3.2 Epädefiniitit muodot

Epädefiniitit muodot olivat muotoja, joiden diskriminantti $D > 0$. Muotoa (k, kn, c) kutsutaan epämääräiseksi muodoksi, ja epämääräisten muotojen muodostamaa ekvivalenssiluokkaa kutsutaan epämääräiseksi luokaksi.

Tässä kappaleessa oletamme, että diskriminantti $D > 0$. Kun $D < 0$ todistettiin, että jokainen redusoitu muoto muodosti oman ekvivalenttiluokkansa. Positiivisille diskriminanteille tämä ei ole totta, ja usein päädytään tilanteeseen, jossa useampi redusoitu muoto on samassa ekvivalenssiluokassa. Tilanne ei kuitenkaan ole näin kaoottinen tai huolestuttava; nämä redusoidut muodot muodostavat syklejä.

Määritelmä 3.19. Epädefiniittiä muotoa $f = (a, b, c,)$ kutsutaan redusoiduksi, jos

$$0 < b < \sqrt{D} \text{ ja } \sqrt{D} - b < 2|a| < \sqrt{D} + b.$$

Propositio 3.20. *Jos (a, b, c) on redusoitu, silloin $\sqrt{D} - b < 2|c| < \sqrt{D} + b$.*

Todistus. Koska $b^2 - 4ac = D$, tästä seuraa

$$(\sqrt{D} - b)(\sqrt{D} + b) = -4ac = (2|a|)(2|c|).$$

Nyt $0 < b < \sqrt{D}$ ja $\sqrt{D} - b < \sqrt{D} + b$, ja näin ollen koska $\sqrt{D} - b < 2|a| < \sqrt{D} + b$, myös $\sqrt{D} - b < 2|c| < \sqrt{D} + b$.

(Kaavakuvanomaisesti: $xy = zw$ ja $x < z < y$, silloin $x < w < y$. □

Propositio 3.21. *Vakiodiskriminanttia $D > 0$ olevien redusoitujen neliömuotojen määrä on äärellinen.*

Todistus. Koska redusoidun määritelmästä seuraa, että b:n koko on rajattu, myös kaikkien redusoitujen neliömuotojen määrä on rajattu, sillä b ja D määrittävät äärellisen määrän ratkaisuja yhtälölle $b^2 - D = 4ac$. □

Propositio 3.22. *Mikä tahansa epädefiniitti muoto on ekvivalentti samaa diskriminanttia olevan redusoidun neliömuodon kanssa.*

Todistus. Kuten positiividefiniittimuotojen tapauksessa, esitetään algoritmi, joka redusoi muotoa. Jos (a, b, c) ei ole redusoitu, valitaan δ (ei välttämättä yksikäsitteinen), jolle

$$\sqrt{D} - 2|c| < -b + 2c\delta < \sqrt{D},$$

joten

$$(a, b, c) \sim (c, -b + 2c\delta, a - b\delta + c\delta^2).$$

Jos $|a - b\delta + c\delta^2| < |c|$ prosessi toistetaan. Algoritmi päättyy, kun saadaan muoto (A, B, C), missä $|A| \leq |\ C|$ ja $\sqrt{D} - 2|A| < B < \sqrt{D}$. Jos nämä ovat totta, silloin $\sqrt{D} - B < 2|A|$. Lisäksi, koska $|\sqrt{D} - B||\sqrt{D} + B| = 4|A||C|$, väistämättä $|\sqrt{D} + B| > 2|C|$. Jatketaan epäyhtälöllä:

$$|\sqrt{D} + B| > 2|C| > 2|A| > \sqrt{D} - B.$$

Yhtälön ääripäitä tarkastelemalla seuraa, että B on positiivinen, joten $0 < B < \sqrt{D}$, ja siis (A, B, C) on redusoitu. □

Määritelmä 3.23. Kahta muotoa (a, b, a') ja (a', b', c'), joiden diskriminantti on D kutsutaan vierekkäisiksi, jos $b + b' \equiv 0 \mod 2a'$.

Jokaiselle annetulle redusoidulle muodolle on olemassa yksikäsitteinen muoto, joka on vierekkäinen oikealle ja yksikäsitteinen muoto, joka on vierekkäinen vasemmalle.

Propositio 3.24. *Redusoitujen muotojen joukko, joitten diskriminantti on vakio, voidaan jakaa vierekkäisten muotojen sykleihin.*

Todistus. Todistuksen idea on lähteä liikkeelle yhdestä muodosta, ja muodostaa vierekkäisiä muotoja oikealle. Koska redusoituja muotoja on äärellinen määrä, päädytään jossain vaiheessa alkuperäiseen muotoon. Jos kaikki muodot on käyty läpi, prosessi päättyy. Muutoin lähdetään liikkeelle muodosta, jota ei vielä ole listattu. □

Koska matriisi

$$\begin{pmatrix} 0 & -1 \\ 1 & \frac{b+b'}{2a} \end{pmatrix},$$

antaa ekvivalenssin kahden vierekkäisen muodon välille, ja koska ekvivalenssirelaatio on transitiivinen, kaikki saman syklin muodot ovat ekvivalentteja keskenään.

Olemme todistaneet siis toiseen suuntaan seuraavan lauseen.

Lause 3.25. *Kaksi redusoitua muotoa ovat ekvivalentteja, jos ja vain jos ne ovat samassa syklissä.*

Koska suurin osa opiskelijoista oli käynyt Lukuteorian kurssin, ketjumurtoluvut voidaan pitää tunnettuina, ja osoittaa lauseen toiseen suuntaankin. Ensin joitain lemmoja ja määritelmiä.

Ketjumurtoluku on luku, jonka muoto on

$$x = a_0 + \cfrac{1}{a_1 + \cfrac{1}{a_2 + \cfrac{1}{\cdots}}}.$$

Se voi olla äärellinen tai ääretön. Lukuja a_i kutsutaan osamurroiksi, ja usein ketjumurtoluku esitetään näiden avulla

$$[a_0, \ldots, a_N].$$

Jos $a_i \in \mathbb{Z}^+$ kaikille $i \geq 1$, kutsutaan tätä yksinkertaiseksi ketjumurtoluvuksi. Äärellinen yksinkertainen ketjumurtoluku esittää rationaalilukua ja päin vastoin. Yksinkertainen ketjumurtoluku on periodinen, jos $a_i = a_{i+J}$ kaikille $i \geq I$, ja $J \in \mathbb{N}$. Esitys tälle on

$$[a_0, \ldots, a_{I_1}, *a_I, \ldots, *a_{I+J-1}],$$

missä periodia on merkittyä tähdellä.

Lause 3.26. *Jos ω on yhtälön $ax^2 + bx + c = 0$, missä $a, b, c \in \mathbb{Z}$ irrationaallinen juuri, silloin yksinkertainen ketjumurtoluku ω:lle on periodinen. Ja jos ykm ω on periodinen, se on juuri jollekin $ax^2 + bx + c = 0$, missä $a, b, c \in \mathbb{Z}$.*

Lemma 3.27. *Jos ääretön ketjumurtoluku sisältää vain äärellisen määrän negatiivisia osamurtoja, voidaan se muuttaa muotoon, jossa on vain positiivisia osamurtoja äärellisessä ja parillisessa määrässä askelia.*

Lemma 3.28. *Jos $y = \frac{\alpha x+\beta}{\gamma x+\delta}$ missä*

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

silloin $y = [\pm t, a_1, \ldots, a_{2r}, \pm u, x]$, missä $a_i \geq 0$ kaikille i.

Nyt voidaan todistaa lause itse lause toiseen suuntaan.

Todistus. Olkoot $f = (a, b, c)$ ja $f' = (a', b', c')$ kaksi ekvivalenttia redusoitua epädefiniittiä muotoa. Voidaan olettaa, että $a, a' > 0$ jotta pääjuuret ω, ω' ovat aitoja murtolausekkeita (ei kokonaisosaa). Koska muodot ovat ekvivalentteja on olemassa joku

$$\begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathrm{SL}_2(\mathbb{Z}),$$

joka siirtää muodon toiseen. Tämä siirtää myös pääjuuret niin, että $\omega' = \frac{\alpha\omega+\beta}{\gamma\omega+\delta}$. Edellisen nojalla

$$\omega' = [\pm t, a_1, \ldots, a_{2r}, \pm u, \omega] = [\pm t, a_1, \ldots, a_{2r}, \pm u, *d_1, \ldots, *d_{2m}]$$

missä ω on periodinen. Kaikki $a_1, \ldots, d_{2m}$ voidaan tehdä positiivisiksi., lisäksi $\pm t = 0$, sillä ω' ei sisällä kokonaisosaa. Voidaan osoittaa, että (puhtaasti)

periodinen ketjumurtoluku on yksikäsitteinen annetulle $\sqrt{D}$:lle, joten ω' periodinen osa on ω:n periodisen osan syklinen permutaatio. Koska yllä oleva lemma muuttaa osien määrää aina parillisesti, on ω':n periodi ω:n periodi siirrettynä parillisella määrällä osamurtoja. (syklissä vierekkäisten ensimmäisten kerrointen merkki vaihtuu, joten pitää olla parillinen permutaatio). Kun mennään syklissä eteenpäin f:stä, saavutaan redusoituun muotoon, jonka pääjuuri on ω', mutta tämä muoto on f', koska ω' ja diskriminantti D määrittävät muodon yksikäsitteisesti. □

Määritelmä 3.29. Muotoa $(a, -b, c)$ kutsutaan muodon (a, b, c) vastamuodoksi. Muodot (a, b, c) ja (c, b, a) ovat liitännäisiä. Epämääräinen muoto on ekvivalentti oman vastakkaismuotonsa kanssa, sillä jos $b = ka$, valinta $\delta = k$ antaa

$$(a, b, c) \sim (c, -b, a) \sim (a, b - 2a\delta, c - b\delta + a\delta^2) \sim (a, -b, c).$$

Muotoja (a, b, c) ja (c, b, a) kutsutaan liitännäisiksi muodoiksi. Vasta- tai liitännäismuodot ovat ole aidosti ekvivalentteja, sillä matriisit, jotka siirtävät ne toisikseen ovat $\begin{pmatrix} 1 & 0 \\ 0 & -1 \end{pmatrix}$, $\begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$, tai niiden vastamatriisit tässä järjestyksessä. Näiden matriisien determinantti on -1.

Lause 3.30. *Syklissä olevien muotojen lukumäärä, jota myös periodiksi kutsutaan, on aina parillinen.*

Todistus. Redusoidun muodon kertoimet a ja c ovat aina erimerkkisiä. Voidaan siis muodostaa vierekkäisten muotojen pareja $(a, b, c) \sim (c, b', c')$, missä c on negatiivinen ja a, c' ovat positiivisia. Koska vierekkäisyys säilyttää näiden parien vierekkyyden, kokonaislukumääräpareja muodostaa aina syklin. □

Propositio 3.31. *Jos muoto f' ja sen liitännäismuoto f ovat eri sykleissä, on tämä sama totta myös kaikille muodoille molemmissa sykleissä. Tällaisia syklejä kutsutaan liitännäisiksi sykleiksi.*

Todistus. Jos aloitetaan muodosta f, ja muodostetaan sykliä oikealle, saadaan $(a, b, c) \sim (c, b', a')$. Toisaalta f' joka on liitännäismuoto f:lle on (a', b', c) josta sykli vasemmalle antaa (c, b, a). Näin ollen muodot, jotka saadaan kulkemalla f:stä oikealle ovat täsmälleen liitännäismuodot nille muodoille, jotka saadaan, kun kuljetaan f':sta vasemmalle. □

Propositio 3.32. *Jos sykli sisältää epämääräisen muodon, sisältää se täsmälleen kaksi muotoa, ja lisäksi sykli on oma liitännäissyklinsä. Kääntäen, sykli, joka on oma liitännäisensä, sisältää täsmälleen kaksi epämääräistä muotoa.*

Todistus. Jos muodot f ja sen liitännäismuoto f' ovat samassa syklissä, silloin voidaan kulkea f:stä oikealle ja f' vasemmalle, ja saadaan aina liitännäismuotojen parit. Koska sykleillä on äärellinen pituus, lopulta on pakko saapua vierekkäisiin liitännäismuotoihin $(a', b, a) \sim (a, b, a')$. Koska nämä muodot ovat vierekkäisiä $b + b \equiv 0 \mod 2a$, joten $a \mid b$ ja näin (a, b, a') on epämääräinen. Samalla lailla jos kuljetaan f:stä taaksepäin ja f':sta eteenpäin, saavutaan johonkin toiseen epämääräiseen muotoon. Näin ollen itsensä kanssa liitännäinen sykli sisältää kaksi epämääräistä muotoa. Se ei voi sisältää enempää, sillä sykli päättyy siinä vaiheessa, kun kaksi epämääräistä muotoa on löydetty. On helppo nähdä, että sykli, jossa on epämääräinen muoto, on väistämättä liitännäinen itsensä kanssa, koska muoto (a, ak, c) on vierekkäinen oman liitännäismuotonsa (c, ak, a) kanssa. □

Määritelmä 3.33. Redusoitua sykliä $(1, b, c)$ kutsutaan tietyn diskriminantin päämuodoksi, ja sykliä, jossa se on, kutsutaan pääsykliksi.

Esimerkki 3.34. Kun diskriminantti oli negatiivinen, havaittiin, että muodot olivat asymmetrisia, sillä $a \leq c$. Positiivisen diskriminantin tapauksessa tämä ei ole totta. Jos siis löydetään joku redusoitu muoto (a, b, c), jonka ensimmäinen kerroin on vakio a, silloin saadaan suoraan myös redusoidut muodot $(-a, b, -c), (c, b, a)$ ja $(-c, b, -a)$. Lisäksi, koska vastaukset yhtälöön $b^2 \equiv D \mod a$ tulevat pareittain, saadaan redusoidut muodot $(a, -b+2a\sigma, a-b\sigma+c =, (-a, -b+2a\sigma, -a+b\sigma-c), (a-b\sigma+c, -b+2a\sigma, a)$ ja $(-a + b\sigma - c, -b + 2a\sigma, -a)$, missä σ on a:n etumerkki. Nämä muodot puolestaan johtavat muihin muotoihin ja niin edelleen.

$D = 1173 = 3 \cdot 17 \cdot 23$, on olemassa neljä sykliä

$$(1, 33, -21) \sim (-21, 9, 13) \sim (13, 17, -17) \sim (-17, 17, 13) \sim (13, 9, -21) \sim (-21, 33, 1)$$

$$(-1, 33, 21) \sim (21, 9, -13) \sim (-13, 17, 17) \sim (17, 17, -13) \sim (-13, 9, 21) \sim (21, 33, -1)$$

$$(3, 33, -7) \sim (-7, 23, 23) \sim (23, 23, -7) \sim (-7, 33, 3)$$

$$(-3, 33, 7) \sim (7, 23, -23) \sim (-23, 23, 7) \sim (7, 33, -3)$$

Lopuksi muutama lause siitä, milloin annetut muodot esittävät lukuja.

Lause 3.35. *Jos mikä tahansa muoto $f(y, x) = ax^2 + bxy + cy^2$, jonka diskriminantti on D esittää kokonaislukua m, joka on jaollinen parittomalla alkuluvulla p ja jolle $\left(\frac{D}{p}\right) = -1$, silloin väistämättä jollekin positiiviselle kokonaisluvulle k pätee $p^2k \mid m, p^k \mid p$ ja $p^k \mid y$. Mitään kokonaislukua, joka on täsmälleen jaollinen alkuluvun p parittomalla potenssilla, ja jolle $\left(\frac{D}{p}\right) = -1$, ei voi olla primitiivisesti esitettävissä millään primitiivisellä muodolla, jonka diskriminantti on D.*

Lause 3.36. *Jos p on pariton alkuluku, jolle $\left(\frac{D}{p}\right) = 1$, ja b on mikä tahansa ratkaisu kongruenssiin $b^2 \equiv D \mod 4p$, silloin p:lle on primitiivinen esitys muodoilla, jotka kuuluvat luokkiin $(p, b, *)$ ja $(p, -b, *)$, jotka ovat erillisiä muotoja, mutta mitkään muut muodot eivät esitä p:tä.*

Lause 3.37. *Jos p on pariton alkuluku, joka jakaa D:n, silloin p:n voi primitiivisesti esittää muodolla, joka kuuluu luokkiin $(p, 0, *)$ tai $(p, p, *)$ riippuen D:n parillisuudesta, ja mikään muu muoto ei esitä p:tä.*

Lause 3.38. *Jos m on mikä tahansa kokonaisluku ja D diskriminantti, silloin m voidaan primitiivisesti esittää muodoilla, jotka kuuluvat luokkiin $(m, \pm b, *)$, missä b on mikä tahansa ratkaisu kongruenssiin $b^2 \equiv D \mod 4m$, eikä millään muilla muodoilla. Jos $m = \prod p_i^{\alpha_i}$ alkulukuhajotelmana, silloin näiden luokkien joukko on täsmälleen se joukko luokkia, jotka esittävät alkulukuja p_i muodoilla f_i, kuten yllä.*