Tampereen yliopisto

Ilpo Lehtimäki

PYTHAGORAAN KOLMIKOISTA JA MATRIISEISTA

Informaatioteknologian ja viestinnän tiedekunta
Kandidaattitutkielma
Maaliskuu 2021

Tiivistelmä

Ilpo Lehtimäki:Pythagoraan kolmikoista ja matriiseista
Kandidaattitutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Maaliskuu 2021

Tässä tutkielmassa käsitellään Pythagoraan lauseen toteuttavien kolmikoita eli kolmikoita, jotka toteuttavat yhtälön $x^2 + y^2 = z^2$. Pythagoraan kolmikoissa luvut ovat positiivisia kookonaislukuja ja toteuttavat Pythagoraan yhtälön. Näitä kolmikoita on ääretön määrä.

Luvussa 2 esitetään luettelomaisesti aiheen käsittelyssä tarvittavia määritelmiä ja lauseita. Näistä tutkielmassa merkittävimpiä ovat suurin yhteinen tekijä, vektoriavaruus, ominaisarvot ja matriisin karakteristinen yhtälö.

Luvussa 3 tutustutaan ensin Pythagoraan lauseen toteuttaviin positiivisten kokonaislukujen kolmikoihin ja primitiivisiin Pythagoraan kolmikoihin. Primitiivisen Pythagoraan kolmikon suurin yhteinen tekijä on 1. Seuraavaksi todistetetaan apulauseita, joita tarvitaan päälauseen todistuksessa. Ensin todistetaan apulause, jonka mukaan primitiivisen Pythagoraan kolmikon luvut ovat pareittain keskenään jaottomia. Seuraavaksi todistetaan, että primitiivisessä Pythagoraan kolmikossa x on pariton ja y parillinen, tai päinvastoin. Viimeisenä apulauseena todistetaan aritmetiikan peruslauseen seuraus, jonka mukaan jos kahden keskenään jaottoman kokonaisluvun tulo on jonkin luvun neliö, niin molemmat luvut ovat joidenkin lukujen neliöitä. Tämän jälkeen todistetaan lause, jolla voidaan generoida mikä tahansa primitiivinen Pythagoraan kolmikko.

Luvussa 4 käsitellään kokonaislukualkioisten neliömatriisien kolmikoita, jotka toteuttavat yhtälön $A^2 + B^2 = C^2$. Myös näitä kolmikoita kutsutaan Pythagoraan kolmikoiksi ja niitä on ääretön määrä. Luvussa todistetaan lause, jolla voidaan generoida mikä tahansa kokonaislukualkioisten neliöämatriisien Pythagoraan kolmikko. Tämän lauseen todistusta varten todistetaan yksi aputulos. Apulauseessa todistetaan, että jokainen matriisi P voidaan esittää muodossa $P = 2(UV + VU)$, missä U ja V ovat tietynlaisia neliömatriiseja. Tutkielman on kirjoitettu Rosenin kirjaa Elementary

number theory and its applications ja Arnoldin ja Eudelzonin artikkelia On matrix Pythagorean triples mukaillen.

Avainsanat: Pythagoraan kolmikot, matriisit, Pythagoraan lause

Tämän julkaisun alkuperäisyys on tarkastettu Turnitin OriginalityCheck -ohjelmalla.

Sisällys

1 Johdanto **5**

2 Esitietoja **6**

2.1 Lukuteorian perusteita 6

2.1.1 Jaollisuus 6

2.1.2 Kongruenssi 6

2.1.3 Alkuluvut 7

2.1.4 Suurin yhteinen tekijä 7

2.2 Lineaarialgebran perusteita 8

2.2.1 Vektoriavaruus 8

2.2.2 Ominaisarvot ja ominaisvektorit 10

3 Pythagoraan kolmikot **11**

4 Pythagoraan matriisit **16**

Lähteet **19**

1 Johdanto

Pythagoraan lauseen mukaan suorakulmaisen kolmioiden sivuille pätee yhtälö $x^2 + y^2 = z^2$. Tässä tutkielmassa tarkastellaan Pythagoraan lauseen toteuttavia positiivisten kokonaislukujen kolmikoita, sekä Pythagoraan lauseen toteuttavia matriisien kolmikoita.

Luvussa 2 esitetään valmisteluna tarvittavia lukuteorian ja lineaarialgebran määritelmiä ja lauseita, joita tarvitaan luvuissa 3 ja 4.

Luvussa 3 todistetaan kaava, jolla voidaan generoida kaikki Pythagoraan lauseen toteuttavat positiivisten kokonaislukujen kolmikot. Näitä kolmikoita kutsutaan Pythagoraan kolmikoiksi ja niitä on ääretön määrä.

Luvussa 4 sovellamme luvussa 3 todistettua kaavaa ja todistamme kaavan, jolla voidaan generoida mikä tahansa neliömatriisien kolmikko, joka toteuttaa Pythagoraan lauseen matriisen tulon suhteen.

Lukijan odotetetaan tuntevan lukuteorian ja lineaarialgebran perusteet. Pääläh-deteoksina käytetään luvussa 3 Rosenin kirjaa Elementary number theory and its applications ja luvussa 4 Arnoldin ja Eudelzonin artikkelia On matrix Pythagorean triples.

2 Esitietoja

Luvussa 2 käsitellään tutkielman aiheen käsittelyssä tarvittavia lukuteorian ja lineaarialgebran perusteita. Luvussa esitetään määritelmät jaollisuudelle, kongruenssille, alkuluvuille ja suurimmalle yhteiselle tekijälle, sekä näihin liittyviä lauseita. Lisäksi esitetään aritmetiikan peruslause. Luvun tiedot ovat peräisin lähteestä [4].

2.1 Lukuteorian perusteita

2.1.1 Jaollisuus

Määritelmä 2.1 (vrt. [4, s. 36–37])**.** Olkoot $a, b \in \mathbb{Z}$ ja olkoon $a \neq 0$. Sanotaan, että *a jakaa b:n*, jos on olemassa $c \in \mathbb{Z}$ siten, että $b = ac$. Jos a jakaa b:n, sanotaan myös, että a on b:n *jakaja* tai *tekijä*. Lisäksi sanotaan, että a on b:n *monikerta* ja b on *jaollinen* luvulla a.

Jos a jakaa b:n merkitään $a \mid b$. Jos b ei ole jaollinen a:lla merkitään $a \nmid b$.

Lause 2.1. *Jos $a, b, c \in \mathbb{Z}$ siten, että $a \mid b$ ja $b \mid c$, niin $a \mid c$.*

Todistus (ks. [4, s. 37]). □

Lause 2.2. *Jos $a, b, c, m, n \in \mathbb{Z}$ siten, että $c \mid a$ ja $c \mid b$, niin $c \mid (ma + nb)$.*

Todistus (ks. [4, s. 37]). □

2.1.2 Kongruenssi

Määritelmä 2.2 (vrt. [4, s. 145])**.** Olkoon $m \in \mathbb{Z}_+$. Jos $a, b \in \mathbb{Z}$ ja $m \mid (a - b)$, sanotaan a:n *olevan kongruentti modulo m* luvun b kanssa.

Jos a on kongruentti b:n kanssa modulo m, merkitään $a \equiv b \pmod{m}$. Jos $m \nmid (a - b)$, niin merkitään $a \not\equiv b \pmod{m}$.

Lause 2.3. *Jos $a, b \in \mathbb{Z}$, niin $a \equiv b \pmod{m}$, jos ja vain jos on olemassa $k \in \mathbb{Z}$ siten, että $a = b + km$.*

Todistus (ks. [4, s. 146]). □

Lause 2.4. *Jos $a, b, c, d, m \in \mathbb{Z}$ ja $m > 0$ siten, että $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$, niin*

(i) $a + c \equiv b + d \pmod{m}$,

(ii) $a - c \equiv b - d \pmod{m}$,

(iii) $ac \equiv bd \pmod{m}$.

Todistus (ks. [4, s. 149]). □

2.1.3 Alkuluvut

Määritelmä 2.3 (vrt. [4, s. 70])). Lukua 1 suurempia kokonaislukuja, jotka ovat jaollisia vain itsellään, vastaluvuillaan ja luvulla 1 sanotaan *alkuluvuiksi*.

Esimerkki 2.1 (vrt. [4, s. 70])). Kokonaisluvut 2, 3, 5, 13, 101 ja 163 ovat alkulukuja.

Lause 2.5. *Alkulukuja on ääretön määrä.*

Todistus (ks. [4, s. 71]). □

Lause 2.6 (Aritmetiikan peruslause). *Jokainen lukua 1 suurempi positiivinen kokonaisluku voidaan esittää yksikäsitteisenä alkulukujen tulona tekijöiden järjestystä lukuun ottamaatta. Tätä esitystä sanotaan* alkulukuhajotelmaksi.

Todistus (ks. [4, s. 112–133]). □

2.1.4 Suurin yhteinen tekijä

Määritelmä 2.4 (vrt. [4, s. 39])). Olkoot $a, b \in \mathbb{Z}$ siten, että $a \neq 0$ ja $b \neq 0$. Lukujen a ja b *suurin yhteinen tekijä* on suurin kokonaisluku, joka jakaa a:n ja b:n. Olkoon lukujen a ja b suurina yhteinen tekijä k. Tällöin merkitään $\mathrm{syt}(a, b) = k$.

Määritelmä 2.5 (vrt. [4, s. 39])). Olkoot $a, b \in \mathbb{Z}$ siten, että $a \neq 0$ ja $b \neq 0$. Lukujen a ja b sanotaan olevan *keskenään jaottomia*, jos $\mathrm{syt}(a, b) = 1$.

Määritelmä 2.6 (vrt. [4, s. 39])). Olkoot $a_1, a_2, ..., a_n \in \mathbb{Z}$ siten, että kaikki luvut eivät ole nollia. Tällöin *suurin yhteinen tekijä* on suurin kokonaisluku, joka jakaa kaikki joukon luvut.

Apulause 2.1. Olkoot $a_1, a_2, ..., a_n \in \mathbb{Z}$ siten, että kaikki luvut eivät ole nollia. Tällöin $\mathrm{syt}(a_1, a_2, ..., a_{n-1}, a_n) = \mathrm{syt}(a_1, a_2, ..., a_{n-2}, \mathrm{syt}(a_{n-1}, a_n)$.

Todistus (ks. [4, s. 98]). □

2.2 Lineaarialgebran perusteita

2.2.1 Vektoriavaruus

Määritelmä 2.7 (vrt. [1, s. 184])**.** Olkoon V epätyhjä joukko, jossa on määritelty operaatiot yhteenlasku ja skalaarilla kertominen. Joukkoa V sanotaan *vektoriavaruudeksi*, jos seuraavat ehdot ovat voimassa.

1. Jos $\boldsymbol{u}, \boldsymbol{v} \in V$, niin $\boldsymbol{u} + \boldsymbol{v} \in V$
2. $\boldsymbol{u} + \boldsymbol{v} = \boldsymbol{v} + \boldsymbol{u}$
3. $\boldsymbol{u} + (\boldsymbol{v} + \boldsymbol{w}) = (\boldsymbol{u} + \boldsymbol{v}) + \boldsymbol{w}$
4. $\exists \mathbf{0} \in V : \forall \boldsymbol{u} \in V : \mathbf{0} + \boldsymbol{u} = \boldsymbol{u} + \mathbf{0} = \boldsymbol{u}$
5. $\forall \boldsymbol{u} \in V : \exists - \boldsymbol{u} \in V : \boldsymbol{u} + (-\boldsymbol{u}) = (-\boldsymbol{u}) + \boldsymbol{u} = \mathbf{0}$
6. Jos k on skalaari ja $\boldsymbol{u} \in V$, niin $k\boldsymbol{u} \in V$.
7. $k(\boldsymbol{u} + \boldsymbol{v}) = k\boldsymbol{u} + k\boldsymbol{v}$
8. $(k + m)\boldsymbol{u} = k\boldsymbol{u} + m\boldsymbol{u}$
9. $k(m\boldsymbol{u}) = h(km)\boldsymbol{u}$
10. $1\boldsymbol{u} = \boldsymbol{u}$,

kun $\boldsymbol{u}, \boldsymbol{v}, \boldsymbol{w} \in V$ ja $k, m \in \mathbb{R}$. Alkioita $\boldsymbol{u} \in V$ sanotaan *vektoreiksi*. Vektoria $\mathbf{0} \in V$ sanotaan *nollavektoriksi*. Vektoria $-\boldsymbol{u} \in V$ sanotaan vektorin $\boldsymbol{u} \in V$ *vastavektoriksi*. Lukua $k \in \mathbb{R}$ sanotaan *skalaariksi*.

Esimerkki 2.2 (vrt. [1, s. 185])**.** Joukko $V = \mathbb{R}^n$ on vektoriavaruus, jossa operaatiot ovat

$$\boldsymbol{u} + \boldsymbol{v} = (u_1, u_2, ..., u_n) + (v_1, v_2, ..., v_n) = (u_1 + v_1, u_2 + v_2, ..., u_n + v_n)$$

ja

$$k\boldsymbol{u} = (ku_1, ku_2, ..., ku_n),$$

kun $\boldsymbol{u}, \boldsymbol{v} \in \mathbb{R}^n$ ja $k \in \mathbb{R}$. Tällöin joukko $V = \mathbb{R}^n$ toteuttaa kaikki määritelmän 2.7 aksioomat.

Määritelmä 2.8 (vrt. [1, s. 191])**.** Olkoon V vektoriavaruus ja $\emptyset \neq W \subseteq V$. Tällöin W on vektoriavaruuden V *aliavaruus*, jos W itsessään on vektoriavaruus avaruudessa V määriteltyjen operaatioiden suhteen.

Lause 2.7 (Aliavaruuskriteeri)**.** *Olkoon V vektoriavaruus ja $\emptyset \neq W \subseteq V$. Tällöin W on avaruuden V aliavaruus, jos ja vain jos seuraavat ehdot ovat voimassa.*

i. Jos $\boldsymbol{u}, \boldsymbol{v} \in W$, niin $\boldsymbol{u} + \boldsymbol{v} \in W$.

ii. Jos k on skalaari ja $\boldsymbol{u} \in W$, niin $k\boldsymbol{u} \in W$.

Todistus (ks. [1, s. 192]). □

Määritelmä 2.9 (vrt. [1, s. 195])**.** Olkoon $\boldsymbol{w}$ vektoriavaruuden V vektori. Vektorin $\boldsymbol{w}$ sanotaan vektoreiden $\boldsymbol{v}_1, \boldsymbol{v}_2, ..., \boldsymbol{v}_r \in V$ *lineaarikombinaatioksi*, jos $\boldsymbol{w}$ voidaan esittää muodossa

$$\boldsymbol{w} = k_1\boldsymbol{v}_1 + k_2\boldsymbol{v}_2 + ... + k_r\boldsymbol{v}_r,$$

missä $k_1, k_2, ..., k_r \in \mathbb{R}$ ovat skalaareja.

Määritelmä 2.10 (vrt. [1, s. 203])**.** Jos $S = \{\boldsymbol{v}_1, \boldsymbol{v}_2, ..., \boldsymbol{v}_r\}$ on kahden tai useamman vektorin joukko vektoriavaruudessa V, niin joukon S sanotaan olevan *lineaarisesti riippumaton*, jos yhtäkään joukon S vektoria ei voida esittää muiden joukon vektorien lineaarikombinaationa. Jos joukko ei ole lineaarisesti riippumaton, sanotaan sen olevan *linearisesti riippuva*.

Lause 2.8. *Epätyhjä joukko $S = \{\boldsymbol{v}_1, \boldsymbol{v}_2, ..., \boldsymbol{v}_r\}$ vektoriavaruudessa V on lineaarisesti riippumaton, jos ja vain jos yhtälön*

$$k_1\boldsymbol{v}_1 + k_2\boldsymbol{v}_2 + ... + k_r\boldsymbol{v}_r = 0$$

ainoa ratkaisu on $k_1 = k_2 = ... = k_r = 0$.

Todistus (ks. [1, s. 210]). □

Määritelmä 2.11 (vrt. [1, s. 214])**.** Olkoon $S = \{\boldsymbol{v}_1, \boldsymbol{v}_2, ..., \boldsymbol{v}_n\}$ äärellinen joukko vektoreita vektoriavaruudessa V. Tällöin S:n sanotaan olevan V:n *kanta*, jos:

i. S virittää V:n,

ii. S on lineaarisesti riippumaton.

2.2.2 Ominaisarvot ja ominaisvektorit

Määritelmä 2.12 (vrt. [1, s. 291])**.** Olkoon A $n \times n$-matriisi. Tällöin vektoria $\boldsymbol{x} \in \mathbb{R}^n \setminus \{\boldsymbol{0}\}$ sanotaan A:n *ominaisvektoriksi*, jos $A\boldsymbol{x}$ on vektorin $\boldsymbol{x}$ skalaarimonikerta, toisin sanoen

$$A\boldsymbol{x} = \lambda \boldsymbol{x}$$

jollakin skalaarilla $\lambda \in \mathbb{R}$. Skalaaria λ sanotaan matriisin A *ominaisarvoksi* ja vektoria $\boldsymbol{x}$ sanotaan *ominaisarvoa λ vastaavaksi ominaisvektoriksi*.

Esimerkki 2.3 (vrt. [1, s. 292])**.** Vektori $\boldsymbol{x} = \begin{bmatrix} 1 \\ 2 \end{bmatrix}$ on matriisin

$$A = \begin{bmatrix} 3 & 0 \\ 8 & -1 \end{bmatrix}$$

ominaisarvoa $\lambda = 3$ vastaava ominaisvektori, koska

$$A\boldsymbol{x} = \begin{bmatrix} 3 & 0 \\ 8 & -1 \end{bmatrix} \begin{bmatrix} 1 \\ 2 \end{bmatrix} = \begin{bmatrix} 3 \\ 6 \end{bmatrix} = 3\boldsymbol{x}.$$

Geometrisesti havaitaan, että kerrottaessa A:lla vektorin $\boldsymbol{x}$ kasvaa kolminkertaiseksi.

Lause 2.9. *Olkoon A $n \times n$-matriisi. Tällöin λ on $A : n$ ominaisarvo jos ja vain jos λ toteuttaa yhtälön*

$$\det(\lambda I - A) = 0.$$

Tämän sanotaan olevan A:n karakteristinen yhtälö.

Todistus (ks. [1, s. 292]). □

3 Pythagoraan kolmikot

Pythagoraan lauseen mukaan suorakulmaisen kolmion kateettien neliöidensumma on yhtäsuuri kuin hypotenuusan neliö. Jotta voitaisiin löytää kaikki suorakulmaiset kolmiot, joiden sivujen pituudet ovat positiivisia kokonaislukuja, on löydettävä kaikki positiivisten kokonaislukujen kolmikot (x, y, z), jotka toteuttavat yhtälön $x^2+y^2 = z^2$.

Luvun tiedot on yhdistetty lähteistä [3] ja [4].

Määritelmä 3.1. *Pythagoraan kolmikoksi* sanotaan sellaista positiivisten kokonaislukujen kolmikkoa (x, y, z), joka toteuttaa yhtälön $x^2 + y^2 = z^2$.

Esimerkki 3.1. Kolmikot $(3, 4, 5)$ ja $(7, 24, 25)$ ovat Pythagoraan kolmikoita, sillä $3^2 + 4^2 = 5^2$ ja $7^2 + 24^2 = 25^2$.

Määritelmä 3.2. Pythagoraan kolmikko on *primitiivinen*, jos $\mathrm{syt}(x, y, z) = 1$.

Esimerkki 3.2. Pythagoraan kolmikot $(3, 4, 5)$ ja $(5, 12, 13)$ ovat primitiivisiä, sillä $\mathrm{syt}(3, 4, 5) = 1$ ja $\mathrm{syt}(5, 12, 13) = 1$. Pythagoraan kolmikko $(6, 8, 10)$ puolestaan ei ole primitiivinen, koska $\mathrm{syt}(6, 8, 10) = 2$.

Olkoon (x, y, z) Pythagoraan kolmikko siten, että $\mathrm{syt}(x, y, z) = d$. Tällöin on olemassa kokonaisluvut x_1, y_1, z_1 siten, että $x = dx_1$, $y = dy_1$, $z = dz_1$ ja $\mathrm{syt}(x_1, y_1, z_1) = 1$. Lisäksi, koska

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

niin myös

$$(x/d)^2 + (y/d)^2 = (x/d)^2,$$

joten

$$x_1^2 + y_1^2 = x_1^2.$$

Näin ollen (x_1, y_1, z_1) on primitiivinen Pythagoraan kolmikko ja kolmikko (x, y, z) on tämän primitiivisen Pythagoraan kolmikon monikerta.

Huomataan, että primitiivisen (tai minkä tahansa) Pythagoraan kolmikon monikerta on myös Pythagoraan kolmikko. Olkoon (x_1, y_1, z_1) primitiivinen Pythagoraan kolmikko. Tällöin

$$x_1^2 + y_1^2 = z_1^2,$$

joten

$$(dx_1)^2 + (dy_1)^2 = (dz_1)^2,$$

eli (dx_1, dy_1, dz_1) on Pythagoraan kolmikko.

Tästä seurauksena kaikki Pythagoraan kolmikot voidaan löytää muodostamalla primitiivisien Pythagoraan kolmikoiden monikertoja. Kaikkien primitiivisien Pythagoraan kolmikoiden löytämiseen tarvitaan seuraavia apulauseita.

Apulause 3.1. Jos (x, y, z) on primitiivinen Pythagoraan kolmikko, niin $\operatorname{syt}(x, y) = \operatorname{syt}(x, z) = \operatorname{syt}(y, z) = 1$.

Todistus (vrt. [4, s. 523]). Olkoon (x, y, z) primitiivinen Pythagoraan kolmikko ja $\operatorname{syt}(x, y) > 1$. Tällöin on olemassa alkuluku p siten, että $p \mid \operatorname{syt}(x, y)$, jolloin $p \mid x$ ja $p \mid y$. Tästä seuraa, että $p \mid (x^2 + y^2) = z^2$. Eli $p \mid z^2$, joten $p \mid z$. Tämä on ristiriita, sillä $\operatorname{syt}(x, y, z) = 1$. Näin ollen $\operatorname{syt}(x, y) = 1$. Samaan tapaan voidaan osoittaa $\operatorname{syt}(x, z) = \operatorname{syt}(y, z) = 1$. □

Apulause 3.2. Jos (x, y, z) on primitiivinen Pythagoraan kolmikko, niin x on parillinen ja y on pariton tai x on pariton ja y on parillinen.

Todistus (vrt. [4, s. 523–524]). Olkoon (x, y, z) primitiivinen Pythagoraan kolmikko. Apulauseen 3.1 nojalla $\operatorname{syt}(x, y) = 1$. Siis x ja y eivät voi molemmat olla parillisia. Myöskään x ja y eivät voi molemmat olla parittomia. Oletetaan, että x ja y olisivat molemmat parittomia. Tällöin on voimassa

$$x^2 \equiv y^2 \equiv 1 \pmod 4.$$

Nimittäin, koska x on pariton, se on muotoa $x = 2k + 1$. Siis $x^2 = 4k^2 + 4k + 1 \equiv 1 \pmod 4$. Joten

$$z^2 = x^2 + y^2 \equiv 2 \pmod 4.$$

Tämä on mahdotonta, sillä jos z on parillinen, niin $z^2 \equiv 0 \pmod 4$. Jos z on pariton, niin $z^2 \equiv 1 \pmod 4$. Näin ollen x on parillinen ja y on pariton tai x on pariton ja y on parillinen. □

Viimeinen tarvittava apulause on aritmetiikan peruslauseen (lause 2.6) seuraus. Lauseen mukaan jos kahden keskenään jaottoman kokonaisluvun tulo on jonkun luvun neliö, niin molempien lukujen täytyy myös olla joidenkin lukujen neliöitä.

Apulause 3.3. Olkoot $r, s, t \in \mathbb{Z}_+$ siten, että $\operatorname{syt}(r, s) = 1$ ja $rs = t^2$. Tällöin on olemassa $m, n \in \mathbb{Z}$ siten, että $r = m^2$ ja $s = n^2$.

Todistus (vrt. [4, s. 524]). Jos $r = 1$ niin $\text{syt}(r, s) = 1$ ja $s = t^2$. Jos $m = 1$, niin $r = m^2$. Myös kun $n = t$, niin $s = n^2$. Apulause on siis tosi, kun $r = 1$. Tapaus $s = 1$ osoitetaan samaan tapaan. Oletetaan, että $r > 1$ ja $s > 1$. Olkoot lukujen r, s ja t alkulukuhajotelmat

$$r = p_1^{a_1} p_2^{a_2} \dots p_u^{a_u},$$

$$s = p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \dots p_v^{a_v},$$

ja

$$t = q_1^{b_1} q_2^{b_2} \dots q_k^{b_k}$$

Koska $\text{syt}(r, s) = 1$, hajotelmissa esiintyvät alkuluvut ovat erisuuria. Koska $rs = t^2$, niin

$$p_1^{a_1} p_2^{a_2} \dots p_u^{a_u} p_{u+1}^{a_{u+1}} p_{u+2}^{a_{u+2}} \dots p_v^{a_v} = q_1^{2b_1} q_2^{2b_2} \dots q_k^{2b_k}.$$

Aritmetiikan peruslauseen (lause 2.6) nojalla alkulukujen eksponentit ovat samat yhtälön molemmilla puolilla. Siksi jokaisen p_i täytyy olla yhtäsuuri q_j:n kanssa, joten $a_i = 2b_j$. Tästä seuraa, että jokainen exponentti a_i on parillinen ja $a_i/2$ on kokonaisluku. Nähdään, että $r = m^2$ ja $s = n^2$, jossa m ja n ovat kokonaisluvut

$$m = p_1^{a_1/2} p_2^{a_2/2} \dots p_u^{a_u/2}$$

ja

$$n = p_{u+1}^{a_{u+1}/2} p_{u+2}^{a_{u+2}/2} \dots p_v^{a_v/2}.$$

□

Lause 3.1. *Olkoot $x, y, z \in \mathbb{Z}_+$ siten, että y on parillinen. Kolmikko (x, y, z) on primitiivinen Pythagoraan kolmikko, jos ja vain jos on olemassa keskenään jaottomat positiiviset kokonaisluvut m ja n siten, että*

$$x = m^2 + n^2,$$

$$y = 2mn,$$

$$z = m^2 + n^2,$$

missä m on pariton ja n parillinen tai m on parillinen ja n on pariton.

Todistus (vrt. [4, s. 525–526]). Olkoon (x, y, z) primitiivinen Pythagoraan kolmikko. Apulauseen 3.2 nojalla x on pariton ja y parillinen tai päinvastoin. Koska oletetaan, että y on parillinen, niin x on pariton. Myös z on pariton, sillä apulauseen 3.1 nojalla $\text{syt}(y, z) = 1$ ja jos y ja z ovat molemmat parillisia, niin $\text{syt}(y, z) = 2$, joka

on ristiriita. Seurauksena $z + x$ ja $z - x$ ovat molemmat parillisia, joten on olemassa positiiviset kokonaisluvut r ja s, joilla $r = (z + x)/2$ ja $s = (z - x)/2$.

Koska $x^2 + y^2 = z^2$, niin saadaan $y^2 = z^2 - x^2 = (z + x)(z - x)$. Tästä saadaan

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

Olkoon $\operatorname{syt}(r, s) = d$. Koska $d \mid r$ ja $d \mid s$, niin apulauseen 2.2 nojalla $d \mid (r + s) = z$ ja $d \mid (r - s) = x$. Tästä seuraa $d \mid \operatorname{syt}(x, z) = 1$, joten $d = 1$.

Apulauseen 3.3 mukaan on olemassa $m, n \in \mathbb{Z}_+$ siten, että $r = m^2$ ja $s = n^2$. Kirjoittamalla x, y ja z lukujen m ja n funktioina saadaan

$$\begin{aligned} x &= r - s = m^2 - n^2, \\ y &= \sqrt{4rs} = \sqrt{4m^2n^2} = 2mn, \\ z &= r + s = m^2 + n^2. \end{aligned}$$

Osoitetaan, että $\operatorname{syt}(m, n) = 1$. Lukujen m ja n suurimman yhteisen tekijän tulisi jakaa myös $x = m^2 - n^2$, $y = 2mn$ ja $z = m^2 + n^2$. Tiedetään myös, että $\operatorname{syt}(x, y, z) = 1$, josta seuraa $\operatorname{syt}(m, n) = 1$.

Huomataan myös, että m ja n eivät voi molemmat olla parittomia, sillä näin ollessa x, y ja z olisivat kaikki parillisia, joka olisi ristiriidassa ehdon $\operatorname{syt}(x, y, z) = 1$ kanssa. Nähdään myös, että m ja n eivät voi myöskään olla molemmat parillisia, sillä $\operatorname{syt}(m, n) = 1$. Siis m on parillinen ja n pariton tai päinvastoin. On siis osoitettu, että jokainen primitiivinen Pythagoraan kolmikko täyttää lauseen ehdot.

Todistetaan vielä käänteisesti, että jokainen kolmikko (x, y, z)

$$\begin{aligned} x &= m^2 - n^2, \\ y &= 2mn, \\ z &= m^2 + n^2, \end{aligned}$$

missä $m, n \in \mathbb{Z}_+$ siten, että $m > m$, $\operatorname{syt}(m, n) = 1$ ja $m \not\equiv n \pmod 2$, on primitiivinen Pythagoraan kolmikko. Ensin huomataan, että $m^2 - n^2$, $2mn$ ja $m^2 + n^2$ muodostavat Pythagoraan kolmikon, sillä

$$\begin{aligned} x^2 + y^2 &= (m^2 - n^2)^2 + (2mn)^2 \\ &= (m^4 - 2m^2n^2 + n^4) + 4m^2n^2 \\ &= m^4 + 2m^2n^2 + n^4 \\ &= (m^2 + n^2)^2 \\ &= z^2. \end{aligned}$$

Osoitetaan tämän olevan primitiivinen Pythagoraan kolmikko todistamalla lukujen x, y ja z olevan keskenään jaottomia. Oletetaan $\operatorname{syt}(x, y, z) = d > 1$. Tällöin on olemassa alkuluku $p \mid (x, y, z)$. Huomataan, että $p \neq 2$, koska x on pariton, sillä $x = m^2 - n^2$, missä m^2 on pariton ja n^2 on parillinen, tai päinvastoin. Nähdään myös, että $p \mid x$, $p \mid z$, $p \mid (z + x)$ ja $p \mid (z - x) = 2n^2$. Tästä seuraa $p \mid m$ ja $p \mid n$, joka on ristiriita, sillä $\operatorname{syt}(m, n) = 1$. Siis $\operatorname{syt}(x, y, z) = 1$ ja (x, y, z) on primitiivinen Pythagoraan kolmikko.

□

Esimerkki 3.3. Olkoot $m = 6$ ja $n = 5$. Nyt $\operatorname{syt}(m, n) = 1$, $m \not\equiv n \pmod 2$ ja $m > n$. Lauseen 3.1 nojalla kolmikko (x, y, z), missä

$$\begin{aligned} x &= m^2 - n^2 = 6^2 - 5^2 = 11, \\ y &= 2mn = 2 \cdot 6 \cdot 5 = 60, \\ z &= m^2 + n^2 = 6^2 + 5^2 = 61, \end{aligned}$$

on primitiivinen Pythagoraan kolmikko.

4 Pythagoraan matriisit

Luvussa 3 esitettiin proseduuri, jolla voidaan generoida mikä tahansa primitiivinen Pythagoraan kolmikko. Tässä luvussa laajennetaan tätä proseduuria ja esitetään parametrisointi Pythagoraan matriiseille. Luvun tiedot ovat peräisin lähteestä [2].

Määritelmä 4.1. Kokonaislukuarvoisten $n \times n$-matriisien kolmikkoa $\{A, B, C\}$ sanotaan *Pythagoraan kolmikoksi*, jos kolmikko toteuttaa relaation

$$A^2 + B^2 = C^2.$$

Tällaisia kolmikoita on ääretön määrä. Ottamalla Pythagoraan kolmikko $(a_j, b_j, c_j)_{j=1,\dots,n}$ voidaan muodostaa diagonaalimatriisit $A = diag[a_1, \dots, a_n]$, $B = diag[b_1, \dots, b_n]$ ja $C = diag[c_1, \dots, c_n]$. Nämä matriisit toteuttavat selvästi vaaditun relaation. Tässä luvussa on kuitenkin tarkoitus esittää konstruktio, jolla saadaan generoitua ei-triviaaleja kolmikoita. Esitetään seuraavaksi ei-triviaali esimerkki.

Esimerkki 4.1. Matriisit $A = \begin{bmatrix} 30 & 13 \\ 3 & 0 \end{bmatrix}$, $B = \begin{bmatrix} 4 & 8 \\ 12 & 16 \end{bmatrix}$ ja $C = \begin{bmatrix} -26 & -25 \\ -15 & 4 \end{bmatrix}$ ovat Pythagoraan kolmikko, sillä

$$\begin{bmatrix} 30 & 13 \\ 3 & 0 \end{bmatrix}^2 + \begin{bmatrix} 4 & 8 \\ 12 & 16 \end{bmatrix}^2 = \begin{bmatrix} -26 & -25 \\ -15 & 4 \end{bmatrix}^2.$$

Tulee huomata, että nämä matriisit eivät kommutoi.

Lause 4.1. *Olkoon P $n \times n$-matriisi siten, että $P \in M_n(\mathbb{Q})$. Tällöin on olemassa n^2-parametrinen perhe matriiseja $A, C \in M_n(\mathbb{Q})$ siten, että $P = C^2 - A^2$.*

Lauseen todistukseen tarvitaan seuraavaa aputulosta. Tulee huomata, että kaikille neliömatriiseille U ja V pätee

$$(U - V)^2 + 2UV + 2VU = (U + V)^2.$$

Siis jos voidaan esittää $P = 2(UV + VU)$, niin $(U - V)^2 + P = (U + V)^2$, eli $P = (U + V)^2 - (U - V)^2$. Osoitetaan seuraavaksi tällaisen P:n esityksen olevan mahdollinen.

Apulause 4.1. Olkoon matriisi $U \in M_n(\mathbb{Q})$ siten, että

1. U:n ominaisarvot λ_j toteuttavat degeneroimattomuusehdon

$$\lambda_i + \lambda_j \neq 0$$

2. U:n ominaisvektorit virittävät avaruuden $\mathbb{R}^n$.

Tällöin jokaiselle matriisille $P \in M_n(\mathbb{Q})$ on olemassa yksikäsitteinen matriisi $V \in M_n(\mathbb{Q})$ siten, että $P = 2(UV + VU)$.

Todistus (vrt. [2, s. 159]). Merkitään $\boldsymbol{x}_j$:llä matriisin U ominaisarvoa λ_j vastaavaa ominaisvektoria. Koska ehdon 2 nojalla vektorit $\{\boldsymbol{x}_j\}_{j=1,\dots,n}$ muodostavat kannan avaruudelle $\mathbb{R}^n$, ylläolevan matriisiyhtälön ratkaisemiseksi on riittävää löytää matriisi V siten, että

$$2(UV + VU)\boldsymbol{x}_j = P\boldsymbol{x}_j$$

kaikilla $j = 1, \dots, n$. Koska $\boldsymbol{x}_j$ on U:n ominaisvektori, voidaan kirjoittaa

$$(UV + VU)\boldsymbol{x}_j = U(V\boldsymbol{x}_j) + \lambda_j V\boldsymbol{x}_j = (U + \lambda_j I)V\boldsymbol{x}_j.$$

Ehdosta 1 ja karakterisesta yhtälöstä seuraa, että kaikki matriisit $U + \lambda_j I$ ovat kääntyviä, joten voidaan kirjoittaa

$$2V\boldsymbol{x}_j = (U + \lambda_j I)^{-1} P\boldsymbol{x}_j.$$

Merkitään vektoria $(U + \lambda_j I)^{-1} P\boldsymbol{x}_j$ merkinnällä $\boldsymbol{y}_j$. Yhdistämällä sarakkeet saadaan $2VX = Y$, kun $X = [\boldsymbol{x}_1|\boldsymbol{x}_2|\dots|\boldsymbol{x}_n]$ ja $Y = [\boldsymbol{y}_1|\boldsymbol{y}_2|\dots|\boldsymbol{y}_n]$. Tästä seuraa, että V voidaan esittää

$$V = \frac{1}{2} Y X^{-1},$$

sillä ehdon 2 mukaan X on kääntyvä, koska sen pystyrivit ovat lineaarisesti riippumattomia. Tulee huomata, että matriisi V on yksikäsitteinen. □

Nyt voidaan todistaa lause, joka mahdollistaa kolmikoiden generoinnin.

Todistus (vrt. [2, s. 159]). Koska $M_n(\mathbb{Q})$ on rengas, voimme aloittaa millä tahansa kääntyvällä matriisilla $X \in M_n(\mathbb{Q})$ ja millä tahansa diagonaalimatriisilla $\Lambda = diag[\lambda_1, \dots, \lambda_n] \in M_n(\mathbb{Q})$, joka täyttää apulauseen 4.1 ensimmäisen ehdon ja muodostaa matriisin $U = X\Lambda X^{-1}$. Tällöin apulauseen 4.1 matriisi $V = \frac{1}{2} Y X^{-1}$ kuuluu myös joukkoon $M_n(\mathbb{Q})$. Siis voimme valita $C = U + V$ ja $A = U - V$. Silloin $P = 2(UV + VU) = B^2$, jolloin $A^2 + B^2 = C^2$. Eli matriisien kolmikko $\{A, B, C\}$ on Pythagoraan kolmikko. □

Esimerkki 4.2. Olkoon matriisi $B = \begin{bmatrix} 2 & 3 \\ 4 & 5 \end{bmatrix}$, jolloin $B^2 = \begin{bmatrix} 16 & 21 \\ 28 & 37 \end{bmatrix}$. Valitaan sitten diagonaalimatriisi $\Lambda = \begin{bmatrix} -2 & 0 \\ 0 & 3 \end{bmatrix}$ jonka alkiot täyttävät apulauseen 4.1 ensimmäisen ehdon. Valitaan kaksi matriisin U ominaisvektoria $x_1 = (1, 1)$ ja $x_2 = (-1, 1)$ jotka täyttävät apulauseen 4.1 ehdot. Tällöin $X = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$, jolloin $U = X\Lambda X^{-1} = \frac{1}{2}\begin{bmatrix} 1 & -5 \\ -5 & 1 \end{bmatrix}$. Nyt yhtälöstä $(U + \lambda_j I)^{-1} P \boldsymbol{x}_j$, jossa λ_j on matriisin U ominaisarvo ja $P = B^2$, saadaan ratkaistua vektorit $\boldsymbol{y}_1 = \frac{1}{4}(-107, 5)$ ja $\boldsymbol{y}_2 = \frac{1}{3}(20, 22)$. Nyt saadaan määritettyä matriisi $V = \frac{1}{48}\begin{bmatrix} -401 & -241 \\ -73 & 103 \end{bmatrix}$. Tulee huomata, että matriisien U ja V alkiot ovat rationaalisia ja täten matriisien $U + V$ ja $U - V$ alkiot ovat myöskin rationaalisia. Kertomalla matriisit B ja Λ luvulla 48 saadaan näiden matriisien alkioista kokonaislukuja. Nyt saadaan Pythagoraan kolmikko

$$(U - V)^2 + B^2 = (U + V)^2.$$

Lähteet

[1] Anton, H. *Elementary Linear Algebra* 11. painos. New York: Wiley, 2013.

[2] Arnold, M. & Eudelzon, A. *On Matrix Pythagorean Triples*. The American Mathematical Monthly, 2019. Vol. 126:2. S. 158-160.

[3] Burton, D. *Elementary number theory*. 6. painos. Boston: McGraw-Hill, 2007.

[4] Rosen, K. *Elementary number theory and its applications*. 6. painos. Reading: Addison-Wesley, 2011.