa 2.1 esitellään Gaussin kokonaislukuihin liittyviä määritelmiä sekä lukuteoreettisia perusominaisuuksia, joita tarvitaan tutkielman seuraavissa luvuissa. Luvuissa 2.2 ja 2.3 osoitetaan, että rationaalisille kokonaisluvuille tunnetut suurin yhteinen tekijä, jakoalgoritmi, Eukleideen algoritmi, alkuluvut sekä aritmetiikan peruslause voidaan ilmaista myös Gaussin kokonaisluvuille. Luvussa 3.1 osoitetaan Gaussin kokonaislukujen avulla, mitkä rationaaliset alkuluvut voidaan esittää kahden neliön summana. Edellistä laajempi tulos, eli mitkä kaikki rationaaliset kokonaisluvut voidaan esittää kahden neliön summana, osoitetaan rationaalisten kokonaislukujen avulla. Lisäksi osoitetaan Gaussin kokonaislukujen avulla, kuinka monella eri tavalla rationaalinen kokonaisluku voidaan esittää kahden neliön summana. Luvussa 3.2 esitetään Gaussin kokonaislukujen avulla, mitkä rationaaliset kokonaisluvut toteuttavat yhtälön $x^2 + y^2 = z^2$.

Sisältö

1 Johdanto

Tässä tutkielmassa tarkastellaan Gaussin kokonaislukuja ja niiden ominaisuuksia. Gaussin kokonaisluvuiksi kutsutaan kompleksilukuja, joissa sekä reaaliosa että imaginaariosa ovat kokonaislukuja. Gaussin kokonaisluvuilla on useita samoja lukuteoreettisia ominaisuuksia kuin rationaalisilla eli tavallisilla kokonaisluvuilla.

Luvussa 2.1 esitetään Gaussin kokonaislukuihin liittyviä peruskäsitteitä ja -ominaisuuksia. Luvussa 2.2 esitetään jakoalgoritmi ja Eukleideen algoritmi Gaussin kokonaisluvuille, määritellään suurin yhteinen tekijä Gaussin kokonaisluvuille ja todistetaan joitakin suurimman yhteisen tekijän ominaisuuksia. Luvussa 2.3 määritellään Gaussin alkuluvun käsite ja esitetään aritmetiikan peruslause Gaussin kokonaisluvuille. Lisäksi osoitetaan rationaalisten alkulukujen ja Gaussin alkulukujen välillä oleva yhteys. Lukujen 2.1- 2.3 alussa on vertailtu rationaalisten kokonaislukujen ja Gaussin kokonaislukujen ominaisuuksia luvussa käsiteltävien määritelmien ja lauseiden osalta.

Luvussa 3.1 todistetaan Gaussin kokonaislukujen avulla, mitkä rationaaliset alkuluvut voidaan esittää kahden neliön summana. Lisäksi todistetaan rationaalisten kokonaislukujen ja alkutekijäesityksen avulla, mitkä kaikki rationaaliset kokonaisluvut voidaan esittää kahden neliön summana. Luvussa 3.2 määritellään Pythagoraan kolmikko sekä primitiivinen Pythagoraan kolmikko ja esitetään Gaussin kokonaislukujen avulla, mitkä rationaaliset kokonaisluvut toteuttavat yhtälön $x^2 + y^2 = z^2$.

Tutkielman päälähteenä on käytetty Kenneth H. Rosenin teosta *Elementary Number Theory and Its Applications*. Kaikkien kappaleiden määritelmät ovat kyseisestä teoksesta. Kunkin lauseen ja apulauseen yhteydessä on erikseen mainittu, mistä lähteestä kyseinen todistus on. Tutkielmassa esitetyt esimerkit ovat tekijän laatimia, ellei toisin mainita.

Lukijan oletetaan hallitsevan kompleksilukujen ja kongruenssien alkeet sekä lineaarisen kongruenssin ratkaisemisen. Lukijalle oletetaan myös tutuksi hyvinjärjestysperiaate sekä perusteet rationaalisten kokonaislukujen lukuteoreettisista ominaisuuksista.

2 Gaussin kokonaisluvut

2.1 Peruskäsitteitä ja -ominaisuuksia

Gaussin kokonaisluvuilla on useita samoja aritmeettisia ominaisuuksia kuin rationaalisilla eli tavallisilla kokonaisluvuilla. Rationaalisten kokonaislukujen tavoin Gaussin kokonaisluvut ovat sulkeutuvia yhteen-, vähennys- ja kertolaskun suhteen, mutta eivät jakolaskun suhteen. Lisäksi Gaussin kokonaisluvuille on rationaalisten kokonaislukujen tavoin määritelty luvun itseisarvo sekä lukujen jaollisuus. Rationaalisten kokonaislukujen joukossa yksiköitä on kaksi kappaletta, luvut 1 ja -1, ja kullakin luvulla on kaksi liitännäistä. Gaussin kokonaislukujen joukossa yksiköitä on neljä kappaletta ja kullakin luvulla on neljä liitännäistä. Tässä luvussa esitetään edellä mainittujen ominaisuuksien lisäksi myös sellaisia Gaussin kokonaislukujen ominaisuuksia, joita ei ole määritelty pelkästään rationaalisille kokonaisluvuille. Näitä ovat mm. luvun konjungaatti ja normi.

Määritelmä 2.1. Kompleksilukua $a + bi$, missä a ja b ovat kokonaislukuja, sanotaan *Gaussin kokonaisluvuksi*. Gaussin kokonaislukujen joukkoa merkitään symbolilla $\mathbb{Z}[i]$.

Tässä tutkielmassa Gaussin kokonaislukuja merkitään kreikkalaisilla kirjaimilla $\alpha, \beta, \gamma, \ldots$

Esimerkki 2.1. Luvut $\alpha = 5 + 13i$, $\beta = -3 + i$ ja $\gamma = 8 = 8 + 0 \cdot i$ ovat Gaussin kokonaislukuja.

Kaikki rationaaliset kokonaisluvut ovat myös Gaussin kokonaislukuja. Niissä luvun imaginääriosa on nolla.

Lause 2.1. *Olkoot α ja β Gaussin kokonaislukuja. Tällöin myös luvut $\alpha+\beta$, $\alpha - \beta$ ja $\alpha\beta$ ovat Gaussin kokonaislukuja.*

Todistus. (vrt. [3, s. 549]) Olkoot $\alpha = a + bi$ ja $\beta = c + di$, missä a, b, c ja d ovat rationaalisia eli tavallisia kokonaislukuja. Tällöin

$$\alpha + \beta = (a + bi) + (c + di) = (a + c) + (b + d)i$$

$$\alpha - \beta = (a + bi) - (c + di) = (a - c) + (b - d)i$$

$$\alpha\beta = (a + bi)(c + di) = ac + adi + bci + bdi^2 = (ac - bd) + (ad + bc)i.$$

Koska selvästi luvut $a \pm c$, $b \pm d$, $ac - bd$ ja $ad + bc$ ovat myös rationaalisia kokonaislukuja, on väite määritelmän 2.1 nojalla tosi.

□

Kahden Gaussin kokonaisluvun osamäärä ei aina ole Gaussin kokonaisluku. Tämä voidaan osoittaa esimerkillä.

Esimerkki 2.2. Olkoot $\alpha = 2$ ja $\beta = 1 - 2i$. Lukujen α ja β osamäärää voidaan sieventää kertomalla ja jakamalla se luvulla $1+2i$. Näin osamääräksi saadaan

$$\frac{\alpha}{\beta} = \frac{2}{1-2i} = \frac{2}{1-2i} \cdot \frac{1+2i}{1+2i} = \frac{2+4i}{1^2-(2i)^2} = \frac{2+4i}{1+4} = \frac{2+4i}{5} = \frac{2}{5} + \frac{4}{5}i.$$

Koska $\frac{2}{5}$ ja $\frac{4}{5}$ eivät ole kokonaislukuja, määritelmän 2.1 perusteella osamäärä $\frac{\alpha}{\beta}$ ei ole Gaussin kokonaisluku.

Seuraavassa määritelmässä on korjattu lähteessä [3, s. 548] ollut painovirhe.

Määritelmä 2.2. Gaussin kokonaisluvun α *konjungaattia* merkitään symbolilla $\overline{\alpha}$ ja se saadaan luvusta α vaihtamalla imaginääriosan etumerkki. Siis Gaussin kokonaisluvun $\alpha = a + bi$ konjungaatti on $\overline{\alpha} = a - bi$.

Seuraavan apulauseen todistusta ei ole esitetty lähdekirjallisuudessa, vaan sen on laatinut tekijä itse.

Apulause 2.1. *Olkoot α ja β Gaussin kokonaislukuja. Tällöin $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.*

Todistus. Olkoot $\alpha = a + bi$ ja $\beta = c + di$ Gaussin kokonaislukuja. Lukujen α ja β tuloksi saadaan $\alpha\beta = (a+bi)(c+di) = (ac-bd)+(ad+bc)i$ ja tällöin tulon $\alpha\beta$ konjungaatti on

$$\overline{\alpha\beta} = (ac-bd)-(ad+bc)i = ac - adi - bd - bci = a(c-di) + i^2bd - bci$$

$$= a(c-di) + bi(di-c) = a(c-di) - bi(c-di) = (a-bi)(c-di) = \overline{\alpha}\overline{\beta}.$$

Siis $\overline{\alpha\beta} = \overline{\alpha}\overline{\beta}$.

□

Määritelmä 2.3. Olkoon $\alpha = a + bi$ Gaussin kokonaisluku. Luvun α *itseisarvoa* merkitään symbolilla $|\alpha|$ ja se saadaan yhtälöstä $|\alpha| = \sqrt{a^2+b^2}$. Luvun α *normia* merkitään symbolilla $N(\alpha)$ ja se on luvun α itseisarvon neliö. Siis $N(\alpha) = |\alpha|^2 = a^2 + b^2$.

Luvun normi mittaa Gaussin kokonaisluvun suuruutta vastaavasti, kuten itseisarvo mittaa rationaalisen kokonaisluvun suuruutta.

Huomautus 2.1. (vrt. [3, s. 548]) Olkoon $\alpha = a+bi$ Gaussin kokonaisluku. Luvun α ja sen konjungaatin $\overline{\alpha}$ tulo on luvun α normi eli

$$\alpha\overline{\alpha} = (a+bi)(a-bi) = a^2 + b^2 = N(\alpha).$$

Lause 2.2. *Olkoot α ja β Gaussin kokonaislukuja. Tällöin normifunktiolla $N : \mathbb{Z}[i] \to \mathbb{Z}_+ \cup \{0\}$ on ominaisuudet*

(i) $N(\alpha)$ *on ei-negatiivinen kokonaisluku*

(ii) $N(\alpha) = 0$, *jos ja vain jos* $\alpha = 0$

(iii) $N(\alpha\beta) = N(\alpha)N(\beta)$.

Todistus. (vrt. [1, s. 196])

(i) Olkoon $\alpha = a + bi$, missä a ja b ovat kokonaislukuja. Tällöin normi $N(\alpha) = a^2 + b^2$ on ei-negatiivinen kokonaisluku, koska selvästi sekä a^2 että b^2 ovat ei-negatiivisia kokonaislukuja.

(ii) Olkoon $\alpha = a + bi$, missä a ja b ovat kokonaislukuja. Tällöin normi $N(\alpha) = a^2 + b^2 = 0$, jos ja vain jos $a = 0$ ja $b = 0$ eli $\alpha = 0 + i \cdot 0 = 0$.

(iii) Huomautuksen 2.1 ja apulauseen 2.1 perusteella tulon $\alpha\beta$ normiksi saadaan $N(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = (\alpha\beta)(\overline{\alpha}\overline{\beta}) = (\alpha\overline{\alpha})(\beta\overline{\beta}) = N(\alpha)N(\beta)$.

□

Määritelmä 2.4. Olkoot α ja β Gaussin kokonaislukuja. Sanotaan, että α *jakaa* luvun β, jos on olemassa sellainen Gaussin kokonaisluku γ, että $\beta = \alpha\gamma$. Jos α jakaa luvun β, merkitään $\alpha \mid \beta$. Jos α ei jaa lukua β, merkitään $\alpha \nmid \beta$.

Esimerkki 2.3. Olkoot $\alpha = 3+i$ ja $\beta = 19+13i$. Nyt $\alpha \mid \beta$, sillä on olemassa sellainen Gaussin kokonaisluku $\gamma = 7 + 2i$, että

$$\alpha\gamma = (3 + i)(7 + 2i) = 21 + 6i + 7i + 2i^2 = 21 + 13i - 2 = 19 + 13i = \beta.$$

Määritelmä 2.5. Olkoon ϵ nollasta poikkeava Gaussin kokonaisluku. Lukua ϵ sanotaan *yksiköksi*, jos se jakaa luvun yksi.

Esimerkki 2.4. Luku i on yksikkö, sillä se on nollasta poikkeava Gaussin kokonaisluku ja $i(-i) = -i^2 = 1$. Siis määritelmän 2.4 perusteella i jakaa luvun 1.

Lause 2.3. *Olkoon α Gaussin kokonaisluku. Luku α on yksikkö, jos ja vain jos $N(\alpha) = 1$.*

Todistus. (vrt. [3], s. 551) Oletetaan ensin, että α on yksikkö, ja todistetaan, että tällöin $N(\alpha) = 1$. Määritelmien 2.4 ja 2.5 perusteella on olemassa sellainen Gaussin kokonaisluku θ, että $\alpha\theta = 1$. Lauseen 2.2 kohdan (iii) perusteella lukujen α ja θ tulon normiksi saadaan $N(\alpha\theta) = N(\alpha)N(\theta) = N(1) = 1^2 = 1$.

Koska α on yksikkö, se on nollasta poikkeava ja yhtälön $\alpha\theta = 1$ perusteella myös θ on nollasta poikkeava. Tällöin lauseen 2.2 perusteella sekä $N(\alpha)$ että $N(\theta)$ ovat positiivisia kokonaislukuja. Koska $N(\alpha)N(\theta) = 1$, on oltava $N(\alpha) = 1$ ja $N(\theta) = 1$.

Oletetaan sitten, että $N(\alpha) = 1$, ja todistetaan, että tällöin α on yksikkö. Huomautuksen 2.1 perusteella $N(\alpha) = \alpha\overline{\alpha} = 1$. Siis määritelmän 2.4 perusteella α jakaa luvun 1 ja määritelmän 2.5 perusteella α on yksikkö.

□

Lause 2.4. *Gaussin kokonaislukujen joukossa olevat yksiköt ovat* ± 1 *ja* $\pm i$.

Todistus. (vrt. [1, s. 197]) Olkoon $\epsilon = a+bi$ yksikkö Gaussin kokonaislukujen joukossa. Lauseen 2.3 perusteella luvun ϵ normi on $N(\epsilon) = a^2+b^2 = 1$. Koska ϵ on Gaussin kokonaisluku, luvut a ja b ovat rationaalisia kokonaislukuja. Tällöin yhtälön $a^2+b^2 = 1$ mahdolliset ratkaisut ovat $(a, b) = (\pm 1, 0), (0, \pm 1)$ ja yksikön ϵ mahdollisiksi arvoiksi saadaan ± 1 ja $\pm i$.

□

Määritelmä 2.6. Olkoot α ja β Gaussin kokonaislukuja. Sanotaan, että luvut α ja β ovat toistensa *liitännäisiä*, jos on olemassa sellainen Gaussin kokonaislukujen yksikkö ϵ, että $\alpha = \epsilon\beta$.

Liitännäisyys Gaussin kokonaislukujen joukossa on ekvivalenssirelaatio.

Huomautus 2.2. Määritelmän 2.6 ja lauseen 2.4 perusteella Gaussin kokonaisluvun α liitännäiset ovat α, $-\alpha$, $i\alpha$ ja $-i\alpha$.

Esimerkki 2.5. Luvun $1+13i$ liitännäiset ovat huomautuksen 2.2 perusteella $1 + 13i$, $-(1 + 13i) = -1 - 13i$, $i(1 + 13i) = i + 13i^2 = -13 + i$ sekä $-i(1 + 13i) = -i - 13i^2 = 13 - i$.

2.2 Jakoalgoritmi ja suurin yhteinen tekijä

Edellisen luvun ominaisuuksien lisäksi Gaussin kokonaisluvuille on olemassa rationaalisten kokonaislukujen tavoin jakoalgoritmi, suurin yhteinen tekijä sekä Eukleideen algoritmi. Tässä kappaleessa osoitetaan myös, että kahden Gaussin kokonaisluvun suurin yhteinen tekijä voidaan esittää kyseisten kahden luvun lineaarikombinaationa ja tämä lineaarikombinaatio on jaollinen suurimmalla yhteisellä tekijällä - aivan kuten rationaalisilla kokonaisluvuilla. Luvussa todistetaan vielä muun muassa, että jos kahdella Gaussin kokonaisluvulla on kaksi suurinta yhteistä tekijää, ovat nämä tekijät toistensa liitännäisiä.

Lause 2.5. *Gaussin kokonaislukujen jakoalgoritmi. Olkoot α ja β Gaussin kokonaislukuja ja β nollasta poikkeava. Tällöin on olemassa sellaiset Gaussin kokonaisluvut γ ja δ, että*

$$\alpha = \beta\gamma + \delta$$

ja $0 \leq N(\delta) < N(\beta)$. Kuten rationaalisilla kokonaisluvuilla, lukua γ kutsutaan osamääräksi *ja lukua δ kutsutaan* jakojäännökseksi.

Todistus. (vrt. [1, s. 198-199]) Olkoot $\alpha = a + bi$ ja $\beta = c + di$ Gaussin kokonaislukuja ja β nollasta poikkeava. Sievennetään lukujen α ja β osamäärää kertomalla ja jakamalla se luvun β konjungaatilla. Näin osamääräksi saadaan

$$\frac{\alpha}{\beta} = \frac{a+bi}{c+di} \cdot \frac{c-di}{c-di} = \frac{ac - adi + bci - bdi^2}{c^2 - cdi + cdi - (di)^2} = \frac{ac+bd}{c^2+d^2} + \frac{bc-ad}{c^2+d^2}i = e + fi,$$

missä $e = \frac{ac+bd}{c^2+d^2}$ ja $f = \frac{bc-ad}{c^2+d^2}$. Olkoon g lukua e lähinnä oleva kokonaisluku ja vastaavasti h lukua f lähinnä oleva kokonaisluku. Näin saadaan epäyhtälöt

$$|g - e| \leq \frac{1}{2} \quad \text{ja} \quad |h - f| \leq \frac{1}{2}.$$

Olkoon $\gamma = g + hi$. Tällöin osamäärä $\frac{\alpha}{\beta}$ voidaan kirjoittaa

$$\frac{\alpha}{\beta} = e + fi + \gamma - \gamma = e + fi + \gamma - (g + hi) = \gamma + (e - g) + (f - h)i.$$

Kerrotaan yhtälö puolittain luvulla β, jolloin saadaan, että

$$\alpha = \beta\gamma + [(e - g) + (f - h)i]\beta.$$

Olkoon $\delta = [(e - g) + (f - h)i]\beta$, jolloin edellinen yhtälö saadaan muotoon

$$\alpha = \beta\gamma + \delta.$$

Luvut α ja β ovat oletuksen mukaan Gaussin kokonaislukuja. Lisäksi γ on Gaussin kokonaisluku, koska g ja h ovat rationaalisia kokonaislukuja. Siis myös $\delta = \alpha - \beta\gamma$ on lauseen 2.1 perusteella Gaussin kokonaisluku. Määritelmän 2.3 ja lauseen 2.2 kohdan (iii) perusteella luvun δ normiksi saadaan

$$N(\delta) = N((e - g) + (f - h)i)N(\beta) = [(e - g)^2 + (f - h)^2]N(\beta).$$

Koska $|g - e| \leq \frac{1}{2}$ ja $|h - f| \leq \frac{1}{2}$, edellinen yhtälö saadaan muotoon

$$N(\delta) = [(e - g)^2 + (f - h)^2]N(\beta) \leq \left[\left(\frac{1}{2}\right)^2 + \left(\frac{1}{2}\right)^2\right]N(\beta) = \frac{1}{2}N(\beta) < N(\beta).$$

Lisäksi lauseen 2.2 perusteella $0 \leq N(\delta)$. Siis $0 \leq N(\delta) < N(\beta)$.

Huomioidaan vielä, että ristiriitaa ei aiheudu, sillä oletuksen mukaan β on nollasta poikkeava ja tällöin lauseen 2.2 perusteella $N(\beta) \neq 0$.

□

Esimerkki 2.6. ([3, s. 556], harjoitustehtävä 17 b) Olkoot $\alpha = 18 + 15i$ ja $\beta = 3 + 4i$. Osamäärä $\frac{\alpha}{\beta}$ saadaan laskettua vastaavasti, kuten lauseen 2.5 todistuksessa. Kerrotaan ja jaetaan ensin osamäärä luvun β konjungaatilla ja sievennetään. Tällöin saadaan

$$\frac{\alpha}{\beta} = \frac{18+15i}{3+4i} \cdot \frac{3-4i}{3-4i} = \frac{54-72i+45i+60}{3^2-(4i)^2} = \frac{114-27i}{25} = \frac{114}{25} - \frac{27}{25}i.$$

Seuraavaksi valitaan lukuja $\frac{114}{25} = 4,56$ ja $-\frac{27}{25} = -1,08$ lähinnä olevat kokonaisluvut, jotka ovat 5 ja -1. Siis osamääräksi saadaan $\gamma = 5 - i$ ja jakojäännös δ voidaan laskea seuraavasti

$$\delta = \alpha - \beta\gamma = 18+15i-(3+4i)(5-i) = 18+15i-15+3i-20i-4 = -1-2i.$$

Lasketaan lukujen δ ja β normit, jolloin saadaan $N(\delta) = (-1)^2 + (-2)^2 = 5$ ja $N(\beta) = 3^2 + 4^2 = 25$. Siis $0 \leq N(\delta) < N(\beta)$ ja lauseen 2.5 ehdot toteutuvat.

Jakoalgoritmin avulla saadaan yksi vaihtoehto luvuille γ ja δ. Muitakin vaihtoehtoja kuitenkin on. Esimerkiksi jakajaksi voidaan valita $\gamma = 4 - i$. Tällöin jakojäännökseksi saadaan

$$\delta = \alpha - \beta\gamma = 18 + 15i - (3 + 4i)(4 - i) = 2 + 2i.$$

Lisäksi $N(\delta) = 2^2+2^2 = 8$, ja kuten edellä $N(\beta) = 25$. Siis $0 \leq N(\delta) < N(\beta)$.

Määritelmä 2.7. Olkoot α ja β Gaussin kokonaislukuja. Gaussin kokonaisluku γ on lukujen α ja β *suurin yhteinen tekijä*, jos sillä on ominaisuudet

(i) $\gamma \mid \alpha$ ja $\gamma \mid \beta$

(ii) jos δ on sellainen Gaussin kokonaisluku, että $\delta \mid \alpha$ ja $\delta \mid \beta$, niin $\delta \mid \gamma$.

Jos γ on lukujen α ja β suurin yhteinen tekijä, merkitään $(\alpha, \beta) = \gamma$.

Lause 2.6. *Olkoot α ja β sellaisia Gaussin kokonaislukuja, että ainakin toinen niistä on nollasta poikkeava. Tällöin*

(i) *on olemassa Gaussin kokonaisluku γ, joka on lukujen α ja β suurin yhteinen tekijä*

(ii) *jos γ on lukujen α ja β suurin yhteinen tekijä, on olemassa sellaiset Gaussin kokonaisluvut μ ja ν, että $\gamma = \mu\alpha + \nu\beta$.*

Todistus. (vrt. [3, s. 560-561]) Olkoot μ ja ν Gaussin kokonaislukuja. Lauseen 2.1 perusteella myös $\mu\alpha + \nu\beta$ on Gaussin kokonaisluku. Olkoon S muotoa $\mu\alpha+\nu\beta$ olevien, nollasta poikkeavien Gaussin kokonaislukujen normien joukko. Tällöin lauseen 2.2 perusteella joukon S jokainen alkio on positiivinen kokonaisluku. Sekä $N(1\cdot\alpha+0\cdot\beta) = N(\alpha)$ että $N(0\cdot\alpha+1\cdot\beta) = N(\beta)$ kuuluvat joukkoon S. Koska oletuksen mukaan ainakin toinen luvuista α ja β on nollasta poikkeava, on lauseen 2.2 perusteella ainakin toinen luvuista $N(\alpha)$ ja $N(\beta)$ nollasta poikkeava. Siis joukko S ei ole tyhjä joukko.

Koska S on epätyhjä positiivisten kokonaislukujen joukko, siinä on hyvinjärjestysperiaatteen mukaan pienin alkio. Olkoon $\gamma = \mu_0\alpha + \nu_0\beta$, missä μ_0 ja ν_0 ovat Gaussin kokonaislukuja, ja olkoon $N(\gamma)$ joukon S pienin alkio. Siis kaikilla Gaussin kokonaisluvuilla μ ja ν pätee epäyhtälö

$$N(\gamma) \leq N(\mu\alpha + \nu\beta).$$

Osoitetaan, että γ on lukujen α ja β suurin yhteinen tekijä. Olkoon δ sellainen Gaussin kokonaisluku, että $\delta \mid \alpha$ ja $\delta \mid \beta$. Määritelmän 2.4 perusteella on olemassa sellaiset Gaussin kokonaisluvut ρ ja σ, että $\alpha = \delta\rho$ ja $\beta = \delta\sigma$. Luku γ voidaan nyt kirjoittaa muodossa

$$\gamma = \mu_0\alpha + \nu_0\beta = \mu_0\delta\rho + \nu_0\delta\sigma = \delta(\mu_0\rho + \nu_0\sigma).$$

Siis $\delta \mid \gamma$ ja määritelmän 2.7 kohta (ii) toteutuu.

Osoitetaan seuraavaksi, että γ jakaa jokaisen muotoa $\mu\alpha+\nu\beta$ oleva Gaussin kokonaisluvun. Näin saadaan osoitettua, että $\gamma \mid \alpha$ ja $\gamma \mid \beta$, koska $\alpha = 1 \cdot \alpha + 0 \cdot \beta$ ja $\beta = 0 \cdot \alpha + 1 \cdot \beta$. Olkoon $\tau = \mu_1\alpha + \nu_1\beta$, missä μ_1 ja ν_1 ovat Gaussin kokonaislukuja. Lauseen 2.5 perusteella luku τ voidaan kirjoittaa myös muodossa

$$\tau = \gamma\eta + \varsigma,$$

missä η ja ς ovat Gaussin kokonaislukuja ja $0 \leq N(\varsigma) < N(\gamma)$. Ratkaistaan ς edellisestä yhtälöstä ja sijoitetaan lukujen τ ja γ paikalle niille aiemmin määritellyt yhtälöt. Näin saadaan

$$\varsigma = \tau - \gamma\eta = (\mu_1\alpha + \nu_1\beta) - (\mu_0\alpha + \nu_0\beta)\eta = (\mu_1 - \mu_0\eta)\alpha + (\nu_1 - \nu_0\eta)\beta.$$

Siis myös ς on muotoa $\mu\alpha + \nu\beta$ oleva Gaussin kokonaisluku. Luku γ valittiin siten, että sen normi on pienin muotoa $\mu\alpha+\nu\beta$ olevien Gaussin kokonaislukujen normien joukossa. Koska myös ς on samaa muotoa ja $0 \leq N(\varsigma) < N(\gamma)$, täytyy olla $N(\varsigma) = 0$. Tällöin lauseen 2.2 kohdan (ii) perusteella $\varsigma = 0$. Näin ollen luvun τ yhtälöksi saadaan $\tau = \gamma\eta$ ja määritelmän 2.4 perusteella $\gamma \mid \tau$. Näin ollen γ jakaa jokaisen muotoa $\mu\alpha + \nu\beta$ olevan Gaussin kokonaisluvun, erityisesti $\gamma \mid \alpha$ ja $\gamma \mid \beta$. Siis määritelmän 2.7 kohta (i) toteutuu.

□

Lause 2.7. *Olkoot α ja β sellaisia Gaussin kokonaislukuja, että ainakin toinen niistä on nollasta poikkeava. Jos sekä γ_1 että γ_2 ovat lukujen α ja β suurimpia yhteisiä tekijöitä, ovat γ_1 ja γ_2 toistensa liitännäisiä.*

Todistus. (vrt. [3, s. 561]) Oletetaan, että γ_1 ja γ_2 ovat molemmat lukujen α ja β suurimpia yhteisiä tekijöitä. Määritelmän 2.7 kohdan (i) perusteella $\gamma_1 \mid \alpha$, $\gamma_1 \mid \beta$, $\gamma_2 \mid \alpha$ ja $\gamma_2 \mid \beta$ sekä kohdan (ii) perusteella $\gamma_1 \mid \gamma_2$ ja $\gamma_2 \mid \gamma_1$. Määritelmän 2.4 perusteella on olemassa sellaiset Gaussin kokonaisluvut ϵ ja θ, että $\gamma_2 = \epsilon\gamma_1$ ja $\gamma_1 = \theta\gamma_2$. Sijoitetaan ensimmäinen yhtälö jälkimmäiseen, jolloin saadaan

$$\gamma_1 = \theta\epsilon\gamma_1.$$

Jaetaan yhtälö puolittain luvulla γ_1. Näin voidaan tehdä, koska luvuista α ja β ainakin toinen on nollasta poikkeava ja siksi niiden suurin yhteinen tekijä ei voi olla nolla. Edellinen yhtälö saadaan muotoon

$$\theta\epsilon = 1.$$

Siis lukujen θ ja ϵ täytyy olla yksiköitä. Koska $\gamma_1 = \theta\gamma_2$ ja koska θ on yksikkö, ovat luvut γ_1 ja γ_2 toistensa liitännäisiä.

□

Apulause 2.2. *(vrt. [3, s. 556], harjoitustehtävä 8) Olkoot α, β, γ, μ ja ν Gaussin kokonaislukuja. Jos $\gamma \mid \alpha$ ja $\gamma \mid \beta$, niin $\gamma \mid (\mu\alpha + \nu\beta)$.*

Todistus. Koska $\gamma \mid \alpha$ ja $\gamma \mid \beta$, on määritelmän 2.4 perusteella olemassa sellaiset Gaussin kokonaisluvut δ ja θ, että $\alpha = \gamma\delta$ ja $\beta = \gamma\theta$. Tällöin voidaan kirjoittaa

$$\mu\alpha + \nu\beta = \mu\gamma\delta + \nu\gamma\theta = \gamma(\mu\delta + \nu\theta).$$

Siis määritelmän 2.4 perusteella $\gamma \mid (\mu\alpha + \nu\beta)$.

□

Seuraavan apulauseen todistusta ei ole esitetty lähdekirjallisuudessa, vaan sen on laatinut tekijä itse. Lähdekirjallisuudessa on kuitenkin esitetty vastaava todistus rationaalisille kokonaisluvuille (ks. [3, s. 91]).

Apulause 2.3. *Olkoot α, β ja γ Gaussin kokonaislukuja. Tällöin suurimmille yhteisille tekijöille pätee yhtälö $(\beta\gamma + \alpha, \beta) = (\alpha, \beta)$.*

Todistus. Osoitetaan, että lukujen α ja β yhteiset tekijät ovat täsmälleen samat kuin lukujen $\beta\gamma+\alpha$ ja β yhteiset tekijät. Näin saadaan osoitettua, että $(\beta\gamma+\alpha, \beta) = (\alpha, \beta)$. Olkoon θ lukujen α ja β yhteinen tekijä. Määritelmän 2.7 perusteella $\theta \mid \alpha$ ja $\theta \mid \beta$. Tällöin apulauseen 2.2 perusteella $\theta \mid (\beta\gamma + 1 \cdot \alpha)$ eli $\theta \mid (\beta\gamma + \alpha)$. Siis θ on myös lukujen $\beta\gamma + \alpha$ ja β yhteinen tekijä. Olkoon puolestaan σ lukujen $\beta\gamma+\alpha$ ja β yhteinen tekijä. Määritelmän 2.7 perusteella $\sigma \mid (\beta\gamma+\alpha)$ ja $\sigma \mid \beta$. Tällöin apulauseen 2.2 perusteella $\sigma \mid (1 \cdot (\beta\gamma+\alpha) - \beta\gamma)$ eli $\sigma \mid \alpha$. Siis σ on myös lukujen α ja β yhteinen tekijä. On osoitettu, että jokainen lukujen α ja β tekijä on myös lukujen $\beta\gamma + \alpha$ ja β tekijä. Siis $(\beta\gamma + \alpha, \beta) = (\alpha, \beta)$.

□

Seuraavan lauseen todistusta ei ole esitetty lähdekirjallisuudessa, vaan sen on laatinut tekijä itse. Lähdekirjallisuudessa on kuitenkin esitetty vastaava todistus rationaalisille kokonaisluvuille (ks. [3, s. 98]). Lisäksi on korjattu kirjan lauseessa ollut painovirhe (ks. [3, s. 562]).

Lause 2.8. *Eukleideen algoritmi Gaussin kokonaisluvuille. Olkoot $\rho_0 = \alpha$ ja $\rho_1 = \beta$ nollasta poikkeavia Gaussin kokonaislukuja. Sovelletaan Gaussin kokonaislukujen jakoalgoritmiä (ks. lause 2.5) peräkkäin siten, että saadaan $\rho_j = \rho_{j+1}\gamma_{j+1} + \rho_{j+2}$, missä $N(\rho_{j+2}) < N(\rho_{j+1})$, $j = 0, 1, 2, \ldots, n-2$ ja $\rho_{n+1} = 0$. Tällöin viimeinen nollasta poikkeava jakojäännös ρ_n on lukujen α ja β suurin yhteinen tekijä.*

Todistus. Olkoot $\rho_0 = \alpha$ ja $\rho_1 = \beta$ nollasta poikkeavia Gaussin kokonaislukuja. Soveltamalla jakoalgoritmiä (ks. lause 2.5) peräkkäin saadaan

$$\begin{aligned}
\rho_0 &= \rho_1\gamma_1 + \rho_2, && 0 \leq N(\rho_2) < N(\rho_1)\\
\rho_1 &= \rho_2\gamma_2 + \rho_3, && 0 \leq N(\rho_3) < N(\rho_2)\\
&\vdots\\
\rho_j &= \rho_{j+1}\gamma_{j+1} + \rho_{j+2}, && 0 \leq N(\rho_{j+2}) < N(\rho_{j+1})\\
&\vdots\\
\rho_{n-2} &= \rho_{n-1}\gamma_{n-1} + \rho_n, && 0 \leq N(\rho_n) < N(\rho_{n-1})\\
\rho_{n-1} &= \rho_n\gamma_n.
\end{aligned}$$

Voidaan päätellä, että lopulta jakojäännökseksi saadaan nolla, koska jakojäännösten normien lukujonossa $N(\beta) = N(\rho_1) > N(\rho_2) > N(\rho_3) > \cdots \geq 0$ on korkeintaan $N(\beta)$ termiä. Apulauseen 2.3, edellä esitettyjen yhtälöiden ja ominaisuuden $(\rho_i, \rho_{i+1}) = (\rho_{i+1}, \rho_i)$ perusteella lukujen α ja β suurimmaksi

yhteiseksi tekijäksi saadaan

$$\begin{aligned}(\alpha,\beta) &= (\rho_0,\rho_1) = (\rho_1\gamma_1+\rho_2,\rho_1) = (\rho_1,\rho_2) = (\rho_2\gamma_2+\rho_3,\rho_2) = \cdots \\ &= (\rho_{n-1}\gamma_{n-1}+\rho_n,\rho_{n-1}) = (\rho_{n-1},\rho_n) = (\rho_n\gamma_n+0,\rho_n) = (\rho_n,0) \\ &= \rho_n.\end{aligned}$$

Siis $(\alpha,\beta) = \rho_n$ eli lukujen α ja β suurin yhteinen tekijä on viimeinen nollasta poikkeava jakojäännös.

□

Eukleideen algoritmin avulla kahden Gaussin kokonaisluvun suurin yhteinen tekijä voidaan kirjoittaa näiden kahden luvun lineaarikombinaationa. Ensin suurin yhteinen tekijä ratkaistaan Eukleideen algoritmin avulla ja sen jälkeen algoritmiä sovelletaan "takaperin", kuten seuraavassa esimerkissä tehdään.

Esimerkki 2.7. Olkoot $\alpha = 120+50i$ ja $\beta = 25+13i$. Sovelletaan edellisessä lauseessa esitettyä algoritmia, jolloin saadaan ratkaistua lukujen α ja β suurin yhteinen tekijä. Siis

$$\begin{aligned}120+50i &= (25+13i)\cdot 5+(-5-15i)\\ 25+13i &= (-5-15i)(-1+i)+(5+3i)\\ -5-15i &= (5+3i)(-2-2i)+(-1+i)\\ 5+3i &= (-1+i)(-1-4i).\end{aligned}$$

Siis lukujen $120+50i$ ja $25+13i$ suurin yhteinen tekijä on $-1+i$.

Esitetään nyt $-1+i$ lukujen $120+50i$ ja $25+13i$ lineaarikombinaationa. Ratkaistaan ensin jakojäännökset kolmesta ensimmäisestä yhtälöstä, jolloin saadaan yhtälöt

$$\begin{aligned}-5-15i &= (120+50i)-(25+13i)\cdot 5\\ 5+3i &= (25+13i)-(-5-15i)(-1+i)\\ -1+i &= (-5-15i)-(5+3i)(-2-2i).\end{aligned}$$

Sijoitetaan toisen jakojäännöksen yhtälö kolmannen jakojäännöksen yhtälöön, jolloin saadaan

$$\begin{aligned}-1+i &= (-5-15i)-(5+3i)(-2-2i)\\ &= (-5-15i)-[(25+13i)-(-5-15i)(-1+i)](-2-2i)\\ &= (-5-15i)\cdot 5-(25+13i)(-2-2i).\end{aligned}$$

Seuraavaksi sijoitetaan ensimmäisen jakojäännöksen yhtälö edelliseen yhtälöön ja saadaan

$$\begin{aligned} -1+i &= [(120+50i)-(25+13i)\cdot 5]\cdot 5-(25+13i)(-2-2i) \\ &= (120+50i)\cdot 5+(25+13i)(-23+2i). \end{aligned}$$

Siis luku $-1+i$ voidaan kirjoittaa lukujen $120+50i$ ja $25+13i$ lineaarikombinaationa seuraavasti $-1+i=(120+50i)\cdot 5+(25+13i)(-23+2i)$.

2.3 Gaussin alkuluvut

Gaussin kokonaisluvuille on rationaalisten kokonaislukujen tavoin määritelty alkuluvut, ja rationaalisille kokonaisluvuille tunnettu aritmetiikan peruslause on voimassa myös Gaussin kokonaisluvuilla. Määritelmät poikkeavat hieman toisistaan johtuen joukkojen erilaisista yksiköistä. Jos rationaalinen alkuluku jakaa kahden tai useamman rationaalisen kokonaisluvun tulon, se jakaa jonkin tulontekijöistä. Todistetaan vastaava tulos myös Gaussin kokonaisluvuille. Luvussa todistetaan lisäksi, että jos Gaussin kokonaisluvun normi on rationaalinen kokonaisluku, on kyseinen Gaussin kokonaisluku Gaussin alkuluku, kun taas sen normi ei ole.

Määritelmä 2.8. Nollasta poikkeavaa Gaussin kokonaislukua π sanotaan *Gaussin alkuluvuksi*, jos se ei ole yksikkö ja sen ainoat jakajat ovat luvun π liitännäiset sekä yksiköt.

Lause 2.9. *Olkoon π Gaussin kokonaisluku ja olkoon $N(\pi)=p$, missä p on rationaalinen alkuluku. Tällöin π ja $\overline{\pi}$ ovat Gaussin alkulukuja, mutta p ei ole.*

Todistus. (vrt. [3, s. 552]) Tehdään vastaoletus, että π ei ole Gaussin alkuluku. Tällöin π voidaan kirjoittaa muodossa $\pi=\alpha\beta$, missä α ja β ovat Gaussin kokonaislukuja. Tällöin $N(\pi)=N(\alpha\beta)=N(\alpha)N(\beta)$. Alkuperäisestä oletuksesta seuraa, että

$$p=N(\alpha)N(\beta).$$

Koska p on alkuluku ja $N(\alpha)$ sekä $N(\beta)$ ovat positiivisia kokonaislukuja, täytyy olla joko $N(\alpha)=1$ ja $N(\beta)=p$ tai $N(\alpha)=p$ ja $N(\beta)=1$. Tällöin lauseen 2.3 perusteella toinen luvuista α ja β on yksikkö. Siis lukua π ei voida kirjoittaa kahden Gaussin kokonaisluvun tulona ilman, että toinen niistä olisi yksikkö. Näin ollen vastaoletus on väärä ja π on Gaussin alkuluku.

Huomautuksen 2.1 perusteella $N(\pi)=\pi\overline{\pi}$. Koska $N(\pi)=p$, saadaan luku p yhtälöstä $p=\pi\overline{\pi}$. Koska p voidaan kirjoittaa Gaussin alkuluvun ja sen konjungaatin tulona, p ei ole Gaussin alkuluku.

Lisäksi, koska $N(\overline{\pi})=p$, on myös $\overline{\pi}$ Gaussin alkuluku.

□

Esimerkki 2.8. Olkoot $\alpha = -1 + 4i$ ja $\beta = 2 - 5i$. Koska lukujen α ja β normit $N(\alpha) = (-1)^2 + 4^2 = 17$ ja $N(\beta) = 2^2 + (-5)^2 = 29$ ovat rationaalisia alkulukuja, ovat α ja β Gaussin alkulukuja lauseen 2.9 perusteella. Lisäksi luvut 17 ja 29 eivät ole Gaussin alkulukuja, sillä $17 = (-1 + 4i)(-1 - 4i)$ ja $29 = (2 - 5i)(2 + 5i)$.

Lause 2.10. *Olkoon π Gaussin alkuluku ja olkoot α ja β Gaussin kokonaislukuja. Jos $\pi \mid \alpha\beta$, niin joko $\pi \mid \alpha$ tai $\pi \mid \beta$.*

Todistus. (vrt. [3, s. 563]) Tehdään oletus, että $\pi \nmid \alpha$, ja osoitetaan, että tällöin $\pi \mid \beta$. Koska $\pi \nmid \alpha$ ja koska luvun π ainoat jakajat ovat sen liitännäiset $\pm\pi$, $\pm i\pi$ sekä yksiköt ± 1, $\pm i$, täytyy lukujen π ja α suurimman yhteisen tekijän olla yksikkö. Näin ollen lukujen π ja α suurin yhteinen tekijä on luku 1. Luku π on määritelmän 2.8 mukaan nollasta poikkeava, joten lauseen 2.6 perusteella on olemassa sellaiset Gaussin kokonaisluvut μ ja ν, että lukujen α ja π suurin yhteinen tekijä voidaan kirjoittaa muodossa

$$1 = \mu\pi + \nu\alpha.$$

Kerrotaan edellinen yhtälö puolittain luvulla β, jolloin saadaan yhtälö

$$\beta = \beta\mu\pi + \beta\nu\alpha = \pi(\mu\beta) + \nu(\alpha\beta).$$

Koska selvästi $\pi \mid \pi$ ja oletuksen mukaan $\pi \mid \alpha\beta$, voidaan apulauseen 2.2 perusteella todeta, että $\pi \mid (\pi(\mu\beta) + \nu(\alpha\beta))$ eli $\pi \mid \beta$.

□

Apulause 2.4. *Olkoon π Gaussin alkuluku ja olkoot $\alpha_1, \alpha_2, \ldots, \alpha_n$ sellaisia Gaussin kokonaislukuja, että $\pi \mid \alpha_1\alpha_2 \cdots \alpha_n$. Tällöin on olemassa sellainen kokonaisluku j välillä $1 \leq j \leq n$, että $\pi \mid \alpha_j$.*

Todistus. (vrt. [3, s. 563]) Todistetaan väite induktioperiaatteen avulla. Kun $n = 1$, väite on selvästi tosi. Tehdään induktio-oletus, että väite on tosi, kun $n = m$ ja m on positiivinen kokonaisluku. Siis olkoot $\alpha_1, \alpha_2, \ldots, \alpha_m$ sellaisia Gaussin kokonaislukuja, että $\pi \mid \alpha_1\alpha_2 \cdots \alpha_m$. Tällöin on olemassa sellainen kokonaisluku i välillä $1 \leq i \leq m$, että $\pi \mid \alpha_i$. Tehdään seuraavaksi induktioväite, että väite on tosi, kun $n = m + 1$. Siis olkoot $\alpha_1, \alpha_2, \ldots, \alpha_m, \alpha_{m+1}$ sellaisia Gaussin kokonaislukuja, että $\pi \mid \alpha_1\alpha_2 \cdots \alpha_m\alpha_{m+1}$. Induktioväitteeksi saadaan, että on olemassa sellainen kokonaisluku i välillä $1 \leq i \leq m + 1$, että $\pi \mid \alpha_i$. Voidaan kirjoittaa, että $\pi \mid \alpha_1(\alpha_2 \cdots \alpha_m\alpha_{m+1})$ ja lauseen 2.10 perusteella joko $\pi \mid \alpha_1$ tai $\pi \mid \alpha_2 \cdots \alpha_m\alpha_{m+1}$. Jos $\pi \mid \alpha_1$, väite on tosi. Tarkastellaan siis tilannetta $\pi \mid \alpha_2 \cdots \alpha_m\alpha_{m+1}$. Induktio-oletuksen mukaan on olemassa sellainen kokonaisluku i välillä $2 \leq i \leq m + 1$, että $\pi \mid \alpha_i$. Näin

ollen on olemassa sellainen kokonaisluku i välillä $1 \leq i \leq m+1$, että $\pi \mid \alpha_i$ ja induktioperiaatteen nojalla väite on tosi.

□

Lause 2.11. *Aritmetiikan peruslause Gaussin kokonaisluvuille. Olkoon γ sellainen Gaussin kokonaisluku, että se ei ole yksikkö eikä nolla. Tällöin*

(i) *luku γ voidaan kirjoittaa Gaussin alkulukujen tulona*

(ii) *edellä mainittu Gaussin alkulukujen tulo on yksikäsitteinen seuraavasti. Jos $\gamma = \pi_1\pi_2\cdots\pi_s = \rho_1\rho_2\cdots\rho_t$, missä $\pi_1, \pi_2, \ldots, \pi_s, \rho_1, \rho_2, \ldots, \rho_t$ ovat Gaussin alkulukuja, niin $s = t$ ja mahdollisen termien uudelleennumeroimisen jälkeen π_i ja ρ_i ovat toistensa liitännäisiä, kun $1 \leq i \leq s$.*

Todistus. (vrt. [3, s. 564-565])

(i) Todistetaan väite matemaattisella induktiolla käyttäen muuttujana luvun γ normifuktiota $N(\gamma)$. Osoitetaan, että jos väite on tosi kaikilla luvuilla $N(\delta) < N(\gamma)$, niin väite on tosi myös, kun $N(\delta) = N(\gamma)$. Oletuksen perusteella γ ei ole nolla eikä yksikkö, joten lauseiden 2.2 ja 2.3 perusteella tiedetään, että $N(\gamma) \neq 0$ ja $N(\gamma) \neq 1$. Siis $N(\gamma) \geq 2$. Kun $N(\gamma) = 2$, luku γ on lauseen 2.9 perusteella Gaussin alkuluku, koska 2 on rationaalinen kokonaisluku. Siis γ voidaan kirjoittaa Gaussin alkulukujen tulona siten, että ainoana tulontekijänä on luku γ.

Olkoon nyt $N(\gamma) > 2$. Oletetaan, että jokainen Gaussin kokonaisluku δ, joka täyttää ehdon $N(\delta) < N(\gamma)$, voidaan kirjoittaa Gaussin alkulukujen tulona. Jos γ on Gaussin alkuluku, se voidaan kirjoittaa Gaussin alkulukujen tulona siten, että tulontekijöitä on tasan yksi. Jos γ ei ole Gaussin alkuluku, voidaan kirjoittaa $\gamma = \eta\theta$, missä η ja θ ovat Gaussin kokonaislukuja, jotka eivät ole yksiköitä. Koska γ on nollasta poikkeava, ovat myös luvut η ja θ nollasta poikkeavia. Koska luvut η ja θ eivät ole yksiköitä eivätkä nollia, tiedetään lauseiden 2.2 ja 2.3 perusteella, että $N(\eta) > 1$, $N(\theta) > 1$ ja $N(\gamma) = N(\eta\theta) = N(\eta)N(\theta)$. Koska Gaussin kokonaisluvun normi on rationaalinen kokonaisluku, saadaan että $2 \leq N(\eta) < N(\gamma)$ ja $2 \leq N(\theta) < N(\gamma)$. Edellisten epäyhtälöiden ja oletuksen perusteella sekä η että θ ovat sellaisia Gaussin kokonaislukuja, että ne voidaan kirjoittaa Gaussin alkulukujen tulona. Siis $\eta = \pi_1\pi_2\cdots\pi_s$ ja $\theta = \rho_1\rho_2\cdots\rho_t$, missä $\pi_1, \pi_2, \ldots, \pi_s, \rho_1, \rho_2, \ldots, \rho_t$ ovat Gaussin alkulukuja. Luvun γ tuloesitykseksi saadaan nyt $\gamma = \eta\theta = \pi_1\pi_2\cdots\pi_s\rho_1\rho_2\cdots\rho_t$ ja näin ollen myös luku γ voidaan kirjoittaa Gaussin alkulukujen tulona.

(ii) Oletuksen perusteella γ on nollasta poikkeava Gaussin kokonaisluku, joka ei ole yksikkö. Lauseiden 2.2 ja 2.3 perusteella tiedetään, että $N(\gamma) \geq 2$. Jos $N(\gamma) = 2$, on γ lauseen 2.9 perusteella Gaussin alkuluku, koska luku 2 on rationaalinen alkuluku. Tällöin γ voidaan kirjoittaa yksikäsitteisesti Gaussin alkulukujen tulona ja ainoana tulontekijänä on luku γ.

Oletetaan, että väite (ii) on tosi jokaisella sellaisella Gaussin kokonaisluvulla δ, joka toteuttaa ehdon $N(\delta) < N(\gamma)$. Oletetaan lisäksi, että γ voidaan kirjoittaa Gaussin alkulukujen tulona kahdella eri tavalla eli

$$\gamma = \pi_1\pi_2 \cdots \pi_s = \rho_1\rho_2 \cdots \rho_t,$$

missä $\pi_1, \pi_2, \ldots, \pi_s, \rho_1, \rho_2, \ldots, \rho_t$ ovat Gaussin alkulukuja. Jos $s = 1$ ja $t = 1$, kyseessä on Gaussin alkuluku ja tällöin se voidaan kirjoittaa yksikäsitteisesti Gaussin alkulukujen tulona, sillä tulontekijöitä on tasan yksi. Tarkastellaan siis tilannetta $s > 1$ ja $t > 1$. Koska $\pi_1 \mid \pi_1\pi_2 \cdots \pi_s$ ja oletuksen mukaan $\pi_1\pi_2 \cdots \pi_s = \rho_1\rho_2 \cdots \rho_t$, on oltava $\pi_1 \mid \rho_1\rho_2 \cdots \rho_t$. Apulauseen 2.4 perusteella on olemassa sellainen kokonaisluku k välillä $1 \leq k \leq t$, että $\pi_1 \mid \rho_k$. Järjestetään alkuluvut ρ_1, ρ_2, $\cdots$, ρ_t tarvittaessa siten, että $\pi_1 \mid \rho_1$. Koska ρ_1 on oletuksen mukaan Gaussin alkuluku, se on määritelmän 2.8 perusteella jaollinen vain liitännäisillään sekä yksiköillä. Siis luvut π_1 ja ρ_1 ovat toistensa liitännäisiä. Näin ollen $\rho_1 = \epsilon\pi_1$, missä ϵ on yksikkö ja saadaan, että

$$\pi_1\pi_2 \cdots \pi_s = \rho_1\rho_2 \cdots \rho_t = \epsilon\pi_1\rho_2 \cdots \rho_t.$$

Gaussin alkulukuna π_1 on nollasta poikkeava, joten edellinen yhtälö voidaan jakaa puolittain luvulla π_1. Tällöin saadaan yhtälö

$$\pi_2\pi_3 \cdots \pi_s = (\epsilon\rho_2)\rho_3 \cdots \rho_t.$$

Koska π_1 on Gaussin alkuluku, on oltava $N(\pi_1) \geq 2$. Näin ollen

$$1 \leq N(\pi_2\pi_3 \cdots \pi_s) < N(\pi_1\pi_2 \cdots \pi_s) = N(\gamma).$$

Merkitään $\delta = \pi_2\pi_3 \cdots \pi_s = (\epsilon\rho_2)\rho_3 \cdots \rho_t$. Koska $N(\delta) < N(\gamma)$, oletuksen mukaan väite (ii) on tosi luvulla δ. Näin ollen $s - 1 = t - 1$ ja mahdollisen termien uudelleennumeroimisen jälkeen ρ_i on luvun π_i liitännäinen, kun i on välillä $1 \leq i \leq s - 1$.

□

Esimerkki 2.9. Luku $\gamma = 5 + 27i$ voidaan kirjoittaa Gaussin alkulukujen tulona mm. seuraavasti

$$\gamma = (1+i)(2+5i)(3-2i) = (-1+i)(-2-5i)(2+3i) = (1+i)(5-2i)(2+3i).$$

Näissä erilaisissa alkutekijäesityksissä kaikki ensimmäiset tulontekijät ovat toistensa liitännäisiä, kaikki toiset tulontekijät ovat toistensa liitännäisiä ja kaikki kolmannet tulontekijät ovat toistensa liitännäisiä.

3 Gaussin kokonaisluvut ja neliösummat

3.1 Yhtälön $x^2 + y^2 = n$ ratkaisut

Yhtälölle $x^2 + y^2 = n$, missä x, y ja n ovat rationaalisia kokonaislukuja, voidaan löytää ratkaisuja sekä rationaalisten kokonaislukujen että Gaussin kokonaislukujen avulla. Tässä luvussa osoitetaan ensin, että rationaalinen alkuluku on kahden neliön summa, jos ja vain jos kyseinen luku ei ole Gaussin alkuluku. Seuraavaksi osoitetaan, että muotoa $4k+1$ olevat rationaaliset alkuluvut ovat kahden neliön summia. Tämän jälkeen esitetään, miten rationaalinen alkuluku voidaan jakaa Gaussin kokonaislukutekijöihin ja samalla osoitetaan, mitkä rationaaliset alkuluvut voidaan esittää kahden neliön summana. Luvussa osoitetaan rationaalisten kokonaislukujen avulla, että kaikki rationaaliset kokonaisluvut, joiden alkutekijäesityksessä muotoa $4k+3$ olevien alkutekijöiden eksponentti on parillinen, ovat kahden neliön summia. Lopuksi osoitetaan Gaussin kokonaislukujen avulla, kuinka monella eri tavalla rationaalinen kokonaisluku voidaan kirjoittaa kahden neliön summana. Näiden lauseiden lisäksi esitetään lauseiden todistamisessa tarvittavia rationaalisia kokonaislukuja koskevia määritelmiä ja apulauseita.

Lause 3.1. *Rationaalinen alkuluku p voidaan esittää kahden neliön summana, jos ja vain jos se ei ole Gaussin alkuluku.*

Todistus. (vrt. [2, s. 314]) Oletetaan ensin, että p on rationaalinen alkuluku, joka voidaan kirjoittaa kahden neliön summana eli $p = a^2 + b^2$, missä luvut a ja b ovat nollasta poikkeavia rationaalisia kokonaislukuja. Tällöin p voidaan kirjoittaa muodossa $p = a^2 + b^2 = (a + bi)(a - bi)$. Nyt määritelmän 2.4 perusteella luku $a + bi$ jakaa luvun p ja tällöin määritelmän 2.8 perusteella p ei ole Gaussin alkuluku.

Oletetaan nyt, että p ei ole Gaussin alkuluku. Tällöin p voidaan kirjoittaa kahden Gaussin kokonaisluvun tulona eli $p = (c + di)(e + fi)$, missä $c + di$ ja $e + fi$ eivät ole yksiköitä. Luvun p normiksi saadaan

$$N(p) = p^2 = N((c + di)(e + fi)) = N(c + di)N(e + fi).$$

Koska $c + di$ ja $e + fi$ eivät ole yksiköitä, täytyy olla $p = N(c + di)$ ja $p = N(e + fi)$. Siis $p = c^2 + d^2$ ja $p = e^2 + f^2$ eli luku p voidaan kirjoittaa kahden neliön summana.

□

Seuraavat kaksi määritelmää ja apulause koskevat rationaalisia kokonaislukuja ja ne on esitetty lähdekirjallisuudessa Gaussin kokonaislukuja käsittelevän luvun ulkopuolella (ks. [3, s. 402-406]).

Määritelmä 3.1. Olkoon m positiivinen rationaalinen kokonaisluku. Jos kongruenssilla $x^2 \equiv a \pmod{m}$ on ratkaisu ja $(a, m) = 1$, sanotaan, että luku a on *neliönjäännös modulo* m. Jos kongruenssilla $x^2 \equiv a \pmod{m}$ ei ole ratkaisua, sanotaan, että luku a on *neliönepäjäännös modulo* m.

Määritelmä 3.2. Olkoon p pariton rationaalinen alkuluku ja olkoon a luvulla p jaoton rationaalinen kokonaisluku. *Legendren symboli* $\left(\frac{a}{p}\right)$ määritellään seuraavasti

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } a \text{ on neliönjäännös modulo } p, \\ -1, & \text{jos } a \text{ on neliönepäjäännös modulo } p. \end{cases}$$

Apulause 3.1. *Olkoon p pariton rationaalinen alkuluku. Tällöin*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1, & \textit{jos } p \equiv 1 \pmod{4}, \\ -1, & \textit{jos } p \equiv -1 \pmod{4}. \end{cases}$$

Todistus. Ks. [3, s. 406].

Lause 3.2. *Olkoon p rationaalinen alkuluku, joka voidaan kirjoittaa muodossa $4k+1$, missä k on positiivinen kokonaisluku. Tällöin luku p on kahden neliön summa.*

Todistus. (vrt. [3, s. 570-571]) Olkoon rationaalinen alkuluku p muotoa $4k+1$, missä k on positiivinen kokonaisluku. Lauseen 3.1 perusteella tulee osoittaa, että p ei ole Gaussin alkuluku. Koska $p = 4k+1$, niin selvästi $p \equiv 1 \pmod{4}$ ja apulauseen 3.1 perusteella $\left(\frac{-1}{p}\right) = 1$. Tällöin määritelmän 3.2 mukaan -1 on neliönjäännös modulo p ja määritelmän 3.1 perusteella on olemassa sellainen rationaalinen kokonaisluku x, että kongruenssilla $x^2 \equiv -1 \pmod{p}$ on ratkaisu. Näin ollen $p \mid x^2+1$. Luku x^2+1 voidaan jakaa tekijöihin, jolloin saadaan, että $p \mid (x+i)(x-i)$. Jos p on Gaussin alkuluku, niin lauseen 2.10 perusteella $p \mid x+i$ tai $p \mid x-i$. Tiedetään, että Gaussin alkuluvulla p jaolliset Gaussin kokonaisluvut ovat muotoa $pa+pbi = p(a+bi)$. Kumpikaan luvuista $x+i$ ja $x-i$ ei ole tätä muotoa ja kuitenkin $p \mid x+i$ tai $p \mid x-i$. Näin ollen voidaan todeta, että p ei ole Gaussin alkuluku.

Koska p ei ole Gaussin alkuluku, on olemassa sellaiset Gaussin kokonaisluvut α ja β, että $p = \alpha\beta$, missä α ja β eivät ole yksiköitä. Tällöin luvun p normiksi saadaan

$$N(p) = p^2 = N(\alpha\beta) = N(\alpha)N(\beta).$$

Koska luvut α ja β eivät ole yksiköitä, tiedetään lauseen 2.3 perusteella, että $N(\alpha) \neq 1$ ja $N(\beta) \neq 1$. Siis täytyy olla $N(\alpha) = N(\beta) = p$. Koska α ja β ovat Gaussin kokonaislukuja, ovat ne muotoa $\alpha = a + bi$ ja $\beta = c + di$, missä a, b, c ja d ovat rationaalisia kokonaislukuja. Tällöin voidaan kirjoittaa

$p = N(\alpha) = a^2 + b^2$ ja $p = N(\beta) = c^2 + d^2$. Siis luku p voidaan kirjoittaa kahden neliön summana.

□

Esimerkki 3.1. Rationaalinen alkuluku 37 on muotoa $4k + 1$, joten lauseen 3.2 perusteella se voidaan kirjoittaa kahden neliön summana. Luku 37 voidaan kirjoittaa kahden neliön summana seuraavasti $37 = 6^2 + 1^2$.

Seuraavassa lauseessa esitetään, miten rationaalinen alkuluku p voidaan jakaa Gaussin kokonaislukutekijöihin. Samalla osoitetaan, mitkä rationaaliset alkuluvut voidaan kirjoittaa kahden neliön summana. Luku p on kongruentti jonkun luvuista 0, 1, 2 tai 3 kanssa modulo 4. Rationaalisia alkulukuja näistä eivät ole tapaukset $x \equiv 2 \pmod 4$, kun $x > 2$, ja $x \equiv 0 \pmod 4$. Tarkastellaan siis tapauksia $x = 2$, $x \equiv 1 \pmod 4$ ja $x \equiv 3 \pmod 4$.

Lause 3.3. *Olkoon p rationaalinen alkuluku. Tällöin p voidaan jakaa Gaussin kokonaislukutekijöihin seuraavien sääntöjen mukaan.*

(i) *Jos $p = 2$, niin $p = (1 + i)(1 - i)$, missä $1 + i$ ja $1 - i$ ovat molemmat Gaussin alkulukuja ja niiden molempien normi on 2. Tällöin luku p on kahden neliön summa.*

(ii) *Jos $p \equiv 3 \pmod 4$, niin $p = \pi$ on Gaussin alkuluku ja $N(\pi) = p^2$. Tällöin luku p ei ole kahden neliön summa.*

(iii) *Jos $p \equiv 1 \pmod 4$, niin $p = \pi\overline{\pi}$, missä π ja $\overline{\pi}$ ovat Gaussin alkulukuja, jotka eivät ole toistensa liitännäisiä ja $N(\pi) = N(\overline{\pi}) = p$. Tällöin luku p on kahden neliön summa.*

Todistus. (vrt. [3], s. 571-572)

(i) Jos $p = (1 + i)(1 - i)$, niin huomautuksen 2.1 perusteella luvulle p saadaan yhtälö $p = (1 + i)(1 - i) = 1^2 + 1^2 = 2$. Siis luku p on kahden neliön summa. Lisäksi $N(1 + i) = 1^2 + 1^2 = 2$ ja $N(1 - i) = 1^2 + (-1)^2 = 2$, joten lauseen 2.9 perusteella luvut $1+i$ ja $1-i$ ovat Gaussin alkulukuja.

(ii) Olkoon p sellainen rationaalinen alkuluku, että se toteuttaa kongruenssin $p \equiv 3 \pmod 4$. Tehdään vastaoletus, että p ei ole Gaussin alkuluku. Tällöin se voidaan kirjoittaa kahden Gaussin kokonaisluvun tulona eli $p = \alpha\beta$, missä α ja β ovat Gaussin kokonaislukuja, joista kumpikaan ei ole yksikkö. Luvut α ja β voidaan kirjoittaa muodossa $\alpha = a + bi$ ja $\beta = c + di$, missä luvut a, b, c ja d ovat kokonaislukuja. Lauseen 2.2 kohdan (iii) perusteella luvun p normiksi saadaan $N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$. Sijoitetaan edelliseen yhtälöön normien

paikoille tulokset $N(p) = p^2$, $N(\alpha) = a^2 + b^2$ ja $N(\beta) = c^2 + d^2$, jolloin yhtälö saadaan muotoon

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

Koska luvut α ja β eivät ole yksiköitä, tiedetään lauseen 2.3 perusteella, että $N(\alpha) = a^2 + b^2 \neq 1$ ja $N(\beta) = c^2 + d^2 \neq 1$. Näin ollen on oltava $N(\alpha) = a^2 + b^2 = p$ ja $N(\beta) = c^2 + d^2 = p$. Alkuperäisen oletuksen mukaan kuitenkin $p \equiv 3 \pmod 4$, joten p ei voi olla kahden neliön summa. (Kahden neliön summa on kongruentti joko luvun 0, 1 tai 2 kanssa modulo 4.) Siis vastaoletus on väärä ja näin ollen $p = \pi$ on Gaussin alkuluku ja $N(\pi) = p^2$.

(iii) Olkoon p sellainen rationaalinen alkuluku, että se toteuttaa kongruenssin $p \equiv 1 \pmod 4$. Lauseen 3.2 perusteella on olemassa sellaiset kokonaisluvut a ja b, että $p = a^2 + b^2$. Siis p on kahden neliön summa. Olkoot $\pi = a + bi$ ja $\overline{\pi} = a - bi$. Tällöin $N(\pi)N(\overline{\pi}) = N(p) = p^2$. Siis on oltava $N(\pi) = N(\overline{\pi}) = p$ ja lauseen 2.9 perusteella π ja $\overline{\pi}$ ovat Gaussin alkulukuja.

Osoitetaan vielä, että luvut π ja $\overline{\pi}$ eivät ole toistensa liitännäisiä. Tehdään vastaoletus, että $\pi = \epsilon\overline{\pi}$, missä ϵ on yksikkö. Koska ϵ on yksikkö, se on jokin luvuista 1, -1, i tai $-i$. Jos $\epsilon = 1$, niin $\pi = \overline{\pi}$. Tällöin on oltava $x + yi = x - yi$ ja saadaan, että $y = 0$. Tästä seuraa, että $p = x^2 + y^2 = x^2$. Tämä on kuitenkin mahdotonta, sillä p on alkuluku. Jos $\epsilon = -1$, niin $\pi = -\overline{\pi}$. Tällöin on vastaavasti oltava $x + yi = -x + yi$ ja saadaan, että $x = 0$. Tästä seuraa, että $p = x^2 + y^2 = y^2$, joka on mahdotonta, sillä p on alkuluku. Jos $\epsilon = i$, niin $\pi = i\overline{\pi}$. Tällöin on oltava $x+yi = i(x-yi) = y+xi$ ja saadaan, että $x = y$. Tästä seuraa, että $p = x^2 + x^2 = 2x^2$. Tämä on mahdotonta, sillä p on pariton alkuluku. Jos $\epsilon = -i$, niin $\pi = -i\overline{\pi}$. Tällöin on oltava $x + yi = -i(x - yi) = -y - xi$ ja saadaan, että $x = -y$. Tästä seuraa vastaavasti, että $p = x^2 + (-x)^2 = 2x^2$, joka on mahdotonta, sillä p on pariton alkuluku. Siis mikään yksikkö ϵ ei toteuta yhtälöä $\pi = \epsilon\overline{\pi}$ ja näin ollen luvut π ja $\overline{\pi}$ eivät ole toistensa liitännäisiä.

□

Seuraavat kolme apulausetta koskevat rationaalisia kokonaislukuja ja ne on esitetty lähdekirjallisuudessa Gaussin kokonaislukuja käsittelevän luvun ulkopuolella (ks. [3, s. 90-91, 529-531]).

Apulause 3.2. *Olkoot m ja n sellaisia kokonaislukuja, että ne molemmat ovat kahden neliön summia. Tällöin myös tulo mn on kahden neliön summa.*

Todistus. (vrt. [3, s. 529]) Olkoot $m = a^2 + b^2$ ja $n = c^2 + d^2$, missä a, b, c ja d ovat kokonaislukuja. Tällöin tulo mn saadaan muotoon

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

Siis myös tulo mn voidaan kirjoittaa kahden neliön summana.

□

Apulause 3.3. *Olkoon p alkuluku, joka ei ole muotoa $4k + 3$. Tällöin on olemassa sellaiset kokonaisluvut x ja y, että $p = x^2 + y^2$.*

Todistus. Ks. [3, s. 530-531].

Apulause 3.4. *Olkoot a ja b kokonaislukuja ja $(a, b) = d$. Tällöin $(\frac{a}{d}, \frac{b}{d}) = 1$.*

Todistus. Ks. [3, s. 90-91].

Lause 3.4. *Positiivinen rationaalinen kokonaisluku n voidaan kirjoittaa kahden neliön summana, jos ja vain jos luvun n alkutekijäesityksessä jokaisen muotoa $4k + 3$ olevan alkutekijän eksponentti on parillinen.*

Todistus. (vrt. [3, s. 531-532]) Oletetaan, että luvun n alkutekijäesityksessä ei esiinny sellaisia muotoa $4k + 3$ olevia alkulukuja, joiden eksponentti on pariton. Kirjoitetaan $n = t^2u$, missä u on sellaisten alkulukujen tulo, jotka eivät ole muotoa $4k + 3$, ja t^2 on muotoa $4k + 3$ olevien alkulukujen tulo. Apulauseen 3.3 perusteella jokainen tulon u alkuluku voidaan kirjoittaa kahden neliön summana. Sovelletaan apulausetta 3.2 tuloon u kerran vähemmän kuin mitä tulossa on tulontekijöitä. Tällöin tulo u saadaan muotoon

$$u = x^2 + y^2.$$

Näin ollen myös luku n voidaan kirjoittaa kahden neliön summana, sillä

$$n = t^2u = t^2(x^2 + y^2) = (tx)^2 + (ty)^2.$$

Siis luku n voidaan kirjoittaa kahden neliön summana, jos luvun n alkutekijäesityksessä muotoa $4k + 3$ olevien tekijöiden eksponentti on parillinen.

Oletetaan seuraavaksi, että luvun n alkutekijäesityksessä on sellainen muotoa $4k + 3$ oleva rationaalinen alkuluku p, jonka eksponentti on pariton. Olkoon tämä pariton potenssi $2j + 1$, missä j on ei-negatiivinen rationaalinen kokonaisluku. Oletetaan lisäksi, että luku n on kahden neliön summa eli

$n = x^2 + y^2$. Olkoon $(x, y) = d$. Merkitään $a = \frac{x}{d}$, $b = \frac{y}{d}$ ja $m = \frac{n}{d^2}$. Tällöin apulauseen 3.4 perusteella $(a, b) = 1$. Lisäksi

$$a^2 + b^2 = (\frac{x}{d})^2 + (\frac{y}{d})^2 = \frac{x^2 + y^2}{d^2} = \frac{n}{d^2} = m.$$

Olkoon p^k luvun p korkein potenssi, joka jakaa luvun d. Siis $d = ep^k$. Lisäksi olkoon $n = up^{2j+1}$ luvun n alkutekijäesitys, missä u on sellainen alkulukujen tulo, että siinä ei esiinny muotoa $4k + 3$ olevia alkulukuja, joilla on pariton potenssi. Tällöin luku m voidaan kirjoittaa muodossa

$$m = \frac{n}{d^2} = \frac{up^{2j+1}}{(ep^k)^2} = \frac{up^{2j+1}}{e^2p^{2k}} = \frac{up^{2j-2k+1}}{e^2}.$$

Siis m on jaollinen luvulla $p^{2j-2k+1}$, missä $2j - 2k + 1$ on vähintään 1, sillä potenssin tulee olla ei-negatiivinen. Näin ollen $p \mid m$. Jos $p \mid a$, niin myös $p \mid b$, sillä $b^2 = m^2 - a$. Kuitenkin $(a, b) = 1$, joten täytyy olla $p \nmid a$. Lisäksi $a \nmid p$, sillä p on alkuluku. Näin ollen $(a, p) = 1$ ja on olemassa sellainen rationaalinen kokonaisluku z, että lineaarinen kongruenssi $az \equiv b \pmod{p}$ on ratkeava. Tällöin $a^2 + b^2 \equiv a^2 + (az)^2 \pmod{p}$. Koska $a^2 + b^2 = m$, saadaan edellinen konguenssi muotoon $m \equiv a^2(1 + z^2) \pmod{p}$. Koska $p \mid m$, tiedetään että $a^2(1 + z^2) \equiv 0 \pmod{p}$. Lisäksi, koska $(a, p) = 1$, on oltava $1 + z^2 \equiv 0 \pmod{p}$. Edellisen kongruenssin perusteella saadaan kongruenssi $z^2 \equiv -1 \pmod{p}$ ja määritelmän 3.1 perusteella -1 on neliönjäänös modulo p. Tämä on kuitenkin mahdotonta, sillä -1 ei ole neliönjäännös modulo p, koska $p \equiv 3 \pmod{4}$. Siis oletus, että n on kahden neliön summa, on väärä ja näin ollen lukua n ei voida kirjoittaa kahden neliön summana, jos luvun n alkutekijäesityksessä on sellainen muotoa $4k + 3$ oleva tekijä, jonka eksponentti on pariton.

□

Lause 3.5. *Olkoon n positiivinen kokonaisluku, jolla on alkutekijäesitys*

$$n = 2^m p_1^{e_1} p_2^{e_2} \cdots p_s^{e_s} q_1^{f_1} q_2^{f_2} \cdots q_t^{f_t},$$

missä m on ei-negatiivinen kokonaisluku, luvut p_1, p_2, …, p_s ovat muotoa $4k + 1$ olevia alkulukuja, luvut q_1, q_2, …, q_t ovat muotoa $4k + 3$ olevia alkulukuja, eksponentit e_1, e_2, …, e_s ovat ei-negatiivisia kokonaislukuja ja eksponentit f_1, f_2, …, f_t ovat parillisia ei-negatiivisia kokonaislukuja. Tällöin on yhteensä

$$4(e_1 + 1)(e_2 + 1) \cdots (e_s + 1)$$

tapaa kirjoittaa luku n kahden neliön summana. Tässä neliöiden järjestys summassa sekä neliöön korotettavien kokonaislukujen etumerkki otetaan huomioon.

Todistus. (vrt. [3, s. 572-573]) Luku n voidaan kirjoittaa kahden neliön summana täsmälleen yhtä monella eri tavalla, kuin se voidaan jakaa Gaussin kokonaislukutekijöihin $u+vi$ ja $u-vi$ eli toisin sanoen kirjoittaa muodossa $n=(u+vi)(u-vi)=u^2+v^2$. Erilaisten tapojen määrä kirjoittaa luku n konjungaattien $u+vi$ ja $u-vi$ tulona saadaan ratkaistua luvun n alkutekijäesityksen avulla.

Lauseen 3.2 perusteella jokainen muotoa $4k+1$ oleva alkuluku p_k, joka jakaa luvun n, voidaan kirjoittaa muodossa $p_k = {a_k}^2+{b_k}^2$,missä a_k ja b_k ovat kokonaislukuja. Lisäksi, koska $2=(1+i)(1-i)$ ja $1+i=i(1-i)$, voidaan 2^m kirjoittaa muodossa $2^m=(1+i)^m(1-i)^m=(i(1-i))^m(1-i)^m=i^m(1-i)^{2m}$. Sijoitetaan saadut tulokset luvun n alkutekijäesitykseen, jolloin se saadaan muotoon

$$\begin{aligned} n &= 2^m {p_1}^{e_1}{p_2}^{e_2}\cdots{p_s}^{e_s}{q_1}^{f_1}{q_2}^{f_2}\cdots{q_t}^{f_t} \\ &= i^m(1-i)^{2m}({a_1}^2+{b_1}^2)^{e_1}({a_2}^2+{b_2}^2)^{e_2}\cdots({a_s}^2+{b_s}^2)^{e_s}{q_1}^{f_1}{q_2}^{f_2}\cdots{q_t}^{f_t}. \end{aligned}$$

Jokainen luvuista ${a_k}^2+{b_k}^2$ voidaan kirjoittaa muodossa $(a_k+b_ki)(a_k-b_ki)$. Lisäksi i^m on jokin luvuista 1, -1, i tai $-i$ eli $i^m=\epsilon$, missä ϵ on yksikkö. Nyt luvun n alkutekijäesitys voidaan kirjoittaa muodossa

$$\begin{aligned} n &= \epsilon(1-i)^{2m}(a_1+b_1i)^{e_1}(a_1-b_1i)^{e_1}(a_2+b_2i)^{e_2}(a_2-b_2i)^{e_2} \\ &\quad \cdots(a_s+b_si)^{e_s}(a_s-b_si)^{e_s}{q_1}^{f_1}{q_2}^{f_2}\cdots{q_t}^{f_t}. \end{aligned}$$

Koska Gaussin kokonaisluku $u+vi$ jakaa luvun n, täytyy sen jako yksikköön sekä Gaussin alkutekijöihin olla

$$\begin{aligned} u+vi &= \epsilon_0(1-i)^w(a_1+b_1i)^{g_1}(a_1-b_1i)^{h_1}(a_2+b_2i)^{g_2}(a_2-b_2i)^{h_2} \\ &\quad \cdots(a_s+b_si)^{g_s}(a_s-b_si)^{h_s}{q_1}^{k_1}{q_2}^{k_2}\cdots{q_t}^{k_t}, \end{aligned}$$

missä ϵ_0 on yksikkö ja luvut $w, g_1, \ldots, g_s, h_1, \ldots, h_s$ ja $k_1, \ldots, k_t$ ovat epänegatiivisia kokonaislukuja. jotka toteuttavat epäyhtälöt $w \leq 2m$, $0 \leq g_i \leq e_i$ ja $0 \leq h_i \leq e_i$, kun $1 \leq i \leq s$ sekä $0 \leq k_j \leq f_j$, kun $0 \leq j \leq t$.

Muodostetaan luvun $u+vi$ konjungaatti $u-vi$. Apulauseen 2.1 ja luvun $u+vi$ alkutekijäesityksen perusteella saadaan

$$\begin{aligned} u-vi &= \overline{\epsilon_0}(1+i)^w(a_1-b_1i)^{g_1}(a_1+b_1i)^{h_1}(a_2-b_2i)^{g_2}(a_2+b_2i)^{h_2} \\ &\quad \cdots(a_s-b_si)^{g_s}(a_s+b_si)^{h_s}{q_1}^{k_1}{q_2}^{k_2}\cdots{q_t}^{k_t}. \end{aligned}$$

Apulauseen 2.1 ja lauseen 2.3 perusteella luvun $n=(u+vi)(u-vi)$ esitykseksi saadaan

$$\begin{aligned} n &= \epsilon_0\overline{\epsilon_0}[(1-i)(1+i)]^w[(a_1+b_1i)(a_1-b_1i)]^{g_1+h_1}[(a_2+b_2i)(a_2-b_2i)]^{g_2+h_2} \\ &\quad \cdots[(a_s+b_si)(a_s-b_si)]^{g_s+h_s}{q_1}^{2k_1}{q_2}^{2k_2}\cdots{q_t}^{2k_t} \\ &= 2^w{p_1}^{g_1+h_1}{p_2}^{g_2+h_2}\cdots{p_s}^{g_s+h_s}{q_1}^{2k_1}{q_2}^{2k_2}\cdots{q_t}^{2k_t}. \end{aligned}$$

Verrataan tätä ja alussa esitettyä luvuun n alkutekijäesitystä keskenään, jolloin huomataan, että $w = m$, $g_i + h_i = e_i$, kun $1 \leq i \leq s$ ja $2k_j = f_j$, kun $1 \leq j \leq t$. Näin ollen lukujen w ja k_i arvot on määrätty, kun $1 \leq i \leq t$. Luku g_i voidaan valita $e_i + 1$ eri tavalla, koska g_i on jokin luvuista $0, 1, 2, \ldots, e_i$. Kun luvun g_i arvo on määritetty, voidaan luku h_i valita vain yhdellä tavalla, nimittäin $h_i = e_i - g_i$. Lisäksi yksikkö ϵ_0 voidaan valita neljällä eri tavalla. Näin ollen on yhteensä

$$4(e_1 + 1)(e_2 + 1) \cdots (e_s + 1)$$

tapaa valita tekijä $u + vi$ ja siis yhtä monta tapaa kirjoittaa luku n kahden neliön summana

□

Esimerkki 3.2. Olkoon $n = 900 = 2^2 \cdot 3^2 \cdot 5^2$. Koska alkutekijäesityksen ainoa muotoa $4k + 1$ oleva alkuluku on luku 5, on lauseen 3.5 perusteella $4 \cdot (2 + 1) = 12$ erilaista tapaa kirjoittaa n kahden neliön summana. Nämä eri tavat ovat $(\pm 30)^2 + 0$, $0 + (\pm 30)^2$, $(\pm 18)^2 + (\pm 24)^2$ ja $(\pm 24)^2 + (\pm 18)^2$.

3.2 Yhtälön $x^2 + y^2 = z^2$ ratkaisut

Yhtälön $x^2 + y^2 = z^2$, missä x, y ja z ovat rationaalisia kokonaislukuja, ratkaisut voidaan löytää sekä rationaalisten kokonaislukujen että Gaussin kokonaislukujen avulla. Tässä kappaleessa esitetään yhtälön $x^2 + y^2 = z^2$ ratkaisut Gaussin kokonaislukujen avulla. Todistusta ennen esitetään yhtälön $x^2 + y^2 = z^2$ ratkaisuihin liittyvä määritelmä sekä apulauseita.

Yhtälön $x^2 + y^2 = z^2$ ratkaisua (x, y, z), missä x, y ja z ovat positiivisia kokonaislukuja, sanotaan *Pythagoraan kolmikoksi*. Yhtälön ratkaisujen avulla saadaan muodostettua suorakulmaisia kolmioita, joiden sivujen pituudet ovat kokonaislukuja. Jos (x, y, z) on yhtälön $x^2 + y^2 = z^2$ ratkaisu, saadaan suorakulmainen kolmio, kun kateettien pituuksiksi asetetaan x ja y ja hypotenuusan pituudeksi z.

Esimerkki 3.3. Kolmikot $(3, 4, 5)$, $(8, 15, 17)$ ja $(16, 30, 34)$ ovat Pythagoraan kolmikkoja, sillä $3^2 + 4^2 = 5^2$, $8^2 + 15^2 = 17^2$ ja $16^2 + 30^2 = 34^2$.

Jos (x, y, z) on Pythagoraan kolmikko, ovat kaikki muotoa (kx, ky, kz) olevat kolmikot myös Pythagoraan kolmikkoja, kun k on positiivinen kokonaisluku. Lisäksi, jos (x, y, z) on Pythagoraan kolmikko, on myös kolmikko $(\pm x, \pm y, \pm z)$ yhtälön $x^2 + y^2 = z^2$ ratkaisu kaikilla erilaisilla etumerkkiyhdistelmillä.

Määritelmä 3.3. Pythagoraan kolmikkoa (x, y, z) sanotaan *primitiiviseksi*, jos $(x, y, z) = 1$.

Apulause 3.5. *Olkoon (x, y, z) primitiivinen Pythagoraan kolmikko. Tällöin $(x, y) = (x, z) = (y, z) = 1$.*

Todistus. (vrt. [3, s. 511]) Olkoon (x, y, z) primitiivinen Pythagoraan kolmikko. Tehdään vastaoletus, että $(x, y) > 1$. Tällöin on olemassa sellainen alkuluku p, että $p \mid (x, y)$ ja siis $p \mid x$ ja $p \mid y$. Näin ollen myös $p \mid (x^2 + y^2) = z^2$ ja siis $p \mid z$. Tämä on kuitenkin mahdotonta, sillä määritelmän 3.3 mukaan $(x, y, z) = 1$. Näin ollen vastaoletus on väärä ja $(x, y) = 1$. Vastaavasti voidaan osoittaa, että $(x, z) = (y, z) = 1$.

□

Apulause 3.6. *Olkoon (x, y, z) primitiivinen Pythagoraan kolmikko. Tällöin x on parillinen ja y on pariton tai x on pariton ja y on parillinen.*

Todistus. (vrt. [3, s. 512]) Olkoon (x, y, z) primitiivinen Pythagoraan kolmikko. Apulauseen 3.5 perusteella $(x, y) = 1$, joten x ja y eivät molemmat voi olla parillisia. Jos sekä x että y ovat parittomia, saadaan $x^2 \equiv 1 \pmod 4$ ja $y^2 \equiv 1 \pmod 4$. Tällöin $z^2 = x^2 + y^2 \equiv 2 \pmod 4$. Tämä on kuitenkin mahdotonta, sillä joko $z^2 \equiv 0 \pmod 4$ tai $z^2 \equiv 1 \pmod 4$. Siis joko x on parillinen ja y on pariton tai x on pariton ja y on parillinen.

□

Huomautus 3.1. Koska apulauseen 3.6 perusteella toinen luvuista x ja y on parillinen ja toinen pariton, täytyy luvun z olla pariton.

Apulause 3.7. *Olkoot a ja b positiivisia kokonaislukuja ja olkoot $(a, b) = 1$ ja $ab = c^2$. Tällöin a ja b ovat täydellisiä neliöitä.*

Todistus. Ks. [2, s. 307-308].

Seuraavan lauseen todistuksessa osa laskuista sivuutettiin lähdeteoksessa, mutta tässä esitetään myös nämä lähdeteoksen todistuksesta puuttuvat laskut.

Lause 3.6. *Kolmikko (x, y, z) on primitiivinen Pythagoraan kolmikko, missä y on parillinen, jos ja vain jos*

$$\begin{aligned} x &= s^2 - t^2 \\ y &= 2st \\ z &= s^2 + t^2 \end{aligned}$$

ja s ja t ovat keskenään jaottomia kokonaislukuja, jotka toteuttavat epäyhtälön $s > t > 0$ ja joista toinen on parillinen.

Todistus. (vrt. [2, s. 319]) Jaetaan yhtälö $x^2 + y^2 = z^2$ tekijöihin, jolloin se saadaan muotoon $(x + yi)(x - yi) = z^2$. Olkoon δ lukujen $x + yi$ ja $x - yi$ yhteinen tekijä. Apulauseen 2.2 perusteella δ jakaa myös lukujen $x + yi$ ja $x-yi$ summan ja erotuksen. Toisin sanoen δ jakaa luvut $(x+yi)+(x-yi) = 2x$ ja $(x+yi)-(x-yi) = 2yi$. Jos δ on yksikkö, lukujen $2x$ ja $2yi$ suurin yhteinen tekijä on luku 1. Oletetaan nyt, että δ ei ole yksikkö. Tällöin on oltava $\delta \mid 2x$ ja $\delta \mid 2y$. Koska $z^2 = (x+yi)(x-yi)$, täytyy luvun δ jakaa myös luku z^2, joka on huomautuksen 3.1 perusteella pariton. Siis on oltava $(x + yi, x - yi) = 1$. Apulauseen 3.7 perusteella luvut $x + yi$ ja $x - yi$ ovat täydellisiä neliöitä yksiköillä kertomista vaille.

Saadaan kaksi tapausta: $x + yi = \alpha^2$ ja $x - yi = \beta^2$ tai $x + yi = i\alpha^2$ ja $x - yi = i\beta^2$. Olkoon $\alpha = u + vi$ ja $\beta = m + ni$. Ensimmäisessä tapauksessa saadaan

$$\begin{aligned} x + yi &= \alpha^2 = (u + vi)^2 = u^2 + 2uvi + (vi^2) = (u^2 - v^2) + 2uvi \quad \text{ja} \\ x - yi &= \beta^2 = (m + ni)^2 = m^2 + 2mni + (ni)^2 = (m^2 - n^2) + 2mni. \end{aligned}$$

Näin ollen ensimmäisessä yhtälössä $x = u^2 - v^2$ ja $y = 2uv$. Luvuksi z^2 saadaan

$$\begin{aligned} z^2 = x^2 + y^2 &= (u^2 - v^2)^2 + (2uv)^2 = u^4 - 2u^2v^2 + v^4 + 4u^2v^2 \\ &= u^4 + 2u^2v^2 + v^4 = (u^2 + v^2)^2. \end{aligned}$$

ja tällöin $z = u^2 + v^2$.
Toisesta yhtälöstä saadaan vastaavasti $x = m^2 - n^2$, $y = -2mn$ ja ratkaisemalla z^2 kuten edellä, saadaan $z = m^2 + n^2$.

Toisessa tapauksessa saadaan

$$\begin{aligned} x + yi &= i\alpha^2 = i(u + vi)^2 = u^2i + 2uvi^2 + (vi)^2i = (u^2 - v^2)i - 2uv \quad \text{ja} \\ x - yi &= i\beta^2 = i(m + ni)^2 = m^2i + 2mni^2 + (ni)^2i = (m^2 - n^2)i - 2mn. \end{aligned}$$

Nyt ensimmäisessä yhtälössä $x = -2uv$ ja $y = u^2 - v^2$ ja tällöin $z = u^2 + v^2$. Toisessa yhtälössä $x = -2mn$ ja $y = -(m^2 - n^2)$ ja tällöin $z = m^2 + n^2$.

Neljästä edellä esitetystä yhtälöstä ensimmäinen antaa ratkaisun, jota tässä lauseessa haettiin. Muiden kolmen yhtälön ratkaisuissa yksi tai useampi luvuista x, y ja z on negatiivinen. Myös nämä ratkaisut toteuttavat yhtälön $x^2 + y^2 = z^2$. Lisäksi kahden viimeisen yhtälön ratkaisussa x on parillinen ja y pariton.

□

Viitteet

[1] W. W. Adams & L. J. Goldstein. *Introduction to Number Theory*. Prentice-Hall, Inc. New Jersey. 1976.

[2] M. Erickson & A. Vazzana. *Introduction to Number Theory*. Chapman & Hall/CRC. Boca Raton. 2008.

[3] K. H. Rosen. *Elementary Number Theory and Its Applications*. Pearson/Addison-Wesley. Boston. 2005.