TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Minna Nieminen

Positiivisen kokonaisluvun esittäminen neliöiden summana

Matematiikan ja tilastotieteen laitos
Matematiikka
Huhtikuu 2015

Tampereen yliopisto

Matematiikan ja tilastotieteen laitos

NIEMINEN, MINNA: Positiivisen kokonaisluvun esittäminen neliöiden summana

Pro gradu -tutkielma, 26 s.

Matematiikka

Huhtikuu 2015

Tiivistelmä

Tässä tutkielmassa tarkastellaan positiivisen kokonaisluvun esittämistä kokonaislukujen neliöiden summana.

Ensimmäisessä luvussa esitellään joitakin tutkielmassa tarvittavia määritelmiä.

Toisessa luvussa käsitellään positiivisen kokonaisluvun esittämistä neliöiden summana. Esitetään, mitkä positiiviset kokonaisluvut voidaan esittää kahden kokonaisluvun neliöiden summana, ja osoitetaan, että jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana.

Kolmannessa luvussa käsitellään positiivisen kokonaisluvun esittämistä kahden kokonaisluvun neliöiden summana Gaussin kokonaislukujen teorian avulla. Gaussin kokonaislukujen avulla saadaan selville, monellako eri tavalla positiivinen kokonaisluku voidaan esittää kahden kokonaisluvun neliöiden summana.

Neljännessä luvussa tarkastellaan asiaa geometriselta kannalta ja osoitetaan Minkowskin lauseen avulla, että jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana.

Tutkielmassa on käytetty päälähteenä Kenneth H. Rosenin kirjaa Elementary Number Theory and Its Applications. Toisena lähteenä on käytetty Gareth A. Jonesin ja J. Mary Jonesin kirjaa Elementary Number Therory.

Sisältö

1 Johdanto

Tämä tutkielma käsittelee positiivisen kokonaisluvun esittämistä kokonaislukujen neliöiden summana. Tietyt positiiviset kokonaisluvut voidaan esittää kahden kokonaisluvun neliöiden summana, esimerkiksi $8 = 2^2 + 2^2$.

Ensimmäisessä luvussa esitellään joitakin tutkielmassa tarvittavia käsitteitä. Esitellään kongruenssin ja neliönjäännöksen määritelmät.

Toisessa luvussa käsitellään positiivisen kokonaisluvun esittämistä kokonaislukujen neliöiden summana. Esitetään, minkä tyyppiset luvut voidaan esittää kahden kokonaisluvun neliöiden summana. Osoitetaan, että jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana.

Kolmas luku keskittyy Gaussin kokonaislukuihin. Gaussin kokonaislukujen teorian avulla saadaan selville, monellako eri tavalla positiivinen kokonaisluku voidaan esittää kahden kokonaisluvun neliöiden summana.

Neljännessä luvussa tarkastellaan neliöiden summia geometriselta näkökannalta ja todistetaan myös Minkowskin lauseen avulla tulos, jonka mukaan jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana. Matematiikassa on usein hyödyllistä todistaa sama tulos useammalla eri tavalla, koska se voi auttaa ymmärtämään tulosta paremmin.

Tutkielmassa on käytetty päälähteenä Kenneth H. Rosenin kirjaa Elementary Number Theory and Its Applications. Toisena lähteenä on käytetty Gareth A. Jonesin ja J. Mary Jonesin kirjaa Elementary Number Therory.

2 Valmistelevia tarkasteluja

Tässä luvussa esitellään joitakin tutkielmassa tarvittavia käsitteitä.

Määritelmä 2.1. Olkoon m positiivinen kokonaisluku. Jos a ja b ovat kokonaislukuja, niin sanotaan, että luku a on kongruentti luvun b kanssa modulo m, jos $m \mid (a-b)$. Jos a on kongruentti luvun b kanssa modulo m, niin merkitään $a \equiv b \pmod{m}$.

Määritelmä 2.2. Olkoon m positiivinen kokonaisluku. Sanotaan, että kokonaisluku a on luvun m neliönjäännös, jos $(a,m)=1$ ja kongruenssilla $x^2 \equiv a \pmod{m}$ on ratkaisu. Jos kongruenssilla $x^2 \equiv a \pmod{m}$ ei ole ratkaisua, niin sanotaan, että luku a on luvun m neliönepäjäännös.

Esimerkki 2.1. Mitkä ovat luvun 5 neliönjäännökset? Tätä varten tarvitsee laskea lukujen 1, 2, 3 ja 4 neliöt. Saadaan

$$\begin{aligned} 1^2 \equiv 4^2 \equiv 1 \pmod{5} \\ 2^2 \equiv 3^2 \equiv 4 \pmod{5}. \end{aligned}$$

Siis luvun 5 neliönjäännökset ovat 1 ja 4, ja neliönepäjäännökset ovat 2 ja 3.

Määritelmä 2.3. Olkoon p pariton alkuluku ja a kokonaisluku, joka ei ole jaollinen luvulla p. Legendren symboli $\left(\frac{a}{p}\right)$ määritellään seuraavasti

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

Lause 2.1. *Jos p on pariton alkuluku, niin*

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

Todistus. Ks. [2, s. 406]. □

3 Neliöiden summat

Matemaatikkoja on läpi historian kiinnostanut kokonaislukujen esittäminen neliöiden summana. Kaikkia kokonaislukuja ei kuitenkaan voida esittää kahden kokonaisluvun neliöiden summana. Pykälässä 3.1 esitetään, mitkä positiiviset kokonaisluvut voidaan esittää kahden kokonaisluvun neliöiden summana. Kaikki positiiviset kokonaisluvut voidaan kuitenkin esittää neljän kokonaisluvun neliöiden summana ja se todistetaan pykälässä 3.2.

3.1 Kahden kokonaisluvun neliöiden summat

Kaikkia positiivisia kokonaislukuja ei voida esittää kahden kokonaisluvun neliöiden summana. Tarkastellaan aluksi, mitkä positiiviset kokonaisluvut voidaan esittää kahden kokonaisluvun neliöiden summana.

Esimerkki 3.1. Tarkastellaan aluksi, mitkä luvut yhdestä kymmeneen voidaan esittää kahden kokonaisluvun neliöiden summana. Nähdään, että

$$1 = 0^2 + 1^2$$

$$2 = 1^2 + 1^2$$

lukua 3 ei voida esittää kahden kokonaisluvun neliöiden summana

$$4 = 2^2 + 0^2$$

$$5 = 1^2 + 2^2$$

lukua 6 ei voida esittää kahden kokonaisluvun neliöiden summana

lukua 7 ei voida esittää kahden kokonaisluvun neliöiden summana

$$8 = 2^2 + 2^2$$

$$9 = 3^2 + 0^2$$

$$10 = 3^2 + 1^2.$$

Lause 3.1. *Jos m ja n voidaan esittää kahden kokonaisluvun neliöiden summana, niin myös tulo mn voidaan esittää kahden kokonaisluvun neliöiden summana.*

Todistus (vrt. [2, s. 529]). Olkoon $m = a^2 + b^2$ ja $n = c^2 + d^2$. Nyt

$$mn = (a^2 + b^2)(c^2 + d^2) = a^2c^2 + a^2d^2 + b^2c^2 + b^2d^2 \tag{3.1}$$

$$\begin{aligned} &= (ac)^2 + (bd)^2 + (ad)^2 + (bc)^2 \\ &= (ac)^2 + 2acbd + (bd)^2 + (ad)^2 - 2acbd + (bc)^2 \\ &= (ac + bd)^2 + (ad - bc)^2. \end{aligned}$$

□

Esimerkki 3.2. Luvut 8 ja 17 voidaan esittää kahden kokonaisluvun neliöiden summana seuraavasti: $8 = 2^2 + 2^2$ ja $17 = 4^2 + 1^2$. Lauseen 3.1 perusteella tulo $8 \cdot 17$ voidaan esittää kahden kokonaisluvun neliöiden summana seuraavasti:

$$\begin{aligned} 136 = 8 \cdot 17 &= (2^2 + 2^2)(4^2 + 1^2) \\ &= (2 \cdot 4 + 2 \cdot 1)^2 + (2 \cdot 1 - 2 \cdot 4)^2 \\ &= (8 + 2)^2 + (2 - 8)^2 \\ &= 10^2 + 6^2. \end{aligned}$$

Lause 3.2. *Olkoon p alkuluku. Jos p on muotoa $4m + 1$, missä m on kokonaisluku, niin on olemassa kokonaisluvut x ja y siten, että $x^2 + y^2 = kp$ jollakin positiivisella kokonaisluvulla k, $k < p$.*

Todistus (vrt. [2, s. 530]). Tiedetään lauseen 2.1 perusteella, että -1 on alkuluvun p neliönjäännös. Näin ollen on olemassa kokonaisluku a, $a < p$, siten että $a^2 \equiv -1 \pmod{p}$. Tästä seuraa, että

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

jollakin positiivisella kokonaisluvulla k. Näin ollen

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

missä $x = a$ ja $y = 1$. Tulo kp voidaan siis esittää kahden kokonaisluvun neliöiden summana. Epäyhtälöstä

$$kp = x^2 + y^2 \leq (p-1)^2 + 1 = p^2 - 2p + 1 + 1 = p^2 - 2(p-1) < p^2$$

nähdään, että $k < p$. □

Todistetaan seuraavaksi, että kaikki alkuluvut, jotka eivät ole muotoa $4k + 3$ voidaan esittää kahden kokonaisluvun neliöiden summana.

Lause 3.3. *Jos p on alkuluku ja p ei ole muotoa $4k + 3$, niin on olemassa kokonaisluvut x ja y siten, että $x^2 + y^2 = p$.*

Todistus (vrt. [2, s. 530]). Tiedetään, että 2 on kahden kokonaisluvun neliöiden summa, sillä $2 = 1^2 + 1^2$. Oletetaan nyt, että alkuluku p on muotoa $4k+1$. Olkoon m pienin positiivinen kokonaisluku siten, että yhtälöllä $x^2 + y^2 = mp$ on ratkaisu kokonaisluvuilla x ja y. Lauseen 3.2 ja hyvinjärjestysperiaatteen nojalla tällainen kokonaisluku on olemassa. Osoitetaan, että $m = 1$.

Oletetaan, että $m > 1$. Olkoot a ja b määritelty seuraavasti

$$a \equiv x \pmod{m} \quad \text{ja} \quad b \equiv y \pmod{m},$$

missä

$$-m/2 < a \leq m/2 \quad \text{ja} \quad -m/2 < b \leq m/2. \tag{3.2}$$

Tästä seuraa, että

$$a^2 + b^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod{p}.$$

Täten on olemassa kokonaisluku k siten, että $a^2 + b^2 = km$. Näin saadaan

$$(a^2 + b^2)(x^2 + y^2) = (km)(mp) = km^2p.$$

Lauseen 3.1 perusteella saadaan

$$(a^2 + b^2)(x^2 + y^2) = (ax + by)^2 + (ay - bx)^2.$$

Lisäksi, koska $a \equiv x \pmod{m}$ ja $b \equiv y \pmod{m}$, saadaan

$$ax + by \equiv x^2 + y^2 \equiv 0 \pmod{m}$$

$$ay - bx \equiv xy - yx \equiv 0 \pmod{m}.$$

Täten $(ax + by)/m$ ja $(ay - bx)/m$ ovat kokonaislukuja, joten

$$\left(\frac{ax + by}{m}\right)^2 + \left(\frac{ax - bx}{m}\right)^2 = \frac{(ax + by)^2 + (ay - bx)^2}{m^2} = km^2p/m^2 = kp.$$

Tulo kp voidaan siis esittää kahden kokonaisluvun neliöiden summana. Epäyhtälöistä (3.2) saadaan

$$a^2 + b^2 \leq m^2/4 + m^2/4 = m^2/2,$$

joten $a^2+b^2 = km \leq m^2/2$. Näin ollen $k \leq m/2$, joten $k < m$. On siis oltava, että $k \neq 0$. Jos $k = 0$, niin $a^2+b^2 = 0$, mistä seuraisi, että $a = b = 0$. Tällöin $x \equiv y \equiv 0 \pmod{m}$, ja $m \mid x$ ja $m \mid y$. Näin ollen $m^2 \mid x^2 + y^2$ eli $m^2 \mid mp$, mistä seuraa, että $m \mid p$. Koska m on pienempi kuin p, niin tästä seuraa, että $m = 1$. Mutta sehän oli juuri se, mitä haluttiin osoittaa. □

Seuraavaksi voidaan esittää perustavaa laatua oleva tulos, joka luokittelee mitkä positiiviset kokonaisluvut voidaan esittää kahden kokonaisluvun neliöiden summana.

Lause 3.4. *Positiivinen kokonaisluku n voidaan esittää kahden kokonaisluvun neliöiden summana, jos ja vain jos jokainen kokonaisluvun n muotoa $4k + 3$ olevan alkutekijän eksponentti on parillinen, kun n hajotetaan alkutekijöihinsä.*

Todistus (vrt. [2, s. 531–532]). Oletetaan, että kun n hajotetaan alkutekijöihin kaikkien muotoa $4k+3$ olevien alkulukujen eksponentti on parillinen. Kirjoitetaan

$$n = t^2 u,$$

missä u on alkulukujen tulo. Tulossa u ei esiinny muotoa $4k+3$ olevia alkulukuja. Lauseen 3.3 mukaan jokainen tulossa u oleva alkuluku voidaan kirjoittaa kahden kokonaisluvun neliöiden summana. Lauseen 3.1 nojalla myös u voidaan esittää kahden kokonaisluvun neliöiden summana, joten

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

Tästä seuraa nyt, että n voidaan esittää kahden kokonaisluvun neliöiden summana, nimittäin

$$n = (tx)^2 + (ty)^2.$$

Oletetaan nyt, että on olemassa alkuluku p, $p \equiv 3 \pmod 4$, joka esiintyy luvun n alkutekijähajotelmassa parittomana potenssina, esimerkiksi potenssina $2j+1$. Lisäksi oletetaan, että n on kahden kokonaisluvun neliöiden summa, $n = x^2 + y^2$. Olkoon kokonaislukujen x ja y suurin yhteinen tekijä $(x, y) = d$, ja olkoot $a = \frac{x}{d}$, $b = \frac{y}{d}$ ja $m = \frac{n}{d^2}$. Lukujen a ja b suurin yhteinen tekijä $(a, b) = 1$ ja

$$a^2 + b^2 = m.$$

Oletetaan, että p^k on suurin alkuluvun p potenssi, joka jakaa luvun d. Nyt, koska

$$m = n/d^2 \quad \text{ja} \quad \frac{p^{2j+1}}{(p^k)^2} = p^{2j-2k+1} \mid m,$$

missä $2j - 2k + 1 \geq 1$. Täten $p \mid m$. Tiedetään, että p ei jaa lukua a, koska jos $p \mid a$, niin $p \mid b$, koska $b^2 = m - a^2$ ja $(a, b) = 1$. Täten on olemassa kokonaisluku z siten, että

$$az \equiv b \pmod p.$$

Tästä seuraa, että

$$a^2 + b^2 \equiv a^2 + (az)^2 = a^2(1 + z^2) \pmod p.$$

Koska $a^2 + b^2 = m$ ja $p \mid m$ nähdään, että

$$a^2(1 + z^2) \equiv 0 \pmod p.$$

Koska $(a, p) = 1$ niin seuraa, että $1+z^2 \equiv 0 \pmod p$, joten $z^2 \equiv -1 \pmod p$, mikä on mahdotonta, koska -1 ei ole luvun p neliönjäännös, sillä $p \equiv 3 \pmod 4$ (lause 2.1). Näin ollen lukua n ei voida esittää kahden kokonaisluvun neliöiden summana. Siis minkään muotoa $4k+3$ olevan alkuluvun määrä luvun n alkutekijöissä ei ole pariton. □

Esimerkki 3.3. Tarkastellaan lukua $200655 = 3^2 \cdot 5 \cdot 7^3 \cdot 13$. Huomataan, että $5 \equiv 1 \pmod 4$ ja $13 \equiv 1 \pmod 4$, mutta $3 \equiv 3 \pmod 4$ ja $7 \equiv 3 \pmod 4$. Luvun 3 eksponentti on parillinen, mutta luvun 7 eksponentti on pariton. Näin ollen lukua 200655 ei voida esittää kahden kokonaisluvun neliöiden summana.

Esimerkki 3.4. Tarkastellaan lukua $28665 = 3^2 \cdot 5 \cdot 7^2 \cdot 13$. Huomataan taas, että $5 \equiv 1 \pmod 4$, $13 \equiv 1 \pmod 4$, $3 \equiv 3 \pmod 4$ ja $7 \equiv 3 \pmod 4$. Nyt sekä luvun 7 että luvun 3 eksponentit ovat parilliset, joten luku 28665 voidaan esittää kahden kokonaisluvun neliöiden summana. Tiedetään, että $5 \cdot 13 = 65 = 1^2 + 8^2$, joten

$$\begin{aligned} 28665 &= 3^2 \cdot 5 \cdot 7^2 \cdot 13 \\ &= \left(1^2 + 8^2\right)(7 \cdot 3)^2 \\ &= (1 \cdot 7 \cdot 3)^2 + (8 \cdot 7 \cdot 3)^2 \\ &= 21^2 + 168^2. \end{aligned}$$

3.2 Neljän kokonaisluvun neliöiden summat

Koska kaikkia positiivisia kokonaislukuja ei voida esittää kahden kokonaisluvun neliöiden summana, herää kysymys, mikä on pienin neliöiden määrä millä voidaan esittää. Tarkastellaan ensin kolmen kokonaisluvun neliöiden summana esittämistä.

Esimerkki 3.5. Luku 6 voidaan esittää kolmen kokonaisluvun neliöiden summana. Nähdään, että

$$6 = 2^2 + 1^2 + 1^2.$$

Luku 6 voidaan siis esittää kolmen kokonaisluvun neliöiden summana, mutta seuraavassa esimerkissä huomataan, että lukua 7 ei voida.

Esimerkki 3.6. Lukua 7 ei voida esittää kolmen kokonaisluvun neliöiden summana. Nähdään, että

$$7 = 7 + 0 = 2^2 + 1^2 + 1^2 + 1^2$$

$$7 = 1 + 6 = 1^2 + 2^2 + 1^2 + 1^2$$

$$7 = 2 + 5 = 1^2 + 1^2 + 2^2 + 1^2$$

$$7 = 3 + 4 = 1^2 + 1^2 + 1^2 + 2^2.$$

Tästä huomataan, että vaikka lukua 7 ei voida esittää kolmen kokonaisluvun neliöiden summana, niin se voidaan esittää neljän kokonaisluvun neliöiden summana. Jokainen positiivinen kokonaisluku voidaankin esittää neljän kokonaisluvun neliöiden summana.

Lause 3.5. *Jos m ja n ovat positiivisia kokonaislukuja, jotka molemmat voidaan esittää neljän kokonaisluvun neliöiden summana, niin tulo mn voidaan myös esittää neljän kokonaisluvun neliöiden summana.*

Todistus (vrt. [2, s. 532]). Olkoot $m = a^2+b^2+c^2+d^2$ ja $n = e^2+f^2+g^2+h^2$. Nyt tulo

$$mn = (a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) \tag{3.3}$$

$$= (ae+bf+cg+dh)^2+(af-be+ch-dg)^2+(ag-bh-ce+df)^2+(ah+bg-cf-de)^2.$$

Osoitetaan yhtälö (3.3) oikeaksi kertomalla sulut auki yhtälön molemmilta puolilta. Aloitetaan yhtälön vasemmalta puolelta. Nähdään, että

$$\begin{aligned}(a^2 + b^2 + c^2 + d^2)(e^2 + f^2 + g^2 + h^2) = {} & a^2e^2 + a^2f^2 + a^2g^2 + a^2h^2 \\ & +b^2e^2 + b^2f^2 + b^2g^2 + b^2h^2 \\ & +c^2e^2 + c^2f^2 + c^2g^2 + c^2h^2 \\ & +d^2e^2 + d^2f^2 + d^2g^2 + d^2h^2.\end{aligned} \tag{3.4}$$

Tarkastellaan yhtälön oikeata puolta neljässä eri osassa. Saadaan, että

$$\begin{aligned}(ae + bf + cg + dh)^2 = {} & a^2e^2 + 2aebf + b^2f^2 + 2aecg + 2aedh \\ & + 2bfdh + 2bfcg + c^2g^2 + 2cgdh + d^2h^2\end{aligned} \tag{3.5}$$

$$\begin{aligned}(af - be + ch - dg)^2 = {} & a^2f^2 - 2aebf + b^2e^2 + 2afch - 2afdg \\ & - 2bech + 2bedg + c^2h^2 - 2cgdh + d^2g^2\end{aligned} \tag{3.6}$$

$$\begin{aligned}(ag - bh - ce + df)^2 = {} & a^2g^2 - 2agbh + b^2h^2 - 2agce + 2agdf \\ & + 2bhce - 2bhdf + c^2e^2 - 2cedf + d^2f^2\end{aligned} \tag{3.7}$$

$$\begin{aligned}(ah + bg - cf - de)^2 = {} & a^2h^2 + 2ahbg + b^2g^2 - 2ahcf - 2ahde \\ & - 2bgcf - 2bgde + c^2f^2 + 2cedf + d^2e^2.\end{aligned} \tag{3.8}$$

Laskemalla yhtälöiden (3.5)-(3.8) oikeat puolet yhteen, saadaan summaksi yhtälön (3.4) oikeapuoli. □

Esimerkki 3.7. Luvut 3 ja 7 voidaan esittää neljän kokonaisluvun summana seuraavasti: $3 = 1^2+1^2+1^2+0^2$ ja $7 = 2^2+1^2+1^2+1^2$. Lauseen 3.5 mukaan tulo $3\cdot7$ voidaan esittää neljän kokonaisluvun neliöiden summana seuraavasti:

$$\begin{aligned}21 = 3 \cdot 7 = {} & (1^2 + 1^2 + 1^2 + 0^2)(2^2 + 1^2 + 1^2 + 1^2) \\ = {} & (1 \cdot 2 + 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1)^2 + (1 \cdot 1 - 1 \cdot 2 + 1 \cdot 1 - 0 \cdot 1)^2 \\ & + (1 \cdot 1 - 1 \cdot 1 - 1 \cdot 2 + 0 \cdot 1)^2 + (1 \cdot 1 + 1 \cdot 1 - 1 \cdot 1 - 0 \cdot 2)^2 \\ = {} & 4^2 + 0^2 + 2^2 + 1^2.\end{aligned}$$

Lause 3.6. *Jos p on pariton alkuluku, niin on olemassa kokonaisluku k, $k < p$ siten, että yhtälöllä $kp = x^2 + y^2 + z^2 + w^2$ on ratkaisu kokonaisluvuilla x, y, z ja w.*

Todistus (vrt. [2, s. 532–533]). Osoitetaan aluksi, että on olemassa sellaiset kokonaisluvut x ja y, että

$$x^2 + y^2 + 1 \equiv 0 \pmod{p},$$

missä $0 \leq x < p/2$ ja $0 \leq y < p/2$. Olkoon

$$S = \left\{0^2, 1^2, \ldots, \left(\frac{p-1}{2}\right)^2\right\}$$

ja

$$T = \left\{-1 - 0^2, -1 - 1^2, \ldots, -1 - \left(\frac{p-1}{2}\right)^2\right\}.$$

Mitkään kaksi joukon S alkiota eivät ole keskenään kongruentteja modulo p. Samoin mitkään kaksi joukon T alkiota eivät ole keskenään kongruentteja modulo p. Joukkojen T ja S yhdiste $T \cup S$ sisältää $p+1$ erisuurta kokonaislukua. Laatikkoperiaatteen mukaan tässä yhdisteessä on kaksi kokonaislukua, jotka ovat kongruentteja modulo p. Tästä seuraa, että on olemassa kokonaisluvut x ja y siten, että

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

missä $0 \leq x < (p-1)/2$ ja $0 \leq y < (p-1)/2$. Saadaan, että

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

Tästä seuraa, että

$$x^2 + y^2 + 1^2 + 0^2 = kp,$$

jollakin kokonaisluvulla k. Koska $x^2 + y^2 + 1 < 2((p-1)/2)^2 + 1 < p^2$ seuraa, että $k < p$. □

Nyt voidaan todistaa, että jokainen alkuluku on neljän kokonaisluvun neliöiden summa.

Lause 3.7. *Olkoon p alkuluku. Tällöin yhtälöllä $x^2 + y^2 + z^2 + w^2 = p$ on ratkaisu, missä x, y, z ja w ovat kokonaislukuja.*

Todistus (vrt. [2, s. 533–534]). Tulos on tosi, kun $p = 2$, koska $2 = 1^2 + 1^2 + 0^2 + 0^2$.

Oletetaan sitten, että p on pariton alkuluku. Olkoon m pienin kokonaisluku siten, että yhtälöllä $x^2 + y^2 + z^2 + w^2 = mp$ on ratkaisu, missä x, y, z ja w ovat kokonaislukuja. (Lauseen 3.6 ja hyvinjärjestysperiaatteen perusteella

tällainen kokonaisluku m on olemassa.) Lause seuraa, jos voidaan osoittaa, että $m = 1$. Tämän vuoksi oletetaan, että $m > 1$, ja löydetään pienempi tällainen kokonaisluku.

Jos m on parillinen, niin joko x, y, z ja w ovat kaikki parittomia, parillisia tai kaksi on paritonta ja kaksi on parillista. Kaikissa näissä tapauksissa voimme tarvittaessa uudelleen järjestää nämä kokonaisluvut siten, että $x \equiv y \pmod 2$ ja $z \equiv w \pmod 2$. Tästä seuraa, että $(x-y)/2$, $(x+y)/2$, $(z-w)/2$ ja $(z+w)/2$ ovat kokonaislukuja ja

$$\left(\frac{x-y}{2}\right)^2 + \left(\frac{x+y}{2}\right)^2 + \left(\frac{z-w}{2}\right)^2 + \left(\frac{z+w}{2}\right)^2 = (m/2)\, p.$$

Siis $(m/2)p$ voidaan esittää neljän kokonaisluvun neliöiden summana, missä $m/2 < m$. Tämä on ristiriita, koska oletuksen mukaan m on pienin sellainen kokonaisluku, että $mp = x^2 + y^2 + z^2 + w^2$.

Oletetaan seuraavaksi, että m on pariton ja $m > 1$. Olkoot a, b, c ja d sellaiset kokonaisluvut, että

$$\begin{aligned} &a \equiv x \pmod m, \quad b \equiv y \pmod m, \\ &c \equiv z \pmod m \quad \text{ja} \quad d \equiv w \pmod m, \end{aligned}$$

missä

$$-m/2 < a, b, c, d < m/2.$$

Nyt saadaan, että

$$a^2 + b^2 + c^2 + d^2 \equiv x^2 + y^2 + z^2 + w^2 \pmod m.$$

Tämä voidaan kirjoittaa

$$a^2 + b^2 + c^2 + d^2 = km, \tag{3.9}$$

missä k on kokonaisluku ja

$$0 \le a^2 + b^2 + c^2 + d^2 < 4(m/2)^2 = m^2.$$

Siis $0 \le k < m$. Jos $k = 0$, niin $a = b = c = d = 0$, joten $x \equiv y \equiv z \equiv w \equiv 0 \pmod m$. Tästä seuraa, että $m^2 \mid mp$, mikä on mahdotonta, koska $1 < m < p$. Tästä seuraa, että $k > 0$.

Saadaan

$$(x^2 + y^2 + z^2 + w^2)(a^2 + b^2 + c^2 + d^2) = mp \cdot km = m^2 kp.$$

Yhtälö saadaan lauseen 3.5 todistuksesta muotoon

$$\begin{aligned} &(ax + by + cz + dw)^2 + (bx - ay + dz - cw)^2 + (cx - dy - az + bw)^2 \\ &+ (dx + cy - bz - aw)^2 = m^2 kp. \end{aligned}$$

Jokainen neliöön korotettu termi on jaollinen luvulla m, koska

$$\begin{aligned}
ax + by + cz + dw &\equiv x^2 + y^2 + z^2 + w^2 \equiv 0 \pmod{m} \\
bx - ay + dz - cw &\equiv yx - xy + wz - zw \equiv 0 \pmod{m} \\
cx - dy - az + bw &\equiv zx - wy - xz + yw \equiv 0 \pmod{m} \\
dx + cy - bz - aw &\equiv wx + zy - yz - xw \equiv 0 \pmod{m}.
\end{aligned}$$

Olkoot X, Y, Z ja Y kokonaisluvut, jotka on saatu jakamalla nämä luvulla m. Saadaan siis,

$$\begin{aligned}
X &= (ax + by + cz + dw)/m \\
Y &= (bx - ay + dz - cw)/m \\
Z &= (cx - dy - az + bw)/m \\
W &= (dx + cy - bz - aw)/m.
\end{aligned}$$

Tästä seuraa, että

$$X^2 + Y^2 + Z^2 + W^2 = m^2 kp/m^2 = kp.$$

Tämä on ristiriidassa luvun m valinnan suhteen, joten luvun m täytyy olla 1. □

Nyt voidaan todistaa, että jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana.

Lause 3.8. *Jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana.*

Todistus (vrt. [2, s. 535]). Oletetaan, että n on positiivinen kokonaisluku. Aritmetiikan peruslauseen mukaan n on alkulukujen tulo. Lauseen 3.7 mukaan jokainen näistä alkutekijöistä voidaa esittää neljän kokonaisluvun neliöiden summana. Soveltamalla lausetta 3.5 riittävän monta kertaa, voidaan myös n esittää neljän kokonaisluvun neliöiden summana. □

Esimerkki 3.8. Lukua $200655 = 3^2 \cdot 5 \cdot 7^3 \cdot 13$ ei voitu esittää kahden kokonaisluvun neliöiden summana, mutta se voidaan esittää neljän kokonaisluvun neliöiden summana. Tiedetään, että $3^2 = 9 = 3^2 + 0^2 + 0^2 + 0^2$, $5 = 1^2 + 2^2 + 0^2 + 0^2$, $7^3 = 7^2(2^2 + 1^2 + 1^2 + 1^2) = 14^2 + 7^2 + 7^2 + 7^2$ ja $13 = 2^2 + 3^2 + 0^2 + 0^2$. Nyt

$$\begin{aligned}
3^2 \cdot 5 &= \left(3^2 + 0^2 + 0^2 + 0^2\right)\left(1^2 + 2^2 + 0^2 + 0^2\right) \\
&= 3^2 + 6^2 + 0^2 + 0^2
\end{aligned}$$

ja

$$\begin{aligned}
7^3 \cdot 13 &= \left(14^2 + 7^2 + 7^2 + 7^2\right)\left(2^2 + 3^2 + 0^2 + 0^2\right) \\
&= (14 \cdot 2 + 7 \cdot 3)^2 + (14 \cdot 3 - 7 \cdot 2)^2 + \\
&(-7 \cdot 2 + 7 \cdot 3)^2 + (-7 \cdot 3 - 7 \cdot 2)^2 \\
&= 49^2 + 28^2 + 7^2 + (-35)^2 \\
&= 49^2 + 28^2 + 7^2 + 35^2.
\end{aligned}$$

Näin ollen luku 200655 voidaan kirjoittaa neljän kokonaisluvun neliöiden summana seuraavasti:

$$\begin{aligned}
200655 = 3^2 \cdot 5 \cdot 7^3 \cdot 13 &= \left(3^2 + 6^2 + 0^2 + 0^2\right)\left(49^2 + 28^2 + 7^2 + 35^2\right) \\
&= (3 \cdot 49 + 6 \cdot 28)^2 + (3 \cdot 28 - 6 \cdot 49)^2 + (3 \cdot 7 - 6 \cdot 35)^2 + (3 \cdot 35 + 6 \cdot 7)^2 \\
&= 315^2 + (-210)^2 + (-189)^2 + 147^2 \\
&= 315^2 + 210^2 + 189^2 + 147^2.
\end{aligned}$$

4 Gaussin kokonaisluvut ja neliöiden summat

Tässä luvussa tarkastellaan neliöiden summia Gaussin kokonaislukujen avulla. Pykälässä 4.1 esitellään Gaussin kokonaislukuja ja alkulukuja sen verran mikä on tarpeellista pykälän 4.2 kannalta. Kokonaisluvuista puhuttaessa tarkoitetaan kokonaislukuja perinteisessä mielessä, Gaussin kokonaisluvuista puhuttaessa käytetään aina koko nimitystä. Vastaavasti alkuluvuista puhuttaessa tarkoitetaan alkulukuja perinteisessä mielessä ja Gaussin alkuluvuista puhuttaessa käytetään koko nimitystä. Pykälässä 4.2 todistetaan, kuinka monella eri tavalla positiivinen kokonaisluku voidaan esittää kahden kokonaisluvun neliöiden summana.

4.1 Gaussin kokonaisluvuista ja alkuluvuista

Määritelmä 4.1. Kompleksilukua $\alpha = a + bi$, missä a ja b ovat kokonaislukuja, sanotaan Gaussin kokonaisluvuksi.

Esimerkki 4.1. Luvut $\alpha = 2 + i$ ja $\beta = 15 + 0 \cdot i = 15$ ovat Gaussin kokonaislukuja.

Kaikki kokonaisluvut ovat siis myös Gaussin kokonaislukuja, niissä imaginääriosa on nolla.

Lause 4.1. *Olkoot $\alpha = a + bi$ ja $\beta = c + di$ Gaussin kokonaislukuja. Tällöin myös summa $\alpha + \beta$, erotus $\alpha - \beta$ ja tulo $\alpha\beta$ ovat Gaussin kokonaislukuja.*

Todistus. Ks. [2, s. 549]. □

Määritelmä 4.2. Gaussin kokonaisluvun $\alpha = a + bi$ konjugaatti, merkitään $\overline{\alpha}$, on Gaussin kokonaisluku $\overline{\alpha} = a - bi$.

Määritelmä 4.3. Olkoon $\alpha = a + bi$ Gaussin kokonaisluku. Gaussin kokonaisluvun α itseisarvo on $|\alpha| = \sqrt{a^2 + b^2}$ ja normi $|\alpha|^2 = a^2 + b^2 = N(\alpha)$.

Lause 4.2. *Olkoot α ja β Gaussin kokonaislukuja. Tällöin normifunktiolla N on seuraavat ominaisuudet*

1. *$N(\alpha)$ on ei-negatiivinen kokonaisluku*
2. *$N(\alpha\beta) = N(\alpha)N(\beta)$*
3. *$N(\alpha) = 0$, jos ja vain jos $\alpha = 0$.*

Todistus. Ks. [2, s. 548]. □

Määritelmä 4.4. Olkoot α ja β Gaussin kokonaislukuja. Sanotaan, että α jakaa luvun β, jos on olemassa Gaussin kokonaisluku γ siten, että $\beta = \alpha\gamma$. Jos α jakaa luvun β, kirjoitetaan $\alpha \mid \beta$. Jos α ei jaa lukua β, kirjoitetaan $\alpha \nmid \beta$.

Esimerkki 4.2. Gaussin kokonaisluku $2+i$ jakaa Gaussin kokonaisluvun 15, sillä

$$(2+i)(6-3i) = 12-6i+6i-3i^2 = 12+3 = 15.$$

Määritelmä 4.5. Gaussin kokonaislukua ϵ sanotaan yksiköksi, jos ϵ jakaa luvun 1. Kun ϵ on yksikkö, $\epsilon\alpha$ on Gaussin kokonaisluvun α liitännäinen.

Lause 4.3. *Gaussin kokonaisluku ϵ on yksikkö, jos ja vain jos $N(\epsilon) = 1$.*

Todistus. Ks. [2, s. 551]. □

Lause 4.4. *Gaussin kokonaisluvut, jotka ovat yksikköjä, ovat 1, -1, i ja $-i$.*

Todistus. Ks. [2, s. 551]. □

Esimerkki 4.3. Gaussin kokonaisluvun $2+i$ liitännäiset ovat

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

Määritelmä 4.6. Nollasta eroava Gaussin kokonaisluku π on Gaussin alkuluku, jos se ei ole yksikkö ja se on jaollinen vain yksiköillä ja liitännäisillään.

Lause 4.5. *Jos π on Gaussin kokonaisluku ja $N(\pi) = p$, missä p on alkuluku, niin π ja $\overline{\pi}$ ovat Gaussin alkulukuja, mutta p ei ole Gaussin alkuluku.*

Todistus. Ks. [2, s. 552]. □

Esimerkki 4.4. Gaussin kokonaisluku $2+i$ on Gaussin alkuluku, koska

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

ja 5 on alkuluku. Alkuluku 5 ei ole Gaussin alkuluku, koska

$$(2+i)(2-i) = 4-2i+2i+1 = 5.$$

Lause 4.6. *Jos π on Gaussin alkuluku ja α ja β ovat Gaussin kokonaislukuja siten, että $\pi \mid \alpha\beta$, niin $\pi \mid \alpha$ tai $\pi \mid \beta$.*

Todistus. Ks. [2, s. 563]. □

Lause 4.7. *Jos π on Gaussin alkuluku ja $\alpha_1, \alpha_2, \ldots, \alpha_m$ ovat Gaussin kokonaislukuja siten, että $\pi \mid \alpha_1\alpha_2\cdots\alpha_m$, niin on olemassa kokonaisluku j siten, että $\pi \mid \alpha_j$, missä $1 \leq j \leq m$.*

Todistus. Ks. [2, s. 563]. □

Lause 4.8. *Oletetaan, että γ on nollasta eroava Gaussin kokonaisluku, joka ei ole yksikkö. Nyt*

1. *γ voidaan kirjoittaa Gaussin alkulukujen tulona ja*
2. *tämä tekijöihin jako on yksikäsitteinen siten, että 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 kaikki Gaussin kokonaislukuja, niin $s = t$ ja tarvittaessa uudelleen indeksoituina π_i ja ρ_i ovat toistensa liitännäisiä, kun $1 \leq i \leq s$.

Todistus. Ks. [2, s. 564–565]. □

4.2 Neliöiden summat Gaussin kokonaislukujen avulla

Pykälässä 3.1 todistettiin, että jokainen alkuluku, joka on muotoa $4k + 1$ voidaan esittää kahden kokonaisluvun neliöiden summana. Todistetaan tämä seuraavaksi käyttäen apuna Gaussin kokonaislukuja.

Lause 4.9. *Jos p on alkuluku muotoa $4k + 1$, missä k on positiivinen kokonaisluku, niin p on kahden kokonaisluvun neliöiden summa.*

Todistus (vrt. [2, s. 570–571]). Oletetaan, että p on muotoa $4k + 1$, missä k on positiivinen kokonaisluku. Todistamalla, että p voidaan kirjoittaa kahden kokonaisluvun neliöiden summana, osoitamme, että p ei ole Gaussin alkuluku. Tiedetään (lause 2.1), että -1 on luvun p neliönjäännös. Siis on olemassa kokonaisluku t siten, että $t^2 \equiv -1 \pmod{p}$. Tästä seuraa, että $p \mid (t^2 + 1)$. Näin ollen $p \mid (t+i)(t-i)$. Jos p on Gaussin kokonaisluku, niin lauseesta 4.6 seuraa, että $p \mid t + i$ tai $p \mid t - i$. Nämä molemmat ovat mahdottomia, koska Gaussin kokonaisluvut, jotka ovat jaollisia luvulla p ovat muotoa

$$p(a + bi) = pa + pbi,$$

missä a ja b ovat kokonaislukuja. Kumpikaan $t+i$ tai $t-i$ ei ole tätä muotoa. Tästä seuraa, että p ei ole Gaussin alkuluku.

Koska p ei ole Gaussin alkuluku, on olemassa Gaussin kokonaisluvut α ja β (kumpikaan ei ole yksikkö) siten, että $p = \alpha\beta$. Ottamalla puolittain normit tästä yhtälöstä saadaan

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

Koska kumpikaan luvuista α ja β ei ole yksikkö, tiedetään lauseen 4.3 perusteella, että $N(\alpha) \neq 1$ ja $N(\beta) \neq 1$. Tästä seuraa, että $N(\alpha) = N(\beta) = p$. Siis, jos $\alpha = a + bi$ ja $\beta = c + di$, tiedetään, että

$$p = N(\alpha) = a^2 + b^2 \quad \text{ja} \quad p = N(\beta) = c^2 + d^2.$$

Tästä seuraa, että alkuluku p on neliöiden summa. □

Lause 4.10. *Jos π on Gaussin alkuluku, niin on olemassa täsmälleen yksi sellainen alkuluku p, että $\pi \mid p$.*

Todistus (vrt. [2, s. 571]). Jaetaan aluksi alkuluku $N(\pi)$ alkutekijöihin,

$$N(\pi) = p_1 p_2 \cdots p_t,$$

missä p_j on alkuluku ja $j = 1, 2, \ldots, t$. Koska $N(\pi) = \pi\overline{\pi}$, seuraa, että $\pi \mid N(\pi)$, joten $\pi \mid p_1 p_2 \cdots p_t$. Lauseen 4.7 mukaan tästä seuraa, että $\pi \mid p_j$ jollakin kokonaisluvulla j $(1 \leq j \leq t)$. Nyt on osoitettu, että π jakaa alkuluvun.

Vielä on osoitettava, että π ei voi jakaa kahta eri alkulukua. Oletetaan nyt, että $\pi \mid p_1$ ja $\pi \mid p_2$, missä p_1 ja p_2 ovat eri alkulukuja. Koska $(p_1, p_2) = 1$, tiedetään, että on olemassa kokonaisluvut m ja n siten, että $mp_1 + np_2 = 1$. Lisäksi, koska $\pi \mid p_1$ ja $\pi \mid p_2$, nähdään, että $\pi \mid 1$. Mutta tästähän seuraa, että π on yksikkö, mikä on mahdotonta. Näin ollen π ei jaa kahta eri alkulukua. □

Seuraavaksi esitetään mitkä alkuluvut ovat myös Gaussin alkulukuja ja jaetaan Gaussin alkulukutekijöihin ne, jotka eivät ole.

Lause 4.11. *Jos p on alkuluku, niin p voidaan hajottaa tekijöihin Gaussin kokonaislukujen joukossa seuraavasti:*

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

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

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

Todistus (vrt. [2, s. 571–572]).

1. Huomataan, että $2 = -i(1+i)^2 = i(1-i)^2$, missä tekijät $-i$ ja i ovat yksikköjä. Lisäksi $N(1+i) = N(1-i) = 1^2 + 1^2 = 2$. Koska $N(1+i) = N(1-i)$ on alkuluku, niin lauseen 4.5 mukaan $1+i$ ja $1-i$ ovat Gaussin alkulukuja.

2. Olkoon p alkuluku ja $p \equiv 3 \pmod 4$. Oletetaan, että $p = \alpha\beta$, missä $\alpha = a + bi$ ja $\beta = c + di$ ovat Gaussin kokonaislukuja ja kumpikaan α eikä β ole yksikkö. Lauseen 4.2 mukaan $N(p) = N(\alpha\beta) = N(\alpha)N(\beta)$. Koska $N(p) = p^2$, $N(\alpha) = a^2 + b^2$ ja $N(\beta) = c^2 + d^2$, huomataan, että $p^2 = (a^2 + b^2)(c^2 + d^2)$. Kumpikaan α eikä β ole yksikkö, joten kummankaan normi ei ole 1. Tästä seuraa, että $N(\alpha) = a^2 + b^2 = p$ ja $N(\beta) = c^2 + d^2 = p$. Tämä on kuitenkin mahdotonta, koska $p \equiv 3 \pmod 4$, joten p ei ole kahden neliön summa.

3. Olkoon p alkuluku ja $p \equiv 1 \pmod 4$. Lauseen 4.9 mukaan on olemassa kokonaisluvut a ja b, että $p = a^2 + b^2$. Jos $\pi_1 = a - bi$ ja $\pi_2 = a + bi$, niin $p^2 = N(p) = N(\pi_1)N(\pi_2)$, joten $N(\pi_1) = N(\pi_2) = p$. Lauseen 4.5 perusteella π_1 ja π_2 ovat Gaussin alkulukuja.

   Seuraavaksi osoitetaan, että π_1 ja π_2 eivät ole liitännäisiä. Oletetaan, että $\pi_1 = \epsilon\pi_2$, missä ϵ on yksikkö. Jos $\epsilon = 1$, niin $\pi_1 = \pi_2$. Tämä tarkoittaa, että $x + yi = x - yi$, joten $y = 0$. Tästä seuraa, että $p = x^2 + y^2 = x^2$, mikä on mahdotonta, koska p on alkuluku. Vastaavasti, jos $\epsilon = -1$, niin $\pi_1 = -\pi_2$. Tästä seuraa, että $x + yi = -x + yi$, joten $x = 0$. Tästä seuraa, että $y^2 = p$, mikä on mahdotonta. Jos $\epsilon = i$, niin $x + iy = i(x - iy) = y + ix$, joten saadaan, että $x = y$. Vastaavasti jos $\epsilon = -i$, niin $x + iy = -i(x - iy)$, joten $x = -y$. Molemmissa tapauksissa saadaan, että $p = x^2 + y^2 = 2x^2$, mikä on mahdotonta, koska p on pariton alkuluku. On osoitettu, että mikään yksikkö ϵ ei toteuta yhtälöä $\pi_1 = \epsilon\pi_2$. Tästä seuraa, että π_1 ja π_2 eivät ole toistensa liitännäisiä.

□

Nyt on tarvittavat tulokset, jotta saadaan selville kuinka monella eri tavalla positiiviset kokonaisluvut voidaan esittää kahden kokonaisluvun neliöiden summana.

Lause 4.12. *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 on m ei-negatiivinen kokonaisluku, $p_1, p_2, \ldots, p_s$ ovat muotoa $4k+1$ olevia alkulukuja, $q_1, q_2, \ldots, q_t$ ovat muotoa $4k+3$ olevia alkulukuja, eksponentit $e_1, e_2, \ldots, e_s$ ovat ei-negatiivisia kokonaislukuja ja eksponentit $f_1, f_2, \ldots, f_t$ ovat parillisia ei-negatiivisia kokonaislukuja. Tällöin on yhteensä

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

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

Todistus (vrt. [2, s. 572–573]). Kun halutaan laskea, kuinka monella eri tavalla luku n voidaan kirjoittaa kahden kokonaisluvun neliöiden summana, eli yhtälön $n = a^2+b^2$ ratkaisujen lukumäärä, niin voimme laskea, monellako eri tavalla luku n voidaan jakaa Gaussin kokonaislukutekijöihin $a + bi$ ja $a - bi$ eli tosin sanoen kirjoittaa muodossa $n = (u+iv)(u-iv)$. Käytetään luvun n tekijöihin jakoa siihen, että lasketaan monellako tavalla luku n voidaan jakaa tekijöihin kahden konjugaatin tulona, eli $n = (u + iv)(u - iv)$. Huomataan, että lauseen 4.9 mukaan jokaisella muotoa $4k+1$ olevalla alkuluvulla p_k, joka

jakaa luvun n, on olemassa kokonaisluvut a_k ja b_k siten, että $p_k = a_k^2 + b_k^2$. Koska $1 + i = i(1 - i)$, saadaan, että

$$2^m = (1+i)^m(1-i)^m = (i(1-i))^m(1-i)^m = i^m(1-i)^{2m}.$$

Siis

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

Huomataan, että $\epsilon = i^m$ on yksikkö, koska se saa jonkin arvoista 1, -1, i tai $-i$. Tämä tarkoittaa, että luvun n tekijöihin jako yksikön ja Gaussin alkulukujen tuloksi on

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

Koska Gaussin kokonaisluku $u+iv$ jakaa luvun n, sen tekijöihin jaon yksiköksi ja Gaussin kokonaisluvuiksi täytyy olla seuraavaa muotoa

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

missä ϵ_0 on yksikkö, ω, $g_1, \ldots, g_s$, $h_1, \ldots, h_s$ ja $k_1, \ldots, k_t$ ovat ei-negatiivisia kokonaislukuja ja $0 \leq \omega \leq 2m$, $0 \leq g_i \leq e_i$, $0 \leq h_i \leq e_1$ kaikilla $i = 1, \ldots, s$, ja $0 \leq k_j \leq f_j$ kaikilla $j = 1, \ldots, t$. Muodostettaessa konjugaattia luvulle $u + iv$ huomataan, että

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

Nyt yhtälö

$$n = (u+iv)(u-iv)$$

voidaan kirjoittaa muotoon

$$n = 2^{\omega}p_1^{g_1+h_1}\cdots p_s^{g_s+h_s}q_1^{2k_1}\cdots q_t^{2k_t}.$$

Kun verrataan tätä luvun n tekijöihin jakoon yksiköksi ja Gaussin alkuluvuiksi, huomataan, että $\omega = m$, $g_i + h_i = e_j$ kaikilla $i = 1, \ldots, s$ ja $2k_j = f_j$ kaikilla $j = 1, \ldots, t$. Nähdään, että arvot luvuille ω ja k_i kaikilla $k = 1, \ldots, t$ on määrätty, mutta luvulle g_i on $e_i + 1$ vaihtoehtoa, nimittäin $g_i = 0, 1, 2, \ldots, e_i$. Kun luku g_i on määrätty, niin on myös $h_i = e_i - g_i$. Lisäksi on neljä eri vaihtoehtoa yksiköksi ϵ_0. Voidaan päätellä, että on $4(e_1+1)(e_2+1)\cdots(e_s+1)$ vaihtoehtoa tekijälle $u+iv$ ja tavalle kirjoittaa luku n kahden kokonaisluvun neliöiden summana. □

Esimerkki 4.5. Tarkastellaan, monellako eri tavalla luku 5 voidaan esittää kahden neliön summana. Tiedetään, että

$$5 = 5^1,$$

joten on $4(1+1) = 8$ tapaa esittää luku 5 kahden kokonaisluvun neliöiden summana. Nämä ovat

$$\begin{aligned}
5 &= 1^2 + 2^2 \\
5 &= (-1)^2 + 2^2 \\
5 &= (-1)^2 + (-2)^2 \\
5 &= 1^2 + (-2)^2 \\
5 &= 2^2 + 1^2 \\
5 &= 2^2 + (-1)^2 \\
5 &= (-2)^2 + (-1)^2 \\
5 &= (-2)^2 + 1^2.
\end{aligned}$$

Esimerkki 4.6. Tarkastellaan monellako eri tapaa luku 28665 voidaan esittää kahden kokonaisluvun neliöiden summana. Tiedetään, että

$$28665 = 3^2 \cdot 5 \cdot 7^2 \cdot 13,$$

joten on $4\,(1+1)\,(1+1) = 16$ tapaa esittää luku 28665 kahden kokonaisluvun neliöiden summana. Nämä ovat

$$\begin{aligned}
28665 &= 21^2 + 168^2 \\
28665 &= (-21)^2 + 168^2 \\
28665 &= (-21)^2 + (-168)^2 \\
28665 &= 21^2 + (-168)^2 \\
28665 &= 168^2 + 21^2 \\
28665 &= 168^2 + (-21)^2 \\
28665 &= (-168)^2 + (-21)^2 \\
28665 &= (-168)^2 + 21^2 \\
28665 &= 84^2 + 147^2 \\
28665 &= (-84)^2 + 147^2 \\
28665 &= (-84)^2 + (-147)^2 \\
28665 &= 84^2 + (-147)^2 \\
28665 &= 147^2 + 84^2 \\
28665 &= 147^2 + (-84)^2 \\
28665 &= (-147)^2 + (-84)^2 \\
28665 &= (-147)^2 + 84^2.
\end{aligned}$$

5 Minkowskin lause

Tarkastellaan neliösummia seuraavaksi geometrisesta näkökannasta.

Määritelmä 5.1. Hila avaruudessa $\mathbb{R}^n$ on joukko, joka on muotoa

$$\Lambda = \{\alpha_1 v_1 + \cdots + \alpha_n v_n \mid \alpha_i \in \mathbb{Z}\},$$

missä $v_1, \ldots, v_n$ muodostavat vektoriavaruuden $\mathbb{R}^n$ kannan. Sanotaan, että $v_1, \ldots, v_n$ on hilan Λ kanta.

Lause 5.1. *Jos Λ on hila avaruudessa $\mathbb{R}^n$, niin Λ on ryhmän $(\mathbb{R}^n, +)$ aliryhmä.*

Todistus. Ks. [1, s. 207]. □

Määritelmä 5.2. Jos Λ on hila avaruudessa $\mathbb{R}^n$, niin vektorit $v, w \in \mathbb{R}^n$ ovat ekvivalentteja (modulo Λ), $v \sim w$, jos $v - w \in \Lambda$. Ekvivalenssiluokat ovat ryhmän $\mathbb{R}^n$ aliryhmän Λ sivuluokat $\Lambda + v\,(= v + \Lambda)$. Jos $v_1, \ldots, v_n$ on hilan Λ kanta, niin joukkoa

$$F = \{\alpha_1 v_1 + \cdots + \alpha_n v_n \mid 0 \leq \alpha_i < 1\}$$

kutsutaan hilan Λ perusalueeksi. Joukot $F + l$ $(l \in \Lambda)$ ruuduttavat avaruuden $\mathbb{R}^n$ eli peittävät sen ilman päällekkäisyyksiä.

Lause 5.2. *Jokaiselle $v \in \mathbb{R}^n$ on olemassa yksikäsitteinen $w \in F$ siten että $v \sim w$.*

Todistus. Ks. [1, s. 208] □

Vaihtoehtoinen tulkinta tälle tulokselle on, että jokainen $v \in \mathbb{R}^n$ on joukossa

$$F + l = \{f + l \mid f \in F\}$$

yksikäsitteisellä $l \in \Lambda$ (nimittäin, $l = v - w$ siten, että $v = w + l \in F + l$). Näitä joukkoja $F + l$ kutsutaan joukon F translaatioiksi, koska ne on saatu joukosta F translaatiolla. Lause 5.2 väittää, että nämä translaatiot ruuduttavat $\mathbb{R}^n$ eli peittävät $\mathbb{R}^n$ ilman päällekkäisyyksiä.

Lauseen 5.2 avulla voidaan määritellä funktio $\phi : \mathbb{R}^n \to F$ $(\phi(v) = w)$, missä $v \sim w \in F$. Näin w on yksikäsitteinen sivuluokan $v + \Lambda$ edustaja, joka sisältyy joukkoon F.

Tarkennetaan viimeistä huomautusta määrittelemällä joukon $X \subset \mathbb{R}^n$ n-dimensioinen tilavuus, joka on

$$\mathrm{vol}(X) = \int \int \ldots \int 1 dx_1 dx_2 \ldots dx_n,$$

jos se on olemassa ja äärellinen, missä integrointi on yli $(x_1, x_2, \ldots, x_n) \in X$. Kun $n = 1, 2$ tai 3 niin tämä tarkoittaa joukon X pituutta, pinta-alaa tai tilavuutta.

Lause 5.3. *Jos* $\texttt{vol}(X) > \texttt{vol}(F)$*, niin rajoittuma* $\phi\,|_X$ *ei ole yksi yhteen. Eli jos* X *on riittävän suuri, niin joukossa* X *on ainakin kaksi eri pistettä, jotka ovat ekvivalentteja.*

Todistus. Ks. [1, s. 210]. □

Määritelmä 5.3. Joukon $\mathbb{R}^n$ osajoukko X on keskitetysti symmetrinen, jos millä tahansa $v \in X$ myös $-v \in X$. Osajoukko X on konveksi, jos millä tahansa $v, w \in X$ myös jana vw kuuluu osajoukkoon X, eli $tv + (1-t)w \in X$ kaikilla t, $0 \leq t \leq 1$.

Seuraavaksi esitettävä lause on Minkowskin lause.

Lause 5.4. *Olkoon* Λ *hila joukossa* $\mathbb{R}^n$ *perusalueenaan* F*, ja olkoon* X *keskitetysti symmetrinen konveksi joukko joukossa* $\mathbb{R}^n$ *ja* $\texttt{vol}(X) > 2^n\texttt{vol}(F)$*. Tällöin* X *sisältää hilan* Λ *ei-nolla hilapisteen.*

Todistus. Ks. [1, s. 211]. □

Minkowskin lauseen soveltamiseen tarvitsee laskea perusalueiden tilavuuksia. Tämä on helpompaa determinanttien avulla. Oletetaan, että $\{v_1, \ldots, v_n\}$, missä jokainen $v_i = (\alpha_{i1}, \ldots, \alpha_{in}) \in \mathbb{R}^n$, on hilan Λ kanta. Jos A on $n \times n$ matriisi (α_{ij}), joka on muodostettu näistä vektoreista v_i, niin

$$\mathrm{vol}\,(F) = |\det(A)|\,.$$

Matriisin A indusoima lineaarinen kuvaus $\mathbb{R}^n \to \mathbb{R}^n$ tekee joukon $\mathbb{R}^n$ standardi kantavektoreista e_i joukon Λ kantavektoreita v_i. Lisäksi se kuvaa joukon

$$C = \{\alpha_1 e_1 + \cdots + \alpha_n e_n \mid 0 \leq \alpha_i < 1\}$$

hilan Λ perusalueeksi

$$F = \{\alpha_1 v_1 + \cdots + \alpha_n v_n \mid 0 \leq \alpha_i < 1\}\,.$$

Koska $\mathrm{vol}(C) = 1$ ja jokainen lineaarinen kuvaus A moninkertaistaa tilavuutta $|\det(A)|$ verran, seuraa, että $\mathrm{vol}(F) = |\det(A)|$.

Nyt voidaan todistaa, että jokainen alkuluku p muotoa $p \equiv 1 \pmod 4$ voidaan esittää kahden kokonaisluvun neliöiden summana.

Lause 5.5. *Jokainen muotoa* $p \equiv 1 \pmod 4$ *oleva alkuluku voidaan esittää kahden kokonaisluvun neliöiden summana.*

Todistus (vrt. [1, s. 212–213]). Olkoon p pariton alkuluku. Silloin 1 on neliönjäännös, jos ja vain jos $p \equiv 1 \pmod 4$ (ks.[1, Corollary 7.7]). Näin ollen $u^2 \equiv -1 \pmod p$ jollakin kokonaisluvulla u. Oletetaan seuraavaksi, että seuraava ehto on voimassa: on olemassa $x, y \in \mathbb{Z}$ siten, että

$$y \equiv ux \pmod p \quad \text{ja} \quad 0 < x^2 + y^2 < 2p. \tag{5.1}$$

Nyt

$$x^2 + y^2 \equiv x^2 + u^2x^2 \equiv x^2 - x^2 \equiv 0 \pmod{p},$$

joten

$$x^2 + y^2 = kp$$

jollakin kokonaisluvulla k. Epäyhtälöistä (5.1) seuraa, että $0 < kp < 2p$, joten $k = 1$ ja $x^2 + y^2 = p$, kuten edellytettiin. Näin ollen riittää todistaa (5.1). Tämä voidaan todistaa käyttämällä Minkowskin lausetta, koska ensimmäinen ehto $y \equiv ux \pmod{p}$ (5.1) määrää hilan Λ joukossa $\mathbb{R}^2$, ehto $x^2+y^2 < 2p$ määrää keskitetysti symmetrisen konveksin joukon X, nimittäin kiekon $B_2(\sqrt{2p})$ ja ehto $0 < x^2+y^2$ määrää ei-nolla pisteen (x, y). Minkowskin lause takaa pisteen (x, y), joka täyttää nämä ehdot, olemassa olon. Näin ollen on todistettu (5.1).

Nyt täytyy vielä tarkistaa kaikki Minkowskin lauseen hypoteesit. Olkoon

$$\Lambda = \left\{(x, y) \in \mathbb{Z}^2 \mid y \equiv ux \pmod{p}\right\}.$$

Tämä on ryhmän $\mathbb{R}^2$ aliryhmä, joka sisältää lineaarisesti riippumattomat vektorit $v_1 = (1, u)$ ja $v_2 = (0, p)$. Kun $(x, y) \in \Lambda$, niin olkoot $\alpha_1 = x$ ja $\alpha_2 = (y - ux)/p$; nämä ovat kokonaislukuja, $\alpha_1 v_1 + \alpha_2 v_2 = (x, y)$, joten Λ on vektoreiden v_1 ja v_2 virittämä. Näin ollen Λ on hila, jonka kannan muodostavat vektorit v_1 ja v_2, joten sillä on perusalueenaan F, jolla on 2-dimensioinen tilavuus (eli pinta-ala)

$$\texttt{vol}(F) = \left|\det \begin{pmatrix} 1 & u \\ 0 & p \end{pmatrix}\right| = p.$$

Nyt olkoon

$$X = B_2\left(\sqrt{2p}\right) = \left\{(x, y) \in \mathbb{R}^2 \mid x^2 + y^2 < 2p\right\}$$

avoin origokeskinen kiekko säteenään $r = \sqrt{2p}$. Tämä on pistesymmetrinen ja konveksi ja sen tilavuus (pinta-ala) on

$$\texttt{vol}(X) = \pi r^2 = 2\pi p.$$

Nyt $\pi > 2\sqrt{2} > 2$, joten $\mathrm{vol}(X) > 2^2\mathrm{vol}(F)$. Näin ollen Minkowskin lause antaa ei-nolla hila pisteen $(x, y) \in X \cap \Lambda$. On siis olemassa kokonaislukupari x ja y, jotka toteuttavat ehdot (5.1). □

Nyt voidaan todistaa, että jokainen ei-negatiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana.

Lause 5.6. *Jokainen ei-negatiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana.*

Todistus (vrt. [1, s. 213–214]). Riittää osoittaa, että jokainen pariton alkuluku voidaan esittää neljän kokonaisluvun neliöiden summana. Osoitetaan aluksi, että on olemassa kokonaisluvut u ja v, jotka toteuttavat kongruenssin $u^2 + v^2 \equiv -1 \pmod{p}$. Olkoon tällaiselle parille u ja v

$$\Lambda = \left\{(x, y, z, t) \in \mathbb{Z}^4 \mid z \equiv ux + vy \quad \text{ja} \quad t \equiv vx - uy \pmod{p}\right\}.$$

Tiedetään, että Λ on hila avaruudessa $\mathbb{R}^4$ kantanaan vektorit $v_1 = (1, 0, u, v)$, $v_2 = (0, 1, v, -u)$, $v_3 = (0, 0, p, 0)$ ja $v_4 = (0, 0, 0, p)$. Nyt tiedetään, että hilan Λ perusalueella F on tilavuus

$$\texttt{vol}\,(F) = \left|\det \begin{pmatrix} 1 & 0 & u & v \\ 0 & 1 & v & -u \\ 0 & 0 & p & 0 \\ 0 & 0 & 0 & p \end{pmatrix}\right| = 1 \cdot 1 \cdot p \cdot p = p^2.$$

Olkoon

$$X = B_4\left(\sqrt{2p}\right) = \left\{(x, y, z, t) \in \mathbb{R}^4 \mid x^2 + y^2 + z^2 + t^2 < 2p\right\}$$

avoin kuula, jonka säde on $r = \sqrt{2p}$. Tämä on keskitetysti symmetrinen ja konveksi ja sen tilavuus on 4-dimensioinen

$$\texttt{vol}\,(X) = \frac{\pi^2 r^4}{2} = 2\pi^2 p^2.$$

Nyt $\pi^2 > 8$, joten $\text{vol}(X) > 2^4\text{vol}(F)$ ja näin ollen Minkowskin lause implikoi, että X sisältää ei-nolla hilapisteen. On siis olemassa kokonaisluvut x, y, z ja t siten, että $0 < x^2 + y^2 + z^2 + t^2 < 2p$, $z \equiv ux + vy \pmod{p}$ ja $t \equiv vx - uy \pmod{p}$. Siis

$$\begin{aligned} x^2 + y^2 + z^2 + t^2 &\equiv x^2 + y^2 + u^2x^2 + 2uvxy + v^2y^2 + v^2x^2 - 2uvxy + u^2y^2 \\ &\equiv \left(1 + u^2 + v^2\right)\left(x^2 + y^2\right) \\ &\equiv 0 \pmod{p}, \end{aligned}$$

koska $u^2 + v^2 \equiv -1 \pmod{p}$. Siis voidaan päätellä, että $x^2 + y^2 + z^2 + t^2 = p$. □

Viitteet

[1] Jones, Gareth A. ja ja Jones, J. Mary *Elementary Number Theory*. Springer, 1998.

[2] Rosen, Kenneth H. *Elementary Number Theory and Its Applicatons*. 5th ed., Pearson/Addison-Wesley, 2005.