TAMPEREEN YLIOPISTO
Pro gradu -tutkielma

Heikki Hietava

Neliöiden summat

Informaatiotieteiden yksikkö
Matematiikka
Kesäkuu 2011

Tampereen yliopisto

Informaatiotieteiden yksikkö

HIETAVA, HEIKKI: Neliöiden summat

Pro gradu -tutkielma, 23 s.

Matematiikka

Kesäkuu 2011

Tiivistelmä

Tietyt positiiviset kokonaisluvut voidaan esittää kahden kokonaisluvun neliöiden summana, esimerkiksi $5^2 = 2^2+1^2$. Kaikkia kokonaislukuja ei kuitenkaan voida esittää kahden eikä edes kolmen kokonaisluvun neliöiden summana. Vuonna 1770 Joseph Lagrange todisti tämän tutkielman keskeisimmän lauseen: jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana, joista osa voi olla nollia. Edellä mainittu lause todistetaan tämän tutkielman luvun 3.2 lopussa.

Tässä tutkielmassa käsitellään kokonaislukujen neliöiden summia ja niiden ominaisuuksia. Valmistelevien tarkastelujen jälkeen tutkitaan kahden kokonaisluvun neliöiden summia ja tämän jälkeen syvennytään neljän kokonaisluvun neliöiden summien tapauksiin. Lopuksi tarkastellaan vielä ns. Waringin probleemaa. Tutkielman keskeisimpinä lähdeteoksina käytetään Thomas Koshyn opusta *Elementary Number Theory with Applications*, sekä Charles Vanden Eyndenin kirjaa *Elementary Number Theory*.

Sisältö

1 Johdanto **4**

2 Valmistelevia tarkasteluja **5**
2.1 Jaollisuus 5
2.2 Suurin yhteinen tekijä 5
2.3 Alkuluku 6
2.4 Kanoninen alkutekijäesitys 6
2.5 Kongruensseista 6
2.6 Neliönjäännökset 7
2.7 Legendren symboli 8

3 Neliöiden summista **9**
3.1 Kahden kokonaisluvun neliöiden summat 9
3.2 Neljän kokonaisluvun neliöiden summat 13

4 Waringin probleema **20**

Viitteet **23**

1 Johdanto

Tässä tutkielmassa käsitellään lukuteorian osa-alueelta kokonaislukujen neliöiden summia ja niiden ominaisuuksia. Tarkasteltaessa positiivisia kokonaislukuja havaitaan, että jotkut niistä voidaan esittää kahden kokonaisluvun neliöiden summana. Esimerkiksi luku $13 = 3^2 + 2^2$. Kuitenkaan kaikkia positiivisia kokonaislukuja ei voida esittää kahden eikä edes kolmen kokonaisluvun neliöiden summana. Tutkielman edetessä huomataan, että tarvitaan neljä kokonaislukua, jotta mielivaltainen positiivinen kokonaisluku voidaan esittää kokonaislukujen neliöiden summana.

Luvussa 2 tarkastellaan eräitä algebran ja lukuteorian peruskäsitteitä, joita tarvitaan tutkielman luvun 3 käsittelyssä. Määritelmien ja esimerkkien lisäksi esitellään kolme lausetta, jotka ovat pääosin Haukkasen luentomonisteista *Algebra I* ja *Lukuteoriaa*.

Tämän tutkielman pääluvun, luvun 3, pykälässä 3.1 syvennytään tarkemmin kahden kokonaisluvun neliöiden summien tapauksiin. Tässä alaluvussa todistetaan kolmen apulauseen lisäksi kaksi lausetta. Ensimmäisessä lauseessa todistetaan, että jos alkuluku $p = 2$ tai $p \equiv 1 \pmod 4$, niin silloin alkuluku p on esitettävissä kahden kokonaisluvun neliöiden summana. Toisen lauseen avulla voidaan määrittää, voidaanko tietty positiivinen kokonaisluku esittää kahden kokonaisluvun neliöiden summana.

Pykälässä 3.2 tarkastellaan neljän kokonaisluvun neliöiden summia. Kahden apulauseen ja yhden seurauslauseen lisäksi tässä alaluvussa todistetaan kaksi lausetta. Ensimmäisessä lauseessa todistetaan, että jokainen alkuluku voidaan esittää neljän kokonaisluvun neliöiden summana. Tämän lauseen avulla todistetaan tutkielman merkittävin lause: jokainen kokonaisluku, olkoon se kuinka suuri tahansa, voidaan esittää neljän kokonaisluvun neliöiden summana. Edellä mainittu lause oli useamman matemaatikon haasteena 1600- ja 1700-luvuilla. Joseph Lagrange todisti tämän lauseen ensimmäisenä vuonna 1770.

Luvussa 4 tutustutaan yleisellä tasolla Edward Waringin esittämään otaksumaan, joka tänä päivänä tunnetaan Waringin probleemana. Sen keskeisimpänä kysymyksenä voidaan pitää seuraavaa: onko jokaista luonnollista lukua k kohti olemassa sellainen luku $g(k)$, että jokainen positiivinen kokonaisluku voidaan esittää enintään $g(k)$:n ei-negatiivisen kokonaisluvun k:nnen potenssin summana?

Tutkielman esimerkit pyrkivät helpottamaan lauseiden asiasisällön ymmärtämistä. Esimerkit ovat tekijän kehittämiä ja ratkaisemia, mutta ne ovat pääosin samankaltaisia, kuin lähteiden [5] ja [6] esimerkit ja harjoitustehtävät.

Tutkielma seuraa pääosin Thomas Koshyn teosta *Elementary Number Theory with Applications*, jota tukee Charles Vanden Eyndenin kirja *Elementary Number Theory*. Lukijan oletetaan ymmärtävän käytetyimmät matemaattiset merkintätavat, sekä hallitsevan algebralliset peruslaskutoimitukset. Lisäk-

si todistusten ymmärtämiseksi olisi hyvä tietää muutamia joukko-opin käsitteitä, kuten positiivisten kokonaislukujen hyvinjärjestysperiaate, sekä yleinen laatikkoperiaate.

2 Valmistelevia tarkasteluja

Tässä luvussa tarkastellaan muutamia lukuteorian peruskäsitteitä, joita tarvitaan erityisesti tutkielman pääluvun, luvun 3, käsittelyssä. Tämän luvun määritelmät ovat pääosin Pentti Haukkasen luentomonisteista *Algebra I* ja *Lukuteoriaa*. Merkitään kokonaislukujen joukkoa symbolilla $\mathbb{Z}$ ja positiivisten kokonaislukujen joukkoa symbolilla $\mathbb{Z}_+$. Kaikki tämän tutkielman luvut ovat kokonaislukuja ellei toisin mainita.

2.1 Jaollisuus

Määritelmä 2.1. Luku a on luvun b *tekijä* (eli luku b on *jaollinen* luvulla a eli luku a jakaa luvun b), jos on olemassa sellainen luku $c \in \mathbb{Z}$, että $b = ac$. Jos luku a jakaa luvun b, niin tällöin merkitään $a|b$, muussa tapauksessa $a \nmid b$.

Esimerkki 2.1. Luvun 8 kaikki positiiviset tekijät ovat 1, 2, 4 ja 8. Näin ollen jaollisuuden määritelmän 2.1 perusteella voidaan kirjoittaa $1|8$, $2|8$, $4|8$ ja $8|8$.

2.2 Suurin yhteinen tekijä

Määritelmä 2.2. Olkoot a ja b kokonaislukuja, joista ainakin toinen on erisuuri kuin 0. Silloin luku c on lukujen a ja b *suurin yhteinen tekijä* (syt), jos

$$\begin{aligned} &1) \quad c|a, c|b \text{ ja} \\ &2) \quad d|a, d|b \Rightarrow d \leq c. \end{aligned}$$

Lukujen a ja b suurinta yhteistä tekijää merkitään symbolilla (a, b), joten voidaan kirjoittaa $c = (a, b)$.

Esimerkki 2.2. Luvun 6 positiiviset tekijät ovat 1, 2, 3 ja 6, ja luvulle 16 vastaavasti 1, 2, 4, 8, ja 16. Joten lukujen 6 ja 16 suurin yhteinen tekijä on 2 eli $(6, 16) = 2$.

Esimerkki 2.3. Lukujen 5 ja 15 suurin yhteinen tekijä on 5 eli $(5, 15) = 5$, sillä luvun 5 positiiviset tekijät ovat 1 ja 5, ja luvun 15 positiiviset tekijät ovat 1, 3, 5 ja 15.

2.3 Alkuluku

Määritelmä 2.3. Kokonaisluku $p > 1$ on *alkuluku*, jos sen ainoat positiiviset tekijät ovat 1 ja p.

Esimerkki 2.4. Pienimmät kymmenen alkulukua ovat 2, 3, 5, 7, 11, 13, 17, 19, 23 ja 29.

Huomautus 2.1. Luku 2 on ainoa parillinen alkuluku.

2.4 Kanoninen alkutekijäesitys

Määritelmä 2.4. Positiivisen kokonaisluvun $a > 1$ *kanoninen alkutekijäesitys* on muotoa

$$a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},$$

missä p_1, p_2, ..., p_n ovat luvun a alkulukutekijät (eli alkutekijät), $p_1 < p_2 < \cdots < p_n$ ja jokainen eksponentti $a_i \in \mathbb{Z}_+$.

Huomautus 2.2. Kanonista alkutekijäesitystä sanotaan usein lyhyesti *kanoniseksi esitykseksi*.

Huomautus 2.3. Aritmetiikan peruslause sanoo, että jokainen kokonaisluku $a \geq 2$ voidaan esittää alkulukujen tulona ja tämä tulo on yksikäsitteinen tekijöiden järjestystä lukuunottamatta. (Ks. aritmetiikan peruslauseen todistus [3, s. 13].)

Esimerkki 2.5. Luvun 1080 kanoninen alkutekijäesitys on

$$1080 = 2 \cdot 2 \cdot 2 \cdot 3 \cdot 3 \cdot 3 \cdot 5 = 2^3 \cdot 3^3 \cdot 5.$$

2.5 Kongruensseista

Määritelmä 2.5. Olkoon luku $m \in \mathbb{Z}_+$. Silloin luku a on *kongruentti* luvun b kanssa *modulo* m, jos

$$m|(a - b).$$

Jos luku a on kongruentti luvun b kanssa modulo m, niin tällöin voidaan käyttää merkintää

$$a \equiv b \pmod{m}.$$

Esimerkki 2.6. Luku 19 on kongruentti luvun 3 kanssa modulo 4 eli $19 \equiv 3 \pmod{4}$, sillä $4|(19 - 3)$.

Esimerkki 2.7. Luku 17 ei ole kongruentti luvun 3 kanssa modulo 4 eli $17 \not\equiv 3 \pmod{4}$, sillä $4 \nmid (17 - 3)$.

Määritelmä 2.6. Joukko $\{r_1, r_2, \ldots, r_m\}$ on *täydellinen jäännössysteemi modulo* m, jos $r_i \not\equiv r_j \pmod{m}$ aina, kun $i \neq j$.

Esimerkki 2.8. (Vrt. [4, s. 4].) Joukot $\{1, 2, 3, \ldots, m\}$ ja $\{0, 1, 2, \ldots, m-1\}$ ovat täydellisiä jäännössysteemejä modulo m.

Määritelmä 2.7. *Eulerin funktio* ϕ määritellään kaavalla

$$\phi(n) = |\{r : 1 \leq r \leq n,\ (r, n) = 1\}|,$$

missä $n \in \mathbb{Z}_+$.

Määritelmä 2.8. Joukko $\{r_1, r_2, \ldots, r_{\phi(m)}\}$ on *supistettu jäännössysteemi modulo* m, jos

1) $(r_i, m) = 1$, kun $i = 1, 2, \ldots, \phi(m)$
2) $r_i \not\equiv r_j \pmod{m}$, kun $i \neq j$.

Esimerkki 2.9. (Vrt. [4, s. 5].) Joukko $\{r : 1 \leq r \leq m,\ (r, m) = 1\}$ on supistettu jäännössysteemi modulo m.

Apulause 2.1. *Lineaarisella kongruenssiyhtälöllä*

$$ax \equiv b \pmod{m}$$

on yksikäsitteinen ratkaisu modulo m*, jos ja vain jos* $(a, m) = 1$.

Todistus. Ks. [3, s. 24]. □

2.6 Neliönjäännökset

Määritelmä 2.9. Olkoon positiivinen kokonaisluku $m \geq 2$ ja a sellainen kokonaisluku, että $(a, m) = 1$. Silloin luku a on *neliönjäännös modulo* m, jos kongruenssi $x^2 \equiv a \pmod{m}$ on ratkeava, ja luku a on *epäneliönjäännös modulo* m, jos kongruenssi $x^2 \equiv a \pmod{m}$ ei ole ratkeava.

Esimerkki 2.10. Etsitään neliönjäännökset modulo 7. Nyt määritelmän 2.8 nojalla joukko $A = \{1, 2, 3, 4, 5, 6\}$ on supistettu jäännössysteemi modulo 7. Kun joukon A jäsenet korotetaan kukin neliöönsä, saadaan

$$\begin{aligned} 1^2 &= 1 \equiv 1 \pmod{7} & \qquad 4^2 &= 16 \equiv 2 \pmod{7} \\ 2^2 &= 4 \equiv 4 \pmod{7} & \qquad 5^2 &= 25 \equiv 4 \pmod{7} \\ 3^2 &= 9 \equiv 2 \pmod{7} & \qquad 6^2 &= 36 \equiv 1 \pmod{7}. \end{aligned}$$

Siis, määritelmän 2.9 perusteella luvut $1, 2$ ja 4 ovat neliönjäännöksiä modulo 7 ja luvut $3, 5$ ja 6 ovat epäneliönjäännöksiä modulo 7.

Lause 2.1 (Eulerin kriteeri)**.** *Olkoon luku* p *pariton alkuluku, ja olkoon luku* a *sellainen kokonaisluku, että* $p \nmid a$*. Silloin* a *on neliönjäännös modulo* p*, jos ja vain jos*

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

ja a *on epäneliönjäännös modulo* p*, jos ja vain jos*

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

Todistus. Ks. [4, s. 24]. □

2.7 Legendren symboli

Määritelmä 2.10. Olkoon p pariton alkuluku ja a sellainen kokonaisluku, että $p \nmid a$. Tällöin *Legendren symboli* $\left(\frac{a}{p}\right)$ määritellään kaavalla

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

Esimerkki 2.11. Esimerkin 2.10 neliönjäännökset ja epäneliönjäännökset modulo 7 voidaan nyt lausua Legendren symbolin avulla seuraavasti

$$\left(\frac{1}{7}\right) = \left(\frac{2}{7}\right) = \left(\frac{4}{7}\right) = 1,$$
$$\left(\frac{3}{7}\right) = \left(\frac{5}{7}\right) = \left(\frac{6}{7}\right) = -1.$$

Huomautus 2.4. Eulerin kriteeri, lause 2.1, voidaan lausua nyt myös Legendren symbolin avulla: Olkoon p pariton alkuluku ja a sellainen kokonaisluku, että $p \nmid a$. Silloin a on neliönjäännös modulo p, jos ja vain jos $\left(\frac{a}{p}\right) = 1$. Toisin sanoen kongruenssiyhtälö $x^2 \equiv a \pmod{p}$ on ratkeava, jos ja vain jos $\left(\frac{a}{p}\right) = 1$.

Eulerin kriteerin avulla voidaan identifioida ne alkuluvut p, joille -1 on neliönjäännös modulo p.

Seuraus 2.1. Jos p on pariton alkuluku, niin silloin $\left(\frac{-1}{p}\right) = (-1)^{(p-1)/2}$ eli

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

Todistus. (Vrt. [5, s. 504].) Olkoon alkuluku p pariton. Eulerin kriteerin perusteella

$$\begin{aligned} \left(\frac{-1}{p}\right) &\equiv (-1)^{(p-1)/2} \pmod p \\ &= (-1)^{(p-1)/2}, \text{ kun } (-1)^{(p-1)/2} = \pm 1 \\ &= \begin{cases} 1, & \text{jos } p \text{ on muotoa } 4k+1 \\ -1, & \text{jos } p \text{ on muotoa } 4k+3 \end{cases} \\ &= \begin{cases} 1, & \text{jos } p \equiv 1 \pmod 4 \\ -1, & \text{jos } p \equiv -1 \pmod 4. \end{cases} \end{aligned}$$

□

Seurauslauseen 2.1 perusteella -1 on neliönjäännös modulo p, jos ja vain jos $p \equiv 1 \pmod 4$. Toisin sanoen $x^2 \equiv p-1 \pmod p$ on ratkeava, jos ja vain jos $p \equiv 1 \pmod 4$.

3 Neliöiden summista

Kokonaislukujen esittäminen toisten kokonaislukujen neliöiden summina on kiehtonut monia matemaatikkoja useampien vuosisatojen aikana. Jo ennen ajanlaskun alkua kreikkalainen matemaatikko Diofantos (n. 200 eKr.) tiesi, kuinka tulo $(a^2+b^2)(c^2+d^2)$ voidaan esittää kahden kokonaisluvun neliöiden summana (ks. apulause 3.2). Vuonna 1225 Fibonacci julkaisi tämän lauseen täsmällisen todistuksen. [1, s. 129] On kuitenkin huomattu, että kaikkia positiivisia kokonaislukuja ei voida esittää kahden kokonaisluvun neliöiden summana. Esimerkiksi luku 6 on tällainen positiiviinen kokonaisluku. Pykälässä 3.1 syvennytään tarkemmin kahden kokonaisluvun neliöiden summien problematiikkaan.

3.1 Kahden kokonaisluvun neliöiden summat

Apulause 3.1. *Jos $n \equiv 3 \pmod 4$, niin kokonaislukua n ei voida esittää kahden kokonaisluvun neliöiden summana.*

Todistus. (Vrt. [6, s. 242].) Olkoon $n = x^2+y^2$, missä $x, y \in \mathbb{Z}$. Tarkastellaan nyt joukkoa $A = \{1, 2, 3, 4\}$. Havaitaan, että kaikille luvuille $a \in A$ pätee

$$a^2 \equiv 0 \text{ tai } 1 \pmod 4.$$

Määritelmän 2.6 mukaan joukko A on täydellinen jäännössysteemi modulo 4, joten myös (mielivaltaisille) kokonaisluvuille x ja y pätee

$$x^2, y^2 \equiv 0 \text{ tai } 1 \pmod 4.$$

Näin ollen kokonaisluvulle n voidaan kirjoittaa

$$n = x^2 + y^2 \equiv 0, 1 \text{ tai } 2 \pmod 4.$$

Siispä, jos $n \equiv 3 \pmod 4$, niin lukua n ei voida esittää kahden kokonaisluvun neliöiden summana. □

Esimerkki 3.1. Kokonaisluku $n = 17 \equiv 1 \pmod 4$ voidaan esittää kahden kokonaisluvun neliöiden summana seuraavasti: $17 = 4^2+1^2$. Mutta kokonaislukua $n = 15 \equiv 3 \pmod 4$ ei voida esittää kahden kokonaisluvun neliöiden summana.

Apulause 3.2. *Jos ei-negatiiviset kokonaisluvut m ja n voidaan esittää kahden kokonaisluvun neliöiden summana, niin myös tulo mn voidaan esittää vastaavasti.*

Todistus. Olkoot $m = a^2 + b^2$ ja $n = c^2 + d^2$ ei-negatiivisia kokonaislukuja, missä $a, b, c, d \in \mathbb{Z}$. Silloin tulo mn voidaan kirjoittaa kokonaislukujen yhteenlaskun ja kertolaskun kommutatiivisuuden sekä binomin neliön laskusääntöjen perusteella seuraavasti:

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

Näin väite on todistettu. □

Esimerkki 3.2. Luku $20 = 4^2 + 2^2$ ja luku $10 = 3^2 + 1^2$, joten apulauseen 3.2 perusteella tulo $20 \cdot 10 = 200$ on esitettävissä kahden kokonaisluvun neliöiden summana seuraavasti:

$$\begin{aligned} 20 \cdot 10 = 200 &= (4^2 + 2^2)(3^2 + 1^2) \\ &= (4 \cdot 3 + 2 \cdot 1)^2 + (4 \cdot 1 - 2 \cdot 3)^2 \\ &= 14^2 + (-2)^2 \\ &= 14^2 + 2^2. \end{aligned}$$

Apulause 3.3. *Jos alkuluku* $p \equiv 1 \pmod 4$, *niin silloin on olemassa sellaiset positiiviset kokonaisluvut* x *ja* y, *että*

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

missä $k \in \mathbb{Z}_+$ *ja* $k < p$.

Todistus. (Vrt. [5, s. 604].) Oletetaan, että pariton alkuluku $p \equiv 1 \pmod 4$. Tällöin seurauslauseen 2.1 mukaan -1 on neliönjäännös modulo p. Toisin sanoen on olemassa positiivinen kokonaisluku $a < p$ siten että

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

missä $k \in \mathbb{Z}_+$. Nyt valitsemalla $x = a$ ja $y = 1$ saadaan

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

Siispä tulo kp voidaan esittää kahden kokonaisluvun neliöiden summana. Koko väitteen todistamiseksi pitää vielä osoittaa, että $k < p$. Koska $a \leq p-1$ ja

$$kp = a^2 + 1 < (p-1)^2 + 1 = p^2 - 2p + 1 + 1 = p^2 - 2(p-1),$$

niin $kp < p^2$. Siis, $k < p$ ja väite on todistettu. □

Lause 3.1. *Jos alkuluku* $p = 2$ *tai* $p \equiv 1 \pmod 4$, *niin* p *voidaan esittää kahden kokonaisluvun neliöiden summana.*

Todistus. (Vrt. [5, s. 604].) Oletetaan ensiksi, että $p = 2$. Tällöin $2 = 1^2 + 1^2$, josta väite seuraa.
Oletetaan sitten, että $p \equiv 1 \pmod 4$. Nyt apulauseen 3.3 ja positiivisten kokonaislukujen hyvinjärjestysperiaatteen nojalla on olemassa pienin positiivinen kokonaisluku m siten että

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

missä $x, y \in \mathbb{Z}_+$. Osoitetaan nyt, että $m = 1$.
Tehdään vastaoletus, että $m > 1$. Määritellään sitten kokonaisluvut r ja s seuraavasti:

$$r \equiv x \pmod m \quad \text{ja} \quad s \equiv y \pmod m, \tag{3.1}$$

missä

$$-\frac{m}{2} < r \leq \frac{m}{2} \quad \text{ja} \quad -\frac{m}{2} < s \leq \frac{m}{2}. \tag{3.2}$$

Siten kongruenssiyhtälöiden (3.1) ja jaollisuuden määritelmän 2.1 perusteella

$$r^2 + s^2 \equiv x^2 + y^2 = mp \equiv 0 \pmod m,$$

joten $r^2 + s^2 = mn$, jollakin positiivisella kokonaisluvulla n. Siksi

$$(r^2 + s^2)(x^2 + y^2) = (mn)(mp) = m^2np.$$

Nyt apulauseen 3.2 mukaan

$$(r^2 + s^2)(x^2 + y^2) = (rx + sy)^2 + (ry - sx)^2, \tag{3.3}$$

joten yhtälö (3.3) voidaan kirjoittaa muodossa

$$(rx + sy)^2 + (ry - sx)^2 = m^2np. \tag{3.4}$$

Kongruenssiyhtälöiden (3.1) ja kongruenssin laskusääntöjen nojalla

$$rx + sy \equiv x^2 + y^2 \equiv 0 \pmod m \quad \text{ja} \quad ry - sx \equiv xy - yx \equiv 0 \pmod m.$$

Kongruenssin määritelmän 2.5 perusteella sekä $(rx+sy)/m$ että $(ry-sx)/m$ ovat kokonaislukuja, joten nyt yhtälön (3.4) perusteella

$$np = \left(\frac{rx + sy}{m}\right)^2 + \left(\frac{ry - sx}{m}\right)^2 \tag{3.5}$$

Yhtälöstä (3.5) nähdään, että tulo np voidaan esittää kahden kokonaisluvun neliöiden summana.

Epäyhtälöiden (3.2) perusteella saadaan

$$r^2 + s^2 \leq \left(\frac{m}{2}\right)^2 + \left(\frac{m}{2}\right)^2 = \frac{m^2}{2},$$

joten $r^2 + s^2 = mn \leq m^2/2$. Näin ollen $n \leq m/2$ ja siksi $n < m$. On siis oltava niin, että $n \neq 0$, sillä jos $n = 0$, niin $r^2 + s^2 = 0$ ja $r = 0 = s$. Tällöin olisi $x \equiv 0 \equiv y \pmod{m}$, ja kongruenssin määritelmän 2.5 perusteella $m|x$ ja $m|y$. Näin ollen $m^2|(x^2 + y^2)$ eli $m^2|mp$, josta seuraa, että $m|p$.

Koska apulauseen 3.3 nojalla $m < p$, niin m on oltava 1. Tämä on ristiriidassa oletuksen $m > 1$ kanssa, joten $n \geq 1$. Näin ollen $n \in \mathbb{Z}_+$ ja $n < m$ siten, että tulo np voidaan esittää kahden kokonaisluvun neliöiden summana. Tämä on myös ristiriita, sillä lähtökohtaisesti oletettiin, että luku m on pienin sellainen positiivinen kokonaisluku, että $mp = x^2 + y^2$. Siksi vastaoletus on väärä. Siispä $m = 1$ ja $p = x^2 + y^2$, joka tuli osoittaa. □

Lause 3.2. *Positiivinen kokonaisluku n on esitettävissä kahden kokonaisluvun neliöiden summana, jos ja vain jos minkään alkuluvun $p_i \equiv 3 \pmod{4}$ määrä luvun n alkulukutekijöissä ei ole pariton.*

Huomautus 3.1. Lause 3.2 voidaan muotoilla myös siten, että luku n voidaan esittää kahden kokonaisluvun neliöiden summana, jos ja vain jos luvun n kanonisessa alkutekijäesityksessä kaikkien niiden alkulukujen p_i, jotka ovat kongruentteja luvun 3 kanssa modulo 4, eksponentti on parillinen.

Todistus. (Vrt. [5, s. 605].) Jaetaan todistus kahteen osaan.
($\Rightarrow$) Oletetaan aluksi, että $n = x^2 + y^2$, missä $x, y \in \mathbb{Z}$.
Tehdään vastaoletus, että luvun n kanonisessa alkutekijäesityksessä on tekijä p, jolla on pariton eksponentti $2j+1$, missä $p \equiv 3 \pmod{4}$. Olkoon kokonaislukujen x ja y suurin yhteinen tekijä $(x, y) = d$ ja olkoot $r = x/d$, $s = y/d$ ja $m = n/d^2$. Silloin määritelmän 2.2 mukaan lukujen r ja s suurin yhteinen tekijä $(r, s) = 1$ ja lisäksi

$$r^2 + s^2 = \frac{x^2}{d^2} + \frac{y^2}{d^2} = \frac{x^2 + y^2}{d^2} = \frac{n}{d^2} = m. \tag{3.6}$$

Olkoon p^k suurin alkuluvun p potenssi, joka jakaa luvun d. Nyt koska $m = \frac{n}{d^2}$ ja $\frac{p^{2j+1}}{(p^k)^2} = p^{2j-2k+1}|m$, missä $2j - 2k + 1 \geq 1$, niin $p|m$.

Oletetaan seuraavaksi, että $p|r$. Yhtälön (3.6) perusteella $s^2 = m - r^2$ ja kun $p|m$, niin seuraa, että $p|s$. Tämä on ristiriita, sillä $(r, s) = 1$, joten $p \nmid r$. Näin ollen apulauseen 2.1 perusteella on olemassa kokonaisluku t siten että

$$rt \equiv s \pmod{p}.$$

Tällöin, kun otetaan huomioon, että $p|m$, saadaan

$$0 \equiv m = r^2 + s^2 \equiv r^2 + (rt)^2 = r^2(1 + t^2) \pmod{p}.$$

Koska $(p, r) = 1$, niin seuraa, että $1+t^2 \equiv 0 \pmod{p}$, joten $t^2 \equiv -1 \pmod{p}$. Nyt määritelmän 2.9 mukaan -1 on neliönjäännös modulo p. Mutta tämä on ristiriidassa seurauslauseen 2.1 kanssa ($p \equiv 3 \pmod 4$), joten lukua n ei voida esittää kahden kokonaisluvun neliöiden summana. Siispä vastaoletus on väärä, joten minkään alkuluvun $p_i \equiv 3 \pmod 4$ määrä luvun n alkulukutekijöissä ei ole pariton.
($\Leftarrow$) Oletetaan, että luvun n kanonisessa alkutekijäesityksessä kaikkien alkulukujen $p_i \equiv 3 \pmod 4$ eksponentti on parillinen. Edellä mainitun oletuksen nojalla luku n voidaan kirjoittaa muodossa

$$n = a^2 b,$$

missä lukuun a^2 on kerätty kaikki luvun n alkutekijät $p_i \equiv 3 \pmod 4$ ja luku b on erisuurten alkulujen $p_l \not\equiv 3 \pmod 4$ tulo. Nyt lauseen 3.1 ja apulauseen 3.2 perusteella luku b voidaan esittää kahden kokonaisluvun neliöiden summana. Kun luku a^2 voidaan kirjoittaa muodossa $a^2 = 0^2 + a^2$, niin apulauseen 3.2 nojalla myös luku $a^2 b = n$ voidaan esittää kahden kokonaisluvun neliöiden summana. Näin ollen väite on todistettu. □

Esimerkki 3.3. Tarkastellaan lukua $954845 = 5 \cdot 19^2 \cdot 23^2$. Luvun 954845 alkutekijöissä alkuluku $5 \equiv 1 \pmod 4$ sekä alkuluvut 19 ja 23 ovat kongruentteja luvun 3 kanssa modulo 4, mutta niiden eksponentit ovat parilliset. Näin ollen lauseen 3.2 perusteella luku 954845 voidaan esittää kahden kokonaisluvun neliöiden summana. Huomataan, että $5 = 1^2 + 2^2$, joten

$$\begin{aligned} 9548454 &= 5 \cdot 19^2 \cdot 23^2 \\ &= (1^2 + 2^2)(19 \cdot 23)^2 \\ &= (1 \cdot 19 \cdot 23)^2 + (2 \cdot 19 \cdot 23)^2 \\ &= (437)^2 + (874)^2. \end{aligned}$$

3.2 Neljän kokonaisluvun neliöiden summat

Kuten pykälässä 3.1 todettiin, kaikkia positiivisia kokonaislukuja ei voida esittää kahden kokonaisluvun neliöiden summana. Myöskään kolmen kokonaisluvun neliöiden summa ei riitä kaikkien positiivisten kokonaislukujen esittämiseen kokonaislukujen neliöiden summana. Esimerkiksi $6 = 2^2+1^2+1^2$, mutta lukua 7 ei voida esittää kolmen kokonaisluvun neliöiden summana. Vasta 1700-luvun lopulla ranskalainen matemaatikko Legendre todisti maanmiehensä Fermat'n väittämän, että positiivinen kokonaisluku k voidaan esittää kolmen kokonaisluvun neliöiden summana, jos ja vain jos luku k ei ole muotoa $4^n(8m+7)$, missä m ja n ovat ei-negatiivisia kokonaislukuja [2, s. 261].

Diofantos lienee otaksunut, että jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana. Kuitenkin ranskalainen Bachet oli ensimmäinen, joka esitti tämän selkeästi. Hän todisti otaksuman vuonna 1621 kaikille positiivisille kokonaisluvuille $n \leq 325$. [5, s. 606]

Euler pohti samaa ongelmaa yli neljän vuosikymmenen ajan vuodesta 1730 lähtien, mutta ei pystynyt todistamaan Diofantoksen otaksumaa. Euler kuitenkin julkaisi tärkeitä osatuloksia pitkän tutkimuksensa aikana. Hän todisti vuonna 1743, että tulo $(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2)$ voidaan esittää neljän kokonaisluvun neliöiden summana (ks. apulause 3.4). Kahdeksan vuotta myöhemmin Euler todisti, että kongruenssiyhtälö $x^2+y^2+1 \equiv 0 \pmod{p}$ on ratkeava kaikilla alkuluvuilla p (vrt. apulause 3.5). Osittain näiden tulosten avulla italialais-ranskalainen Lagrange todisti ensimmäisenä tämän tutkielman merkittävimmän lauseen; jokainen positiivinen kokonaisluku voidaan esittää (enintään) neljän kokonaisluvun neliöiden summana (ks. lause 3.4). Todistus julkaistiin vuonna 1770. [2, s. 261]

Tässä pykälässä tutkitaan neljän kokonaisluvun neliöiden summiin liittyviä ominaisuuksia alkaen Eulerin saavuttamista tuloksista.

Apulause 3.4. *Jos luvut m ja n voidaan esittää neljän kokonaisluvun neliöiden summana, niin myös tulo mn voidaan esittää vastaavasti.*

Todistus. Olkoon $m = a^2+b^2+c^2+d^2$ ja $n = e^2+f^2+g^2+h^2$, missä $a, b, \ldots, h \in \mathbb{Z}$. Silloin tulo mn voidaan kirjoittaa seuraavasti:

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2)\\ &= (ae+bf+cg+dh)^2 + (af-be+ch-dg)^2\\ &\quad + (ag-bh-ce+df)^2 + (ah+bg-cf-de)^2.\end{aligned} \tag{3.7}$$

Yhtälö (3.7) voidaan osoittaa oikeaksi, kertomalla sulut auki yhtälön molemmilta puolilta.

$$\begin{aligned}&(a^2+b^2+c^2+d^2)(e^2+f^2+g^2+h^2)\\ &= a^2e^2+a^2f^2+a^2g^2+a^2h^2\\ &\quad + b^2e^2+b^2f^2+b^2g^2+b^2h^2\\ &\quad + c^2e^2+c^2f^2+c^2g^2+c^2h^2\\ &\quad + d^2e^2+d^2f^2+d^2g^2+d^2h^2\end{aligned} \tag{3.8}$$

Jaetaan yhtälön (3.7) oikea puoli neljään osaan.

$$\begin{aligned}(ae+bf+cg+dh)^2 = a^2e^2+b^2f^2+c^2g^2+d^2h^2+2abef+2aceg\\ +2adeh+2bcfg+2bdfh+2cdgh.\end{aligned} \tag{3.9}$$

$$\begin{aligned}(af-be+ch-dg)^2 = a^2f^2+b^2e^2+c^2h^2+d^2g^2-2abef+2acfh\\ -2adfg-2bceh+2bdeg-2cdgh.\end{aligned} \tag{3.10}$$

$$\begin{aligned}(ag-bh-ce+df)^2 = a^2g^2+b^2h^2+c^2e^2+d^2f^2-2abgh-2aceg\\ +2adfg+2bceh-2bdfh-2cdef.\end{aligned} \tag{3.11}$$

$$(3.12)\quad \begin{aligned}(ah+bg-cf-de)^2 = a^2h^2+b^2g^2+c^2f^2+d^2e^2+2abgh-2acfh\\ -2adeh-2bcfg-2bdeg+2cdef.\end{aligned}$$

Kun nyt yhtälöiden (3.9) – (3.12) oikeat puolet lasketaan yhteen, kaksinkertaiset sekatermit $2abef, -2abef$ jne. supistuvat, joten yhteenlaskun summana saadaan yhtälön (3.8) oikea puoli. Näin apulause 3.4 on todistettu. □

Esimerkki 3.4. Luvut 14 ja 21 voidaan esittää neljän kokonaisluvun neliöiden summana seuraavasti: $14 = 3^2+2^2+1^2+0^2$ ja $21 = 4^2+2^2+1^2+0^2$. Nyt apulauseen 3.4 perusteella tulo $14 \cdot 21 = 294$ voidaan esittää neljän kokonaisluvun neliöiden summana. Saadaan

$$\begin{aligned}294 = 14\cdot 21 &= (3^2+2^2+1^2+0^2)(4^2+2^2+1^2+0^2)\\ &= (3\cdot 4+2\cdot 2+1\cdot 1+0\cdot 0)^2+(3\cdot 2-2\cdot 4+1\cdot 0-0\cdot 1)^2\\ &\quad +(3\cdot 1-2\cdot 0-1\cdot 4+0\cdot 2)^2+(3\cdot 0+2\cdot 1-1\cdot 2-0\cdot 4)^2\\ &= 17^2+(-2)^2+(-1)^2+0^2\\ &= 17^2+2^2+1^2+0^2.\end{aligned}$$

Apulause 3.5. *Jos alkuluku p on pariton, niin silloin on olemassa sellaiset kokonaisluvut x ja y, että*

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

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

Todistus. (Vrt. [5, s. 608].) Olkoon alkuluku p pariton ($p > 2$). Tarkastellaan joukkoa

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

Olkoot luvut r^2 ja s^2 erisuuria joukon A jäseniä siten että

$$r^2 \equiv s^2 \pmod{p}.$$

Tällöin oletuksen mukaan $r \equiv \pm s \pmod{p}$. Koska oletuksen mukaan myös $r \neq s$ ja $r, s < p$, niin kongruenssin määritelmän 2.5 nojalla $r \not\equiv s \pmod{p}$. Jos $r \equiv -s \pmod{p}$, niin kongruenssin määritelmän 2.5 perusteella $p|(r+s)$. Tämä on mahdotonta, sillä $0 < r+s < p$. Siis, mitkään kaksi joukon A eri jäsentä eivät ole kongruentteja keskenään modulo p. Vastaavasti mitkään kaksi joukon

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

eri jäsentä eivät ole kongruentteja keskenään modulo p.

Nyt joukkojen A ja B yhdiste $A \cup B$ sisältää yhteensä $\left(\frac{p+1}{2}\right)+\left(\frac{p+1}{2}\right) = p+1$ jäsentä. Nyt yleisen laatikkoperiaatteen nojalla kaksi joukon $A \cup B$ jäsentä ovat kongruentteja keskenään modulo p. Siksi on oltava niin, että jokin joukon A jäsen on kongruentti joukon B jonkin jäsenen kanssa modulo p eli

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

jollain kokonaisluvuilla x ja y, missä $0 \leq x, y < p/2$. Näin ollen

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

ja väite on todistettu. □

Apulauseesta 3.5 seuraa lause, joka on analoginen apulauseen 3.3 kanssa.

Seuraus 3.1. Jos alkuluku p on pariton, niin on olemassa sellainen positiivinen kokonaisluku $k < p$, että tulo kp voidaan esittää neljän kokonaisluvun neliöiden summana.

Todistus. (Vrt. [5, s. 608].) Oletetaan, että alkuluku p on pariton. Silloin apulauseen 3.5 mukaan on olemassa sellaiset kokonaisluvut x ja y, että

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

missä $0 \leq x < p/2$ ja $0 \leq y < p/2$. Näin ollen kongruenssin määritelmän 2.5 ja jaollisuuden määritelmän 2.1 perusteella

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

jollakin positiivisella kokonaisluvulla k. Siis, tulo kp on esitettävissä neljän kokonaisluvun neliöiden summana.

Osoitetaan vielä, että $k < p$. Arvioidaan nyt neliöiden summia ylöspäin muuttujien x ja y määritelmien avulla. Kun $0 \leq x, y < p/2$, niin

$$x^2 + y^2 + 1 < \left(\frac{p}{2}\right)^2 + \left(\frac{p}{2}\right)^2 + 1 = \frac{p^2}{2} + 1 < p^2.$$

Siis $kp < p^2$ ja näin ollen $k < p$. Siispä $kp = x^2 + y^2 + 1^2 + 0^2$, missä $k < p$. Näin väite on todistettu. □

Esimerkki 3.5. Olkoon alkuluku $p = 11$. Silloin apulauseen 3.5 mukainen joukko A voidaan kirjoittaa muodossa

$$A = \left\{ 0^2, 1^2, 2^2, 3^2, 4^2, 5^2 \right\} = \{ 0, 1, 4, 9, 16, 25 \}$$

ja joukko B vastaavasti

$$\begin{aligned} B &= \left\{ -1 - 0^2, -1 - 1^2, -1 - 2^2, -1 - 3^2, -1 - 4^2, -1 - 5^2 \right\} \\ &= \{ -1, -2, -5, -10, -17, -26 \}. \end{aligned}$$

Nyt apulauseen 3.5 perusteella jokin joukon A jäsen x^2 on kongruentti joukon B jonkin jäsenen $-1-y^2$ kanssa modulo p. Esimerkiksi $3^2 = 9 \equiv -2 = -1-1^2 \pmod{11}$ ja $1 + 3^2 + 1^2 \equiv 0 \pmod{11}$. Siis $x = 3$ ja $y = 1$. Seurauksen 3.1 mukaan on olemassa positiivinen kokonaisluku $k < p$ siten että

$$x^2 + y^2 + 1^2 + 0^2 = kp$$
$$3^2 + 1^2 + 1^2 + 0^2 = k \cdot 11$$

eli $k = 1 < 11 = p$.

Seuraava lause on analoginen lauseen 3.1 kanssa.

Lause 3.3. *Jokainen alkuluku voidaan esittää neljän kokonaisluvun neliöiden summana.*

Todistus. (Vrt. [5, s. 609].) Olkoon luku p alkuluku. Jos $p = 2$, niin $2 = 1^2 + 1^2 + 0^2 + 0^2$, joten väite on tosi, kun $p = 2$.
Oletetaan sitten, että alkuluku p on pariton ($p > 2$). Nyt positiivisten kokonaislukujen hyvinjärjestysperiaatteen ja seurauslauseen 3.1 nojalla on olemassa pienin positiivinen kokonaisluku m siten että

$$mp = w^2 + x^2 + y^2 + z^2, \tag{3.13}$$

joillakin kokonaisluvuilla w, x, y ja z, missä $1 \leq m < p$.

Oletetaan aluksi, että kyseinen positiivinen kokonaisluku m on parillinen. Tällöin myös tulo mp on parillinen. Koska $mp = w^2 + x^2 + y^2 + z^2$, niin kokonaisluvuilla w, x, y ja z pitää olla sama pariteetti (parillinen tai pariton) tai tasan kaksi em. kokonaisluvuista on parittomia.

Oletetaan, että $w \equiv x \pmod{2}$ ja $y \equiv z \pmod{2}$. Silloin kongruenssin määritelmän 2.5 nojalla

$$\frac{w+x}{2}, \quad \frac{w-x}{2}, \quad \frac{y+z}{2} \quad \text{ja} \quad \frac{y-z}{2}$$

ovat kokonaislukuja ja tällöin

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

Siis $\frac{m}{2}p$ voidaan esittää neljän kokonaisluvun neliöiden summana, missä $\frac{m}{2} < m$. Tämä on ristiriita, sillä oletuksen mukaan m on pienin sellainen positiivinen kokonaisluku, että $mp = w^2 + x^2 + y^2 + z^2$, joten m on pariton.

Osoitetaan seuraavaksi, että $m = 1$. Tehdään vastaoletus, että $m > 1$. Olkoot a, b, c ja d sellaisia ei-negatiivisia kokonaislukuja, että

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

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

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

Siis kongruenssin määritelmän 2.5 perusteella voidaan kirjoittaa

$$a^2 + b^2 + c^2 + d^2 = mn, \tag{3.14}$$

missä n on jokin ei-negatiivinen kokonaisluku ja

$$0 \leq a^2 + b^2 + c^2 + d^2 < 4\left(\frac{m}{2}\right)^2 = m^2.$$

Nyt koska $0 \leq mn < m^2$, niin $0 \leq n < m$.

Jos $n = 0$, niin silloin $a = b = c = d = 0$, joten $w \equiv x \equiv y \equiv z \equiv 0 \pmod{m}$. Tällöin $m^2|(w^2 + x^2 + y^2 + z^2)$, josta seuraa, että $m^2|mp$, joten $m|p$. Tämä on ristiriita, sillä $1 < m < p$ ja p on alkuluku. Näin ollen $n \geq 1$ ja $1 \leq n < m$.

Nyt yhtälöiden (3.13) ja (3.14) sekä apulauseen 3.4 avulla saadaan

$$\begin{aligned}&(w^2 + x^2 + y^2 + z^2)(a^2 + b^2 + c^2 + d^2)\\ &= (wa + xb + yc + zd)^2 + (wb - xa + yd - zc)^2\\ &\quad + (wc - xd - ya + zb)^2 + (wd + xc - yb - za)^2.\end{aligned}$$

Siksi tulo $(mp)(mn)$ voidaan kirjoittaa muodossa

$$(mp)(mn) = m^2np = r^2 + s^2 + t^2 + u^2, \tag{3.15}$$

missä

$$\begin{aligned}r &= wa + xb + yc + zd\\ s &= wb - xa + yd - zc\\ t &= wc - xd - ya + zb\\ u &= wd + xc - yb - za.\end{aligned}$$

Huomataan, että

$$r = wa + xb + yc + zd \equiv w^2 + x^2 + y^2 + z^2 \equiv 0 \pmod{m}.$$

Vastaavasti myös $s \equiv t \equiv u \equiv 0 \pmod{m}$, joten kokonaisluvut r, s, t ja u ovat kaikki jaollisia luvulla m. Näin ollen yhtälöstä (3.15) saadaan

$$\begin{aligned}np &= \left(\frac{r^2}{m^2}\right) + \left(\frac{s^2}{m^2}\right) + \left(\frac{t^2}{m^2}\right) + \left(\frac{u^2}{m^2}\right)\\ &= \left(\frac{r}{m}\right)^2 + \left(\frac{s}{m}\right)^2 + \left(\frac{t}{m}\right)^2 + \left(\frac{u}{m}\right)^2,\end{aligned}$$

missä $n < m$. Tämä on ristiriita, sillä oletuksen mukaan positiivinen kokonaisluku m on pienin sellainen kokonaisluku, että

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

joten $m = 1$. Näin ollen yhtälöstä (3.13) saadaan, että $p = w^2 + x^2 + y^2 + z^2$, joten mikä tahansa alkuluku p voidaan esittää neljän kokonaisluvun neliöiden summana. Väite on todistettu. □

Lause 3.4. *Jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana.*

Todistus. (Vrt. [5, s. 610].) Olkoon n positiivinen kokonaisluku. Jos $n = 1$, niin $1 = 1^2 + 0^2 + 0^2 + 0^2$, joten väite on tosi, kun $n = 1$.
Oletetaan sitten, että $n > 1$. Nyt määritelmän 2.4 mukaan positiivisen kokonaisluvun n kanoninen esitys voidaan kirjoittaa muodossa

$$n = \prod_i p_i^{a_i}, \tag{3.16}$$

missä alkuluvut p_i ovat luvun n alkutekijät ja jokainen eksponentti $a_i \in \mathbb{Z}_+$. Nyt lauseen 3.3 perusteella jokainen alkulukutekijä p_i voidaan esittää neljän kokonaisluvun neliöiden summana. Siksi apulauseen 3.4 nojalla $p_i^{a_i}$ voidaan esittää neljän kokonaisluvun neliöiden summana ja näin ollen myös tulo

$$\prod_i p_i^{a_i} = n$$

voidaan esittää neljän kokonaisluvun neliöiden summana. Siis väite on todistettu. □

Huomautus 3.2. Lähteen [5, s. 610] todistuksen alkupuolella esitetään kanoninen alkutekijäesitys positiiviselle kokonaisluvulle $n \geq 1$. Luvun n määrittely pitäisi kuitenkin olla $n \geq 2$, kuten kanonisen esityksen määritelmä 2.4 sen toteaa.

Esimerkki 3.6. Esitettävä luku 71687 neljän kokonaisluvun neliöiden summana.
Aritmetiikan peruslauseen nojalla luku 71687 voidaan jakaa alkulukutekijöihinsä, jolloin saadaan kanoninen esitys $71687 = 7^3 \cdot 11 \cdot 19$. Lisäksi tiedetään, että $7 = 2^2 + 1^2 + 1^2 + 1^2$, $11 = 3^2 + 1^2 + 1^2 + 0^2$ ja $19 = 4^2 + 1^2 + 1^2 + 1^2$. Nyt

$$\begin{aligned} 7^3 &= 7^2(2^2 + 1^2 + 1^2 + 1^2) \\ &= 14^2 + 7^2 + 7^2 + 7^2 \end{aligned}$$

ja apulauseen 3.4 mukaan tulo $11 \cdot 19$ voidaan kirjoittaa muodossa

$$\begin{aligned}
11 \cdot 19 &= (3^2 + 1^2 + 1^2 + 0^2)(4^2 + 1^2 + 1^2 + 1^2) \\
&= (3 \cdot 4 + 1 \cdot 1 + 1 \cdot 1 + 0 \cdot 1)^2 + (3 \cdot 1 - 1 \cdot 4 + 1 \cdot 1 - 0 \cdot 1)^2 \\
&\quad + (3 \cdot 1 - 1 \cdot 1 - 1 \cdot 4 + 0 \cdot 1)^2 + (3 \cdot 1 + 1 \cdot 1 - 1 \cdot 1 - 0 \cdot 4)^2 \\
&= 14^2 + 0^2 + (-2)^2 + 3^2 \\
&= 14^2 + 3^2 + 2^2 + 0^2.
\end{aligned}$$

Näin ollen luku 71687 voidaan kirjoittaa apulauseen 3.4 perusteella seuraavasti:

$$\begin{aligned}
71687 &= 7^3 \cdot 11 \cdot 19 \\
&= (14^2 + 7^2 + 7^2 + 7^2)(14^2 + 3^2 + 2^2 + 0^2) \\
&= (14 \cdot 14 + 7 \cdot 3 + 7 \cdot 2 + 7 \cdot 0)^2 + (14 \cdot 3 - 7 \cdot 14 + 7 \cdot 0 - 7 \cdot 2)^2 \\
&\quad + (14 \cdot 2 - 7 \cdot 0 - 7 \cdot 14 + 7 \cdot 3)^2 + (14 \cdot 0 + 7 \cdot 2 - 7 \cdot 3 - 7 \cdot 14)^2 \\
&= 231^2 + (-70)^2 + (-49)^2 + (-105)^2 \\
&= 231^2 + 105^2 + 70^2 + 49^2.
\end{aligned}$$

4 Waringin probleema

Vuonna 1770 englantilainen matemaatikko Edward Waring julkaisi kirjassaan *Meditationes Algebraicae* otaksuman, joka tänä päivänä tunnetaan Waringin probleemana. Waring esitti tuolloin ongelman, jonka mukaan jokainen positiivinen kokonaisluku voidaan esittää enintään neljän (kokonaisluvun) neliön, yhdeksän kuution, jopa 19 kokonaisluvun neljännen potenssin jne. summana. Tämän otaksuman on tulkittu tarkoittavan seuraavaa: onko jokaista luonnollista lukua k kohti olemassa sellainen luku $g(k)$, että jokainen positiivinen kokonaisluku voidaan esittää enintään $g(k)$:n ei-negatiivisen kokonaisluvun k:nnen potenssin summana? Toisin sanoen jokainen positiivinen kokonaisluku n voidaan esittää ainakin yhdellä tavalla seuraavasti:

$$n = a_1^k + a_2^k + \cdots + a_{g(k)}^k,$$

missä $a_1, a_2, \ldots, a_{g(k)}$ ovat ei-negatiivisia kokonaislukuja (voivat olla samoja). Lisäksi huomataan, että vakio $g(k)$ riippuu vain luvusta k, ei esitettävästä luvusta n. [2, s. 266]

Saksalainen David Hilbert todisti Waringin probleeman vasta vuonna 1909. Hänen todistuksensa on laaja ja monimutkainen, eikä se anna vakion $g(k)$ lauseketta. [5, s. 611] Pykälän 3.2 lauseessa 3.4 todistettiin Waringin probleeman tapaus $g(2) = 4$ eli jokainen positiivinen kokonaisluku voidaan esittää enintään neljän kokonaisluvun neliöiden summana. Vuonna 1912 saksalainen A. Wieferich ja englantilainen A. J. Kempner osoittivat, että $g(3) = 9$ eli jokainen positiivinen kokonaisluku voidaan esittää enintään 9 kokonaisluvun kuutioiden summana [5, s. 611].

Seuraavassa lauseessa todistetaan, että $g(4) \leq 53$. Tämän todisti ensimmäisenä ranskalainen matemaatikko Joseph Liouville vuonna 1859. [2, s. 266]

Lause 4.1. *Jokainen positiivinen kokonaisluku voidaan esittää 53 kokonaisluvun neljännen potenssin summana.*

Todistus. (Vrt. [6, s. 251].) Väitteen todistamiseksi tarvitaan seuraavaa tietoa

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 &= 6(a^2+b^2+c^2+d^2)(a^2+b^2+c^2+d^2) \\ &= 6(a^4+2a^2b^2+2a^2c^2+2a^2d^2+b^4 \\ &\quad +2b^2c^2+2b^2d^2+c^4+2c^2d^2+d^4) \\ &= 6(a^4+b^4+c^4+d^4) \\ &\quad +12(a^2b^2+a^2c^2+a^2d^2+b^2c^2+b^2d^2+c^2d^2). \end{aligned} \tag{4.1}$$

Newtonin binomikaavaa apuna käyttäen voidaan kirjoittaa

$$(a \pm b)^4 = a^4 \pm 4a^3b + 6a^2b^2 \pm 4ab^3 + b^4. \tag{4.2}$$

Nyt yhtälön (4.2) avulla yhtälö (4.1) voidaan esittää 12 kokonaisluvun neljännen potenssin summana seuraavasti

$$\begin{aligned} 6(a^2+b^2+c^2+d^2)^2 &= (a+b)^4+(a-b)^4+(a+c)^4+(a-c)^4 \\ &\quad +(a+d)^4+(a-d)^4+(b+c)^4+(b-c)^4 \\ &\quad +(b+d)^4+(b-d)^4+(c+d)^4+(c-d)^4. \end{aligned} \tag{4.3}$$

Nyt lauseen 3.4 perusteella jokainen positiivinen kokonaisluku voidaan esittää neljän kokonaisluvun neliöiden summana. Merkitään tätä lausekkeella $a^2 + b^2 + c^2 + d^2$. Yhtälöstä (4.3) havaitaan, että jokainen kokonaisluku, joka on kuusi kertaa jonkin kokonaisluvun $(a^2 + b^2 + c^2 + d^2)$ neliö, voidaan esittää 12 kokonaisluvun neljännen potenssin summana.

Olkoon nyt n mielivaltainen positiivinen kokonaisluku. Määritellään luku n seuraavasti

$$n = 6s + r, \tag{4.4}$$

missä $0 \leq r < 6$ ja $s \in \mathbb{Z}_+$. Koska s on positiivinen kokonaisluku, niin lauseen 3.4 perusteella se voidaan esittää neljän kokonaisluvun neliöiden summana. Merkitään $s = w^2 + x^2 + y^2 + z^2$. Näin ollen yhtälö (4.4) voidaan kirjoittaa muodossa

$$n = 6w^2 + 6x^2 + 6y^2 + 6z^2 + r. \tag{4.5}$$

Nyt yhtälön (4.5) oikean puolen ensimmäiset neljä termiä voidaan esittää yhtälön (4.3) perusteella 12 kokonaisluvun neljännen potenssin summana. Koska luku r, joka on korkeintaan 5, voidaan esittää viiden kokonaisluvun neljännen potenssin summana, niin mielivaltainen positiivinen kokonaisluku n voidaan esittää $12+12+12+12+5 = 53$ kokonaisluvun neljännen potenssin summana. Näin väite on todistettu. □

Liouvillen tulosta, $g(4) \leq 53$, on myöhemmin tarkennettu useampaan kertaan. Amerikkalainen H. E. Thomas osoitti vuonna 1974, että $g(4) \leq 22$. Kaksitoista vuotta myöhemmin intialainen R. Balasubramanian sekä ranskalaiset J. Deshouillers ja F. Dress todistivat, että $g(4) = 19$. [5, s. 612]

Tutkittaessa tapausta $g(3) = 9$ on havaittu, että luvut

$$23 = 2 \cdot 2^3 + 7 \cdot 1^3 \text{ ja}$$
$$239 = 2 \cdot 4^3 + 4 \cdot 3^3 + 3 \cdot 1^3$$

ovat ainoat positiiviset kokonaisluvut, jotka vaativat 9 ei-negatiivista kokonaislukua, jotta luvut voidaan esittää kuutioiden summana. Lisäksi on todettu, että lukua 239 suuremmat kokonaisluvut voidaan esittää 8 ei-negatiivisen kokonaisluvun kuutioiden summana. Vuonna 1942 venäläinen Y. Linnik todisti, että vain äärellinen joukko kokonaislukuja vaatii 8 kuutiota. Jostakin luvusta lähtien riittää vain 7 ei-negatiivista kokonaislukua, jotta luku voidaan esittää kuutioiden summana. [2, s. 266]

Matemaatikkoja on kiehtonut tieto: kun $k \geq 3$, niin kaikki kyllin suuret kokonaisluvut vaativat vähemmän kuin $g(k)$ ei-negatiivista kokonaislukua, jotta ne voidaan esittää k:nnen potenssin summana. On ollut tarpeellista määrittää vakio $G(k)$, joka merkitsee sellaista positiivista kokonaislukua s, että kaikki kyllin suuret kokonaisluvut voidaan esittää enintään s:n ei-negatiivisen kokonaisluvun k:nnen potenssin summana. Havaitaan, että $G(k) \leq g(k)$. Vakion $G(k)$ tarkkoja arvoja tiedetään vain kaksi, $G(2) = 4$ ja $G(4) = 16$. Muilla luonnollisen luvun k arvoilla vakiolle $G(k)$ on pystytty tähän päivään mennessä määrittämään vain ylä- ja alarajoja. Taulukossa 1 on listattu ensimmäiset kahdeksan vakion $g(k)$ arvot sekä vakion $G(k)$ arvot ylä- ja alarajoineen. [2, s. 267]

$g(k)$	$G(k)$
$g(2) = 4$	$G(2) = 4$
$g(3) = 9$	$4 \leq G(3) \leq 7$
$g(4) = 19$	$G(4) = 16$
$g(5) = 37$	$6 \leq G(5) \leq 17$
$g(6) = 73$	$9 \leq G(6) \leq 24$
$g(7) = 143$	$8 \leq G(7) \leq 33$
$g(8) = 279$	$32 \leq G(8) \leq 42$

Taulukko 1: Vakioiden $g(k)$ ja $G(k)$ arvoja, kun $2 \leq k \leq 8$ (vrt. [2, s. 267]).

Viitteet

[1] Burn, R.P.: *A Pathway into Number Theory*. 2nd ed. Cambridge University Press, 1997.

[2] Burton, D.M.: *Elementary Number Theory*. 5th ed. New York: McGraw-Hill Companies, Inc., 2005.

[3] Haukkanen, P.: *Algebra I*, luentomoniste. Tampereen yliopisto.
`http://mtl.uta.fi/Opetus/Algebra/algI04.pdf`
[viitattu 23.2.2011]

[4] Haukkanen, P.: *Lukuteoriaa*, luentomoniste. Tampereen yliopisto.
`http://mtl.uta.fi/Opetus/Algebra/Lukuteoria/lukuteoria.pdf`
[viitattu 23.2.2011]

[5] Koshy, T.: *Elementary Number Theory with Applications*. 2nd ed. Burlington: Academic Press, 2007.

[6] Vanden Eynden, C.: *Elementary Number Theory*. 2nd ed. New York: McGraw-Hill Companies, Inc., 2001.