Diofantoksen yhtälöistä ja Gaussin luvuista

Pro Gradu-tutkielma

Tero Syrjä

Matematiikan laitos

Oulun yliopisto

Kevät 2015

Sisältö

Luku 1

Johdanto

Tämä on Pro Gradu-tutkielma Oulun yliopiston matematiikan laitokselle. Tutkielmassa käsitellään perinteisiä lukuteorian aiheita: Diofantoksen yhtälöitä, Gaussin lukuja, Pythagoraan kolmikkoja ja neliöiden summia. Lukuteoria on yksi matematiikan vanhimmista aloista, sen varhaisimpien merkintöjen löytyessä Babylonian ajoilta. Lukuteoriaan sisältyy monia erilaisia aihe-alueita, mutta tiivistetysti voidaan sanoa lukuteorian tutkivan lukuja.

Tutkielman toisessa luvussa on esitelty tämän tutkielman kannalta tärkeitä perusasioita, jotka ovat oleellisia lauseiden ja lemmojen todistuksissa. Suurimman yhteisen tekijän lisäksi perusasioista käydään läpi kongruenssi, neliönjäännös sekä Legendren symboli. Tämän luvun sisältöön viitataan useasti tutkielman edetessä.

Varsinainen tutkielma alkaa kolmannesta luvusta. Tässä luvussa aloitetaan Diofantoksen yhtälöiden tutkiminen lineaarisella Diofantoksen yhtälöllä. Se on ensimmäistä astetta oleva kahden muuttujan kokonaislukukertoiminen yhtälö. Tässä luvussa tutkitaan milloin lineaarisella Diofantoksen yhtälöllä on kokonaislukuratkaisuja.

Neljännessä luvussa siirrymme lineaarisista Diofantoksen yhtälöistä toi-

sen asteen Diofantoksen yhtälöihin. Ne ovat kahden muuttujan toisen asteen yhtälöitä. Toisen asteen Diofantoksen yhtälöiden kokonaislukuratkaisuja kutsutaan Pythagoran kolmikoiksi. Ratkaisukolmikon lukujen ollessa keskenään jaottomia saadaan primitiivinen Pythagoraan kolmikko. Lisäksi tässä luvussa käydään läpi, mitä vaatimuksia näiden kolmen luvun on täytettävä, jotta ne muodostavat primitiivisen Pythagoran kolmikon.

Viidennessä luvussa laajennetaan edelleen Diofantoksen yhtälöiden käsittelyä. Tämän luvun pohjana on Fermat'n suuri lause. Fermat'n suuren lauseen mukaan ei ole olemassa kolmea kokonaislukua niin, että kun kaksi ensimmäistä korotetaan lukua kaksi suurempaan potenssiin ja lasketaan yhteen saadaan kolmas luku korotettuna samaan potenssiin kuin kaksi aiempaa. Tämän vuoksi laajennetaan tarkastelua Gaussin lukuihin. Ne ovat imaginaarilukuja, mutta niiden käyttäytymisellä on paljon yhtäläisyyksiä kokonaislukujen käyttäytymisen kanssa. Tällaisia reaalilukujen kanssa tuttuja ominaisuuksia, kuten esimerkiksi suurin yhteinen tekijä ja alkuluku käydään tässä luvussa läpi Gaussin luvuille.

Kuudennessa ja viimeisessä luvussa laajennetaan tietoutta kahden ja neljän neliön summasta. Tässä luvussa esitetään ehtoja sille, milloin luku voidaan esittää kahden neliön summana. Tutkielma loppuu todistukseen, jossa osoitetaan jokaisen positiivisen kokonaisluvun voitavan esittää neljän neliön summana.

Tutkielmassa on käytetty pääasiallisena lähteenä teosta [1]. Muina lähteinä on käytetty Tapani Matala-ahon luentomateriaalia [2] ja kirjaa [3].

Luku 2

Perusteet

Merkintä *syt* tarkoittaa suurinta yhteistä tekijää. Määritellään se kokonaisluvuille seuraavasti.

Määritelmä 2.0.1. Olkoot annettuna $a, b \in \mathbb{Z}$. Tällöin luku $d \in \mathbb{N}$ on lukujen a ja b suurin yhteinen tekijä ja merkitään $d = syt(a, b)$, mikäli
1. $d \mid a$ ja $d \mid b$.
2. Jos $f \mid a$ ja $f \mid b$, niin on oltava, että $f \mid d$.

Esimerkki 2.0.2. *a)* $syt(12, 9) = 3$.
b) $syt(1001, 66) = 11$, *sillä* $1001 = 7 \cdot 11 \cdot 13$ *ja* $660 = 2 \cdot 3 \cdot 11$.

Seuraava lausetta kutsutaan jakoalgoritmiksi. Suorittamalla algoritmia yhä uudelleen saaduille luvuille voidaan määrittää kahden luvun *syt*.

Lause 2.0.3. *Olkoon* $a, b \in \mathbb{Z}$ *siten, että* $b > 0$. *Tällöin ovat olemassa yksikäsitteiset luvut* $q, r \in \mathbb{Z}$, $0 \leq r < b$, *jotka toteuttavat yhtälön*

$$a = bq + r \tag{2.1}$$

Todistus. Osoitetaan ensin olemassaolo. Olkoon

$$S = \{a - bk : k \in \mathbb{Z}, a - kb \geq 0\}.$$

Alkio a sisältyy joukkoon S, jos $a \geq 0$. Jos $a < 0$, $a - ba = (-a)(-1 + b)$ on joukon S alkio. Jos S sisältää nolla-alkion, on olemassa kokonaisluku q siten, että $a = bq$. Tässä tapauksessa $r = 0$ ja yhtälöllä (2.1) on ratkaisu. Jos nolla-alkio ei sisälly joukkoon S, niin hyvinjärjestysperiaatteen mukaan epätyhjällä joukolla on pienin alkio. Olkoon $r \in \mathbb{Z}$ pienin positiivinen joukon S alkio ja valitaan q siten, että $r = a - bq$. Jos $r \geq b$, niin

$$r - b = a - bq - b = a - (q + 1)b,$$

joka on joukon S alkio. Jos $r = b$, on alkio $r - b = 0$, mikä on ristiriidassa sen kanssa että joukkoon S ei kuulu nolla-alkiota. Täten $r > b$, jolloin $r - b > 0$ ja $r - b < r$. Tämä on ristiriidassa sen kanssa, että r on joukon S pienin positiivinen alkio. On siis oltava $0 \leq r < b$.

Osoitetaan seuraavaksi yksikäsitteisyys. Olkoon

$$a = bq_1 + r_1 = bq_2 + r_2,$$

missä $0 \leq r_1 < b$, $0 \leq r_2 < b$ ja $r_1 < r_2$. Tällöin

$$b(q_1 - q_2) = r_2 - r_1 \geq 0.$$

Koska $r_2 < b$, niin $r_2 - r_1 < b$ mistä saadaan

$$0 \leq b(q_1 - q_2) < b.$$

Koska $q_1, q_2 \in \mathbb{Z}$, on oltava $q_1 - q_2 = 0$, eli $q_1 = q_2$. Tällöin myös $r_1 = r_2$. □

Merkintä $b \equiv c \pmod{m}$ määritellään kokonaisluvuille seuraavasti.

Määritelmä 2.0.4. Olkoon $b, c, m \in \mathbb{Z}$, $m > 1$. Tällöin luku b on kongruentti luvun c kanssa *modulo* m ja kirjoitetaan $b \equiv c \pmod{m}$, jos ja vain jos $m \mid (b - c)$.

Esimerkki 2.0.5. *Tarkastellaan lukujen* 3 *ja* 13 *kongruenssia. Nyt* $13-3=10$ *ja luvun* 10 *ykköstä suurempia tekijöitä ovat* $2, 5$ *ja* 10. *Täten* $13 \equiv 3 \pmod 2$, $3 \equiv 13 \pmod 5$ *ja* $3 \equiv 13 \pmod{10}$.

Seuraava lause ja siihen liittyvä tulos $x^2 \equiv -1 \pmod p$, missä p on alkuluku, on hyvä käydä jo tässä vaiheessa läpi.

Lause 2.0.6. *Kongruenssille*

$$(n-1)! \equiv -1 \pmod n, \tag{2.2}$$

missä $n \in \mathbb{Z}$ *on olemassa ratkaisu, jos ja vain jos luku* n *on alkuluku.*

Todistus. Tehdään ensin vastaoletus. Oletetaan, että luku n on yhdistetty luku, $n = ab$, missä $a, b \in \mathbb{Z}$ siten, että $a \geq b > 1$. Tällöin luku $a \leq n-1$. Tehdään jatko-oletus $a > b$, jolloin luvut a ja b ovat jotkin kertoman $(n-1)!$ tekijät, siis

$$(n-1)! = (n-1)(n-2)\cdots a \cdots b \cdots 2 \cdot 1.$$

Yhtälö (2.2) voidaan kirjoittaa muodossa

$$(n+1)! + 1 = nk, \tag{2.3}$$

missä $n \in \mathbb{Z}$. Koska $n = ab$, yhtälön (2.3) oikea puoli on $nk = abk$. Yhtälön (2.3) vasen puoli voidaan kirjoittaa muodossa

$$(n-1)(n-2)\cdots a \cdots b \cdots 2 \cdot 1 + 1.$$

Vähentämällä yhtälöstä (2.3) puolittain $(n-1)!$ saadaan

$$\begin{aligned} 1 &= abk - (n-1)(n-2)\cdots a \cdots b \cdots 2 \cdot 1 \\ &= a(bk - (n-1)(n-2)\cdots b \cdots 2 \cdot 1). \end{aligned}$$

Koska $a \in \mathbb{Z}$, $a > 1$ ja selvästi $(bk - (n-1)(n-2)\cdots b \cdots 2 \cdot 1) \in \mathbb{Z}$, syntyy ristiriita, sillä $a(bk-(n-1)(n-2)\cdots b\cdots 2\cdot 1) \neq 1$. Täten n ei ole yhdistetty luku.

Tarkastellaan seuraavaksi tilanne, missä $a = b$, jolloin $n = a^2$. Näin ollen luku a on jokin kertoman $(n-1)!$ tekijä ja

$$(n-1)! = (n-1)(n-2)\cdots a \cdots 2 \cdot 1.$$

Täten yhtälö (2.3) voidaan kirjoittaa muodossa

$$(n-1)(n-2)\cdots a \cdots 2 \cdot 1 + 1 = a^2 k.$$

Vähentämällä näin saadusta yhtälöstä puolittain $(n-1)(n-2)\cdots a\cdots 2\cdot 1$ saadaan

$$\begin{aligned} 1 &= a^2 k - (n-1)(n-2)\cdots a \cdots 2 \cdot 1 \\ &= a(ak - (n-1)(n-2)\cdots 2 \cdot 1). \end{aligned}$$

Edelleen, koska $a \in \mathbb{Z}$, $a > 1$ ja $ak - (n-1)(n-2)\cdots 2 \cdot 1 \in \mathbb{Z}$. Täten $a(ak - (n-1)(n-2)\cdots 2 \cdot 1) \neq 1$ ja saadaan ristiriita sen kanssa että n on yhdistetty luku.

Oletetaan, että n on alkuluku. Tällöin jokaisella $x \in \mathbb{Z}_n^*$ kohti on olemassa yksikäsitteinen $y \in \mathbb{Z}_n^*$, joille $xy \equiv 1 \pmod{n}$. Jos $x = y$, niin $x^2 \equiv 1 \pmod{n}$. Tällöin $n \mid x^2 - 1$. Koska $x^2 - 1 = (x+1)(x-1)$, pätee $n \mid (x+1)(x-1)$. Luvun n ollessa alkuluku, on oltava $x = n-1$, $x = 1$ tai $x = -1$. Joka tapauksessa on joko $x \equiv 1 \pmod{n}$ tai $x \equiv -1 \pmod{n}$. Kunnan $\mathbb{Z}_n^*$ kaikkien alkioiden tulo on $(n-1)!$. Nyt $1 \equiv 1 \pmod{n}$ ja $n - 1 \equiv -1 \pmod{n}$. Lopuilla kunnan $\mathbb{Z}_n^*$ alkioilla on yksikäsitteinen käänteisalkio tässä kunnassa. Alkion ja sen käänteisalkion tulo on kongruentti $1 \bmod n$, joten näistä alkioista saamme $(n-3)/2$ kappaletta tuloja, jotka ovat kongruentteja $1 \bmod n$. Näin ollen

$$(n-1)! \equiv 1^{(n-3)/2} \cdot 1 \cdot (-1) \equiv -1 \pmod{n}.$$

□

Tehdään lisätarkasteluja edellistä lausetta koskien. Parittomalle alkuluvulle p pätee

$$\begin{aligned}(p-1)! &= \big(1\cdot 2\cdots(\frac{p-1}{2})\big)\cdot\big((\frac{p+1}{2})\cdots(p-2)\cdot(p-1)\big)\\ &\equiv \big(1\cdot 2\cdots(\frac{p-1}{2})\big)\cdot\big((\frac{-p+1}{2})\cdots(-2)\cdot(-1)\big) \pmod p\\ &\equiv \big(1\cdot 2\cdots(\frac{p-1}{2})\big)^2(-1)^{(p-1)/2} \pmod p.\end{aligned}$$

Koska p on pariton alkuluku, niin $p \equiv 1$ tai $3 \pmod 4$. Siis $p = 1+4k$ tai $p = 3+4k$, missä $k \in \mathbb{Z}$. Jos $p = 1+4k$, niin

$$(-1)^{(p-1)/2} = (-1)^{(1+4k-1)/2} = (-1)^{2k} = 1.$$

Jos $p = 3+4k$, niin

$$(-1)^{(p-1)/2} = (-1)^{(3+4k-1)/2} = (-1)^{1+2k} = (-1)(-1)^{2k} = -1.$$

Näin ollen, jos $p = 1+4k$ ja jos merkitään $x = \big(1\cdot 2\cdots(\frac{p-1}{2})\big)$, niin

$$(p-1)! \equiv x^2 \pmod p.$$

Yhtälön(2.2) mukaan $(n-1)! \equiv -1 \pmod n$, joten

$$x^2 \equiv -1 \pmod p \tag{2.4}$$

Määritelmä 2.0.7. Olkoon $a \in \mathbb{Z}^*{}_n$. Jos yhtälöllä

$$a \equiv x^2 \pmod p \tag{2.5}$$

on ratkaisu jollain $x \in \mathbb{Z}, x \neq 0$, on a neliönjäännös *modulo* p. Jos yhtälöllä (2.5) ei ole ratkaisua, ei a ole neliönjäännös *modulo* p. Neliönjäännösten *modulo* p joukko on

$$R = \{x^2 : x \in \mathbb{Z}_n^*\}.$$

Ei-neliönjäännösten *modulo* p joukko on

$$N = \mathbb{Z}_p^* \setminus R.$$

Esimerkki 2.0.8. *Tarkastellaan kuntaa* $\mathbb{Z}_7^*$. *Kunnan* $\mathbb{Z}_7^*$ *alkiot ovat* $\{1,2,3,4,5,6\}$ *ja näiden neliöt modulo* 7 *ovat* $\{1,4,2,2,4,1\}$. *Täten* $R = \{1,2,4\}$ *ja* $N = \{3,5,6\}$.

Määritelmä 2.0.9. Legendren symboli $(\frac{a}{p})$ määritellään seuraavasti

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \quad jos \quad a \equiv 0 \pmod{p} \\ 1 \quad jos \quad a \in R \\ -1 \quad jos \quad a \in N. \end{cases}$$

Lause 2.0.10. *Parittomalle alkuluvulle* p *pätee*

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \quad jos \quad p = 4k+1 \\ -1 \quad jos \quad p = 4k+3. \end{cases}$$

Todistus. Määritelmän 2.0.9 nojalla

$$\left(\frac{-1}{p}\right) = \begin{cases} 1 \quad jos \quad -1 \in R \\ -1 \quad jos \quad -1 \in N. \end{cases}$$

Nyt $-1 \in R$ jos $x^2 \equiv -1 \pmod{p}$. Lauseen 2.0.6 lisätarkastelujen nojalla tämä pätee, jos $n = 4k+1$. Jälkimmäinen ehto $-1 \in N$ toteutuu, kun $x^2 \not\equiv -1 \pmod{p}$. Lauseen 2.0.6 lisätarkastelut osoittavat että tämä pätee parittomalle alkuluvulle p, kun $p = 3 + 4k$. □

Legengren symbolille pätee myös seuraava kaava, kun p on pariton alkuluku

$$(\frac{a}{p})(\frac{b}{p}) = (\frac{ab}{p}).$$

Luku 3

Lineaarinen Diofantoksen yhtälö

Määritelmä 3.0.11. Olkoot a, b ja c kokonaislukuja. Muotoa

$$ax + by = c \tag{3.1}$$

olevia yhtälöitä kutsutaan lineaarisiksi Diofantoksen yhtälöiksi. Yhtälön (3.1) kokonaislukuratkaisua $x, y \in \mathbb{Z}$ kutsutaan Diofantoksen yhtälön ratkaisuksi.

Lause 3.0.12. *Olkoot $a, b \in \mathbb{Z}$ siten, että ainakin toinen on nollasta eroava. Tällöin $syt(a, b)$ on pienin positiivinen arvo summalle $ax+by$, missä $x, y \in \mathbb{Z}$, eli $syt(a, b)$ on pienin positiivinen lineaarikombinaatio luvuista a ja b.*

Todistus. Valitsemalla $x = a$ ja $y = b$ saadaan

$$ax + by = a^2 + b^2 > 0,$$

joten positiivinen lineaarikombinaatio on olemassa. Olkoon luku g pienin näistä lineaarikombinaatioista ja merkitään $g = ax_0 + by_0$. Lauseen 2.0.3 nojalla ovat olemassa luvut $q, r \in \mathbb{Z}$, $0 \leq r < g$ siten, että

$$a = qg + r = (ax_0 + by_0)q + r = qax_0 + qby_0 + r,$$

josta

$$r = a - qax_0 - qby_0 = a(1 - qx_0) + b(-qy_0),$$

joten r on lukujen a ja b lineaarikombinaatio. Luku g asetettiin olemaan pienin positiivinen lineaarikombinaatio luvuista a ja b ja luku r on jakoalgoritmin ehtojen mukaisesti $0 \leq r < g$. Tällöin luvulle r ainoa mahdollinen arvo on 0. Tämä tarkoittaa sitä, että $a = qg$ ja $g \mid a$. Koska $g = ax_0 + by_0$, myös $g \mid b$. Siis luku g on tekijänä luvuissa a ja b.

On vielä osoitettava, että g on lukujen a ja b suurin yhteinen tekijä. Olkoon luku d sellainen, että $d \mid a$ ja $d \mid b$. Tällöin $a = kd$ ja $b = md$, missä $k, m \in \mathbb{Z}$ ja

$$a + b = kd + md = d(k + m).$$

Selvästi $d \mid (a + b)$. Myös $d \mid g$, sillä

$$g = ax_0 + by_0 = kdx_0 + mdy_0 = d(kx_0 + my_0).$$

Näin ollen $d \leq g$ ja $g = syt(a, b)$. □

Esimerkki 3.0.13. *Tarkastellaan lukuja* 9 *ja* 6. *Näille luvuille* $syt(9, 6) = 3$. *Pienin positiivinen arvo summalle* $9x + 6y$ *saadaan kun* $x = 1$ *ja* $y = -1$, *jolloin* $9x + 6y = 9 - 6 = 3 = syt(9, 6)$.

Lause 3.0.14. *Lineaarisella Diofantoksen yhtälöllä*

$$ax + by = c \tag{3.2}$$

on ratkaisu, jos ja vain jos $syt(a, b) \mid c$.

Todistus. Jos $c = syt(a, b)$, niin Lauseen 3.0.12 mukaan yhtälöllä (3.2) on ratkaisu.

Olkoon $c = k \cdot syt(a,b)$, missä $k \in \mathbb{Z}$. Lauseen 3.0.12 mukaan on olemassa luvut $x_0, y_0 \in \mathbb{Z}$ siten, että yhtälöllä $ax_0 + by_0 = syt(a,b)$ on ratkaisu. Kertomalla tätä yhtälöä puolittain luvulla k saadaan

$$a(kx_0) + b(ky_0) = k \cdot syt(a,b) = c.$$

Olkoon $c \neq k \cdot syt(a,b)$, missä $k \in \mathbb{Z}$. Kuitenkin $syt(a,b) \mid a$ ja $syt(a,b) \mid b$, joten $syt(a,b) \mid (a+b)$ eli $a + b = m \cdot syt(a,b)$, missä $m \in \mathbb{Z}$. Täten lukujen a ja b *syt* jakaa kaikki lukujen a ja b lineaarikombinaatiot. Syntyy ristiriita sen kanssa, että $c \neq k \cdot syt(a,b)$. On siis oltava $syt(a,b) \mid c$. □

Esimerkki 3.0.15. *Tarkastellaan lineaarista Diofantoksen yhtälöä, joka on muotoa* $7x + 13y = c$. *Nyt* $syt(7,13) = 1$ *ja jakoalgoritmia käyttämällä saadaan*

$$\begin{aligned} 13 &= 1 \cdot 7 + 6 \\ 7 &= 1 \cdot 6 + 1, \end{aligned}$$

josta

$$\begin{aligned} 1 &= 7 - 1 \cdot 6 \\ &= 7 - (13 - 7) \\ &= -1 \cdot 13 + 2 \cdot 7. \end{aligned}$$

Nyt $syt(7,13) \mid c$ *ja tällöin lineaarisen Diofantoksen yhtälön* $7x + 13y = c$ *kaikki ratkaisut ovat muotoa* $k \cdot (2 \cdot 7) + k \cdot \big((-1) \cdot 13\big) = k \cdot c$, *missä* $k \in \mathbb{Z}$.

Lause 3.0.16. *Olkoot* $a, b, c \in \mathbb{Z}$ *ja* $g = syt(a,b)$. *Oletetaan, että yhtälöllä*

$$ax + by = c \tag{3.3}$$

on ratkaisu $x_0, y_0 \in \mathbb{Z}$. *Tällöin yhtälön* (3.3) *kaikki ratkaisut ovat muotoa* $x = x_0 + mb/g$ *ja* $y = y_0 - ma/g$, *missä* $m \in \mathbb{Z}$.

Todistus. Sijoittamalla $x = x_0 + mb/g$ ja $y = y_0 - ma/g$ suoraan yhtälöön (3.3) saadaan

$$\begin{aligned} a(x_0 + mb/g) + b(y_0 - ma/g) &= ax_0 + amb/g + by_0 - bma/g \\ &= ax_0 + by_0 \\ &= c. \end{aligned}$$

Täten $x = x_0 + mb/g$ ja $y = y_0 - ma/g$ on yhtälön (3.3) ratkaisu. Pitää vielä osoittaa, että kaikki ratkaisut ovat tätä muotoa. Olkoon (x_1, y_1) jokin yhtälön (3.3) ratkaisu. Tällöin

$$ax_1 + by_1 = ax_0 + by_0,$$

josta saadaan vähentämällä puolittain ax_0 ja by_1

$$a(x_1 - x_0) = b(y_0 - y_1). \tag{3.4}$$

Nähdään, että $b|\big(a(x_1 - x_0)\big)$. Tällöin myös $(b/g)|\big((a/g)(x_1 - x_0)\big)$. Koska b/g ja a/g ovat keskenään jaottomia, niin $(b/g)|(x_1 - x_0)$. Tällöin

$$x_1 - x_0 = mb/g, \qquad m \in \mathbb{Z},$$

josta saadaan

$$x_1 = x_0 + mb/g.$$

Väitteen $y_1 = y_0 - ma/g$ todistus tapahtuu vastaavalla tavalla palaamalla yhtälöön (3.4). □

Lause 3.0.17. *Olkoot $a, b \in \mathbb{Z}^+$ ja $g = syt(a, b)$. Jos $g \mid c$ ja $c > ab/g$, niin yhtälöllä $ax + by = c$ on ratkaisu joillain $x, y \in \mathbb{Z}^+$.*

Todistus. Yhtälö $ax + by = c$ muodostaa suoran xy-tasossa kulkien pisteiden $(c/a, 0)$ ja $(0, c/b)$ kautta. Merkitään janaa, jonka päätepisteinä ovat nämä pisteet, kirjaimella L ja näin saadun janan pituutta kirjaimella l. Täten

$$l = \sqrt{(c/a - 0)^2 + (c/b - 0)^2} = \sqrt{\frac{c^2b^2}{a^2b^2} + \frac{a^2c^2}{a^2b^2}} = \frac{c\sqrt{a^2 + b^2}}{ab}.$$

Koska $syt(a, b) \mid c$, yhtälöllä on kokonaislukuratkaisu (x_0, y_0). Lauseen 3.0.16 nojalla kaikki kokonaislukuratkaisut voidaan esittää muodossa $(x_0 + mb/g, y_0 - ma/g)$. Peräkkäisten m:n arvojen muodostama suora kulkee pisteiden

$$(x_0 + mb/g, y_0 - ma/g)$$

ja

$$(x_0 + (m + 1)b/g, y_0 - (m + 1)a/g)$$

kautta. Näiden pisteiden x-koordinaattien välinen etäisyys on

$$\mid x_0 + (m + 1)b/g - x_0 - mb/g \mid = b/g.$$

Vastaavasti y-koordinaattien välinen etäisyys on

$$\mid y_0 - (m + 1)a/g - y_0 + ma/g \mid = a/g.$$

Näin ollen luvun m peräkkäisten arvojen muodostamien pisteiden välinen etäisyys on

$$E = \sqrt{a^2/g^2 + b^2/g^2} = \sqrt{a^2 + b^2}/g.$$

Lauseen oletuksena on $c > ab/g$, joten $\frac{c}{ab} > \frac{1}{g}$. Kertomalla epäyhtälö puolittain luvulla $\sqrt{a^2 + b^2}$ saadaan

$$\frac{c\sqrt{a^2 + b^2}}{ab} > \frac{\sqrt{a^2 + b^2}}{g},$$

eli $l > E$. Näin ollen janalta L löytyy kokonaislukuratkaisu (x, y). □

Esimerkki 3.0.18. *Tutkitaan yhtälön* $12x+13y = 200$ *ratkaisuja, kun* $x, y \in \mathbb{Z}^+$.

Nyt $syt(12, 13) = 1$ *ja* $200 > 12 \cdot 13$*, joten on olemassa alkuehdon täyttävä ratkaisu* x, y*. Huomataan, että* $(x, y) = (8, 8)$ *on eräs ratkaisu, kuten myös* $(x, y) = (-200, 200)$.

Luku 4

Pythagoraan kolmikko

Määritelmä 4.0.19. Yhtälön

$$x^2 + y^2 = z^2 \tag{4.1}$$

ratkaisua $(x, y, z) \in \mathbb{Z}^3$ kutsutaan Pythagoraan kolmikoksi. Pythagoraan kolmikko (x, y, z) on primitiivinen, jos $syt(x, y, z) = 1$.

Lause 4.0.20. *Primitiiviselle Pythagoraan kolmikolle* (x, y, z) *pätee* $syt(x, y) = syt(x, z) = syt(y, z) = 1$.

Todistus. Olkoot $d = syt(x, y)$. Oletetaan, että $d > 1$ jolloin on olemassa alkuluku p siten, että $p \mid d$. Tällöin $p \mid syt(x, y)$ ja $p \mid x$ sekä $p \mid y$. Tästä seuraa, että $p \mid z^2$ ja koska p on alkuluku, niin $p \mid z$. Näin ollen $syt(x, y, z) \geq p$, mikä on ristiriita sen kanssa että primitiiviselle Pythagoraan kolmikolle on $syt(x, y, z) = 1$. Oletus $d > 1$ on väärä, joten $d = 1$. Saatiin osoitettua, että $syt(x, y) = 1$. Tapaukset $syt(x, z) = 1$ ja $syt(y, z) = 1$ voidaan osoittaa vastaavasti. □

Esimerkki 4.0.21. *Tarkastellaan lukuja* $3, 4$ *ja* 5. *Nämä luvut muodostamavat Pythagoraan kolmikon, sillä* $3^2 + 4^2 = 25 = 5^2$. *Lukujen* 3 *ja* 4 *suurin yhteinen tekijä on* 1, *kuten myös* $syt(3, 5) = 1$ *ja* $syt(4, 5) = 1$. *Tällöin*

syt$(3,4,5) = 1$ *ja kolmikko on primitiivinen. Kun yhtälöä* $3^2 + 4^2 = 5^2$ *kerrotaan puolittain luvulla* k^2*, missä* $k \in \mathbb{Z}^+$*, saadaan* $(3k)^2 + (4k)^2 = (5k)^2$*. Näin voidaan muodostaa ääretön määrä Pythagoraan kolmikoita tuntemalla jokin primitiivinen Pythagoraan kolmikko* (x, y, z)*.*

Kaikki Pythagoraan kolmikot voidaan siis esittää muodossa (kx, ky, kz), missä (x, y, z) on primitiivinen Pythagoraan kolmikko. Tarkastellaan primitiivistä Pythagoraan kolmikkoa (x, y, z) tarkemmin. Yhtälöstä $x^2 + y^2 = z^2$ seuraa, että ainakin yhden luvuista tulee olla parillinen.

Tutkitaan lukujen pariteettia. Jos luvut x ja y ovat parittomia, myös niiden neliöt ovat parittomia ja tällöin summa $x^2 + y^2$ on parillinen. Näin ollen luvun z on oltava parillinen.

Tarkastellaan seuraavaksi tilannetta, jossa joko x tai y on parillinen. Olkoon x parillinen, jolloin sen neliö on myös parillinen. Tällöin y on pariton ja sen neliö on myös pariton. Tällöin summa $x^2 + y^2$ on pariton, joten luvun z on oltava pariton.

Edellisen perusteella täsmälleen yksi luvuista x, y tai z on parillinen. Oletetaan, että z on toinen parittomista luvuista. Nimittäin, jos z on parillinen, niin luvut x ja y ovat parittomia. Tällöin $x^2 \equiv y^2 \equiv 1 \pmod 4$, kun taas $z^2 \equiv 0 \pmod 4$. Laskemalla yhtälö $x^2 + y^2 = z^2$ modulo 4 saadaan yhtälön vasemmasta puolesta $x^2 + y^2 \equiv 1 + 1 = 2$ ja oikeasta puolesta $z^2 \equiv 0$. Syntyy ristiriita sen oletuksen kanssa, että luku z on parillinen. Näin ollen z on pariton ja jompikumpi luvuista x tai y on parillinen.

Oletetaan että x on parillinen. Järjestelmällä yhtälön (4.1) termejä uudestaan saamme

$$(z + y)(z - y) = x^2.$$

Koska luvut y ja z ovat parittomia, niin $z+y$ ja $z-y$ ovat molemmat parillisia.

Näin ollen edellinen yhtälö voidaan kirjoittaa muotoon

$$\left(\frac{z+y}{2}\right)\left(\frac{z-y}{2}\right) = \left(\frac{x}{2}\right)^2,$$

jossa molemmat vasemmanpuoleiset tekijät ovat kokonaislukuja. Olkoon

$$syt(\frac{z+y}{2}, \frac{z-y}{2}) = d \in \mathbb{Z}^+.$$

Tällöin d jakaa sekä luvun $\frac{z+y}{2}$, että luvun $\frac{z-y}{2}$. Tällöin luku d jakaa myös niiden summan ja erotuksen. Koska

$$\left(\frac{z+y}{2}\right) + \left(\frac{z-y}{2}\right) = z,$$

$$\left(\frac{z+y}{2}\right) - \left(\frac{z-y}{2}\right) = y,$$

niin $d \mid z$ ja $d \mid y$. Koska luvut z ja y ovat primitiivisestä Pythagoraan kolmikosta, niin $syt(z, y) = 1$. Tästä seuraa, että $d = 1$. Tiedetään siis, että $\left(\frac{z+y}{2}\right)$ ja $\left(\frac{z-y}{2}\right)$ ovat keskenään jaottomia ja niiden tulo on jonkin luvun neliö. Tarvitaan seuraavaa lemmaa, jotta voidaan ratkaista yhtälöt

$$\left(\frac{z+y}{2}\right) = s^2$$

$$\left(\frac{z-y}{2}\right) = t^2,$$

missä $t, s \in \mathbb{Z}^+$.

Lemma 4.0.22. *Oletetaan, että $a, b \in \mathbb{Z}^+$, $syt(a, b) = 1$ ja $ab = c^2$. Tällöin a ja b ovat kokonaisluvun neliöitä.*

Todistus. Oletetaan, että luvut a ja b voidaan jakaa tekijöihin seuraavasti. Luvulle a on esitys

$$a = A_1^{\alpha_1} \cdot A_2^{\alpha_2} \cdots A_k^{\alpha_k},$$

missä A_i ovat alkulukuja kun $i \in \{1, 2, \ldots, k\}$ ja $\alpha_i \in \mathbb{Z}^+$ kaikilla $i \in \{1, 2, \ldots, k\}$. Luvulle b on esitys

$$b = B_1^{\beta_1} \cdot B_2^{\beta_2} \cdots B_j^{\beta_j},$$

missä B_i ovat alkulukuja kun $i \in \{1, 2, \ldots, j\}$ ja $\beta_i \in \mathbb{Z}^+$ kaikilla $i \in \{1, 2, \ldots, j\}$. On osoitettava että kaikilla luvun i arvoilla α_i on parillinen. Koska $syt(a, b) = 1$, niin A_i ei jaa lukua $b = B_1^{\beta_1} \cdot B_2^{\beta_2} \cdots B_j^{\beta_j}$ millään i:n arvolla. Näin ollen luvun c^2 esityksessä olevan luvun A_i potenssi on α_i, eli

$$c^2 = A_1^{\alpha_1} \cdot A_2^{\alpha_2} \cdots A_k^{\alpha_k} \cdot B_1^{\beta_1} \cdot B_2^{\beta_2} \cdots B_j^{\beta_j}.$$

Jos luvulle c tekijän A_i potenssi on γ_i, niin $\alpha_i = 2\gamma_i$. Täten α_i on parillinen kaikilla $i \in \{1, 2, \ldots, k\}$. Sama pätee myös luvulle b, β_i on parillinen kaikilla $i \in \{1, \ldots, j\}$. Näin ollen luvut a ja b ovat kokonaisluvun neliöitä. □

Koska $\left(\frac{z+y}{2}\right)$ ja $\left(\frac{z-y}{2}\right)$ ovat keskenään jaottomia, niin myös s ja t ovat keskenään jaottomia. Toisaalta $s^2t^2 = (x/2)^2$, joten

$$x = 2st.$$

Ratkaisemalla y ja z lukujen s ja t suhteen, saadaan

$$y = s^2 - t^2$$

$$z = s^2 + t^2.$$

Näin ollen voidaan kolmikko (x, y, z) esittää lukujen s ja t avulla seuraavasti: $(2st, s^2 - t^2, s^2 + t^2)$. Luvuille s ja t on kuitenkin joitain rajoituksia. Aiemman perusteella tiedetään, että niiden tulee olla keskenään jaottomia. Koska luku y on pariton, toinen luvuista s tai t on pariton. Koska y on positiivinen, niin on oltava $s > t$. Jos etsitään lukupareja (s, t) jotka toteuttavat nämä ehdot, saadaan primitiivisiä Pythagoran kolmikkoja.

Lause 4.0.23. *Kolmikko* (x, y, z) *on Pythagoraan primitiivinen kolmikko, missä* x *on parillinen, jos ja vain jos*

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

jossa $t, s \in \mathbb{Z}^+$ *ovat keskenään jaottomia ja joille pätee* $s > t > 0$ *ja* s *tai* t *on parillinen.*

Todistus. Nyt

$$\begin{aligned} x^2 + y^2 &= 4s^2t^2 + s^4 - 2s^2t^2 + t^4 \\ &= s^4 + 2s^2t^2 + t^4 \\ &= z^2, \end{aligned}$$

joten luvut muodostavat Pythagoraan kolmikon. Tarkastellaan lukujen $2st$, $s^2 - t^2$ ja $s^2 + t^2$ suurinta yhteistä tekijää. Olkoon $d = syt(2st, s^2 - t^2, s^2 + t^2)$ ja oletetaan, että $d > 1$. Näin ollen $d|s^2 - t^2$ eli $d|(s+t)(s-t)$. Koska joko s tai t on pariton, luvut $(s + t)$ ja $(s - t)$ ovat parittomia ja myös niiden tulo $(s + t)(s - t)$ on pariton. Täten myös d on pariton. Koska $d|2st$, niin joko $d|s$ tai $d|t$, mutta ei molempia, sillä luvut t ja s ovat keskenään jaottomia. Edelleen, koska $d|(s + t)(s - t)$, niin joko $d|(s + t)$ tai $d|(s - t)$.

Olkoon ensin $d|(s + t)$. Jos $d|s$ niin välttämättä myös luku d jakaa luvun t, mikä on ristiriita sen kanssa että d jakaa vain toisen luvuista s ja t. Jos $d|t$, edellistä päättelyä toistamalla saadaan $d|s$. Syntyy jälleen ristiriita, sillä luvun d tulee jakaa vain toinen luvuista s ja t.

Olkoon seuraavaksi $d|(s - t)$. Jos $d|t$, niin siitä seuraa, että $d|s$. Valitsemalla $d|s$ seuraa, että $d|t$. Nämä molemmat ovat ristiriitoja sen kanssa, että d jakaa vain toisen luvuista s ja t. Näin ollen ei ole olemassa lukua

$d = syt(2st, s^2 - t^2, s^2 + t^2)$, jolle pätee $d > 1$. Täten ainoa vaihtoehto on triviaali ratkaisu $syt(2st, s^2 - t^2, s^2 + t^2) = 1$. □

Luku 5

Gaussin luvuista

Tässä luvussa käytetään kreikkalaisia kirjaimia, kun on kyse Gaussin luvuista ja roomalaisia kirjaimia, kun on kyse kokonaisluvuista.

Määritelmä 5.0.24. Gaussin luku on kompleksiluku $a + bi$, missä $a, b \in \mathbb{Z}$.

Esimerkki 5.0.25. *Valitsemalla $b = 0$, saadaan kaikki reaaliset kokonaisluvut. Määritelmän nojalla nämä ovat Gaussin lukuja.*

Määritelmä 5.0.26. Olkoot α ja β Gaussin lukuja ja $\alpha \neq 0$. Jos on olemassa Gaussin luku γ siten, että $\beta = \alpha\gamma$, niin α jakaa luvun β ja merkitään $\alpha|\beta$.

Esimerkki 5.0.27. *Tarkastellaan lukuja $2 + i$ ja $1 + 3i$. Huomataan, että $(2 + i)(1 + i) = 1 + 3i$, joten $(2 + i)|(1 + 3i)$.*

Määritelmä 5.0.28. Gaussin luvun $a + bi$ normi on

$$N(a + bi) = a^2 + b^2 \tag{5.1}$$

Esimerkki 5.0.29. *Luvun $5 + 9i$ normi on $N(5 + 9i) = 5^2 + 9^2 = 25 + 81 = 106$.*

Määritelmä 5.0.30. Olkoot α muotoa $\alpha = x+yi$ oleva Gaussin luku. Luvun α kompleksikonjugaatti $\overline{\alpha} = x - yi$.

Lause 5.0.31. *Olkoot α Gaussin luku. Luvun α normi on luvun α ja luvun α kompleksikonjugaatin tulo.*

Todistus. Olkoon luku α muotoa $\alpha = x + yi$. Tällöin $N(\alpha) = x^2 + y^2$. Luvun α kompleksikonjugaatti $\overline{\alpha} = x - yi$, jolloin

$$\alpha \cdot \overline{\alpha} = (x + yi)(x - yi) = x^2 + xyi - xyi - y^2 i^2 = x^2 + y^2.$$

□

Lause 5.0.32. *Olkoot α ja β Gaussin lukuja. Tällöin on voimassa*

$$N(\alpha \cdot \beta) = N(\alpha) \cdot N(\beta). \tag{5.2}$$

Todistus. Luvut α ja β voidaan kirjoittaa seuraavasti $\alpha = x+yi$ ja $\beta = a+bi$. Tällöin

$$\begin{aligned} N(\alpha \cdot \beta) &= N\big((x + yi) \cdot (a + bi)\big) \\ &= N\big((xa - yb) + (xb + ya) \cdot i\big) \\ &= (xa - yb)^2 + (xb + ya)^2 \\ &= x^2a^2 + y^2b^2 + x^2b^2 + y^2a^2 \\ &= (x^2 + y^2)(a^2 + b^2) \\ &= N(\alpha) \cdot N(\beta). \end{aligned}$$

□

Lause 5.0.33. *Olkoot α ja β Gaussin lukuja niin, että $\alpha \mid \beta$. Tällöin $N(\alpha) \mid N(\beta)$ kokonaislukujen $\mathbb{Z}$ renkaassa.*

Todistus. Jos $\alpha \mid \beta$, niin $\beta = \alpha \cdot \gamma$, missä γ on jokin Gaussin luku. Lauseen 5.0.32 perusteella $N(\beta) = N(\alpha)N(\gamma)$, joten $N(\alpha) \mid N(\beta)$. □

Määritelmä 5.0.34. Gaussin luku ϵ on yksikkö, jos $\epsilon \cdot \lambda = 1$ jollain Gaussin luvulla λ.

Esimerkki 5.0.35. *Gaussin lukujen muodostaman renkaan yksiköt ovat* 1, $-1, i$ *ja* i.

Lause 5.0.36. *Gaussin luku* ϵ *on yksikkö jos ja vain jos* $N(\epsilon) = 1$.

Todistus. Olkoon luku ϵ muotoa $\epsilon = a + bi$. Jos $N(\epsilon) = 1$, niin $a^2 + b^2 = 1$. Koska $a, b \in \mathbb{Z}$, niin edellisen yhtälön ratkaisut ovat $a = \pm 1, b = 0$ tai $a = 0, b = \pm 1$. Siis

$$\epsilon = \pm 1 + 0 \cdot i = \pm 1$$

tai

$$\epsilon = 0 \pm 1 \cdot i = \pm i.$$

Jos $\epsilon = a + ib$ on yksikkö, niin $\epsilon = \pm 1$ tai $\epsilon = \pm i$. Jos $\epsilon = \pm 1$, niin $\pm 1 \cdot \pm 1 = 1$. Toisaalta, jos $\epsilon = \pm i$, niin

$$\pm i \cdot \mp i = -i^2 = -(-1) = 1.$$

Siis $\epsilon \mid 1$. Tällöin Lauseen 5.0.33 perusteella $N(\epsilon) \mid N(1)$. Koska $N(1) = 1^2 + 0^2 = 1$, niin $N(\epsilon) \mid 1$. $N(\epsilon)$ on positiivinen kokonaisluku, joten ainoa ratkaisu on $N(\epsilon) = 1$. □

Määritelmä 5.0.37. Gaussin luvut α ja β ovat liitännäisiä, jos $\alpha = \epsilon \cdot \beta$, missä ϵ on yksikkö.

Esimerkki 5.0.38. *Gaussin luvun* $3 + i$ *liitännäinen on* $(3 + i) \cdot i = 3i - 1 = -1 + 3i$. *Myös* $(3 + i) \cdot (-i) = -3i + 1 = 1 - 3i$ *on liitännäinen. Koska yksikkö* ϵ *voi saada* 4 *eri arvoa, niin jokaisella nollasta eroavalla Gaussin luvulla on neljä eri liitännäistä. Loput kaksi liitännäistä luvulle* $3 + i$ *ovat* $(3 + i) \cdot (-1) = -3 - i$ *ja* $(3 + i) \cdot 1 = 3 + i$ *eli luku itse.*

Määritelmä 5.0.39. Olkoon $\kappa \neq 0$ Gaussin luku. Jos κ saadaan kertomalla keskenään kaksi Gaussin lukua, joista kumpikaan ei ole yksikkö, on κ Gaussin yhdistetty luku. Jos κ ei ole yhdistetty luku, niin se on Gaussin alkuluku.

Esimerkki 5.0.40. *Luku* 2 *on reaalilukujen kunnassa jaoton. Gaussin lukujen muodostamassa renkaassa se voidaan jakaa tekijöihin, sillä* $(1+i)(1-i) = 1-i^2 = 2$. *Näin ollen se on Gaussin yhdistetty luku.*

Tarkastellaan vielä lukua $1-i$. *Oletetaan, että se voidaan jakaa tekijöihin, eli* $1-i = \alpha\beta$. *Lauseen 5.0.32 perusteella* $N(1-i) = N(\alpha)N(\beta)$. *Koska* $N(1-i) = 1^2 + (-1)^2 = 2$, *niin* $N(\alpha)N(\beta) = 2$. *Tämä on mahdollista vain, jos* $N(\alpha) = 1$ *ja* $N(\beta) = 2$ *tai* $N(\alpha) = 2$ *ja* $N(\beta) = 1$. *Jos* $N(\alpha) = 1$, *niin Lauseen 5.0.36 mukaan se on yksikkö. Koska* α *on yksikkö, niin määritelmän 5.0.39 perusteella* $1-i$ *on Gaussin alkuluku. Vastaavasti, jos* $N(\beta) = 1$, *niin* β *on yksikkö ja kuten edellä, on* $1-i$ *Gaussin alkuluku.*

Luku $1+i$ *voidaan samalla tavalla osoittaa Gaussin alkuluvuksi.*

Lause 5.0.41. *Olkoon* α *Gaussin luku ja* $N(\alpha) = p$, *missä* p *on alkuluku. Tällöin* α *on Gaussin alkuluku.*

Todistus. Oletetaan, että α on Gaussin yhdistetty luku, $\alpha = \beta\gamma$, missä β ja γ ovat Gaussin lukuja. Tällöin $N(\alpha) = N(\beta)N(\gamma)$. Koska $N(\beta)$ ja $N(\gamma)$ ovat positiivisia kokonaislukuja, ei niiden tulo voi olla alkuluku. Syntyy ristiriita sen oletuksen kanssa, että α on Gaussin yhdistetty luku, joten α on Gaussin alkuluku. □

Esimerkki 5.0.42. *Tarkastellaan Gaussin lukua* 3. *Oletetaan sen olevan yhdistetty luku,* $3 = \alpha\beta$, *jolloin* $N(3) = 9 = N(\alpha)N(\beta)$. *Koska* α *ja* β *eivät ole yksikköjä, niin* $N(\alpha) = N(\beta) = 3$. *Jos* $\alpha = x + yi$, *niin* $N(\alpha) = x^2 + y^2$. *Lukua* 3 *ei voi esittää kahden kokonaisluvun neliön summana, joten* 3 *ei ole Gaussin yhdistetty luku. Tällöin se on Gaussin alkuluku.*

Lause 5.0.43. *Alkuluku on Gaussin yhdistetty luku, jos ja vain jos se on kahden neliön summa.*

Todistus. Olkoon p alkuluku siten, että se on kahden neliön summa, $p = a^2 + b^2$, missä $a, b \in \mathbb{Z}$. Luku $a^2 + b^2$ voidaan esittää Gaussin lukujen avulla muodossa $(a + bi)(a - bi)$, joten p on Gaussin yhdistetty luku

Olkoon alkuluku p Gaussin yhdistetty luku. Tällöin $p = (a + bi)(c + di)$, missä $a + bi$ ja $c + di$ eivät ole yksikköjä. Määritelmän 5.0.28 perusteella $N(p) = p^2$ ja

$$p^2 = N(a + bi)N(c + di).$$

Koska $a + bi$ ja $c + di$ eivät ole yksikköjä ja p on alkuluku, niin on oltava $N(a + bi) = N(c + di) = p$. Täten $p = N(a + bi) = a^2 + b^2$. □

Lause 5.0.44. *Olkoot α ja β Gaussin lukuja niin, että $\beta \neq 0$. Tällöin ovat olemassa sellaiset Gaussin luvut ϑ ja η siten, että*

$$\alpha = \beta \cdot \vartheta + \eta \tag{5.3}$$

ja $N(\eta) < N(\beta)$.

Todistus. Olkoot $\alpha = a + bi$, $\beta = c + di$ ja $z = \alpha/\beta$. Tällöin

$$\begin{aligned} z = \frac{a + bi}{c + di} &= \frac{(a + bi)(c - di)}{(c + di)(c - di)} = \frac{ac - adi + cbi + bd}{c^2 + d^2} \\ &= \frac{ac + bd}{c^2 + b^2} + \frac{bc - ad}{c^2 + d^2} \cdot i. \end{aligned}$$

Olkoot $x = \frac{ac+bd}{c^2+b^2}$ ja $y = \frac{bc-ad}{c^2+d^2}$, jolloin $z = x + yi$. Olkoot m ja n rationaalilukuja, joille pätee $\mid x - m \mid \leq 1/2$ ja $\mid y - n \mid \leq 1/2$. Asetetaan $\vartheta = m + ni$ ja $\eta = \alpha - \beta\vartheta$. Koska

$$\begin{aligned} N(z - \vartheta) &= N(x + yi - m - ni) = N((x - m) + (y - n)i) \\ &= (x - m)^2 + (y - n)^2 \leq 1/4 + 1/4 = 1/2 < 1, \end{aligned}$$

niin

$$\begin{aligned} N(\eta) &= N(\alpha - \beta\vartheta) = N(\beta(\alpha/\beta - \vartheta)) = N(\beta(z - \vartheta)) \\ &= N(\beta)N(z - \vartheta) < N(\beta) \cdot 1 = N(\beta). \end{aligned}$$

□

Esimerkki 5.0.45. *Suoritetaan jakoalgoritmi luvuille* $\alpha = 12 + 8i$ *ja* $\beta = 4 - i$. *Lasketaan ensin jakolasku* α/β. *Laventamalla saadaan*

$$\frac{12+8i}{4-i} = \frac{(12+8i)(4+i)}{(4-i)(4+i)} = \frac{48+12i+32i-8}{16+4i-4i+1} = \frac{40+44i}{17} = \frac{40}{17} + \frac{44}{17}i.$$

Valitaan luvut m *ja* n *siten, että* $\mid 40/17 - m \mid \leq 1/2$ *ja* $\mid 44/17 - n \mid \leq 1/2$, *jolloin* $m = 2$ *ja* $n = 3$. *Tällöin luku* $\vartheta = m + ni = 2 + 3i$ *ja*

$$\eta = \alpha - \beta\vartheta = 12 + 8i - (4-i)(2+3i) = 12 + 8i - 8 - 12i + 2i - 3 = 1 - 2i.$$

Tarkistetaan vielä onko $N(\eta) < N(\beta)$. *Nyt* $N(\eta) = 1^2 + (-2)^2 = 5$ *ja* $N(\beta) = 4^2 + (-1)^2 = 17$, *joten* $N(\eta) < N(\beta)$. *Siis*

$$12 + 8i = (4-i)(2+3i) + 1 - 2i$$

Määritelmä 5.0.46. Olkoot annettuna sellaiset Gaussin luvut α ja β siten, että ainakin toinen on nollasta eroava. Tällöin Gaussin luku $\gamma = a + bi$ on lukujen α ja β suurin yhteinen tekijä ja merkitään $\gamma = syt(\alpha, \beta)$, mikäli:

1. $a > 0$ ja $b \geq 0$, sekä
2. $\gamma \mid \alpha$ ja $\gamma \mid \beta$.
3. Jos $\delta \mid \alpha$ ja $\delta \mid \beta$, niin on oltava, että $N(\gamma) > N(\delta)$.

Esimerkki 5.0.47. *1. Määritelmän 5.0.46 ehdosta 2. seuraa lauseen 5.0.33 perusteella, että jos* $\gamma = syt(\alpha, \beta)$, *niin* $N(\gamma) \mid N(\alpha)$ *ja* $N(\gamma) \mid N(\beta)$.

2. Olkoon annettuna Gaussin luvut $\alpha = 3 + 5i$, $\beta = 1 + 3i$ *ja* $\gamma = 1 + i$. *Huomataan, että* $\gamma \mid \alpha$ *ja* $\gamma \mid \beta$, *sillä*

$$\alpha/\gamma = \frac{3+5i}{1+i} = \frac{(3+5i)(1-i)}{(1+i)(1-i)} = \frac{8+2i}{2} = 4 + i$$

ja

$$\beta/\gamma = \frac{1+3i}{1+i} = \frac{(1+3i)(1-i)}{(1+i)(1-i)} = \frac{4+2i}{2} = 2 + i$$

Nyt $N(3+5i) = 3^2 + 5^2 = 34$ *ja* $N(1+3i) = 1^2 + 3^2 = 10$. *Kohdan 1. perusteella*

$$N(syt(\alpha, \beta)) \mid N(\alpha)$$

ja

$$N(syt(\alpha, \beta)) \mid N(\beta),$$

eli $N(syt(\alpha, \beta)) \mid 34$ *ja* $N(syt(\alpha, \beta)) \mid 10$. *Koska* $34 = 2 \cdot 17$ *ja* $10 = 2 \cdot 5$, *niin* $syt(34, 10) = 2$. *Siis* $N(syt(\alpha, \beta)) = 2$. *Koska*

$$N(\gamma) = N(1+i) = 1^2 + 1^2 = 2$$

ja $\gamma \mid \alpha$ *sekä* $\gamma \mid \beta$, *niin määritelmän 5.0.46 nojalla* $syt(\alpha, \beta) = \gamma$.

Lause 5.0.48. *Olkoot annettuina Gaussin luvut* α *ja* β *niin, että ainakin toinen on nollasta eroava. Tällöin on olemassa Gaussin luvut* γ_n *ja* χ_n *siten, että*

$$\gamma_n \alpha + \chi_n \beta = syt(\alpha, \beta). \tag{5.4}$$

Todistus. Jos $\alpha > \beta = 0$, niin $syt(\alpha, \beta) = \alpha = 1 \cdot \alpha + 0 \cdot \beta$. Olkoot siis $\alpha \geq \beta \neq 0$ ja merkitään $\alpha = \omega_0$ ja $\beta = \omega_1$. Lauseen 5.0.44 perusteella on olemassa Gaussin luvut ϑ_1 ja ω_2 siten, että $N(\omega_2) < N(\omega_1)$ ja

$$\omega_0 = \omega_1 \cdot \vartheta_1 + r_2.$$

Jakoalgoritmia voidaan jatkaa, jolloin saadaan

$$\begin{aligned}
\omega_1 &= \vartheta_2 \omega_2 + \omega_3 \\
\omega_2 &= \vartheta_3 \omega_3 + \omega_4 \\
&\vdots \\
\omega_k &= \vartheta_{k+1} \omega_{k+1} + \omega_{k+2} \\
&\vdots \\
\omega_{n-2} &= \vartheta_{n-1} \omega_{n-1} + \omega_n \\
\omega_{n-1} &= \vartheta_n \omega_n
\end{aligned}$$

siihen asti kunnes saadaan $\omega_{n+1} = 0$, kun $\omega_n \neq 0$. Näin saatu luku ω_n on lukujen α ja β suurin yhteinen tekijä,

$$\omega_n = syt(\alpha, \beta). \tag{5.5}$$

Asetetaan $\Omega_k = \begin{pmatrix} \omega_k \\ \omega_{k+1} \end{pmatrix}$ ja $\Pi_k = \begin{pmatrix} \vartheta_k & 1 \\ 1 & 0 \end{pmatrix}$. Tällöin $\Pi_k^{-1} = \begin{pmatrix} 0 & 1 \\ 1 & -\vartheta_k \end{pmatrix}$ ja

$$\begin{aligned} \Pi_{k+1} \cdot \Omega_{k+1} &= \begin{pmatrix} \vartheta_{k+1} & 1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} \omega_{k+1} \\ \omega_{k+2} \end{pmatrix} \\ &= \begin{pmatrix} \vartheta_{k+1}\omega_{k+1} + \omega_{k+2} \\ \omega_{k+1} \end{pmatrix} \\ &= \begin{pmatrix} \omega_k \\ \omega_{k+1} \end{pmatrix} \\ &= \Omega_k. \end{aligned}$$

Eukleideen algoritmin nojalla $\Omega_k = \Pi_{k+1}\Omega_{k+1}$ kaikilla $k = 0, 1, \ldots, n-1$. Tällöin pätee

$$\Omega_0 = \Pi_1\Omega_1 = \Pi_1\Pi_2\Omega_2 = \ldots = \Pi_1 \cdots \Pi_k\Omega_k$$

Merkitään seuraavaksi

$$\Gamma_0 = \begin{pmatrix} \gamma_0 & \chi_0 \\ \gamma_1 & \chi_1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix} = I,$$

missä $\gamma_0, \gamma_1, \chi_0$ ja χ_1 ovat Gaussin lukuja. Lisäksi merkitään

$$\Gamma_k = \begin{pmatrix} \gamma_k & \chi_k \\ \gamma_{k+1} & \chi_{k+1} \end{pmatrix} = \Pi_k^{-1}\Pi_{k-1}^{-1} \cdots \Pi_2^{-1}\Pi_1^{-1},$$

missä γ_i ja χ_i ovat Gaussin lukuja kaikilla $i \in \mathbb{Z}$. Tällöin

$$\Gamma_k\Omega_0 = \Pi_k^{-1}\Pi_{k-1}^{-1} \cdots \Pi_2^{-1}\Pi_1^{-1}\Pi_1\Pi_2 \cdots \Pi_{k-1}\Pi_k\Omega_k = I\Omega_k = \Omega_k.$$

Siis

$$\begin{aligned}\Omega_k &= \Gamma_k \Omega_0 \\ &= \begin{pmatrix} \gamma_k & \chi_k \\ \gamma_{k+1} & \chi_{k+1} \end{pmatrix} \begin{pmatrix} \omega_0 \\ \omega_1 \end{pmatrix} \\ &= \begin{pmatrix} \gamma_k\omega_0 + \chi_k\omega_1 \\ \gamma_{k+1}\omega_0 + \chi_{k+1}\omega_1 \end{pmatrix}.\end{aligned}$$

Ja koska $\Omega_k = \begin{pmatrix} \omega_k \\ \omega_{k+1} \end{pmatrix}$, saadaan yhtälöpari

$$\begin{cases} \omega_k = \gamma_k\omega_0 + \chi_k\omega_1 \\ \omega_{k+1} = \gamma_{k+1}\omega_0 + \chi_{k+1}\omega_1 \end{cases}.$$

Selvästi siis $\omega_n = \gamma_n\omega_0 + \chi_n\omega_1$. Alussa asetettiin $\omega_0 = \alpha$ ja $\omega_1 = \beta$, joten $\omega_n = \gamma_n\alpha + \chi_n\beta$. Kohdassa (5.5) saatiin $\omega_n = syt(\alpha, \beta)$ ja luvut γ_n ja χ_n määriteltiin aiemmin Gaussin luvuiksi, niin $syt(\alpha, \beta) = \gamma_n\alpha + \chi_n\beta$ lauseen ehtojen mukaisesti. □

Lause 5.0.49. *Olkoot π Gaussin alkuluku. Jos on voimassa, että $\pi \mid \alpha\beta$, niin silloin joko $\pi \mid \alpha$ tai $\pi \mid \beta$.*

Todistus. Oletetaan, että $\pi \mid \alpha\beta$, mutta $\pi \not| \alpha$. On siis osoitettava, että $\pi \mid \beta$. Koska π on Gaussin alkuluku, niin $syt(\alpha, \pi) = 1$. Lauseen 5.0.48 nojalla on olemassa Gaussin luvut γ ja χ siten, että

$$\gamma\alpha + \chi\pi = 1. \tag{5.6}$$

Kertomalla näin saatu yhtälö (5.6) puolittain luvulla β saadaan

$$\gamma\alpha\beta + \chi\beta\pi = \beta. \tag{5.7}$$

Lauseen oletuksen mukaan $\pi \mid \alpha\beta$, jolloin π jakaa yhtälön (5.7) vasemman puolen $\gamma\alpha\beta + \chi\beta\pi$. Koska $\gamma\alpha\beta + \chi\beta\pi = \beta$ on oltava $\pi \mid \beta$. □

Lemma 5.0.50. *Olkoot p alkuluku. Kongruenssilla*

$$x^2 \equiv -1 \pmod{p} \tag{5.8}$$

on ratkaisuja, jos ja vain jos $p = 2$ tai $p \equiv 1 \pmod 4$.

Todistus. Olkoot $p = 2$. Tällöin $-1 \equiv 1 \pmod 2$ ja $1^2 = 1$, joten ratkaisu on olemassa.

Oletetaan, että $p \equiv 1 \pmod 4$, jolloin $p = 1 + 4k$, missä $k \in \mathbb{Z}$. Lauseen 2.0.6 perusteella kongruenssilla (5.8) on olemassa ratkaisu $x^2 = (p-1)!$, joka Lauseen 2.0.6 lisätarkastelujen perusteella voidaan kirjoittaa muodossa $x = 1 \cdot 2 \cdots 2k$.

Oletetaan, että kongruenssilla (5.8) on ratkaisu $p \equiv 3 \pmod 4$, jolloin $p = 4m + 3$, missä $m \in \mathbb{Z}$. Oletetaan lisäksi, että on olemassa kokonaisluku x, jolle $x^2 \equiv -1 \pmod p$. Tällöin

$$x^{p-1} = (x^2)^{(2m+1)} \equiv (-1)^{(2m+1)} \equiv -1 \pmod{p}.$$

Koska $p \not| x$ ja Fermat'n suuri lause sanoo, että $x^{p-1} \equiv 1 \pmod p$, syntyy ristiriita sen kanssa, että $p \equiv 3 \pmod 4$. On siis oltava $p \equiv 1 \pmod 4$. □

Lause 5.0.51. *Olkoon p alkuluku. Jos $p \equiv 1 \pmod 4$, niin p ei ole Gaussin alkuluku.*

Todistus. Koska $p \equiv 1 \pmod 4$, niin lemman 5.0.50 nojalla on olemassa kokonaisluku x, jolle

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

Näin ollen $p \mid (x^2 + 1)$. Jos p on myös Gaussin alkuluku, niin lauseen 5.0.49 nojalla $p \mid (x + i)$ tai $p \mid (x - i)$. Koska kaikilla $a, b \in \mathbb{Z}$ pätee $p(a + bi) = pa + pbi \neq x \pm i$, sillä $pb \neq \pm 1$. Täten p ei ole Gaussin alkuluku. □

Lemma 5.0.52. *Jos $n \equiv 3 \pmod 4$, niin n ei ole kahden neliön summa.*

Todistus. Olkoot x mielivaltainen kokonaisluku. Luku $x \equiv 0, 1, 2$ tai $3 \pmod 4$, jolloin $x^2 \equiv 0$ tai $1 \pmod 4$. Vastaavasti mielivaltaiselle kokonaisluvulle y pätee $y^2 \equiv 0$ tai $1 \pmod 4$. Näin ollen $x^2 + y^2 \equiv 0, 1$ tai $2 \pmod 4$. Siis kahden neliön summa ei saa arvoa 3 mod 4 millään kokonaisluvuilla. □

Lause 5.0.53. *Olkoot π Gaussin luku. Luku π on Gaussin alkuluku jos ja vain jos π on liitännäinen alkuluvun p kanssa, jolle pätee $p \equiv 3 \pmod 4$ tai $N(\pi) = h$, missä h on alkuluku.*

Todistus. Oletetaan, että $N(\pi) = h$, missä h on alkuluku. Tällöin lauseen 5.0.41 nojalla π on Gaussin alkuluku. Lemman 5.0.52 mukaan, jos $p \equiv 3 \pmod 4$, niin p ei ole kahden neliön summa ja lauseen 5.0.43 perusteella alkuluku on Gaussin yhdistetty luku, jos ja vain jos se on kahden neliön summa. Täten p on Gaussin alkuluku. Määritelmän 5.0.39 nojalla Gaussin alkulukujen liitännäiset ovat myös Gaussin alkulukuja, joten luku π on Gaussin alkuluku.

Oletetaan seuraavaksi, että π on Gaussin alkuluku. Koska $\pi\overline{\pi} = N(\pi) \in \mathbb{Z}$, voidaan jokainen luonnollinen luku esittää Gaussin luvun normin avulla. Lauseen 5.0.41 nojalla löydetään jokaiselle alkuluvulle k Gaussin alkuluku ϑ siten, että $\vartheta\overline{\vartheta} = k$. Täten $\pi \mid p$, missä p on alkuluku. Lauseen 5.0.33 perusteella $N(\pi) \mid N(p)$. Koska $N(p) = p^2$, niin $N(\pi) = p$ tai p^2. Tapauksessa $N(\pi) = p$ saatiin lause todistettua.

Olkoon $N(\pi) = p^2$, jolloin $\pi\overline{\pi} = p^2$. Koska $\pi \mid p$, voidaan kirjoittaa $\pi\beta = p$, jollain Gaussin luvulla β. Ottamalla tästä yhtälöstä normit puolittain saadaan $N(\pi)N(\beta) = N(p)$, josta saadaan $p^2 \cdot N(\beta) = p^2$. Tämä on mahdollista vain jos $N(\beta) = 1$, eli β on yksikkö. Koska β on yksikkö, niin π on luvun p liitännäinen. □

Luku 6

Neliöiden summista

Lause 6.0.54. *Jos m ja n ovat molemmat kahden neliön summia, niin myös tulo mn on kahden neliön summa.*

Todistus. Olkoot luvuilla luvut m ja n kahden neliön summia seuraavasti: $m = a^2 + b^2$ ja $n = c^2 + d^2$. Tällöin lukujen m ja n tulo voidaan esittää seuraavasti

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

□

Lemma 6.0.55. *Kongruenssilla*

$$ax \equiv b \pmod{n}, \tag{6.1}$$

missä $x, b \in \mathbb{Z}$, on ratkaisu ryhmässä $\mathbb{Z}_n$, jos ja vain jos $syt(a, n) \mid b$. Tällöin ratkaisujen lukumäärä ryhmässä $\mathbb{Z}_n$ on $syt(a, n)$.

Todistus. Kongruenssi (6.1) voidaan kirjoittaa muodossa $ax = b + pk$, missä $k \in \mathbb{Z}$. Vähentämällä tästä puolittain luku pk saadaan lineaarinen Diofantoksen yhtälö

$$ax + (-p)k = b. \tag{6.2}$$

Lauseen 3.0.14 mukaan yhtälöllä (6.2) on ratkaisu, jos $syt(a, p) \mid b$. Olkoon $g = syt(a, b)$ ja oletetaan, että (x_0, k_0) on ratkaisu yhtälöön (6.2). Lauseen 3.0.16 mukaan yhtälön (6.2) kaikki ratkaisut x ovat muotoa $x = x_0 + mn/g$, jossa $m \in \mathbb{Z}$. Luvut x_0, n ja g ovat jo kiinnitettyjä ja m on mielivaltainen kokonaisluku, joten kongruenssin (6.1) jokainen ratkaisu on muotoa

$$x_0 + m(n/g).$$

Vielä on löydettävä erillisiin konjugointiluokkiin kuuluvat ratkaisut. Osoitetaan, että jäännösluokkien joukolla

$$\{x_0 + r(n/g) : 0 \leq r < g\} \tag{6.3}$$

on täsmälleen g erillistä alkiota ja se sisältää kaikki ratkaisut ryhmässä $\mathbb{Z}_n$. Jokainen kongruenssin (6.1) ratkaisun $x_0 + m(n/g)$ kokonaisluku m voidaan kirjoittaa muodossa

$$m = gq + r,$$

missä $q, r \in \mathbb{Z}$ ja $0 \leq r < g$. Tällöin

$$\begin{aligned} x_0 + m(n/g) &= x_0 + qn + r(n/g) \\ &\equiv x_0 + r(n/g) \pmod{n}. \end{aligned}$$

Näin ollen jokainen kongruenssin (6.1) ratkaisu kuuluu esitettyyn jäännösluokkaan (6.3).

Oletetaan seuraavaksi, että r_1 ja r_2 ovat kongruenssin (6.1) ratkaisuja ja $0 \leq r_1 < r_2 < g$. Näin ollen $0 < r_2 - r_1 < g$ ja

$$0 < r_2(n/g) - r_1(n/g) < n.$$

Tällöin on voimassa

$$n \not| \big(r_2(n/g) - r_1(n/g)\big)$$

ja sen seurauksena kongruenssiluokat $x_0 + r_1(n/g)$ ja $x_0 + r_2(n/g)$ eivät ole samoja. Koska kaikki erilliset ratkaisut r_i ovat kokonaislukuja ja $0 \leq r_i < g$, missä $i \in \mathbb{Z}$, niin on ratkaisuja r_i oltava yhteensä g kappaletta ryhmässä $\mathbb{Z}_n$. □

Lause 6.0.56. *Olkoon n positiivinen kokonaisluku, jolla on kanoninen alkutekijähajotelma*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \tag{6.4}$$

missä p_i on alkuluku ja $\alpha_i \in \mathbb{Z}^+$ kaikilla $i \in \{1, 2, \ldots, k\}$. Tällöin n on kahden neliön summa, jos ja vain jos α_i on parillinen, kun $p_i \equiv 3 \pmod 4$.

Todistus. Jos α_i on parillinen kaikilla $i \in \{1, 2, \ldots, k\}$, niin $\alpha_i = 2\gamma_i$ ja $p_i^{\alpha_i} = p_i^{2\gamma_i} = (p_i^2)^{\gamma_i}$. Koska $p_i \equiv 3 \pmod 4$, niin $p_i^2 \equiv 1 \pmod 4$ ja $1^{\gamma_i} \equiv 1 \pmod 4$. Siis $p_i^{\alpha_i} \equiv 1 \pmod 4$. Tällöin $n \equiv 1 \pmod 4$ ja lauseen 5.0.52 todistuksen mukaan luku n on kahden neliön summa.

Oletetaan, että α_i on pariton jollekin $p_i \equiv 3 \pmod 4$ ja $n = a^2 + b^2$, missä $a, b \in \mathbb{Z}$. Olkoon $g = syt(a, b)$ ja asetetaan $c = a/g$, $d = b/g$ ja $m = n/g^2$. Näin määritetyt luvut c ja d ovat keskenään jaottomia ja

$$c^2 + d^2 = \frac{a^2 + b^2}{g^2} = n/g^2 = m. \tag{6.5}$$

Koska asetettiin $m = n/g^2$ ja $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, niin $m = \frac{\prod_{i=1}^{k} p_i^{\alpha_i}}{g^2}$. Tällöin sen luvun p_i, joka jakaa luvun m, potenssi α_i on pariton luku ja vähintään 1. Oletetaan, että $p_i \mid c$, jolloin $p_i \mid (m - c^2)$. Koska $m - c^2 = d^2$, jakaa luku p_i luvun d^2. Koska p_i on alkuluku, jakaa p_i luvun d. Syntyy ristiriita, sillä luvut c ja d ovat keskenään jaottomia. Täten $p_i \not| c$. Lemman 6.0.55 mukaan

on olemassa luku x siten, että

$$cx \equiv d \pmod{p_i}.$$

Tarkastelemalla yhtälöä (6.5) *modulo* p_i saadaan

$$0 \equiv c^2 + d^2 \equiv c^2 + (cx)^2 \pmod{p_i}.$$

Edelleen $c^2 + (cx)^2 = c^2(1 + x^2)$, joten $p_i \mid c^2(1 + x^2)$. Edellä saatiin, että $p_i \not| c$, joten on oltava $p_i \mid (1 + x^2)$. Lauseen 2.0.6 mukaan kongruenssilla $x^2 \equiv -1 \pmod{p_i}$ ei ole ratkaisua, joten syntyy ristiriita sen kanssa, että α_i on pariton. □

Lemma 6.0.57. *Olkoon luku p pariton alkuluku. Tällöin on olemassa sellaiset luvut $x, y, k \in \mathbb{Z}$, että*

$$x^2 + y^2 + 1 = kp, \tag{6.6}$$

missä $0 < k < p$.

Todistus. Yhtälö (6.6) voidaan kirjoittaa muodossa

$$x^2 + y^2 + 1 \equiv 0 \pmod{p}. \tag{6.7}$$

Toisaalta $x^2 + y^2 + 1 < p^2$. Pilkotaan todistus kahteen osaan sen mukaan, mihin kongruenssiluokkaan *modulo* 4 alkuluku p kuuluu. Parittomille alkuluvuille on joko $p \equiv 1 \pmod 4$ tai $p \equiv 3 \pmod 4$ voimassa. Käsitellään ensin tapaus $p \equiv 1 \pmod 4$. Tällöin $\left(\frac{-1}{p}\right) = 1$ ja kongruenssilla

$$x^2 \equiv -1 \pmod{p} \tag{6.8}$$

on ratkaisu. Jos ratkaisu x on välillä $]p/2, p[$, on myös olemassa ratkaisu väliltä $]-p, -p/2[$. Tämän välin alkiot löytyvät myös väliltä $]0, p/2[$ kun

tarkastellaan *modulo* p , eli yhtälölle (6.8) on olemassa ratkaisu x, jolle pätee $0 < x < p/2$. Näin valitulle luvulle x on voimassa

$$x^2 + 1 < p^2/4 + 1 < p^2.$$

Koska $p \mid (x^2 + 1)$, niin valitsemalla $y = 0$ saadaan yhtälölle (6.6) ratkaisu.

Oletetaan seuraavaksi, että $p \equiv 3 \pmod 4$. Olkoon a pienin positiivinen luku, joka ei ole neliönjäännös *modulo* p. Koska nyt $\left(\frac{-1}{p}\right) = -1$ ja $\left(\frac{a}{p}\right) = -1$, niin tällöin

$$\left(\frac{-a}{p}\right) = \left(\frac{-1}{p}\right)\left(\frac{a}{p}\right) = (-1)(-1) = 1,$$

eli $\left(\frac{-a}{p}\right) = 1$. Näin ollen on olemassa luku x, joka toteuttaa yhtälön

$$x^2 \equiv -a \pmod p. \tag{6.9}$$

Kuten edellä, löytyy myös tässä tapauksessa yhtälön (6.9) toteuttava luku x väliltä $]0, p/2[$. Koska a oli pienin positiivinen luku, joka ei ole neliönjäännös, niin luku $a - 1$ on neliönjäännös. Tällöin on olemassa luku y, joka toteuttaa ehdon

$$y^2 \equiv a - 1 \pmod p.$$

Edellisten tarkastelujen mukaisesti on olemassa luku y välillä $]0, p/2[$. Nyt

$$x^2 + y^2 \equiv -a + a - 1 \equiv -1 \pmod p$$

ja lisäksi $x^2+y^2+1 < (p/2)^2+(p/2)^2+1 < p^2$, joten ratkaisu löytyy tässäkin tapauksessa. □

Lause 6.0.58. *Jokainen positiivinen kokonaisluku voidaan esittää neljän neliön summana.*

Todistus. Olkoon $m, n \in \mathbb{Z}$. Oletetaan, että luvut m ja n voidaan esittää neljän neliön summana seuraavasti $m = x^2+y^2+z^2+w^2$ ja $n = a^2+b^2+c^2+d^2$,

missä $x, y, z, w, a, b, c, d \in \mathbb{Z}$. Lukujen m ja n tulo voidaan myös esittää neljän neliön summana seuraavasti

$$\begin{aligned}
mn =&(x^2+y^2+z^2+w^2)(a^2+b^2+c^2+d^2)\\
=&x^2a^2+x^2b^2+x^2c^2+x^2d^2+y^2a^2+y^2b^2+y^2c^2+y^2d^2\\
&+z^2a^2+z^2b^2+z^2c^2+z^2d^2+w^2a^2+w^2b^2+w^2c^2+w^2d^2\\
=&x^2a^2+y^2b^2+z^2c^2+w^2d^2+2xyab+2xazc+2xawd+2ybzc\\
&+2ybwd+2wdzc+x^2b^2+y^2a^2+z^2d^2+w^2c^2-2xbya+2xbzc\\
&-2xbwc-2yazd+2yawc-2zdwc+x^2c^2+z^2a^2+w^2b^2+y^2d^2\\
&-2xcza+2xcwb-2xcyd-2zawb+2zayd-2wbyd+x^2d^2+w^2a^2\\
&+y^2c^2+z^2b^2-2xdwa+2xdyc-2xdzb-2wayc+2wazb-2yczb\\
=&(xa+yb+zc+wd)^2+(xb-ya+zd-wc)^2+(xc-za+wb-yd)^2\\
&+(xd-wa+yc-zb)^2.
\end{aligned}$$

On osoitettava, että jokainen alkuluku voidaan esittää neljän neliön summana. Tällöin jokainen yhdistetty luku voidaan esittää neljän neliön summana edellisen tarkastelun nojalla. Alkuluku 2 voidaan esittää neljän neliön summana seuraavasti $2 = 1^1+1^1+0^2+0^2$, joten tutkitaan parittomia alkulukuja. Lemman 6.8 nojalla yhtälöllä

$$x^2+y^2+z^2+w^2 = kp, \tag{6.10}$$

missä $k < p$, on ratkaisu $x, y, z, w \in \mathbb{Z}$. Valitsemalla $z = 1$ ja $w = 0$ saadaan yhtälö (6.6). Valitaan luvut x, y, z ja w niin, että luvun k arvo on pienin mahdollinen. Jos $k = 1$, niin saadaan alkuluvulle p haluttu esitys

$$p = x^2+y^2+z^2+w^2.$$

Tutkitaan jatkossa tapausta $k > 1$.

Olkoon k parillinen. Tällöin luvuille x, y, z ja w pätee, että joko kaikki ovat parittomia, niissä on 2 paritonta ja 2 parillista lukua, tai kaikki 4

lukua ovat parittomia, jotta niiden neliöiden summa olisi parillinen. Parittomia lukuja on joka tapauksessa parillinen määrä tai 0 kappaletta. Jos kaikki luvuista x, y, z ja w ovat parillisia, niin $x = 2h, y = 2j, z = 2k$ ja $w = 2l$, joillain $h, j, k, l \in \mathbb{Z}$ ja yhtälö (6.10) voidaan jakaa puolittain luvulla 2, jolloin saadaan

$$2h^2 + 2j^2 + 2k^2 + 2l^2 = (k/2)p.$$

Täten on löydetty lukua k pienempi luku, joka toteuttaa yhtälön (6.10). Tämä on ristiriidassa sen kanssa, että luku k on pienin mahdollinen yhtälön (6.10) toteuttava luku. Näin ollen kaikki luvuista x, y, z ja w ei voi olla parillisia.

Olkoot luvut x ja y parittomia, sekä w ja z parillisia. Tällöin $x + y$ ja $x - y$ ovat parillisia ja luvut $(x+y)/2, (x-y)/2, z/2, w/2$ toteuttavat yhtälön (6.10) seuraavasti

$$\begin{aligned}
&\left(\frac{x+y}{2}\right)^2 + \left(\frac{x-y}{2}\right)^2 + (z/2)^2 + (w/2)^2 \\
&= \frac{x^2 + 2xy + y^2}{4} + \frac{x^2 - 2xy + y^2}{4} + (z/2)^2 + (w/2)^2 \\
&= x^2/2 + y^2/2 + z^2/4 + x^2/4 \\
&= vp,
\end{aligned}$$

missä $v < k$. Syntyy ristiriita, sillä luku k asetettiin olemaan pienin yhtälön (6.10) toteuttava luku. Täten luvuissa x, y, z ja w ei voi olla kahta parillista ja kahta paritonta lukua.

Käsitellään vielä tapaus, missä kaikki luvuista x, y, z ja w ovat parittomia.

Tällöin luvut $x-y$, $x+y$, $z+w$ ja $z-w$ ovat parillisia ja

$$\begin{aligned}
&\left(\frac{x+y}{2}\right)^2+\left(\frac{x-y}{2}\right)^2+\left(\frac{z+w}{2}\right)^2+\left(\frac{z+w}{2}\right)^2\\
&=\frac{x^2+2xy+y^2}{4}+\frac{x^2-2xy+y^2}{4}+\frac{z^2+2zw+w^2}{4}+\frac{z^2-2zw+w^2}{4}\\
&=x^2/2+y^2/2+z^2/2+w^2/2\\
&=(k/2)p.
\end{aligned}$$

Löydettiin siis lukua k pienempi luku, joka toteuttaa yhtälön (6.10). Tämä on edelleen ristiriita, joten luvut x, y, z ja w eivät ole parittomia. Koska luvuille x, y, z ja w ei ole olemassa esitysmuotoa, on alkuperäinen oletus luvun k parillisuudesta, väärä. Luvun k on oltava pariton.

Olkoon $a, b, c, d \in \mathbb{Z}$ seuraavasti

$$\begin{aligned}
a &\equiv x \pmod{k}\\
b &\equiv y \pmod{k}\\
c &\equiv z \pmod{k}\\
d &\equiv w \pmod{k},
\end{aligned}$$

ja $0 \leq |a|, |b|, |c|, |d| < k/2$. Tällöin

$$a^2+b^2+c^2+d^2 \equiv x^2+y^2+z^2+w^2 \equiv 0 \pmod{k}$$

ja $a^2+b^2+c^2+d^2 = lk$, jollain $l \in \mathbb{Z}^+$. Myös

$$a^2+b^2+c^2+d^2 < (k/2)^2+(k/2)^2+(k/2)^2+(k/2)^2 = k^2,$$

joten $l < k$. Jos $l = 0$, niin

$$a = b = c = d = 0$$

ja

$$k^2 \mid (x^2+y^2+z^2+w^2),$$

koska $x, y, z, w \in \mathbb{Z} \cdot k$. Kuitenkin

$$x^2 + y^2 + z^2 + w^2 = kp,$$

missä $0 < k < p$, joten syntyy ristiriita sen kanssa, että $l = 0$. On siis oltava $l \neq 0$. Aiemmin osoitettiin, että lukujen $a^2 + b^2 + c^2 + d^2$ ja $x^2 + y^2 + z^2 + w^2$ tulo on myös neljän neliön summa. Jos valitaan

$$\begin{aligned} X =& xa + yb + zc + wd \\ Y =& xb - ya + zd - wc \\ Z =& xc - za + wb - yd \\ W =& xd - wa + yc - zb, \end{aligned}$$

niin saadaan

$$X^2 + Y^2 + Z^2 + W^2 = (lk)(kp).$$

Myös

$$\begin{aligned} X &\equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{k} \\ Y &\equiv xy - yx + zw - wz \equiv 0 \pmod{k} \\ Z &\equiv xz - zx + wy - yw \equiv 0 \pmod{k} \\ W &\equiv xw - wx + yz - zy \equiv 0 \pmod{k}, \end{aligned}$$

joten k jakaa kaikki luvuista X, Y, Z ja W. Tällöin

$$(X/k)^2 + (Y/k)^2 + (Z/k)^2 + (W/K)^2 = lp,$$

ja luku lp on neljän neliön summa. Koska $0 < l < k$, syntyy ristiriita sen kanssa, että k on pienin positiivinen ratkaisu yhtälöön (6.10). Täten jokainen alkuluku voidaan esittää neljän neliön summana. □

Kirjallisuutta

[1] Erickson, M. ja Vazzana, A.: Introduction to Number Theory (2008).

[2] Matala-aho, T.: Luentomateriaali: Lukuteorian perusteet (2014). http://cc.oulu.fi/ tma/LTI2014.pdf.

[3] Hugh, E.M.: A first course in number theory (1988).