# 3 Binääriset neliömuodot

**Määritelmä 3.1.** Binäärinen neliömuoto on kahden muuttujan toisen asteen homogeeninen polynomi

$$f(x, y) = ax^2 + bxy + y^2.$$

Toisinaan merkitään neliömuotoa pelkästään kerroinvektorilla $f := (a, b, c)$. Itseasiassa tässäkin esityksessä vain $(a, b)$ ovat tarpeen, sillä $c$ määräytyy niiden perusteella yksikäsitteisesti, kuten myöhemmin nähdään. Toisinaan kirjoitetaan myös $(a, b, *)$ tai $(a, *, *)$ jos toinen ja/tai kolmas kerroin ovat joko tarpeettomia, tuntemattomia tai helposti laskettavissa diskriminantin avulla.

**Määritelmä 3.2.** Neliömuodon $f(x, y) = ax^2 + bxy + cy^2$ diskriminantti $D(f)$ on

$$D(f) = b^2 - 4ac.$$

Huomaa, että $D \equiv 1, 0 \mod 4$, jos $b \equiv D \mod 2$.

**Määritelmä 3.3.** Kutsumme binääristä neliömuotoa $f(x, y) = ax^2 + bxy + cy^2$ primitiiviseksi, jos sen kertoimet $a, b, c$ ovat keskenään suhteellisia alkulukuja.

Lukuteoreettisesta näkökulmasta neliömuodot tulevat kiinnostaviksi, kun mietitään, mitä lukuja voidaan esittää neliömuotojen avulla. Kuten olemme jo tälläkin kurssilla nähneet, yhtälöllä $p = x^2 + y^2$ on ratkaisu, kun $p \equiv 1 \mod 4$. Tästä siis seuraa, että neliömuoto $f(x, y) = x^2 + y^2$ esittää alkulukua $p$ silloin kun $p \equiv 1 \mod 4$.

**Määritelmä 3.4.** Neliömuoto $f(x, y)$ esittää kokonaislukua $n \in \mathbb{Z}$, jos on olemassa $r, s \in \mathbb{Z}$, joille pätee

$$n = f(r, s).$$

Jos $(r, s) = 1$, sanotaan, että $f$ esittää kononaislukua $n \in \mathbb{Z}$ kunnolla.

Klassisia kysymyksiä lukuteoriassa on:

1. Mitä kokonaislukuja annettu muoto esittää?
2. Mitkä muodot esittävät annettua kokonaislukua?
3. Jos neliömuoto esittää kokonaislukua, kuinka monta esitystä on olemassa, ja miten ne voidaan löytää?

Viimeinen kysymys tarkoittaa, että on mahdollista, että kaksi eri neliömuotoa esittävät täsmälleen samat luvut. Ovatko neliömuodot tällöin samat?

Näitä kysymyksiä miettivät jo sellaiset matematiikan suurnimet kuin Fermat ja Euler. Kuitenkin vasta Gauss Disquisitiones Arithmeticaessa 1801 antoi vankan matemaattisen pohjan neliömuotojen teorialle. Noin 1800-luvun puolivälissä havaittiin yhteys neliömuotojen ja neliökuntien luokkalukujen teorian välillä.

Määritellään, milloin kaksi neliömuotoa ovat ekvivalentteja.

Ryhmä $\mathrm{SL}_2(\mathbb{Z})$ toimii neliömuotojen joukossa. Jos

$$\sigma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

toimii se neliömuodossa $\sigma f(x,y) = f(px+qy, rx+sy) = a'x^2 + b'xy + c'y^2$, missä

$$a' = f(p,r), b' = 2apq + 2crs + b(ps+qr), c' = f(q,s).$$

**Määritelmä 3.5.** Kaksi binääristä neliömuotoa $f_1, f_2$ ovat ekvivalentteja, jos ne ovat $\mathrm{SL}_2(\mathbb{Z})$ toiminnassa samalla radalla. Eli, jos on olemassa sellainen $\tau \in \mathrm{SL}_2(\mathbb{Z})$, jolle $\tau f_1(x,y) = f_2(x,y)$.

**Lemma 3.6.** *Jos kaksi neliömuotoa ovat ekvivalentit jos ja vain jos ne esittävät samoja kokonaislukuja.*

*Todistus.* Olkoon $f_1, f_2$ kaksi ekvivalenttia muotoa. Silloin on olemassa $\sigma = \begin{pmatrix} p & q \\ r & s \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$, jolle $\sigma f_1 = f_2$.

Jos muoto $f_1$ esittää kokonaislukua $m$, silloin $m = f_2(x,y)$ joillekin $x, y \in \mathbb{Z}$. Nyt $m = \sigma f_1 = f_2(x', y')$, missä $x' = px + qy, y' = rx + sy$, ja nämä ovat kokonaislukuja. Joten $f_1$ esittää $m$:n.

Toisaalta, jos koska $\sigma^{-1} \in \mathrm{SL}_2(\mathbb{Z})$, $f_1 = \sigma^{-1} f_2$, ja jos $m = f_1(x,y)$ joillekin $x, y \in \mathbb{Z}$, silloin $m = \sigma^{-1} f_2 = f_2(sx - qy, py - rx) = f_2(x', y')$, missä $x', y' \in \mathbb{Z}$. □

**Määritelmä 3.7.** Neliömuotoa $f$ kutsutaan definiitiksi, jos sen diskriminantti on negatiivinen, muussa tapauksessa sitä kutsutaan epädefiniitiksi. Jos kerroin $a > 0$, kutsutaan muotoa positiiviseksi definiitiksi.

**Lemma 3.8.** *Jos neliömuodot $f_1$ ja $f_2$ ovat ekvivalentteja, ovat myös niiden diskriminantit samat.*

*Todistus.* Olkoon $f_1(x,y) = ax^2 + bxy + cy^2$. Olkoon $\sigma f_1(x,y) = f(px + qy, rx + sy) = a'x^2 + b'xy + c'y^2 = f_2(x,y)$, missä

$$a' = f(p,r), b' = 2apq + 2crs + b(ps+qr), c' = f(q,s).$$

Neliömuodon $f_2$ diskriminantti on $b'^2 - 4a'c' = (2apq + 2crs + b(ps + qr))^2 - 4(ap^2 + bpr + cr^2)(aq^2 + bqs + cs^2) = (b^2 - 4ac)(ps - qr)^2 = b^2 - 4ac$, mikä on $f_1$ diskriminantti.

□

Diskriminantti on siis neliömuodon invariantti, mutta ei täysin erota neliömuotoja toisistaan. Jotta löydetään esitys jokaiselle neliömuodolle yksikäsitteisesti, seuraavaksi esitellään reduktioteoriaa.

## 3.1 Positiiviset definiitit neliömuodot

**Määritelmä 3.9.** Primitiivistä positiivista definiittiä neliömuotoa $(a, b, c)$ kutsutaan redusoituksi (surkastetuksi), jos $|b| \leq a \leq c$, ja jos $|b| = a$ tai $a = c$, silloin $b \geq 0$.

**Lause 3.10.** *Vakiodiskriminanttia $-D$ olevien redusoitujen muotojen määrä on äärellinen.*

*Todistus.* Tehtävä 4 sanoo, että $|b| \leq \sqrt{D/3}$. Nyt $-D = b^2 - 4ac$, joten kun $b$ on rajoitettu, on vain äärellinen määrä tapoja jakaa $D + b^2 = 4ac$:hen. □

**Propositio 3.11.** *Jokainen binäärinen neliömuoto on ekvivalentti redusoidun muodon $f(x, y) = ax^2 + bxy + cy^2$ kanssa, jossa $|b| \leq a \leq c$, jos $c = a$ ja $0 \leq b \leq a$.*

*Todistus.* Todistus koostuu algoritmista, joka löytää redusoidun muodon ja säilyttää ekvivalenssin. Erityisesti alkiot $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}, \begin{pmatrix} 1 & \mu \\ 0 & 1 \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z})$ redusoivat muotoja yksi kerrallaan – huomaa myös, että nämä muistuttavat aika tavalla $\mathrm{SL}_2(\mathbb{Z})$:n virittäjäalkioita.

Algoritmi toimii seuraavasti

1. Jos $c < a$, muuta $(a, b, c)$ muotoon $(c, -b, a)$ käyttäen ensimmäistä virittäjää.

2. Jos $b > a$ muuta $(a, b, c)$ muotoon $(a, b_1, c_1)$, missä $b_1 = b + 2\mu a$, missä $\mu$ on valittu siten, että $b_1 < a$ ja $c_1$ voidaan laskea $D = b_1^2 - 4ac_1$ avulla. Tässä käytettiin toista virittäjää.

Nyt kun lähdetään mistä tahansa neliömuodosta liikkeelle, ja käytetään näitä kahta operaatiota peräjälkeen, jokaisella askelella joko $a$ tai $b$ on redusoitu, joten algoritmi päättyy sellaiseen muotoon, jossa $c \geq a$ ja $b \leq a$. Jos $b = -a$, silloin voidaan käyttää toista operaatiota, $\mu = 1$, mikä muuttaa $b$:n $a$:si. Jos $c = a$, ensimmäisen operaation myötä saadaan $b \geq 0$. □

**Esimerkki 3.12.** Surkastetaan muoto $f = 458x^2+214xy+25y^2$. Koska $c < a$ käytetään (1), ja saadaan muoto $(25, -214, 458)$. Nyt $b > a$, joten (2) nojalla kun $\mu = 4$, saadaan $(25, -14, 2)$. Taas $c < a$, joten (1) antaa $(2, 14, 25)$. Taas $b > a$, joten (2) nojalla, kun $\mu = -3$ saadaan $(2, 2, 1)$. Nyt taas (1) antaa $(1, -2, 2)$ ja viimein (2) kun valitaan $k = 1$ tuottaa $(1, 0, 1)$. Matriisi $\sigma = \begin{pmatrix} 3 & 4 \\ -13 & -17 \end{pmatrix}$, ja se antaa $\sigma f = x^2 + y^2$. Huomaa, että kummankin diskriminantti on $-4$, koska myös $214^2 - 4 \cdot 458 \cdot 25 = 45796 - 45800 = -4$. Ja näin ollen myös muoto $f$ esittää alkulukua $p$ kunhan $p \equiv 1 \mod 4$.

**Lause 3.13.** *Lukuunottamatta ekvivalensseja* $(a, b, a) \sim (a, -b, a)$ *ja* $(a, a, c) \sim (a, -a, c)$ *mitkään kaksi redusoitua muotoa eivät voi olla ekvivalentteja.*

*Todistus.* Harjoitustehtävä. □

Näissä tapauksissa valitaan ekvivalenssiluokan edustajaksi muoto jossa $b \geq 0$. Näin on todistettu kaksi tärkeää lausetta binääristen neliömuotojen teoriasta.

**Lause 3.14.** *Jokaisessa positiividefiniittien binääristen neliömuotojen ekvivalenssiluokassa on täsmälleen yksi redusoitu muoto.*

**Lause 3.15.** *Tiettyä diskriminanttia olevien muotojen ekvivalenssiluokkien määrä on äärellinen.*

Jos määrittelemme luokkaluvun seuraavalla tavalla:

**Määritelmä 3.16.** Olkoon $D < 0$ määrätty diskriminantti. Sellaisten primitiivisten positiividefiniittien binääristen neliömuotojen, joiden diskriminantti on $D$, ekvivalenssiluokkien lukumäärä kutsutaan luokkaluvuksi.

On jo siis jo myöskin todistettu, että

**Lause 3.17.** *Luokkaluku* $h_D$ *on äärellinen.*

Vielä yksi määritelmä, jotta tehtäväpaperin geometrinen tulkinta redusoiduille muodoille on järkevä.

**Määritelmä 3.18.** Olkoon $f = (a, b, c)$:n diskriminantti $-D$. Määritellään $f$:n pääjuuri olemaan kompleksiluku

$$z = \frac{-b + \sqrt{-D}}{2a}.$$

Huomaa, että $z$ on yksi ratkaisu yhtälöön $ax^2 + bx + c = 0$.