Johdatus modulimuotoihin ja Linnikin ongelmaan

Anne-Maria Ernvall-Hytönen

1. maaliskuuta 2012

Sisältö

Luku 1

Johdanto

(Tämän johdannon ei ole tarkoitus opettaa lukijoille mitään konkreettista modulimuodoista, eikä kaikkia viitteitä ole tarkoitus ymmärtää vielä tässä vaiheessa, vaan tarkoitus on ainoastaan, että johdannon luettuaan lukija on kirjoittajan kanssa samaa mieltä siitä, että modulimuodot ovat hyvin tärkeitä.)

Modulimuotoihin liitttyvät ongelmat saavuttivat huomattavaa mainetta, kun Andrew Wiles ja Richard Taylor todistivat Fermat'n viimeisen lauseen (tai oikeastaan, viimeisen konjektuurin). Tämä ei kuitenkaan ole ainoa esimerkki modulimuotojen maagisista ominaisuuksista. Klassinen tulos on Jakobin neljän neliön lauseen todistus: modulimuodot eivät ainoastaan kerro, että jokainen positiivinen kokonaisluku on esitettävissä neljän neliön summana, vaan myös kuinka monella tavalla tämä onnistuu. Ehkäpä vielä hieman hämmentävämpi on erään Linnikin ongelman ratkaisu: Keskitytään tarkastelemaan sellaisia n, jotka voidaan esittää kolmen neliön summana (ja joilla ratkaisuja on epätriviaali määrä). Asetellaan nämä ratkaisut hilapisteiksi avaruuteen $\mathbb{R}^3$, ja normeerataan luvulla $\sqrt{n}$, jolloin pisteet romahtavat yksikköpallolle. Kun $n \to \infty$, pisteet jakautuvat pallolla tasaisesti.

Lopuksi, monisteessa on monin paikoin ärsyttävästi tai tyynesti jätetty esimerkkejä ja todistuksia auki. Niiden on tarkoitus ilmestyä luennoilla. Monisteen tarkoitus tällä kurssilla on antaa jonkinlainen käsitys siitä, miten kaikki toimii, mutta sivuuttaa melkoinen määrä yksityiskohtia. Yksityiskohdat ovat luennoilla, laskuharjoituksissa, ja ne löytyvät myös alan kirjoista.

Luvut 2 ja 3 perustuvat Jutilan modulimuotojen monisteeseen [8] sekä Koecherin ja Kriegin kirjaan [11]. Luku 4 perustuu Jutilan monisteeseen [8]. Luku 5 perustuu Jutilan kirjaan eksponenttisummista [7] sekä Huxleyn kirjaan [4]. Luku 6 perustuu puolestaan Duken [2] ja Duken, Friedlanderin ja Iwaniecin [3] artikkeleihin. Luku 7 perustuu Alkanin ja Zaharescun paperiin [1] ja luku 8 Rankinin artikkeliin [13]. Seuraavaksi monisteesta löytyy kirjallisuuslista.

Kirjallisuutta

[1] Emre Alkan ja Alexandru Zaharescu, *Nonvanishing of the Ramanujan tau-function in short intervals*. International Journal of Number Theory 1, no 1, 45–51 (2005).

[2] W. Duke, *An Introduction to the Linnik Problems*. `www.math.ucla.edu/~wdduke/preprints/linnik.pdf`

[3] W. Duke, J. Friedlander ja H. Iwaniec *Bounds for automorphic L-functions*. Inventiones mathematicae 112, 1–8 (1993).

[4] Martin N. Huxley, *Area, lattice points and exponential sums*. Clarendon Press, Oxford, 1996.

[5] Henryk Iwaniec, *Topics in Classical Automorphic Forms*. American Mathematical Society, 1997.

[6] Henryk Iwaniec ja Emmanuel Kowalski, *Analytic Number Theory*. American Mathematica Society, 2004.

[7] Matti Jutila *Lectures on a method in the theory of exponential sums* Tata Institute of Fundamental Research, Bombay. Springer-Verlag, 1987.

[8] Matti Jutila, *Modulimuodot*. Turun yliopiston luentomoniste, syksy 2002.

[9] Matti Jutila, *Neliömuodot*. Turun yliopiston luentomoniste, kevät 2002.

[10] *On exponential sums involving the Ramanujan function* Proceedings of the Indian Academy of Sciences (Mathematical Sciences) 97, no 1-3, 157–166 (1987).

[11] Max Koecher ja Aloys Krieg, *Elliptische Funktionen und Modulformen*. Springer Verlag, 1998.

[12] N. N. Lebedev, *Special functions and their applications*. Dover Publications, inc, 1972.

[13] R. A. Rankin *Sums of Powers of Cusp Form Coefficients II*. Mathematische Annalen 272, 593–900 (1985).

[14] G. Shimura *On modular forms of half integral weight*. Annals of Mathematics (2) 97, 440-481 (1973).

[15] Elias M. Stein ja Rami Shakarchi, *Complex Analysis*. Princeton University Press, 2003.

Luku 2

Möbius-kuvaukset

2.1 Kompleksitason täydennys

On varsin hyödyllistä täydentää kompleksitaso äärettömyyspisteellä, jolloin satunnaiset ääret-tömät arvot eivät esimerkiksi riko jatkuvuutta. Ajatellaan siis kompleksitaso ja äärettömyys-piste yhteensä pallona, jonka etelänapa on origo, pohjoisnapa ääretön (samaistetaan äärettö-mät merkistä, imaginäärisyydestä, reaalisuudesta tai muusta vastaavasta riippumattomasti). Nyt origon kautta kulkevat suorat muodostavat pallon pituuspiirit. Huomattava on, että nämä suorat leikkaavat samoissa kulmissa (suunnistusta vaille) sekä äärettömässä että origossa.

Tämä avaruus tarvitsee myös topologian. Äärettömän ulkopuolella voidaan sujuvasti käyt-tää tavallista euklidisen metriikan virittämää topologiaa. Ei ole kuitenkaan hyvä ajatus eristää ääretöntä, koska silloin funktioiden jatkuvuus menee rikki, jos jossakin äärellisessä pisteessä funktion arvo on ääretön. Täten joudumme harkitsemaan tarkkaan millaisia ympäristöjä luom-me äärettömälle. Toimiva ajatus on tämä: Jos $z \neq \infty$, niin $B_\delta(z) = \{w \in \mathbb{C} : |z - w| < \delta\}$. Äärettömässä taas: $B_\delta(\infty) = \{w \in \mathbb{C} : |w| > \frac{1}{\delta}\}$.

2.2 Möbius-kuvaukset

Möbius-kuvaukset ovat funktioita $f : \mathbb{C} \leftarrow \mathbb{C}$

$$f(z) = \frac{az + b}{cz + d},$$

kun $ad - bc \neq 0$. Olemme kiinnostuneita ensisijaisesti Möbiuskuvauksista, jotka vastaavat matriisiryhmää $\mathrm{SL}(2, \mathbb{Z})$, eli kuvauksista

$$f(z) = \frac{az + b}{cz + d},$$

missä $a, b, c, d \in \mathbb{Z}$ ja $ad - bc = 1$. Merkitään $f_M(z) = \frac{az+b}{cz+d}$, kun $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$ Kuitenkin, jos erikseen ei sanota, niin todistetaan seuraavat lauseet kaikille Möbius-kuvauksille, eikä ainoas-taan ryhmää $\mathrm{SL}(2, \mathbb{Z})$ vastaaville matriiseille. Tarkastellaan ensin näiden perusominaisuuksia:

Lause 1. *Möbius-kuvausten yhdistäminen toimii sympaattisesti yhteen matriisien kertolaskun kanssa, eli*

$$f_{M_1 M_2}(z) = f_{M_1}\left(f_{M_2}(z)\right).$$

Todistus. Harjoitustehtävä 1.1 □

Lause 2. *Möbius-kuvaukset muodostavat ryhmän.*

Todistus. Varsin helppo laskutehtävä, ilmestyy taululle luennoilla. □

Konformisuuden määritelmä on hieman vaihteleva. Hyvin yleinen määritelmä on se, että kuvaus säilyttää kulmat. Tähän riittää se, että kuvaus on holomorfinen ja derivaatta nollasta poikkeava. Toisinaan konformisuuden tulkitaan tarkoittavan holomorfista biljektiota (katso vaikka Steinin ja Shakarchin kirja). On syytä huomata, että esimerkiksi funktio $g(z) = z^2$ on holomorfinen ja sen derivaatta on nollasta poikkeava alueella $\mathbb{C} \setminus \{0\}$, mutta ei siitä bijektiota koko tuolla alueella saa kirveelläkään. Modulimuotojen teoriassa on fiksua elää yhä pinnalla, jossa äärettömyys on normaali piste muiden joukossa. Emme siis annan mahdollisten äärettömien arvojen (toistaiseksi) rikkoa määritelmiä. Käytämme siis yksinkertaisesti Jutilan monisteen hengessä konformisuudelle määritelmää

Määritelmä 3. Kuvaus f on konforminen, jos sen derivaatta on nollasta poikkeava, kun piste ja kuvauksen arvo ovat äärettömästä poikkeavat. Jos taas ainakin toinen on ääretön, niin "normalisoidaan tilanne"kuvauksella $z \to \frac{1}{z}$, ja jos $f(\infty) \neq \infty$, niin f on konforminen äärettömyyspisteessä, jos funktiolle $h(z) = f(1/z)$ pätee $h'(0) \neq 0$. Jos taas $f(z_0) = \infty$ ja $z_0 \in \mathbb{C}$, niin f on konforminen z_0:ssa, jos funktiolle $h(z) = \frac{1}{f(z)}$ pätee $h'(z_0) \neq 0$. Jos $f(\infty) = \infty$, niin f on konforminen äärettömässä, jos $h'(0) \neq 0$ funktiolle $h(z) = \frac{1}{f(1/z)}$.

Lause 4. *Möbius-kuvaukset ovat konformisia.*

Todistus. Kun $z \neq \infty$ sekä $z \neq -\frac{d}{c}$ (jos c=0, nämä pisteet voidaan tulkita samoiksi), tarkastellaan derivaattaa.

$$D\frac{az+b}{cz+d} = \frac{-(az+b)c + a(cz+d)}{(cz+d)^2} = \frac{ad-bc}{(cz+d)^2} \neq 0.$$

□

Jos $c = 0$, niin on helppo nähdä, että kuvaus $\frac{1}{f(1/z)} = \frac{dz}{bz+a}$ on konforminen origossa. Jos $c \neq 0$, niin samoin nähdään helposti kuvauksen $g(1/z)$ konformisuus origossa ja kuvauksen $1/g(z)$ konformisuus pisteessä $-d/c$.

Lause 5. *Jokainen Möbiuksen kuvaus voidaan esittää kompositiona kuvauksista*

$$\begin{aligned} g(z) &= z + \lambda && \textit{siirto} \\ g(z) &= az, a > 0 && \textit{venytys tai kutistus} \\ g(z) &= e^{i\alpha}z, \alpha \in \mathbb{R} && \textit{kierto} \\ g(z) &= -\frac{1}{z} && \textit{peilaus.} \end{aligned}$$

Todistus. Jos $c = 0$, niin voidaan kirjoittaa

$$\frac{az+b}{d} = \left|\frac{a}{d}\right| e^{i \arg(a/d)} z + \frac{b}{d},$$

mikä on ilmeinen kompositio ylläolevista kuvauksista. Jos taas $c \neq 0$, niin

$$\frac{az+b}{cz+d} = \frac{a}{c} - \frac{ad-bc}{c(cz+d)},$$

mikä on myös halutunlainen kompositio. □

Kutsutaan *yleistetyksi* ympyräksi äärettömällä täydennetyssä kompleksitasossa ympyrää sekä suoraa.

Lause 6. *Möbius-kuvaukset kuvaavat yleistetyt ympyrät yleistetyille ympyröille.*

Todistus. Yleistetty ympyrä voidaan xy-tasossa kirjoittaa muodossa

$$a(x^2 + y^2) + bx + cy + d = 0.$$

(Ilmeisesti suorilla $a = 0$ ja muulloin kyseessä on ympyrä.) Ottamalla käyttöön kompleksimuuttuja $z = x + yi$ voidaan yhtälö kirjoittaa muotoon

$$az\overline{z} + Bz + \overline{Bz} + d = 0,$$

missä $B = \frac{1}{2}(b - ci)$. On ilmeistä, että siirrossa, kutistuksessa, venytyksessä ja kierrossa suora tai ympyrä pysyy suorana tai ympyränä. Mielenkiintoinen tapaus siis on, mitä tapahtuu peilauksessa.

Kirjoitetaan $w = -\frac{1}{z}$. Sijoitetaan siis $z = -\frac{1}{w}$ yleistetyn ympyrän lausekkeeseen:

$$a\left(-\frac{1}{w}\right)\overline{\left(-\frac{1}{w}\right)} - B \cdot \frac{1}{w} - \overline{B} \cdot \frac{\overline{1}}{w} + d = 0,$$

eli

$$dw\overline{w} - \overline{B}w - B\overline{w} + a = 0,$$

mikä kuvaa yleistettyä ympyrää. Tästä näemmekin vielä milloin suora muuttuu ympyräksi tai ympyrä suoraksi, sillä a ja d vaihtavat paikkaa. □

Esimerkki 7. Tarkastellaan Cayleyn kuvausta.

Määritelmä 8. Määritellään neljän pisteen kaksoisuhde seuraavasti:

$$(z_1, z_2; z_3, z_4) = \frac{(z_1 - z_2)(z_3 - z_4)}{(z_2 - z_3)(z_4 - z_1)}.$$

Lause 9. *Kaksoissuhde on invariantti Möbiuksen kuvauksissa.*

Todistus. Suoraviivainen lasku suoritetaan luennoilla. □

Esimerkki 10. Tarkastellaan miten kaksoissuhteen avulla saa määritettyä Möbius-kuvauksen, jos kolmen pisteen kuvaukset tiedetään.

Ryhmässä $\mathrm{SL}(2, \mathbb{R})$ on seuraavanlaisia matriiseja:

$$k(\varphi) = \begin{pmatrix} \cos\varphi & \sin\varphi \\ -\sin\varphi & \cos\varphi \end{pmatrix}$$
$$n(x) = \begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$$
$$a(y) = \begin{pmatrix} y^{1/2} & 0 \\ 0 & y^{-1/2} \end{pmatrix}.$$

Merkitään ensimmäistä matriisijoukkoa K:lla, toista N:llä ja viimeistä A:lla. Nyt päästään muotoilemaan Iwasawan hajotelma (johon muinoin Turussa opiskelijat viittailivat nakkina).

Lause 11 (Iwasawan hajotelma)**.** *On olemassa esitys*

$$SL(2,\mathbb{R}) = NAK,$$

eli jokainen matriisi $M \in SL(2,\mathbb{R})$ *voidaan kirjoittaa yksikäsitteisesti muodossa*

$$M = n(x)a(y)k(\varphi),$$

missä parametrit määräytyvät yhtälöstä

$$M(i) = x + yi.$$

Ryhmä K *on pisteen* i *kiintoryhmä, eli niiden matriisien* $M \in SL(2,\mathbb{R})$ *joukko joille* $M(i) = i$*.*

Todistus. Harjoitustehtävät 1.3 ja 1.4 seuraavasti:
1.3. Todista, että K on luvun i kiintoryhmä.
1.4. Totea, että jos $M(i) = x+yi$, niin $M^{-1}n(x)a(y)$ on pisteen i kiintoryhmässä K, ja todista tämän avulla Iwasawan hajotelman olemassaolo ja yksikäsitteisyys. □

2.3 SL$(2,\mathbb{Z})$ ja perusalue

Matriisiryhmä SL$(2,\mathbb{Z}$ koostuu niistä 2×2-matriiseista, joiden kaikki alkiot ovat kokonaislukuja ja determinantti on yksi, eli

$$\mathrm{SL}(2,\mathbb{Z}) = \left\{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} : ad - bc = 1 \text{ ja } a,b,c,d, \in \mathbb{Z} \right).$$

Aloitetaan tarkastelemassa tämän matriisiryhmän virittäjiä.

Lause 12. *Matriisiryhmän SL(*$2,\mathbb{Z}$*) virittävät matriisit* $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$ *sekä* $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$.

Todistus. Huomataan aluksi, että

$$\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$$

sekä

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}^{-1} = \begin{pmatrix} 1 & -m \\ 0 & 1 \end{pmatrix}$$

Olkoon $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}(2,\mathbb{Z})$. Oletetaan, että $|b| > |a|$, sillä jos näin ei ole, niin kerrotaan matriisi oikealta matriisilla $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Kirjoitetaan $c = aq + r$, missä $r < a$. Kerrotaan

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} 1 & -q \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} a & -aq+b \\ c & d \end{pmatrix} = \begin{pmatrix} a & r \\ c & -qc+d \end{pmatrix}.$$

Koska $|a| > |r|$, kerrotaan oikealta matriisilla $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. Jatketaan näin, kunnes matriisin ylärivillä ovat luvut ± 1 ja 0 tässä järjestyksessä. Mikäli kyseessä on -1, kerrotaan matriisilla $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix} = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2$. Näin saadaan matriisi muotoon

$$\begin{pmatrix} 1 & 0 \\ c' & d' \end{pmatrix}.$$

Determinanttiehdon vuoksi on pädettävä $d' = 1$. Käsissämme on siis matriisi

$$\begin{pmatrix} 1 & 0 \\ c' & 1 \end{pmatrix}.$$

Mikäli $c' = 1$, on todistus valmis. Jos näin ei ole, kerrotaan matriisi vasemmalta matriisilla $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$:

$$\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ c' & 1 \end{pmatrix} = \begin{pmatrix} -c' & -1 \\ 1 & 0 \end{pmatrix}.$$

Kerrotaan seuraavaksi oikealta matriisilla $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ ja saadaan

$$\begin{pmatrix} -c & -1 \\ 1 & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix}.$$

Kerrotaan nyt oikealta matriisilla $\begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix}$:

$$\begin{pmatrix} -1 & c \\ 0 & -1 \end{pmatrix} \begin{pmatrix} 1 & c \\ 0 & 1 \end{pmatrix} = \begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}.$$

Tämä onkin matriisi $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}^2$, mikä todistaa väitteen. □

Lause 13. *Ryhmää $SL(2,\mathbb{Z})$ vastaavat Möbius-kuvaukset muodostavat ryhmän.*

Todistus. Lisänä Lauseeseen 2 pitää lähinnä verifioida eräiden operaatioiden sulkeutuneisuus joukkoon $\mathrm{SL}(2,\mathbb{Z})$, mikä tehdään luennolla. □

Esimerkki 14. Tarkastellaan miten matriisi $\begin{pmatrix} 4 & 5 \\ 3 & 4 \end{pmatrix}$ voidaan esittää matriisiryhmän virittäjien $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ sekä $\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$ avulla.

Ylläolevaan esimerkkiin liittyy luonteva harjoitustehtävä (HT 1.6): Esitettävä matriisi $\begin{pmatrix} 7 & 4 \\ 5 & 3 \end{pmatrix}$ virittäjien avulla.

Modulimuotojen kanssa eläessämme ylempi puolitaso

$$\mathbb{H} = \{z \in \mathbb{C} : \Im z > 0\}$$

tulee osoittautumaan erinomaisen hyödylliseksi joukoksi. Todistetaan siis seuraavaksi, että ryhmään $\mathrm{SL}(2,\mathbb{Z})$ liittyvällä Möbius-kuvauksella ylempi puolitaso kuvautuu ylemmälle puolitasolle. Formaalisti tämä tarkoittaa:

Lause 15. *Olkoon $M \in SL(2,\mathbb{Z})$. Nyt*

$$\Im f_M(z) > 0,$$

kun $\Im z > 0$.

Todistus. Harjoitustehtävä 1.2. □

Tässä välissä on hyvä hieman tarkastella Möbius-kuvausten mallia. Todistetaan siis seuraava väite:

Lemma 16. *Jos syt$(c,d) = 1$, niin on olemassa ryhmän $SL(2,\mathbb{Z})$ matriisia vastaava Möbius-kuvaus, joka on muotoa $\frac{az+b}{cz+d}$. Lisäksi tällaisia kuvauksia on ääretön määrä, ja ne saadaan toisistaan kertomalla vasemmalta matriisilla $\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix}$ sopivalla luvun m arvolla.*

Todistus. Ryhmää $\mathrm{SL}(2,\mathbb{Z})$ vastaavalta Möbius-kuvaukselta ei lopulta muuta vaadita kuin että kertoimet ovat kokonaislukuja ja toteuttavat ehdon $ad - bc = 1$. Jos c ja d on annettu ja niiden syt on yksi, niin Diofantoksen yhtälöiden teorian mukaan ylläolevalla yhtälöllä on ääretön määrä ratkaisuja, ja ne ovat muotoa $a = a_0 + cm$ ja $b = b_0 + dm$, missä (a_0, b_0) on yksittäisratkaisu. Koska

$$\begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \cdot \begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} a+mc & b+md \\ c & d \end{pmatrix},$$

tämä myös tarkoittaa sitä, että matriisit saadaan toisistaan täsmälleen kuten väitetty. □

Perusalueeksi kutsutaan sellaista aluetta ylemmässä puolitasossa, että kaikki ylemmän puolitason pisteet voidaan tähän alueeseen siirtää käyttämällä ryhmään $\mathrm{SL}(2,\mathbb{Z})$ liittyviä Möbius-kuvauksia. Osoitetaan seuraavaksi, että alue $\mathcal{F}$, joka koostuu joukosta

$$F = z \in \mathbb{H} : |z| > 1, -\frac{1}{2} < z < \frac{1}{2}$$

täydennettynä reunakäyrällään puolitasossa $\Re z \geq 0$ on perusalue:

Lause 17. *Millä tahansa pisteella $z \in \mathbb{H}$ on olemassa $M \in SL(2,\mathbb{Z})$, jolla $f_M(z) \in \mathcal{F}$.*

Todistus. Valitaan sellaiset kokonaisluvut c ja d, $(c,d) \neq (0,0)$, että $|mz+n| \geq |cz+d|$ kaikilla $m,n \in \mathbb{Z}$, $(m,n) \neq (0,0)$. Selvästi c ja d ovat yhteistekijättömiä. Lemman 16 nojalla on olemassa matriiseja $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$, ja näitä vastaavilla Möbius-kuvauksilla $\left|\frac{az+b}{cz+d}\right| \geq 1$. Kirjoitetaan nyt $\begin{pmatrix} a & b \\ c & d \end{pmatrix} = \begin{pmatrix} 1 & k \\ 0 & 1 \end{pmatrix} \begin{pmatrix} a_0 & b_0 \\ c & d \end{pmatrix}$, missä k on valittu sopivasti, ja kirjoitetaan $z' = \frac{az+b}{cz+d} = k + \frac{a_0 z + b_0}{cz+d}$, jolloin saadaan varmistettua, että $-\frac{1}{2} < \Re z' \leq \frac{1}{2}$. Lisäksi $|z'| \geq 1$. Jos $-\frac{1}{2} < \Re z' < 0$ ja $|z'| = 1$, tehdään vielä siirros $\frac{1}{-z'}$, jonka jälkeen luku on perusalueella. □

Todistetaan vielä, että koko alue tarvitaan, eli että mikään alueen osajoukko ei riitä perusalueeksi:

Lause 18. *Jos $z \in \mathcal{F}$ ja $Mz \in \mathcal{F}$ jollakin $M \in SL(2,\mathbb{Z})$, niin pätee $z = Mz$. Jos $M \neq (\pm 1) \cdot \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$, niin on oltava joko $z = Mz = i$, jolloin $M = (\pm 1) \cdot \begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ tai $z = Mz = \frac{1}{2} + \frac{1}{2} i\sqrt{3}$, jolloin $M = \pm U$ tai $M = \pm U^2$, missä $U = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$.*

Todistus. Aloitetaan tilanteella, jossa z sekä Mz kuuluvat perusalueeseen, ja $Mz = \frac{az+b}{d}$. Tällöin $ad = 1$, eli $Mz = z + \ell$ jollakin $\ell \in \mathbb{Z}$. Oltava siis $\ell = 0$, eli $M = \pm \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}$. Voidaan nyt olettaa, että $z, Mz \in \mathcal{F}$, missä $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix}$, missä $c > 0$. Kirjoitetaan $z = x + iy$. Koska $z, Mz \in \mathcal{F}$, pätee $\frac{1}{2}\sqrt{3} \leq y$ and $\frac{1}{2}\sqrt{3} \leq Mz = \frac{y}{|cz+d|^2}$. Huomataan, että $|cz + d|^2 \geq c^2 y^2$. Sijoitetaan:

$$\frac{1}{2}\sqrt{3} \leq \frac{y}{|cz+d|^2} \leq \frac{y}{c^2 y^2} = \frac{1}{c^2 y} \leq \frac{1}{\frac{1}{2}\sqrt{3} c^2},$$

eli $\frac{3}{4}c^2 \leq 1$, ja koska c on kokonaisluku, $c \neq 0$, ja voimme olettaa, että cÊ on positiivinen (kuten aiemmin todettu), pätee $c = 1$. Tarkastellaan seuraavaksi luvun d suuruutta. Voidaan arvioida

$$|z + d|^2 = (x + d)^2 + y^2 \geq 2y|x + d|.$$

Koska

$$\frac{1}{2}\sqrt{3} \leq \frac{y}{|z+d|^2} \leq \frac{y}{2y|x+d|} = \frac{1}{2|x+d|},$$

saadaan $\sqrt{3}|x+d| \leq 1$, ja koska $|x| \leq \frac{1}{2}$, pätee $d \in \{0, \pm 1\}$. Jaetaan tarkastelu nyt tapauksiin:

1. $d = 0$. Nyt
$$M = \begin{pmatrix} m & -1 \\ 1 & 0 \end{pmatrix} = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}^m \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix},$$
eli $Mz = m - \frac{1}{z}$. Kun $|z| > 1$, pätee $\Re\left(\frac{-1}{z}\right) = \frac{\Re z}{|z|^2} < \frac{1}{2}$, joten $m = 0$, ja tämän seurauksena $|Mz| < 1$. On siis pädettävä $|z| = 1$, ja koska $Mz = m - \overline{z} = (m - x) + iy$, huomataan, että ainoat mahdollisuudet ovat $m = 0$, $z = Mz = i$ ja $M = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ sekä $m = 1$, $z = Mz = \frac{1}{2} + \frac{1}{2} i\sqrt{3}$ ja $M = \begin{pmatrix} 1 & -1 \\ 1 & 0 \end{pmatrix}$. Voimme siirtyä seuraacaan tapaukseen.

2. $d = \pm 1$. Tällöin $|z + d|^2 = (x \pm 1)^2 + y^2 \geq y^2 + \frac{1}{4}$, eli
$$\frac{1}{2}\sqrt{3} \leq \Im Mz \leq f(y),$$
missä $f(y) = \frac{y}{y^2+1/4}$. Koska $f(y)$ on monotonisesti laskeva funktio, kun $y \geq \frac{1}{2}$, ja $f\left(\frac{1}{2}\sqrt{3}\right) = \frac{1}{2}\sqrt{3}$, on pädettävä $\Im Mz = y = \frac{1}{2}\sqrt{3}$. Täten $x = \frac{1}{2}$, ja $z = Mz = \frac{1}{2} + \frac{1}{2} i\sqrt{3}$. Koska $y = \Im Mz = \frac{y}{|z+d|^2}$, on
$$1 = \frac{1}{|d + 1/2|^2 + \left(\sqrt{3}/2\right)^2},$$

eli $|d+1/2| = \frac{1}{2}$, eli $d = -1$, jolloin $M = \begin{pmatrix} * & * \\ 1 & -1 \end{pmatrix}$. Lemman 16 nojalla saadaan

$$M = \begin{pmatrix} 1 & m \\ 0 & 1 \end{pmatrix} \left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right)^2$$

jollakin $m \in \mathbb{Z}$. Koska $\left(\begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 1 \end{pmatrix} \right) \left(\frac{1}{2} + \frac{1}{2}i\sqrt{3}\right) = \frac{1}{2} + \frac{1}{2}i\sqrt{3}$ ja $M\left(\frac{1}{2} + \frac{1}{2}i\sqrt{3}\right) = \frac{1}{2} + \frac{1}{2}i\sqrt{3}$, pätee $m = 0$, eli $M = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}^2$.

□

Muotoillaan nyt seuraava harjoitustehtävä (HT 1.5): Mitä ylemmän lauseen määrittelemälle perusalueelle tapahtuu, kun sitä siirretään matriisia $\begin{pmatrix} 0 & 1 \\ -1 & 0 \end{pmatrix}$ vastaavalla Möbius-kuvauksella?

Luku 3

Modulimuotojen perusominaisuudet

Todetaan ensin sanastosta sen verran, että sekä suomessa että englannissa sanojen käyttö on hieman horjuvaa toisinaan (puhutaan modulimuodoista, heikoista modulimuodoista, modulifunktioista, automorfifunktioista, jne), mutta yleisperiaate on, että muoto viittaa holomorfisuuteen, funktio meromorfisuuteen.

Toisinaan näkee käytettävän mystistä termiä modulaarinen muoto, mitä ei ainakaan minun tietääkseni yksikään suomalainen modulimuotojen tutkija käytä. Sen sijaan ryhmään $\mathrm{SL}(2,\mathbb{Z})$ liittyviin Möbius-kuvauksiin voidaan viitata modulaarisina kuvauksina.

3.1 Modulimuotojen perusteet

Tämän luvun tulisi olla alemman Fourier-sarjoja käsittelevän luvun alla, mutta lukujen järjestys on tämä, jotta modulimuotojen määritelmä on aina tarpeen tullen mahdollisimman helposti löydettävissä.

Aloitetaan määritelmällä, jotta se on helposti löydettävissä aina tarpeen tullen. Jotta voidaan määritellä modulimuoto, tarvitsemme ensin yhden toisen määritelmän.

Määritelmä 19. Olkoon *kappa* kokonaisluku, $g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z})$ ja $f : \mathbb{H} \to \mathbb{C}$ funktio. Silloin

$$(f \mid_\kappa g) = f(g(z))(cz+d)^{-\kappa}.$$

Jos "paino"κ on selvä asiayhteydestä, voidaan kirjoittaa vain $(f \mid g)$

Tästä saamekin heti sopivan harjoitustehtävän seuraavan lauseen todistuksen muodossa:

Lause 20. *Yllämääritelty operaattori toteuttaa eräänlaiset ketjusäännöt: Kirjoitetaan $j(g,z) = cz + d$, kun g on määritelty kuten yllä. Tällöin*

$$j(g_1 g_2) = j(g_1, g_2(z)) j(g_2, z)$$

ja

$$(f \mid (g_1 g_2))(z) = ((f \mid g_1) \mid g_2)(z),$$

kun $g_1, g_2 \in SL(2,\mathbb{Z})$.

Todistus. Harjoitustehtävä 2.3. □

Esitetään nyt modulimuodon määritelmä.

Määritelmä 21. Funktio f on painoa κ oleva modulimuoto, jos

1. f on holomorfinen ylemmässä puolitasossa $\mathbb{H}$ ja äärettömässä.
2. $f \mid_\kappa M = f$ kaikilla $M \in \mathrm{SL}(2,\mathbb{Z})$.

Jos ensimmäinen ehto korvataan sillä, että f on meromorfinen $\mathbb{H}$:ssa ja äärettömässä, niin f on modulifunktio. Jos modulimuodolla f on nollakohta äärettömässä, niin f on kärkimuoto. Jos taas funktio f on painoa nolla oleva modulifunktio, niin sitä kutsutaan automorfifunktioksi.

Ensimmäinen ehto määritelmässä voidaan myös muuttaa muotoon: Funktiolla f on Fourier-kehitelmä, joka on muotoa

$$f(z) = a_0 + \sum_{n=1}^{\infty} a_n e(nz),$$

missä $e(x) = e^{2\pi i x}$. Jos $a_0 = 0$, on f kärkimuoto. Tämä perustellaan myöhemmin monisteessa. Toinen ehto puolestaan voidaan muotoilla uusiksi matriisiryhmän $\mathrm{SL}(2,\mathbb{Z})$ generaattorien $T = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$ ja $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ avulla: Ehto $f \mid_\kappa M = f$ kaikilla $M \in \mathrm{SL}(2,\mathbb{Z})$ on yhtäpitävä sen kanssa, että $f \mid_\kappa T = f$, eli $f(z+1) = f(z)$ ja $f \mid_\kappa S = f$, eli $f\left(-\frac{1}{z}\right) z^{-\kappa} = f(z)$.

On syytä huomata, että valitsemalla määritelmässä matriiksi M matriisin $\begin{pmatrix} -1 & 0 \\ 0 & -1 \end{pmatrix}$ saadaan $f = (-1)^\kappa f$, jolloin $f \equiv 0$ on ainoa ehdon toteuttava funktio, jos κ on pariton. Tämä funktio on kuitenkin mielenkiinnoton, joten keskitytään tilanteeseen, jossa κ on parillinen.

Esimerkki 22. Tarkastellaan modulimuotojen käytöstä tuloissa.

Määritellään Eisensteinin sarjat seuraavasti:

$$G_k(\tau) = \sum_{m^2+n^2 \neq 0; m,n \in \mathbb{Z}} (m + n\tau)^{-k}.$$

Kun $k \geq 4$ on parillinen kokonaisluku, on $G_k(\tau)$ holomorfinen painoa k oleva modulimuoto, vaan ei kärkimuoto. Tämän osoittaminen on harjoitustehtävä 2.1. Harjoitustehtävä 2.2 on konstruoida holomorfinen kärkimuoto funktioiden G_k avulla.

3.2 Fourier-sarjojen teoriaa

Jotta voimme sujuvasti käsitellä modulimuotoja on hyvä hieman kerrata Fourier-sarjojen teoriaa.

Oletetaan, että funktio $f : \mathbb{R} \to \mathbb{C}$ toteuttaa ehdot

1. Funktiolla f on jakso 1.
2. Funktio f on jatkuva jaksovälillä lukuunottamatta mahdollisesti äärellistä määrää epäjatkuvuuspisteitä, joissa on toispuoliset raja-arvot $f(x-)$ ja $f(x+)$.

3. Derivaatta f' on olemassa kaikissa jatkuvuuspisteissä ja epäjatkuvuuspisteissä funktiolla f on toispuoliset derivaatat.

Määritellään funktion f Fourier-kertoimet:

$$a_n = \int_0^1 f(x)e(-nx)dx.$$

Nyt

$$\frac{f(x+) + f(x-)}{2} = \sum_{n=-\infty}^{\infty} a_n e(nx).$$

Muotoillaan seuraavaksi Poissonin summakaava, joka on hyödyllinen jo itsessään, ja linkittyy kurssin myöhäisempään materiaaliin mukavasti, sillä Voronoi-tyyppiset summakaavat, joita tullaan myöhemmin käsittelemään, ovat jossain määrin Poissonin kaavan yleistyksiä.

Lause 23. *Olkoon $f : \mathbb{R} \to \mathbb{C}$ jatkuvasti derivoituva funktio, joka täyttää ehdot*

$$|f(x)|, |f'(x)| \leq c_1 \min(1, |x|^{-c_2})$$

joillakin vakioilla $c_1 > 0$ ja $c_2 > 1$. Kirjoitetaan

$$\hat{f}(x) = \int_{-\infty}^{\infty} f(y)e(xy)dy$$

(funktion f Fourier'n muunnos.) Nyt

$$\sum_{-\infty}^{\infty} f(n) = \sum_{-\infty}^{\infty} \hat{f}(n)$$

Todistus. Kirjoitetaan $F(x) = \sum_{n=-\infty}^{\infty} f(x+n)$. Tällöin $F(0)$ vastaa yhtälön vasenta puolta. Lisäksi $F(x) = F(x+1)$. Lisäksi funktion $F(x)$ määrittelemä sarja suppenee itseisesti ja tasaisesti, joten $F(x)$ voidaan derivoida termeittäin. Funktiolla $F(x)$ on siis Fourier'n kehitelmä. Lasketaan nyt Fourier'n kertoimet:

$$a_m = \int_0^1 F(x)e(-mx)dx = \sum_{n=-\infty}^{\infty} \int_0^1 f(x+n)e(-mx)dx = \int_{-\infty}^{\infty} f(y)e(-my)dy = \hat{f}(-m)$$

Lisäksi $F(0) = \sum_{-\infty}^{\infty} a_m$, mikä todistaa väitteen. □

Tarkastellaan seuraavaksi sarjoja ylemmällä puolitasolla. Merkitään $q = e^{2\pi iz}$, jolloin voidaan kirjoittaa niin sanottu *q-sarja*:

Lause 24. *Funktiolla f, jolla on jakso 1 ja joka on holomorfinen $\mathbb{H}$:ssa, on yksikäsitteinen esitys q-sarjana:*

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Toisaalta jokainen q-sarja, joka suppenee $\mathbb{H}$:ssa, määrittelee siinä holomorfisen 1-jaksoisen funktion.

Todistus. Huomataan aluksi, että

$$f(z) = f\left(\frac{\log q}{2\pi i}\right) = g(q),$$

missä g on määritelty puhkaistussa yksikkökiekossa (origo poistettu). Logaritmin haarat eroavat toisistaan luvun $2\pi i$ monikertojen verran, mutta tämä ei haittaa, koska f on jaksollinen. Huomataan, että g on holomorfinen puhkaistussa yksikkökiekossa, joten sillä on yksikäsitteinen Laurentin kehitelmä

$$g(q) = \sum_{n=-\infty}^{\infty} a_n q^n,$$

mikä antaakin funktiolle f q-sarjan yksikäsitteisesti. Toisaalta, jos on annettu suppeneva q-sarja, niin vastaava muuttujan q funktio on holomorfinen puhkaistussa yksikkökiekossa. Tällöin muuttujan z funktio $f(z) = g(e^{2\pi i q})$ on muuttujan z funktiona holomorfinen ylemmässä puolitasossa. □

Esimerkki 25. Kehitetään q-sarja funktiolle

$$\sum_{n=-\infty}^{\infty} (n-z)^{-k},$$

missä $k \geq 2$ on luonnollinen luku.

Otetaan seuraavaksi määritelmä, joka helpottaa elämää holomorfisten funktioiden kanssa huomattavasti – varsinkin kun kurssin kohteena tulevat olemaan eksponenttisummat.

Määritelmä 26. Olkoon 1-jaksoinen funktio f holomorfinen puolitasossa $\Im z > C(\geq 0)$, missä sillä on esitys

$$f(z) = \sum_{n=-\infty}^{\infty} a_n q^n.$$

Jos on olemassa sellainen indeksi n_0, että $a_{n_0} \neq 0$ ja $a_n = 0$, kun $n < n_0$, sanotaan, että f on äärellistä kertalukua äärettömyydessä, ja että $n_0 = \mathrm{ord}(f, \infty)$. Jos $n_0 \geq 0$, sanomme, että f on homorfinen äärettömyydessä, ja joka tapauksessa meromorfinen äärettömyydessä. Jos $n_0 < 0$, on ääretön funktion (eräs) napa. Jos taas $n_0 > 0$, on ääretön funktion (eräs) nollakohta, ja $|n_0|$ on navan tai nollakohdan kertaluku.

Tämä myös selittää, miten modulimuodon holomorfisuusehto voidaan esittää Fourier-sarjan avulla.

3.3 Modulimuotojen avaruuksien dimensiot

Merkitään M_κ painoa κ olevien modulimuotojen avaruutta, ja S_κ painoa κ olevien kärkimuotojen avaruutta. (Selitykset kirjainvalinnoille tulevat jälleen saksasta: Modulformen ja Spitzenformen.) Harjoitustehtävässä 2.1 havaitaan, että M_κ on epätyhjä. kun $\kappa > 2$ parillinen kokonaisluku. Harjoitustehtävässä 2.2 taas huomataan, että kärkimuotojakin on olemassa. Tämän luvun tarkoitus on selvittää avaruuksien dimensiot sekä karakterisoida avaruuksien rakenteet. Määritellään aluksi kertaluku äärellisissä pisteissä:

Määritelmä 27. Olkoon $f \neq 0$ modulimuoto, ja olkoon sen Laurentin kehitelmä pisteessä w

$$f(z) = \sum_{m \geq r} \gamma(m)(z-w)^m,$$

missä $\gamma(r) \neq 0$. Nyt voidaan määritellä kertaluku seuraavasti:

$$\mathrm{ord}(f, w) = r.$$

Näiden käsittelyä auttaa seuraava lemma:

Lemma 28. *Olkoon $M \in SL(2, \mathbb{Z})$ ja $z \in \mathbb{H}$. Tällöin*

$$ord(f, z) = ord(f, M(z)),$$

kun f on modulifunktio.

Todistus. Harjoitustehtävä 2.4. □

Edellisen lemman nojalla riittää tarkastella laajennettua perusaluetta

$$\mathcal{F}^\star = \mathcal{F} \cup \{\infty\}$$

tarkasteltaessa modulimuodon napoja ja nollakohtia. (Itse asiassa modulimuodollahan ei napoja ole, joten niiden tapauksessa riittää keskittyä nollakohtiin.)

Asetetaan nyt laajennetun perusalueen $\mathcal{F}^\star$ pisteille painot:

$$w(z) = \begin{cases} \frac{1}{2} & \text{kun } z = i \\ \frac{1}{3} & \text{kun } z = e^{\pi i/3} \\ 1 & \text{muulloin} \end{cases}$$

Nyt voidaan muotoilla niin kutsutta painokaava:

Lause 29. *Olkoon $f \neq 0$ painoa k oleva modulifunktio. Silloin*

$$\sum_{z \in \mathcal{F}^\star} w(z) ord(f, z) = \frac{k}{12}.$$

Todistus. Käsitellään monisteessa tapaus, jossa yksikään napa tai nollakohta, $z \neq i, e^{2\pi i/3}, e^{\pi i/3}$ ei ole perusalueen reunalla. Harjoitustehtävänä 2.5 on täydentää todistus tilanteeseen, jossa jokin nollakohta on perusalueen reunalla (vihjeenä todettakoon, että mitään kovin hankalaa ei kannata yrittää - vaadittavat modifikaatiot ovat hyvin pienet). Olkoon funktiolla f q-sarja

$$f(z) = \sum_{n=n_0}^{\infty} a_n q^n,$$

missä $n_0 = \mathrm{ord}(f, \infty)$. On olemassa sellainen $Y > 0$, että funktiolla f ei ole nollakohtia tai napoja puolitasossa $\Im z \geq Y$, sillä funktio

$$g(q) = \sum_{n=n_0}^{\infty} a_n q^n$$

on holomorfinen ja nollasta poikkeava jossakin sopivassa origon puhkaistussa ympäristössä. Integroidaan nyt funktio

$$F(z) = \frac{f'}{f}(z)$$

(niin kutsuttu logaritminen derivaatta) yli tasolta $\Im z = Y$ katkaistun perusalueen $\mathcal{F}$ reunan positiiviseen suuntaan kiertäen kuitenkin pisteet i ja $e^{\pi i/3}$ sekä $e^{e^{2\pi i/3}}$ pienillä ympyrän kaarilla. (Tästä tulee kuva luennoilla) Silloin F on holomorfinen integroimistiellä $\mathcal{C}$, ja sen sisäalueen pisteissä on ilmeisesti voimassa

$$\mathrm{Res}(F, z) = \mathrm{ord}(f, z),$$

ja jos tämä poikkeaa nollasta, niin $\mathrm{ord}(F, z) = -1$. Residylauseen mukaan

$$\frac{1}{2\pi i}\int_{\mathcal{C}} F dz = \sum_{z\in\mathcal{F}, z\neq i, e^{\pi i/3}} \mathrm{ord}(f, z).$$

Lasketaan nyt integraalit yli tien $\mathcal{C}$. Helpointa on ajatella tie useassa palikassa.

Lasketaan aluksi integraali x-akselin suuntaisen $\Im z = Y$ palan yli, oikealta vasemmalle (eli pisteestä $\frac{1}{2} + Yi$ pisteeseen $-\frac{1}{2} + Yi$). Tehdään muuttujanvaihto $q = e^{2\pi i z}$, jolloin q kiertää erään origokeskisen ympyrän negatiiviseen suuntaan. Nyt

$$\frac{1}{2\pi i}\int \frac{f'}{f}(z)dz = \frac{1}{2\pi i}\int \frac{g'}{g}(q)dq = -\mathrm{ord}(f, \infty)$$

(sillä keskimmäinen integraali vastaa funktion g residyä nollassa).

Tarkastellaan seuraavaksi y-akselin suuntaisten integraalien laskentaa. Tämä on kuitenkin helppo tehtävä, sillä nämä kumoavat toisensa (sama integraali, sillä $f(z) = f(z+1)$, mutta vastakkaisiin suuntiin.

Lasketaan nyt yksikköympyrän kaarella olevat kaksi integraalia. Huomataan aluksi, että sijoittamalla $w = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} z = \frac{-1}{z}$ päästään kaarelta toiselle. Integroinnin suunta tosin kääntyy (huomioi lausekkeen miinusmerkki). Siispä

$$\frac{1}{2\pi i}\int_{\text{oikea kaari}} \frac{f'}{f}(z)dz = -\frac{1}{2\pi i}\int_{\text{vasen kaari}} \frac{f'(-1/w)}{f(-1/w)}\frac{dw}{w^2}.$$

Koska f on modulifunktio, niin $f(-1/w) = w^k f(w)$, eli

$$f'(-1/w)w^{-2} = kw^{k-1}f(w) + w^k f'(w).$$

Sijoittaen:

$$\begin{aligned}\frac{1}{2\pi i}\int_{\text{vasen kaari oikealle}} \frac{f'}{f}(z)dz + \frac{1}{2\pi i}\int_{\text{oikea kaari oikealle}} \frac{f'}{f}(z)dz \\ = \frac{1}{2\pi i}\int_{\text{vasen kaari oikealle}} \frac{f'}{f}(z)dz - \frac{1}{2\pi i}\int_{\text{vasen kaari oikealle}} \left(\frac{k}{w} + \frac{f'}{f}(w)\right)dw \\ = -\frac{k}{2\pi i}\int_{\text{vasen kaari oikealle}} \frac{dw}{w} = \frac{k\alpha}{2\pi},\end{aligned}$$

missä α on yksikköympyrän kaarta vastaava keskuskulma. Kun pienet (poisto)ympyrät kutistuvat, $\alpha \to \frac{\pi}{6}$. Täten

$$\frac{1}{2\pi i}\int_{\text{yksikköympyrän kaari perusalueella oikealle}} \frac{f'}{f}(z)dz \to \frac{k}{12}.$$

On vielä laskettava kaikkien kolmen pikkuympyrän (pisteet i, $\frac{1}{2}+\frac{\sqrt{3}}{2}i$ sekä $-\frac{1}{2}+\frac{\sqrt{3}}{2}i$ ympäröivät) integraalit. Olkoon z_0 jokin näistä pisteistä. Voidaan kirjoittaa

$$\frac{f'}{f}(z) = \frac{\text{ord}(f,z_0)}{z-z_0} + h(z),$$

missä h on holomorfinen, ja täten rajoitettu pisteen z_0 ympäristössä. Nyt

$$\frac{1}{2\pi i}\int_{\text{kaari oikealle}} = \frac{1}{2\pi i}\int_{\text{kaari oikealle}} \frac{\text{ord}(f,z_0)}{z-z_0}dz + \frac{1}{2\pi i}\int_{\text{kaari oikealle}} h(z)dz.$$

Jälkimmäinen integraali häviää, kun kaaren sädettä pienennetään. Vain ensimmäinen jää siis jäljelle. Integraalista saadaan $-\frac{1}{2\pi}\cdot$kaarta vastaava kulma$\cdot \text{ord}(f,z_0)$. Kun $z_0 = \pm\frac{1}{2}+\frac{\sqrt{3}}{2}i$, on kaarta vastaava kulma $\frac{\pi}{3}$. Kun taas $z_0 = i$, on kulma π. Tämä todistaa väitteen. □

Merkitään $\Delta(z)$ vakiokerrointa vaille yksikäsitteistä painoa 12 olevaa kärkimuotoa. (Tällaisen kärkimuodon olemassaolo on helppo todeta – seuraavien todistusten avulla huomaamme, että tämä todellakin on yksikäsitteinen.) Ennen seuraavan lausetta, muotoillaan harjoitustehtävä:

Harjoitustehtävä 2.6: $\Delta(z) \neq 0$, kun $z \in \mathbb{H}$.

Muotoillaan nyt lause, joka antaa moduliavaruuden rakenteen.

Lause 30. *Olkoon κ parillinen kokonaisluku. Silloin*

$$M_\kappa = \bigoplus_{4n+6m=\kappa, n\geq 0 m\geq 0} \mathbb{C}g_4^n G_6^m.$$

Erityisesti M_κ on nolla-avaruus, kun $\kappa < 0$ tai $\kappa = 2$ sekä $M_0 = \mathbb{C}$. Lisäksi

$$M_\kappa = \mathbb{C}G_\kappa,$$

kun $\kappa = 4, 6, 8, 10, 14$. Voidaan myös kirjoittaa

$$M_\kappa = \mathbb{C}G_\kappa \bigoplus S_\kappa,$$

kun $\kappa \geq 4$. Lopulta kärkimuotoavaruudelle pätee

$$S_\kappa = \begin{cases} 0, & \text{jos } k < 12 \text{ tai } k = 14 \\ \mathbb{C}\Delta, & \text{jos } k = 12 \\ \Delta M_{\kappa-12} & \text{aina.} \end{cases}$$

Todistus. Jos $\kappa < 0$ tai $\kappa = 2$, on painokaava mahdoton toteuttaa, joten avaruuden on oltava tyhjä. Jos taas $\kappa = 0$ ja $f \in M_0$, missä f ei olisi vakio, olisi funktiolla $f - c$ nollakohta, kun c olisi sopivasti valittu. Painokaava ei kuitenkaan tällekään funktiolle päde (huomioitava, että olisi valittava kaavassa $k = 0$). Siispä $M_0 = \mathbb{C}$.

Voimme nyt keskittyä tilanteeseen $\kappa \geq 4$. Tiedämme, että $G_\kappa \in M_\kappa$, kun $\kappa \geq 4$. Jos $f \in M_\kappa$, niin $f - cG_\kappa = 0$ äärettömyydessä, kun c on sopivasti valittu. Siispä $f - cG_\kappa \in S_\kappa$, ja $f = cG_\kappa + (f - cG_\kappa)$ antaa esityksen suorana summana avaruudelle M_κ.

Painokaava on jälleen mahdoton, jos $f \in S_\kappa$, missä $\kappa < 12$ tai $\kappa = 14$, sillä kärkimuodoilla $\mathrm{ord}(f, \infty \geq 1)$.Tästä seuraa myös, että $M_\kappa = \mathbb{C}G_\kappa$, kun $\kappa = 4, 6, 8, 10, 14$.

Jos taas $f \in S_{12}$, niin $f\Delta \in M_0$ (muistettava, että funktiolla Δ ei ole nollakohtia), sillä $\mathrm{ord}(f, \infty) \geq \mathrm{ord}(\Delta, \infty) = 1$ (tämä tulee suoraan funktion Δ q-sarjasta). Koska $M_0 = \mathbb{C}$, on pädettävä $f = c\Delta$, eli $S_{12} = c\Delta$. Vastaavasti, jos $f \in S_\kappa$, niin $f/\Delta \in M_{\kappa-12}$, eli $f \in \Delta M_{\kappa-12}$.

Voimme nyt siirtyä avaruuden M_κ esittämiseen funktioiden G avulla. Selvästi funktiot $G_4^n G_6^m$ kuuluvat avaruuteen M_κ, kun $4n+6m = \kappa$. Nyt on vielä osoitettava, että nämä funktiot generoivat avaruuden. Voimme olettaa, että $\kappa > 6$. Koska κ on parillinen, voimme itse asiassa olettaa, että $\kappa \geq 8$. Tehdään induktio-oletus, että väite pätee pienemmille painon κ arvoille. Olkoon $f \in M_\kappa$, ja valitaan pari (m, n), joilla $4n + 6m = \kappa$. Modulimuoto $g = G_4^n G_6^m$ ei häviä äärettömyydessä (katso q-sarjoista), joten $f - cg \in S_\kappa$ sopivalla vakiolla c. Nyt $f - cg = \Delta h$, missä $h \in M_{\kappa-12}$. Funktiolle h pätee induktio-oletus, ja koska Δ on funktioiden G_4 ja G_6 polynomi, saadaan funktiolle f halutunlainen esitys.

On kuitenkin vielä todistettava funktioiden $G_4^n G_6^m$ lineaarinen riippumattomuus. Oletetaan, että

$$\sum_{n,m} a_{nm} G_4^n G_6^m = 0,$$

kun $n \geq 0, m \geq 0$, $4n + 6m = \kappa$, $a_{nm} \in \mathbb{C}$. Valitaan luvut (n', m') siten, että n' on mahdollisimman pieni. Jakamalla funktiolla $G_4^{n'} G_6^{m'}$ saadaan yhtälö

$$P\left(G_4^3/G_6^2\right) = 0,$$

missä P on polynomi. Jotta ylläoleva ehto voi toteutua, on funktion G_4^3/G_6^2 oltava vakio. Tämä ei kuitenkaan päde, sillä painokaavan nojalla $G_4\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) = 0$, ja $G_6\left(\frac{1}{2} + \frac{\sqrt{3}}{2}i\right) \neq 0$, mutta $G_4(i) \neq 0$ ja $G_6(i) = 0$. Painokaavan nojalla nämä ovat itse asiassa funktioiden G_4 ja G_6 ainoat nollakohdat laajennetussa perusalueessa. □

Lause 31. *Olkoon $\kappa \geq 0$ parillinen. Nyt*

$$dim M_\kappa = \begin{cases} \left\lfloor \frac{k}{12} \right\rfloor, & kun\ k \equiv 2 \pmod{12} \\ \left\lfloor \frac{k}{12} \right\rfloor, & muulloin. \end{cases}$$

Tämän lisäksi $dim S_\kappa = dim M_\kappa - 1$.

Todistus. Kun $0 \leq \kappa < 12$, väite seuraa suoraa edellisestä lauseesta. Olkoon nyt $\kappa \geq 12$. Tällöin $\dim M_\kappa = \dim S_\kappa + 1$, sekä $\dim S_\kappa = \dim M_{\kappa-12}$, mistä seuraakin $\dim M_\kappa = \dim M_{\kappa-12} + 1$, josta väite seuraa induktiolla □

Harjoitustehtävä 2.7 on osoittaa, että funktion $G_k(z)$ q-sarja on

$$G_k(z) = 2\zeta(k) + 2\frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n,$$

kun $k \geq 4$, $q = e^{2\pi i z}$ ja $\sigma_\alpha = \sum_{d|n} d^\alpha$

Esimerkki 32. Määritellään $E_k(z) = c_k G_k(z)$, missä c on valittu siten, että $E_k(\infty) = 1$. Todetaan, että $E_8 = E_4^2$ ja $E_{10} = E_4 E_6$

Luku 4

Jacobin neljän neliön lause

4.1 Theta-funktioista

Määritellään θ-funktio kaavalla

$$\vartheta(z) = \sum_{n=-\infty}^{\infty} e^{\pi i n^2 z}.$$

On syytä huomata, että nyt emme ihmettele tavallista q-sarjaa, sillä q-sarjassa eksponentissa olisi $2\pi i$ eikä vain πi. Vakiintunutta termiä tällaiselle puoli-q-sarjalle ei ole, mutta esimerkiksi Jutila on monisteessaan puhunut p-sarjoista.

Toinen huomion arvoinen seikka on, että tämä theta-funktio on itse asiassa vain yksi erikoistapaus theta-funktioiden joukossa. Tämänhetkisiin tarkoituksiimme tämä nimenomainen funktio riittää kuitenkin mainiosti.

Eräs theta-funktion mielenkiintoa lisäävä tekijä on seuraava:

Lause 33. *Olkoon* $r_k(n) = \#\{(x_1, x_2, \ldots, x_n) \in \mathbb{Z}^k : x_1^2 + x_2^+ \cdots + x_n^2 = n\}$. *Nyt*

$$\vartheta^n(z) = \sum_{n=0}^{\infty} r_k(n) e^{\pi i z n^2}.$$

Todistus. Ilmeinen. □

Seuraavaksi haluamme todistaa eräänlaiset invarianssiominaisuudet theta-funktiolle:

Lause 34. *Funktio* $\vartheta(z)$ *on holomorfinen ylemmällä puolitasolla* $\mathbb{H}$ *ja*

$$\vartheta(z) = \vartheta(z+2)$$

sekä

$$\vartheta(-1/z) = \sqrt{\frac{z}{i}}\vartheta(z),$$

missä neliöjuuren $\sqrt{\frac{z}{i}}$ *haara on valittu niin, että se on positiivinen, kun* $z = iy$, $y > 0$.

Tämä itse asiassa tarkoitttaa sitä, että ϑ toteuttaa modulimuotojen määritelmän kunhan korvaamme ryhmän $\mathrm{SL}(2,\mathbb{Z})$ matriisien $\begin{pmatrix} 1 & 2 \\ 0 & 1 \end{pmatrix}$ ja $\begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$ virittämällä ryhmällä (kyllä, tämä on ihan fiksu matriisiryhmä, ja tätä kutsutaan usein theta-ryhmäksija merkitään Γ_ϑ), hyväksymme puolipainoiset otukset mukaan sekä teemme muuta säätöä, jotta emme häiriinny imaginääriyksiköstä invarianssikaavan edessä. Näistä kuitenkin (hieman) lisää myöhemmin.

Todistus. Holomorfisuus sekä ensimmäinen invarianssiehto ovat selvät. Voimme siis keskittyä toisen invarianssiehdon todistamiseen. Tämä todistetaan Poissonin summakaavan avulla. Funktioteorian identiteettilauseen nojalla riittää todistaa kaavan pätevyys imaginääriakselin positiivisella puolikkaalla, eli todistaa, että

$$\vartheta(iy) = y^{-1/2}\vartheta\left(\frac{i}{y}\right),$$

kun $y > 0$. Tämä on yhtäpitävää yhtälön

$$\sum_{n=-\infty}^{\infty} e^{-\pi n^2 y} = y^{-1/2} \sum_{n=-\infty}^{\infty} e^{-\pi n^2/y}.$$

Poissonin summakaavan mukaan

$$\sum_{n=-\infty}^{\infty} e^{-\pi n^2 y} = \sum_{n=-\infty}^{\infty} a_n,$$

missä

$$\begin{aligned} a_n = \int_{-\infty}^{\infty} e^{-\pi t^2 y + 2\pi i m t} dt &= e^{-\pi m^2/y} \int_{-\infty}^{\infty} e^{-\pi\left(t\sqrt{y} - im/\sqrt{y}\right)^2} dt \\ &= y^{-1/2} e^{-\pi m^2/y} \int_{-\infty}^{\infty} e^{-\pi u^2} du = y^{-1/2} e^{-\pi m^2/y}, \end{aligned}$$

mikä todistaa väitteen. □

Tämän tuloksen korollaarina saammekin seuraavan mukavan lauseen:

Lause 35. *Funktiolle $f(z) = \vartheta^8(z)$ pätee $f \mid_4 M = f$ kaikilla $M \in \Gamma_\vartheta$.*

Theta-funktion jakso ei siis ole yksi, mutta jotain voimme yhden päässäkin olevista pisteistä sanoa, kuten seuraava lause osoittaa:

Lause 36. *Theta-funktiolle pätee*

$$\vartheta(z) + \vartheta(z+1) = 2\vartheta(4z)$$

sekä (osin edellisen korollaarina)

$$\vartheta\left(1 - \frac{1}{z}\right) = \sqrt{\frac{z}{i}}\left(\vartheta(z/4) - \vartheta(z)\right) = \sqrt{\frac{z}{i}} \sum_{n=-\infty}^{\infty} e^{\pi i (n+1/2)^2 z}.$$

Todistus. Harjoitustehtävä 3.1. □

4.2 Funktiosta $G_2(z)$ ja diskriminanttifunktiosta

Keskitytään nyt aiemmin sivuutettuun Eisensteinin sarjaan $G_2(z)$. Tiedämme jo, että normaali painoa kaksi oleva modulimuoto se ei voi olla, sillä tällaisia funktioita ei ole olemassakaan. Todistetaan nyt melkein invarianssi tälle, sekä joitakin muita mukavia ominaisuuksia. Näiden avulla saamme myös diskriminanttifunktiolle tulokaavan.

Muistin virkistykseksi:

$$G_2(z) = \sum_{n\neq 0} n^{-2} + \sum_{m\neq 0}\left(\sum_{n\in\mathbb{Z}} (mz+n)^{-2}\right).$$

Tälle saamme kauniin q-sarjan:

Lause 37. *Funktio $G_2 : \mathbb{H} \to \mathbb{C}$ on holomorfinen ja jos $z \in \mathbb{H}$, niin*

$$G_2(z) = \frac{\pi^2}{3}\left(1 - 24\sum_{n=1}^{\infty}\sigma_1(n)e^{2\pi inz}\right).$$

On ilmeistä, $G(z) = G(z+1)$. Osoitetaan nyt toisen invarianssikaavan vastine:

Lause 38. *Kun $z \in \mathbb{H}$, niin*

$$G_2(-1/z) = z^2 G_2(z) - 2\pi i z.$$

Todistus. Funktion $G_2(z)$ voi kirjoittaa myös muodossa

$$G_2(z) = \frac{\pi^2}{3}\left(1 + \frac{1}{z^2}\right) + 2\sum_{m\geq 1}\sum_{n\geq 1}\left((mz+n)^{-2} + (mz-n)^{-2}\right),$$

jolloin myös

$$G_2\left(-\frac{1}{z}\right) = \frac{\pi^2}{3}\left(1+z^2\right) + 2z^2\sum_{m\geq 1}\sum_{n\geq 1}\left((nz-m)^2 + (nz-m)^{-2}\right).$$

Täten

$$\frac{1}{2z^2}\left(z^2 G_2(z) - g_2\left(-\frac{1}{z}\right)\right) = \sum_{m\geq 1}\sum_{n\geq 1} A_{mn} - \sum_{n\geq 1}\sum_{m\geq 1} A_{mn}.$$

Koska summat eivät ole itseisesti suppenevia, ei summausjärjestystä voi vaihtaa. Toimitaan siis toisin: Olkoon

$$\begin{aligned} B_{mn} &= \frac{1}{mz+n-1} - \frac{1}{mz+n} + \frac{1}{mz-n} - \frac{1}{mz-n+1} \\ &= \frac{1}{(mz+n)(mz+n-1)} + \frac{1}{(mz-n)(mz-n+1)}. \end{aligned}$$

Nyt

$$A_{mn} - B_{mn} = O\left((m^2+n^2)^{-3/2}\right) = O\left(m^{-3/2}n^{-3/2}\right).$$

Itseisen konvergenssin vuoksi

$$\sum_{m\geq 1}\sum_{n\geq 1}(A_{mn}-B_{mn})=\sum_{n\geq 1}\sum_{m\geq 1}(A_{mn}-B_{mn}),$$

ja näin saadaankin erotukselle lauseke

$$\sum_{m\geq 1}\sum_{n\geq 1}B_{mn}-\sum_{n\geq 1}\sum_{m\geq 1}B_{mn}.$$

Nyt

$$\sum_{n\geq 1}B_{mn}=0$$

Toisaalta

$$\begin{aligned}z\sum_{m\geq 1}B_{mn}&=\sum_{m\geq 1}\left(\frac{1}{m+(n-1)/z}-\frac{1}{m-n/z}+\frac{1}{m-n/z}-\frac{1}{m-(n-1)/z}\right)\\&=\sum_{m\geq 1}\left(\frac{2(n-1)/z}{((n-1)/z)^2-m^2}-\frac{2n/z}{(n/z)^2-m^2}\right)=\varphi(n-1)-\varphi(n),\end{aligned}$$

ja jälleen kotangentin osamurtokehitelmän avulla

$$\varphi(\xi)=\pi\cot(\pi\xi/z)-\frac{1}{\xi/z},$$

paitsi kun $\xi=0$, jolloin $\varphi(0)=0$. Teleskooppisummalla saadaan lausekkeelle

$$\begin{aligned}z\left(\frac{1}{2z^2}\left(z^2G_2(z)-G_2\left(-\frac{1}{z}\right)\right)\right)=z\sum_{n\geq 1}\sum_{m\geq 1}B_{mn}&=-\sum_{n\geq 1}\left(\varphi(n-1)-\varphi(n)\right)\\&=-\varphi(0)+\lim_{n\to\infty}\varphi(n).\end{aligned}$$

Koska $\lim_{y\to-\infty}\cot z=i$, saadaan tästä väite. □

Lause 39. *Painoa* 12 *olevalle kärkimuodolle* $\Delta(z)$ *pätee*

$$\Delta(z)=e^{2\pi iz}\prod_{m=1}^{\infty}\left(1-e^{2\pi imz}\right)^{24}$$

Todistus. Harjoitustehtävä 3.2-3.3. □

4.3 Kongruenssiryhmistä ja modulimuodoista niiden suhteen

Aloitetaan pääkongruenssiryhmän määrittelyllä:

Määritelmä 40. Tasoa n oleva pääkongruenssiryhmä on

$$\Gamma(n)=\left\{M\in\mathrm{SL}(2,\mathbb{Z}):M\equiv\begin{pmatrix}1&0\\0&1\end{pmatrix}\pmod n\right\}.$$

Merkitään vielä

$$\Gamma_n = \mathrm{SL}(2,\mathbb{Z}_n) = \left\{ \begin{pmatrix} \bar{a} & \bar{b} \\ \bar{c} & \bar{d} \end{pmatrix} : \bar{a},\bar{b},\bar{c},\bar{d} \in \mathbb{Z}_n, \bar{a}\bar{d} - \bar{b}\bar{c} = \bar{1} \right\}.$$

Muotoilkaamme nyt lause, joka selventää ryhmien $\mathrm{SL}(2,\mathbb{Z})$ ja $\Gamma(n)$ välisiä suhteita:

Lause 41. *Kuvaus*

$$\phi : SL(2,\mathbb{Z}) \to \Gamma_n,\ M \to \bar{M},$$

missä $\bar{M}$ merkitsee matriisia M redusoituna modulo n, on surjektiivinen ryhmähomomorfismi, jonka ydin $\Gamma(n)$ on $SL(2,\mathbb{Z})$:n äärelistä indeksiä oleva normaali aliryhmä. Lisäksi

$$SL(2,\mathbb{Z})/\Gamma(n) \cong \Gamma_n.$$

Todistus. Ryhmähomomorfismius on selvä, samoin kuin että $\Gamma(n)$ on kuvauksen ydin. Täten ryhmäteorian mukaan $\Gamma(n)$ on $\mathrm{SL}(2,\mathbb{Z})$:n normaali aliryhmä, ja indeksi $[\mathrm{SL}(2,\mathbb{Z}) : \Gamma(n)]$ äärellisyys seuraa ryhmän Γ_n äärellisyydestä. Isomorfiaa carten pitää vielä osoittaa surjektiivisuus (mikä, hämmentävää kyllä, ei ole täysin triviaali ominaisuus tässä).

Olkoon annettu matriisi $\bar{K} \in \Gamma_n$. On selvää, että $\bar{K}$ on jonkin matriisin $K = \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix}$ kuva reduktiossa, mutta kyseenalaista on se, kuuluuko tämä matriisi joukkoon $\mathrm{SL}(2,\mathbb{Z})$. Osoitetaan, että tarpeen tullen muuttamalla matriisin K alkioita, päästään matriisiin K', jonka kuva reduktiossa on myös $\overline{(K)}$, ja $K' \in \mathrm{SL}(2,\mathbb{Z})$.

Determinanttiehto matriisille $\bar{K}$ luetaan matriisille K tarkoittavan

$$\alpha\delta - \beta\gamma = 1 \pmod{n}.$$

Täten $(\gamma, \delta, n) = 1$. Tästä ei vielä seuraa, että $(\gamma, \delta) = 1$, mutta huomioidaan, että luku δ voidaan korvata luvulla $\delta + nx$, jolle $(\gamma, \delta + nx) = 1$. (Tämän voi perustella hyvin monella tavalla.) Voimme siis olettaa, että $(\gamma, \delta) = 1$. Aiemmin todistetun lauseen nojalla on olemassa matriiseja ryhmässä $\mathrm{SL}(2,\mathbb{Z})$, joiden alarivi on (γ, δ). Kirjoitetaan nyt $\alpha\delta - \gamma\beta = 1 + sn$. Nyt yhtälö $\gamma y - \delta x = s$ on ratkeava. Muodostetaan nyt matriisi $\begin{pmatrix} \alpha + nx & \beta + yn \\ \gamma & \delta \end{pmatrix}$. Tämän matriisin determinantti on 1 ja sen kuva on vaadittu. □

Tämän jälkeen indeksi $[\mathrm{SL}(2,\mathbb{Z}) : \Gamma(n)]$ onkin helppo laskea:

Lause 42. *Indeksi $SL(2,\mathbb{Z}) : \Gamma(n)$ voidaan laskea kaavasta*

$$[SL(2,\mathbb{Z}) : \Gamma(n)] = n^3 \prod_{p|n} \left(1 - p^{-2}\right).$$

Todistus. Harjoitustehtävä 3.4. □

Lause 43. *Matriisit $L, M \in SL(2,\mathbb{Z})$ ovat samassa ryhmän $\Gamma(n)$ sivuluokassa tarkalleen silloin, kun $L \equiv M \pmod{n}$.*

Todistus. Ilmeinen. □

Nyt pääsemmekin kongruenssiryhmän määrittelyyn:

Määritelmä 44. Ryhmän $\mathrm{SL}(2,\mathbb{Z})$ aliryhmä Λ on tasoa n oleva kongruenssiryhmä, jos $\Gamma(n) \leq \Lambda$ jollakin $n \in \mathbb{N}$. Pienin mahdollinen luku n on ryhmän Λ johtaja.

Yksi varsin tärkeä esimerkki kongruenssiryhmästä on seuraava:

$$\Gamma_0(n) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}(2,\mathbb{Z}) : c \equiv 0 \pmod{n} \right\}.$$

Esimerkki 45. Tarkastellaan tätä ryhmää.

Määritellään vielä karakterit kongruenssiryhmille:

Määritelmä 46. Kongruenssiryhmän Λ karakteri χ on ryhmähomomorfismi

$$\chi : \Lambda \to \{z \in \mathbb{C} : |z| = 1\}.$$

Lisäksi karakteri on äärellinen, jos $\chi^m = \chi_0$ jollakin $m \in \mathbb{N}$, missä $\chi_0(L) = 1$ kaikilla $L \in \Lambda$. Karakteria χ_0 kutsutaan pääkarakteriksi. Edelleen sanotaan, että χ on karakteri $(\bmod\ n)$, jos $\Gamma(n) \leq \Lambda$ ja $\chi(M) = 1$ kaikilla $M \in \Gamma(n)$.

Esimerkki 47. Jos $p > 2$ on alkuluku niin

$$\chi\left(\begin{pmatrix} a & b \\ c & d \end{pmatrix}\right) = \left(\frac{d}{p}\right)$$

on ryhmän $\Gamma_0(p)$ karakteri, joka on selvästi äärelinen. Lisäksi se on ilmeisesti karakteri $(\bmod\ p)$, sillä jos $M = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma(p)$, niin $c \equiv 0 \pmod{p}$ ja $d \equiv 1 \pmod{p}$, eli $\chi(M) = 1$.

Huomaamme, että karakteri modulo n on äärellinen, sillä jos χ on kongruenssiryhmän Λ karakteri, niin $\Gamma(n) \trianglelefteq \Lambda$ ja tekijäryhmän $\Lambda/\Gamma(n)$ kertaluku m on äärellinen. Tällöin $L^m \in \Gamma(n)$ kaikilla $L \in \Lambda$, eli $\chi^m(L) = 1$. Muistetaan vielä theta-ryhmä. Tarvitsemme sille myöhemmin seuraavaa tulosta:

Lause 48. *Pätee*

$$\Gamma_\vartheta = \gamma(2) \cup \Gamma(2)S,$$

missä $S = \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$. *Lisäksi* $[SL(2,\mathbb{Z}) : \Gamma_\vartheta] = 3$.

Todistus. Harjoitustehtävä 3.5. □

Tarvitsemme vielä tulevaisuudessa ryhmän $\mathrm{SL}(2,\mathbb{Z})$ jakoa ryhmän Γ_ϑ suhteen sivuluokkiin. Muotoilkaamme siis seuraava lause:

Lause 49. *On voimassa hajotelma*

$$SL(2,\mathbb{Z}) = \Gamma_\vartheta \cup (\Gamma_\vartheta T) \cup (\Gamma_\vartheta U) = \Gamma_\vartheta \cup (T\Gamma_\vartheta) \cup (U^2\Gamma_\vartheta),$$

missä $U = \begin{pmatrix} -1 & 1 \\ -1 & 0 \end{pmatrix}$ *(ja* $U^2 = \begin{pmatrix} 0 & -1 \\ 1 & -1 \end{pmatrix}$.

Todistus. Koska tiedämme indeksin $[\mathrm{SL}(2,\mathbb{Z}) : \Gamma_\vartheta] = 3$, riittää osoittaa sivuluokkien eroaminen toisistaan. Osoitetaan niiden eroavaisuus modulo 2. Huomataan aluksi, että ryhmän Γ_ϑ jäsenet ovat muotoa $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}$ sekä $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix}\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} \equiv \begin{pmatrix}0 & 1\\ 1 & 0\end{pmatrix}$. Ensimäisellä kerrottaessa alkiot pysyvät ennallaan, eli $\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} T \equiv T, T\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \equiv T, \begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} U \equiv U$ ja $U^2\begin{pmatrix}1 & 0\\ 0 & 1\end{pmatrix} \equiv U^2$. On vielä tarkasteltava toisella matriisilla, eli matriisilla $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix}$ kertomista. Huomataan, että $T\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 1\\ 1 & 0\end{pmatrix}$, $U^2\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} = \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$ ja $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} T \equiv \begin{pmatrix}0 & 1\\ 1 & 1\end{pmatrix}$ ja $\begin{pmatrix}0 & -1\\ 1 & 0\end{pmatrix} U \equiv \begin{pmatrix}1 & 0\\ 1 & 1\end{pmatrix}$, mistä huomaammekin väitteen todeksi, sillä sivuluokat todella eroavat. □

Määritelkäämme vielä yksi erityisluonteinen karakteri:

Määritelmä 50. Olkoon $\chi_\vartheta : \Gamma_\vartheta \to \{\pm 1\}$ funktio, joka toteuttaa ehdon

$$\chi_\vartheta(M) = \begin{cases} 1, & \text{kun } M \in \Gamma(2) \\ -1 & \text{muulloin.} \end{cases}$$

On helppo nähdä, että tämä funktio on todellakin äärellinen karakteri.

Voimme vihdoinkin siirtyä modulimuotoihin. Tarvitsemme aluksi määritelmän modulimuodoille jonkin tietyn kongruenssiryhmän ja karakterin suhteen.

Määritelmä 51. Olkoon $\kappa \in \mathbb{Z}$, Λ kongruenssiryhmä, χ ryhmän Λ karakteri. Sanotaan, että funktio $\mathbb{H} \to \mathbb{C}$ on painoa k oleva modulimuoto ryhmälle Λ ja karakterille χ, jos

1. f on holomorfinen ylemmällä puolitasolla $\mathbb{H}$
2. $f \mid_\kappa L = \chi(L) f$ kaikilla $L \in \Lambda$
3. $f \mid_\kappa M$ on holomorfinen äärettömässä aina kun $M \in \Gamma$.

Tätä ryhmää merkitään $M_\kappa(\Lambda, \chi)$. Modulimuoto on kärkimuoto, jos funktiola $f \mid_\kappa M$ no nollakohta äärettömässä aina kun $M \in \mathrm{SL}(2,\mathbb{Z})$. Kärkimuotojen joukolle käytetään merkintää $S_{\kappa(\Lambda.\chi)}$.

Huomaamme välittömästi, että $M_\kappa(\Lambda,\chi)M_\ell(\Lambda,\chi') \subseteq M_{\kappa+\ell}(\Lambda,\chi,\chi')$. Siirtykäämme nyt käsittelemään varsin konkreettisia funktioita. Merkitään

$$g(z) = \frac{1}{3}(4E_2(2z) - E(z/2)),$$

missä $E_2(z)$ on normeerattu $G_2(z)$. Nyt

Lause 52. *Funktiot $\vartheta(z)^4$ ja $g(z)$ ovat modulimuotoja ryhmän $M(\Gamma_\vartheta, \chi_\vartheta)$ suhteen.*

Todistus. Funktion $\vartheta(z)$ tapauksessa tiedämme, että $\vartheta(z) = \vartheta(z+2)$ ja $\vartheta(-1/z) = \sqrt{\frac{z}{i}}\vartheta(z)$, eli $\vartheta^4(z) = \vartheta^4(z+2)$ ja $\vartheta^4(-1/z) = -z^2\vartheta^4(z) = \chi_{\vartheta(S)} z^2 \vartheta^4(z)$. Holomorfisuutta varten riittää

tarkastella siirrot matriisilla U. Tässä on hyödyksi laskuharjoituksena todistettu/todistettava kaava, jonka mukaan

$$\left(\vartheta^4 \mid_U\right)(z) = z^{-2}\vartheta^4\left(1-\frac{1}{z}\right) = -\left(\sum_{n=-\infty}^{infty} e^{\pi i(n+1/2)^2 z}\right)^4,$$

mikä on holomorfinen äärettömässä.

Sirtykäämme nyt tarkastelemaan funktiota $g(z)$. Huomataan aluksi, että $E_2(z) = \frac{3}{\pi^2}G_2(z)$. Täten

$$E_2\left(-\frac{1}{z}\right) = z^2 E_2(z) - \frac{6iz}{\pi}.$$

Koska $E_2(z+1) = E_2(z)$, niin

$$g(z+2) = \frac{1}{3}\left(4E_2\left(2(z+2)\right) - E\left((z+2)/2\right)\right) = \frac{1}{3}\left(4E_2(2z) - E\left(z/2\right)\right) = g(z).$$

Lisäksi

$$z^{-2}g\left(-1/z\right) = \frac{1}{3}\left(4z^{-2}E\left(-\frac{2}{z}\right) - z^{-2}E_2\left(-\frac{1}{2z}\right)\right) = -g(z),$$

kuten vaadittu. Lopulta osoitetaan vielä holomorfisuus äärettömässä matriisilla U suoritetun siirron jälkeen. Lasketaan:

$$\begin{aligned} z^{-2}g\left(1-\frac{1}{z}\right) &= \frac{z^{-2}}{3}\left(4E_2\left(2-\frac{2}{z}\right) - E_2\left(\frac{1}{2}-\frac{1}{2z}\right)\right) \\ &= \frac{z^{-2}}{3}\left(4E_2\left(-\frac{2}{z}\right) - E_2\left(-\frac{z+1}{2z}\right)\right) = \frac{1}{3}\left(E_2\left(z/2\right) - E_2\left((z+1)/2\right)\right), \end{aligned}$$

mikä on selvästi holomorfinen äärettömässä. □

4.4 Modulimuotojen tunnistaminen

Selvittäkäämme seuraavaksi mitä on tiedettävä kahdesta samassa avaruudessa elävästä modulimuodosta voidaksemme osoittaa, että ne ovat samat.

Aloitetaan lämmittelyongelmalla:

Lause 53. *Jos $f \in M_\kappa$, niin ord$(f,\infty) \leq \left\lfloor \frac{\kappa}{12} \right\rfloor$ ja ord$(f,\infty) < \dim M_\kappa$. Jos siis funktion f Fourier'n sarjan $\left\lfloor \frac{\kappa}{12} \right\rfloor + 1$ ensimmäistä kerrointa ovat nollia, on f nollafunktio.*

Todistus. Painokaavan nojalla $\frac{\kappa}{12} \geq \mathrm{ord}(f,\infty)$, jos κ ei ole $\equiv 2 (\mathrm{mod}\ 12)$, ja jos taas $\kappa \equiv 2 \pmod{12}$, niin

$$\frac{\kappa}{12} \geq \mathrm{ord} + \frac{1}{2} + \frac{1}{3} + \frac{1}{3}.$$

Siispä $\mathrm{ord}(f,\infty) \leq \left\lfloor \frac{\kappa}{12} \right\rfloor$. Dimensiokaavan mukaan on $\dim M_\kappa = \left\lfloor \frac{12}{\kappa} \right\rfloor + 1$ tai $\left\lfloor \frac{12}{\kappa} \right\rfloor$, tässä järjestyksessä, eli joka tapauksessa $\dim M_\kappa - 1 \geq \mathrm{ord}(f,\infty)$. □

Siirrytään nyt tarkastelemaan Fourier'n sarjoja.

Lause 54. *Olkoon Λ kongruenssiryhmä, $\Gamma(n) \leq \Lambda$ ja χ karakteri* $(\bmod\ n)$*. Jos $f \in M_\kappa(\Lambda, \chi)$ ja $M \in SL(2,\mathbb{Z})$, niin funktiolla $f\mid_\kappa M$ on Fourier'n sarja*

$$(f \mid_\kappa M)(z) = \sum_{m=0}^{\infty} \alpha_f(m; M) e^{2\pi i m z/n},$$

kun $z \in \mathbb{H}$. Lisäksi kertoimille $\alpha_f(m; M)$ on voimassa

$$\alpha_f(m, LM) = \chi(L)\alpha_f(m; M),$$

kun $L \in \Lambda$ ja $M \in SL(2,\mathbb{Z})$.

Todistus. On helppo huomata, että $M^{-1}\Gamma(n)M = \Gamma(n)$. Jos $f \in M_\kappa(\Lambda, \chi)$, niin $f \in M_\kappa(\Gamma(n))$, sillä $\chi(L) = 1$ kaikilla $L \in \Gamma(n)$. Nyt myös $\chi_M(L) = \chi(MLM^{-1}) = 1$ kaikilla $L \in \Gamma(n)$, ja $f\mid_\kappa M \in M_\kappa(\Gamma(n))$. Koska $T^n = \begin{pmatrix} 1 & n \\ 0 & 1 \end{pmatrix} \in \Gamma(n)$, niin funktiolla $f\mid_\kappa M$ on jakso n. Funktiolla

$$g(z) = (f \mid_\kappa M)(nz)$$

on jakso 1, ja se on holomorfinen äärettömässä. Sillä on siis Fourier'n sarja

$$g(z) = \sum_{m=0}^{\infty} \alpha_j(m; M) e^{2\pi i m z},$$

mikä todistaa väitteen. □

Muotoillaan seuraavaksi lause, joka kertoo miten konfruenssiryhmien suhteen olevista modulimuodoista saadaan konstruoitua modulimuotoja täyden moduliryhmän suhteen.

Lause 55. *Olkoon Λ kongruenssiryhmä, $f \in M_\kappa(\Lambda)$ ja*

$$SL(2,\mathbb{Z}) = \cup_{j=1}^{\ell} \Lambda M_j$$

ryhmän $SL(2,\mathbb{Z})$ esitys oikeiden sivuluokkien unionina. Merkitään

$$Sp(f) = \sum_{j=1}^{\ell} f \mid_\kappa M_j$$

ja

$$\pi(f) = \prod_{j=1}^{\ell} f \mid_\kappa M_j.$$

Nyt $Sp(f) \in M_\kappa$ ja $\pi(f) \in M_{\kappa\ell}$.

Todistus. Koska $f\mid_\kappa L = f$ kaikilla $L \in \Lambda$, ovat $Sp(f)$ ja $\pi(f)$ riippumattomia sivuluokkien edustajien M_j valinnasta. Erityisesti joukko $\{M_j M\}$, missä $M \in \mathrm{SL}(2,\mathbb{Z})$ on kiinteä, voidaan valita edustajistoksi. Väitteet seuraavat tästä, sillä M ei tee muuta kuin permutoi järjestyksen. □

Vihdoinkin pääsemme varsinaiseen asiaan:

Lause 56. *Olkoon Λ tasoa n oleva kongruenssiryhmä ja χ sen karakteri* (mod n). *Määritellään*

$$\Lambda^\star = \{L \in \Lambda : \chi(L) = 1\}$$

ja $\ell = [SL(2,\mathbb{Z}) : \Lambda^\star]$. Jos funktiolle $f \in M_\kappa(\Lambda, \chi)$ on jollekin $M \in SL(2,\mathbb{Z})$ voimassa

$$\alpha_f(m; M) = 0$$

aina, kun $0 \leq m \leq \frac{\ell\kappa n}{12}$, niin $f = 0$. Lisäksi $\dim M_\kappa(\Lambda, \chi) \leq \left\lfloor \frac{\ell\kappa n}{12} \right\rfloor + 1$.

Todistus. Funktio f voidaan käsittää kuuluvaksi avaruuteen $M_\kappa(\Lambda^\star)$. Muodostetaan $\pi(f)$ avaruuden $\Lambda^\star$ suhteen, jolloin $g = \pi(f) \in M_{\kappa\ell}$. Funktiolle g saamme helposti Fourier'n sarjat kertomalla tulossa $\pi(f)$ esiintyvät sarjat

$$(f \mid_\kappa M_j)(z) = \sum_{m=0}^{\infty} \alpha_f(m; M_j) e^{2\pi i m z/n}$$

keskenään. Voimme itse asiassa olettaa, että $M = M_j$ jollakin j (tässä M on sama M kuin mikä esiintyy teoreeman määrittelyssä). Nyt funktion g Fourier'n sarjassa

$$g(z) = \sum_{m=0}^{\infty} \alpha_g(m) e^{2\pi i m z}$$

on välttämättä $\alpha_g(m) = 0$, kun $0 \leq m \leq \frac{\kappa\ell}{12}$, eli $\operatorname{ord}(g, \infty) > \left\lfloor \frac{\kappa\ell}{12} \right\rfloor$. Tällöin $g = 0$. Siispä jokin $f \mid_\kappa M_j$ on nolla, ja myös $f = 0$.

Lauseen viimeinen osa: Jos pätisi $\dim M_\kappa(\Lambda, \chi) > \left\lfloor \frac{\kappa\ell n}{12} \right\rfloor + 1$, niin voitaisiin muodostaa sellainen $f \in M_\kappa(\Lambda, \chi)$, $f \neq 0$, jonka Fourier'n kertoimet häviäisivät indeksiin $\left\lfloor \frac{\kappa\ell n}{12} \right\rfloor$ saakka. Tämä on kuitenkin jo todistetun nojalla mahdotonta. □

Vihdoin pääsemme Jacobin neljän neliön lauseen todistukseen. Muistellaan vielä, että merkittiin

$$r_k(n) = \{(x_1, x_2, \ldots, x_k) \in \mathbb{Z}^k : x_1^2 + x_2^2 + \cdots + x_k^2 = n\}$$

Lause 57. *Kun $n \in \mathbb{N}$, niin*

$$r_4(n) = 8 \sum_{d \mid m, 4 \nmid d} d$$

Todistus. Olemme todistaneet jo, että ϑ^4 ja $g = \frac{1}{3}(4E_2(2z) - E(z/2))$ elävät avaruudessa $M_2(\Gamma_\vartheta, \chi_\vartheta)$. Selvästi

$$\vartheta^4(z) = \sum_{n=0}^{\infty} r_4(n) e^{\pi i z n}.$$

Määritetään nyt funktion g Fourier'n sarja $\sum_{m=0}^{\infty} = \sum_{m=0}^{\infty} \alpha_g(m) q^m$. Suoraan määritelmästä havaitaan, että kun $m \geq 1$, niin $\alpha_g(m) = 8\sigma(m) - 32\sigma(m/4)$, kun $4 \mid m$ ja $8\sigma(m)$ muulloin. Tämä esitys vastaa lauseen esitystä. Nyt on verrattava riittävä määrä kertoimia. Lasketaan ensin tämä kerrointen määrä. Selvästi $\kappa = 2$, $\ell = 6$ ja $n = 2$. Siispä $\frac{\ell\kappa n}{12} = \frac{6 \cdot 2 \cdot 2}{12} = 2$. On siis verrattava kertoimet $\alpha_g(0)$, $\alpha_g(1)$ ja $\alpha_g(2)$ sekä $r_4(0)$, $r_4(1)$ a $r_4(2)$. Ensinnäkin

$$\begin{aligned}
\alpha_g(0) &= \frac{1}{3}(4 - 1) = 1 \\
\alpha_g(1) &= \frac{1}{3}(4 \cdot 0 + 24) = 8 \\
\alpha_g(1) &= \frac{1}{3}(4 \cdot 0 + 72) = 24
\end{aligned}$$

Seuraavaksi määritetään kertoimet r_4. Ensinnäkin luku 0 voidaan esittää vain yhdellä tavalla neljän neliön summana: $0^2 + 0^2 + 0^2 + 0^2$. Tässä ei luonnollisestikaan etumerkit tilannetta muuta. Luvulla 1 esityksiä on järjestystä ja merkkejä vaille yksi, eli $1^2+0^2+0^2+0^2$. Etumerkit ja järjestyksen huomioiden on näitä kahdeksan. Luvulla 2 esityksiä on taas etumerkkejä ja järjestystä vailla yksi: $1^2+1^2+0^2+0^2$. Etumerkit huomioiden näitä on jo neljä, ja järjestyksen huomioiden 6, eli yhteensä $4 \cdot 6 = 24$. Siispä

$$\begin{aligned} r_4(0) &= 1 \\ r_4(1) &= 8 \\ r_4(1) &= 24 \end{aligned}$$

Lause on nyt todistettu. □

Voimme vielä muotoilla kahdeksan neliön lauseen. Sen todistus on harjoitustehtävä:

Lause 58. *Kun $n \in \mathbb{N}$, niin*

$$r_8(n) = 16 \sum_{d|n} (-1)^{m-d} d^3.$$

Todistus. Harjoitustehtävä 4.1 ja 4.2 □

Käykäämme luvun lopuksi täydelllisyyden vuoksi läpi hieman neliöiden summana esitysten tuloksia. On ilmeistä, että yhden neliön summana voidaan esittää vain neliöt, joten niistä ei sen enempää. Kahden neliön summat ovat jo mielenkiintoisempia:

Lause 59. *Luku $n \in \mathbb{N}$ on esitettävissä kahden neliön summana jos ja vain jos luku n on esitettävissä muodossa*

$$d^2 \prod_{p|n, p \equiv 1 \pmod 4} p.$$

Tämä on todistettavissa esimerkiksi Gaussin kokonaislukujen teorian avulla suhteellisen helposti. Siirtykäämme siis kolmen neliön summiin. Näissä tulos on juuri se, mitä toivoa voisi, mutta todistus ei ole ihan yksinkertainen:

Lause 60. *Luku $n \in \mathbb{N}$ on esitettävissä kolmen neliön summana kunhan n ei ole muotoa $4^j(8k + 7)$.*

Kolmen neliön summien lystikäs ominaisuus on ratkaisujen tasainen jakautuminen. Tähän perehdymme myöhemmin kurssilla.

Neliöinä esittäminen on yleisemmin osa Waringin ongelmaa: Kuinka monta k:tta potenssia tarvitaan, jotta luku voidaan varmasti esittää niiden summana? Neliöillä tämä ilmeisesti on neljä.

Toinen yleistys on esimerkiksi tarkastella luvun n esityksiä muodossa $ax^2 + by^2 + cz^2$. (Sopivilla, tosin hyvin harvoilla, lukukolmikon (a, b, c) valinnoilla kaikki parittomat luvut voidaan tässä muodossa esittää.)

Luku 5

Voronoi-tyyppiset summakaavat

5.1 Integraalilemmoja

Ennen kuin päästään Voronoi-tyyppisiin summakaavoihin asti, tarvitaan jonkin verran lemmoja summien käsittelyyn. Ensimmäinen lemma on niin kutsuttu ensimmäisen derivaatan testi, joka on erinomaisen hyödyllinen tulos, kunhan tarkasteltava derivaatta on koko ajan nollasta poikkeava (eli integroitava otus oskilloi koko ajan). Lienee myös selvää lukijalle, että jos tarkastelemamme funktion derivaatta onkin koko ajan negatiivinen, eikä positiivinen, kuten oletettu, niin samanlainen tulos pätee.

Lemma 61 (Ensimmäisen derivaatan testi)**.** *Olkoot $f(x)$ ja $g(x)$ sellaisia reaalisia funktioita välillä $[a,b]$, että $f'(x)$ on monotoninen, $f'(x) \geq \lambda > 0$ välillä (a,b), funktion $g(x)$ täysi vaihtelu välillä $[a,b]$ olkoon G_0 ja $G = \max_{a\leq x\leq b} |g(x)|$ Silloin*

$$\int_a^b g(x)e(f(x))dx \leq \frac{G+G_0}{\pi\lambda}.$$

Seuraava tulos on toisen derivaatan testi. Se tuottaa iloa, jos funktio ei oskilloi koko ajan, mutta funktion käytös muuttuu riittävästi.

Lemma 62 (Toisen derivaatan testi)**.** *Olkoot $f(x)$ ja $g(x)$ sellaisia reaalisia funktioita välillä $[a,b]$, että $f(x)$ on kahdesti derivoituva, $|f''(x)| \geq \lambda > 0$, $|g(x)| \leq G$, ja funktion g täysi vaihtelu olkoon G_0. Silloin*

$$\int_a^b g(x)e(f(x))dx \leq \frac{G+G_0}{\sqrt{\pi\lambda}}$$

Todistus. Tarkastellaan yksinkertaisuuden vuoksi tilannetta, jossa $g(x) = 1$. Olkoon $\delta = \frac{1}{\sqrt{\pi\lambda}}$. Jos välilä on satulapiste, $x_0 \in [a+\delta, b-\delta]$, niin arvioidaan sen ympäristö $[x_0-\delta, x_0+\delta]$ triviaalisti, ja muut integraalit ensimmisen derivaatan testillä huomioiden, että $|f'(x)| \geq \delta\lambda$. Muut tapaukset (eli satulapisteettömät ja satulapisteen toisenlaiset sijainnit) ovat samanlaisia. □

Osittaissummaus tuottaa iloa, jos tunnetaan arvio jollekin summalle, ja pitäisi arvioida summaa, jossa alkuperäisen summan summattavia on muutettu jollakin sympaattisella funktiolla.

Lemma 63 (Osittaissummaus)**.** *Olkoon $\lambda_1 \leq \lambda_2 \leq \dots$ reaalilukujono, jolla* $\lim_{n\to\infty}$ *ja olkoon g jatkuvasti derivoituva funktio välillä $[\lambda, \infty)$. Olkoon $(a_n)_{n=1}^{\infty}$ mielivaltainen kompleksilukujono. Nyt*

$$\sum_{\lambda_n \leq x} a(n)g(\lambda_n) = A(x)g(x) - \int_{\lambda_1}^{x} A(t)g'(t)dt,$$

missä

$$A(t) = \sum_{\lambda_1 \leq \lambda_n \leq t} a_n.$$

Lause 64 (Perronin kaava)**.** *Olkoon $a(n)$ aritmeettinen funktio, $F(s) = \sum_{n=1}^{\infty} a(n)n^{-s}$ (Dirichlet'n sarja), $s = \sigma + it$. Oletetaan lisäksi, että $|a(n)| \ll \Psi(n)$, missä $\Psi(n)$ on kasvava. Oletetaan lisäksi, että*

$$\sum_{n=1}^{\infty} |a(n)|n^{-\sigma} \ll (\sigma - 1)^{-\alpha},$$

kun $\sigma \to 1 + 0$. Kirjoitetaan $A(x) = \sum_{n\leq x} a(n)$ Nyt

$$A(x) = \frac{1}{2\pi i}\int_{b-iT}^{b+iT} F(s)x^s s^{-1}ds + O\left(x^b T^{-1}(b-1)^{-\alpha}\right) + O\left(xT^{-1}\Psi(2x)\log(2x)\right) + O\left(\Psi(2x)\right).$$

5.2 Kuvitelmia ja totuuksia kärkimuodoista

Diskriminanttifunktio on eräänlainen standardi esimerkki kärkimuodosta. Nyrkkisääntönä voi sanoa, että jos jokin analyyttinen ominaisuus pätee diskriminanttifunktiolle, niin kohtuullisella todennäköisyydellä se pätee monille muillekin kärkimuodoille (täyden moduliryhmän suhteen).

Diskriminanttifunktion Fourier-kertoimet $\tau(n)$ (eli Ramanujanin τ-funktion arvot) toteuttavat Hecken yhtälön, samoin kuin monen muunkin kärkimuodon Fourier-kertoimet $a(n)$: Merkitään $a(n) = b(n)n^{(\kappa-1)/2}$ (tämä normalisointi tuottaa iloa myöhemminkin). Nyt

$$b\left(p^{k+1}\right) = b(p^k)b(p) - b(p^{k-1}),$$

missä p on alkuluku. Lisäksi $b(nm) = b(n)b(m)$ kun $\text{syt}(n, m) = 1$.

Yllä oleva "moni muukin kärkimuoto"tarkoittaa sitä, että avaruudessa S_κ voidaan valita kanta, joka koostuu ainoastaan kärkimuodoista, joiden Fourier-kertoimet toteuttavat Hecken yhtälön, eli joiden Fourier-kertoimet ovat Hecken ominaisarvoja.

Keskittykäämme nyt vain Hecken ominaisarvoihin. Deligne todisti, että nämä toteuttavat arvion

$$|a(n)| \leq n^{(\kappa-1)/2}d(n),$$

eli tällä kurssilla hyödyllinen muotoilu:

$$b(n) \ll d(n) \ll n^{\varepsilon},$$

missä $d(n) = \sigma_0(n) = \sum_{d|n} 1$. Arvio tekijäfunktiolle $d(n)$ on varsin alkeellinen, mutta hieman työläs todistaa.(Delignen tulos on edellisen kaavarivin vasemmanpuoleinen epäyhtälö, ja sen todistusta ei tämän kurssin aikana tulla näkemään, sillä se on käsittämättömän hankala ja pitkä, ja vaatisi yksinään kokonaisen kurssin tai peräti kurssisarjan.)

Ylläoleva Delignen tulos tunnetaan yleisesti Ramanujanin ja Peterssonin konjektuurina, ja se on konjekturoitu esimerkiksi ryhmän $GL(3)$ suhteen määritellyille kärkimuodoille, samoin monille erikoisille ryhmän $\mathrm{SL}(2,\mathbb{Z})$ tai sen aliryhmien määrittämille kärkimuodoille, mutta yleisesti se ei ole tunnettu. (Kannattaa huomioida, että yleisesti modulimuodoille ei tällainen päde – tästä esimerkiksi Eisensteinin sarjat ovat selvä esmerkki.)

Lehmerin konjektuurina tunnetaan väite, jonka mukaan $\tau(n) \neq 0$. Tämä konjektuuri on yleistetty Hecken ominaisarvoille (muillehan ei voikaan). Hämmentävää kyllä, tämän konjektuurin todistus on edennyt pidemmälle diskriminanttifunktion tapauksessa kuin yleisesti: Tiedetään, että kun $n \in [x, x + cx^{1/4}]$, niin tällä välillä on ainakin yksi nollasta poikkeava Fourier-kerroin. Tässä käytetään hyväksi Ramanujanin τ-funktion kongruenssiominaisuuksia.

5.3 Funktionaaliyhtälö

Holomorfiselle kärkimuodolle voidaan kirjoittaa Dirichlet'n sarja

$$\varphi(s) = \sum_{n=1}^{\infty} a(n) n^{-s}.$$

Tälle voidaan kirjoittaa Eulerin tulo:

Lause 65. *Olkoot Fourier-kertoimet $a(n) = n^{(\kappa-1)/2} b(n)$ Hecken ominaisarvoja. Tällöin Dirichlet'n sarjalla on esitys Eulerin tulona:*

$$\tilde{\varphi}(s) = \sum_{n=1}^{\infty} b(n) n^{-s} = \prod_{p \in \mathbb{P}} \left(1 - \frac{b(p)}{p^s} + \frac{1}{p^{2s}}\right)^{-1}.$$

Todistus. Harjoitustehtävä 4.3. □

Yleisemmin, tähän sarjaan voidaan ottaa mukaan myös eksponenttitekijä:

$$\varphi(s, r) = \sum_{n=1}^{\infty} a(n) e(nr) n^{-s},$$

missä $r = \frac{h}{k}$ rationaaliluku (ja merkitään $\tilde{\varphi}(s, r)$ normeeratulle sarjalle). Esimerkiksi Delignen tuloksen

$$|a(n)| \leq d(n) n^{(\kappa-1)/2} \ll n^{\varepsilon}$$

perusteella havaitaan, että Dirichlet'n sarjat suppenevat, kun $n > \frac{\kappa+1}{2}$. Tähän on kuitenkin alkeellisempikin tapa. Muotoillaan aluksi Rankinin ja Selbergin keskiarvolause:

Lause 66. *Olkoot painoa κ olevan kärkimuodon Fourier-kertoimet $b(n)n^{(\kappa-1)/2}$. Tällöin*

$$\sum_{n \leq M} |b(n)|^2 = AM + O\left(M^{3/5}\right),$$

missä A on eräs vakio.

(Virhetermin uskotaan olevan parempikin, mutta kukaan ei ole sitä onnistunut paremmaksi todistamaan.) Tämän lauseen todistus käydään kurssin aivan lopussa läpi, mikäli siihen on aikaa. T'mä on kuitenkin monta kertalukua yksinkertaisempi kuin Delignen estimaatin todistus.

Käyttäen esimerkiksi Chebysevin epäyhtälöä (tai suuruusjärjestystä tai melkein mitä vaan), saadaan

$$\left(\frac{\sum_{m\leq M}|b(m)|}{M}\right)^2 \leq \frac{\sum_{m\leq M}|b(m)|^2}{M} \asymp 1,$$

eli

$$\sum_{m\leq M}|b(m)| \ll M.$$

(Itse asiassa Rankin on myöhemmin todistanut tämän itseisarvosumman olevan suurinpiirtein $M\,(\log M)^{-\delta}$.

Tämän arvion pohjalta voidaan kuitenkin osoittaa seuraava lause todeksi:

Lause 67. *Summa $\sum_{n=1}^{\infty} b(n)n^{-s}$ suppenee itseisesti (ja on holomorfinen funktio), kun $\Re s = \sigma > 1$.*

Todistus. Käyttäkäämme osittaissummausta:

$$\begin{aligned}\sum_{n\leq M}|b(n)n^{-s}| = \sum_{n\leq M}|b(n)|n^{-\sigma} &= M^{-\sigma}\left(\sum_{n\leq M}|b(n)|\right) - \int_1^M \left(\sum_{n\leq t}|b(n)|\right) t^{-\sigma-1}(-\sigma)dt \\ &= O\left(M^{1-\sigma}\right) + \sigma\int_1^M t^{-\sigma}dt = O\left(M^{1-\sigma}\right),\end{aligned}$$

mikä todistaakin väitteet. □

Holomorfisilla kärkimuodoilla on samankaltainen funktionaaliyhtälö kuin Riemannin zeta-funktiolla. Kuitenkin erona on, että Riemannin zeta-funktiolla pisteet s ja $1-s$ vastaavat toisiaan, kun taas kärkimuodoilla vastaavuus on pisteillä s ja $\kappa - s$, joskin normalisoinnin jälkeen vastaavuus saadaan samoille pisteille kuin Riemannin zeta-funktiolla (katso korollaari).

Lause 68. *Holomorfiseen kärkimuotoon liittyvälle Dirichlet'n sarjalle pätee*

$$\left(\frac{k}{2\pi}\right)^s \Gamma(s)\varphi(s,h/k) = (-1)^{\kappa/2}\Gamma(\kappa-s)\left(\frac{k}{2\pi}\right)^{\kappa-s}\varphi(\kappa-s,-\overline{h}/k).$$

Todistus. Ohessa hahmotelma, yksityiskohtien täydentäminen on harjoitustehtävä 4.4-4.6:

1. Olkoon $\tau = \frac{h}{k} + \frac{iz}{k}$ ja $\tau' = -\frac{\overline{h}}{k} + \frac{i}{zk}$. Osoita, että $f(\tau') = (-1)^{\kappa/2}z^{\kappa}f(\tau)$.
2. Kirjoita funktionaaliyhtälön vasen puoli niin, että purat gammafunktion integraaliesitykseen (merk. $e\left(\frac{x}{k}\right) = e_k(x)$):

   $$\left(\frac{k}{2\pi}\right)^s \Gamma(s)\varphi(s,h/k) = \sum_{n=1}^{\infty} a(n)e_k(nh)\int_0^{\infty} x^{s-1}e^{-2\pi nx/k}dx = \int_0^{\infty} x^{s-1}f\left(\frac{h}{k}+\frac{ix}{k}\right)dx.$$

   ota integraali välillä $(0,1)$ erityiseen tarkasteluun, käytä kohdan 1) kaavaa siihen ja tee muuttujanvaihto niin, että integraali vaihtuu väliltä $(0,1)$ välille $(1,\infty)$. Summaa tämä integraali alkuperäisen välin $(1,\infty)$ yli olevan integraalin kanssa yhteen ja manipuloi saavuttaaksesi seuraavan tehtävän lähtökohta.

3. Osoita, että edellisen kohdan kaksi integraalia välin $(1,\infty)$ yli:

$$\int_1^\infty \left(x^{s-1} f\left(\frac{h}{k}+\frac{ix}{k}\right) + (-1)^{\kappa/2} x^{\kappa-1-s} f\left(-\frac{\bar{h}}{k}+\frac{ix}{k}\right)\right) dx$$

ovat yhtäpitäviä funktionaaliyhtälön oikean puolen kanssa.

□

Välittömänä korollaarina saadaan Hecken funktionaaliyhtälö:

Korollaari 69. *Eksponenttitermittömälle Dirichlet'n sarjalle pätee*

$$(2\pi)^{-s}\,\Gamma(s)\varphi(s) = (-1)^{\kappa/2}\,(2\pi)^{s-\kappa}\,\Gamma(\kappa-s)\varphi(\kappa-s)$$

Merkitään nyt $\tilde{a}(n) = a(n)n^{-(\kappa-1)/2}$ ja $\tilde{\varphi}(s,r) = \sum_{n=1}^\infty \tilde{a}(n)n^{-s}$. Helposti saadaan seuraava korollaari:

Korollaari 70. *Normeeratulle Dirichlet'n sarjalle pätee*

$$\left(\frac{k}{2\pi}\right)^{t+\frac{\kappa-1}{2}} \Gamma(t+\frac{\kappa-1}{2})\tilde{\varphi}(t,h/k) = (-1)^{\kappa/2}\left(\frac{k}{2\pi}\right)^{\frac{\kappa+1}{2}-t} \Gamma\left(\frac{\kappa+1}{2}-t\right)\tilde{\varphi}(1-t,-\overline{h}/k)$$

Todistus. Lienee ilmeinen. □

5.4 Voronoi-tyyppinen summakaava

Voronoi-tyyppisiä summakaavoja on useita erilaisia. Pääpiirteittäinen idea on, että Fourier-kerrointen summa (mahdollisesti muilla funktioilla höystettynä) muunnetaan toisenlaiseksi Fourier-kertoimien summaksi, tavoitteena saavuttaa uudelle summalle jossain mielessä paremmat ominaisuudet kuin vanhalle. Seuraavaksi todistetaan Huxleyn mukaan yhdenlainen Voronoi-tyyppinen summakaava, ja tämän jälkeen löytyy tekstistä vielä toisenlainen, mutta sen todistus jää harjoitustehtäväksi.

Aloitetaan Hölderin epäyhtälön muotoilulla.

Lause 71. *Olkoot p ja q reaalilukuja, joilla pätee $1 \le p,q < \infty$ ja $\frac{1}{p}+\frac{1}{q}=1$. Nyt*

$$\int |fg| \le \left(\int |f|^p\right)^{1/p}\left(\int |g|^q\right)^{1/q}$$

ja

$$\sum |a_j b_j| \le \left(\sum |a_j|^p\right)^{1/p}\left(\sum |b_j|^q\right)^{1/q}.$$

Todistetaan alkuun pari lemmaa. Kannattaa huomata, että näissä lemmoissa ei missään oleteta, että modulimuodot F tai G olisivat modulimuotoja koko ryhmän $\mathrm{SL}(2,\mathbb{Z})$ suhteen.

Lemma 72 (Rankinin sarja)**.** *Kun $G(z)$ on painoa κ oleva kärkimuoto, jonka Fourier-kertoimet ovat $b(\ell)$, on sarja*

$$R(s) = \sum_{\ell=1}^\infty \frac{|b(\ell)|^2}{\ell^s}$$

suppeneva, kun $\Re s > \kappa$, ja sillä on analyyttinen jatke, ja yksinkertainen napa pisteessä $s=\kappa$.

Tämä on yleistys edellisellä luennolla esitetystä Rankinin lauseesta. Ainakin toistaiseksi todistus sivuutetaan.

Tämän avulla saadaan kuitenkin seuraava korollaari, joka tuottaa vielä iloa:

Korollaari 73. *On olemassa vakio B, jolla*

$$\sum_{\ell=1}^{L} \frac{|b(\ell)|^2}{\ell^\kappa} \leq B^2 \log 2L.$$

Todistus. Funktio $|(s-\kappa)R(s)|$ on jatkuva, joten määritellään

$$A = \max_{\kappa \leq s \leq \kappa+2} |(s-\kappa)R(s)|$$

(huomioitava, että maksimointi tapahtuu reaaliakselilla). Asetetaan $s = \kappa + \frac{1}{\log 2L}$. Nyt

$$A \log 2L \geq R(s) \geq \sum_{\ell=1}^{L} \frac{|b(\ell)|^2}{\ell^s} \geq \frac{1}{e} \sum_{\ell=1}^{L} \frac{|b(\ell)|^2}{\ell^\kappa},$$

mistä korollaari saadaankin valinnalla $B^2 = eA$. □

Lemma 74. *Olkoot $F(z)$ ja $G(z)$ painoa κ olevia modulimuotoja, joiden Fourrier-sarjat ovat muotoa*

$$F(z) = \sum_m a(m) e(mz)$$

ja

$$G(z) = \sum_\ell b(\ell) e\left(\frac{\ell z}{c}\right),$$

ja jotka toteuttavat ehdon

$$z^{-\kappa} G\left(-\frac{1}{z}\right) = F(z).$$

Olkoon (x) kahdesti jatkuvasti derivoituva funktio, joka on tuettu välillä $M \leq x \leq M_2$. Silloin

$$\sum_{M \leq m \leq M_2} a(m) g(m) = (-1)^{\kappa/2} 2\pi \sum_\ell b(\ell) \int_M^{M_2} \left(\frac{cx}{\ell}\right)^{(\kappa-1)/2} J_{\kappa-1}\left(4\pi\sqrt{\frac{\ell x}{c}}\right) g(x) dx,$$

missä J_κ on J-Besselin funktio.

Lienee syytä mainita, että asymptoottisesti

$$J_\nu(z) \sim \left(\frac{2}{\pi z}\right)^{1/2} \cos\left(z - \frac{1}{2}\nu\pi - \frac{1}{4}\pi\right).$$

Todistus. Kirjoitetaan $\mu = \frac{1}{2\pi M}$ ja asetetaan $h(x) = e^{2\pi\mu x} g(x)$. Olkoon

$$\hat{h}(x) = \int_M^{M_2} h(u) e(-ux) du$$

funktion $h(x)$ Fourier-muunnos. Nyt

$$\int_{-\infty}^{\infty} \hat{h}(x)F(x+i\mu)dx = \int_{-\infty}^{\infty} \hat{h}(x) \sum_m a(m)e(mx)e^{-2\pi m\mu}dx$$
$$= \sum_m a(m)h(m)e^{-2\pi m\mu} = \sum_m a(m)g(m).$$

Yllä käytettin Fourier-muunnoksen käänteismuunnoksen kaavaa. Nyt

$$\sum_m a(m)g(m) = \int_{\infty}^{\infty} \hat{h}(x)(x+i\mu)^{-\kappa} G\left(-\frac{1}{x+i\mu}\right) dx$$
$$= \int_{-\infty}^{\infty} \hat{h}(x)(x+i\mu)^{-\kappa} \sum_\ell b(\ell)e\left(-\frac{\ell}{c(x+i\mu)}\right) dx.$$

Derivoidaan kahdesti ja käytetään ensimmäisen derivaatan testiä:

$$\hat{h}(x) = \int_M^{M_2} h(u)e(-ux)du = \left[-\frac{1}{2\pi ix}h(u)e(-ux)\right] + \frac{1}{2\pi ix}\int_M^{M_2} h'(u)e(-ux)$$
$$= \left[\frac{1}{(2\pi ix)^2}h'(u)e(-ux)\right]_M^{M_2} - \frac{1}{(2\pi x)^2}\int_M^{M_2} h''(u)e(-ux)dx$$
$$\ll \frac{1}{|x|^2}\int_M^{M_2} h''(u)e(-ux) \ll_h \frac{1}{|x|^3}.$$

Implikoitu vakio riippuu toki funktion g suuruudesta, mutta jos g ajatellaan kiinnitetyksi, niin sen jälkeen ylläoleva arvio on kunnossa. Käytetään lemmaa ja korollaaria valinnalla $s = \frac{2\kappa+3}{4}$ ja Hölderin epäyhtälöä, jolloin saadaan

$$\left|\sum_\ell b(\ell)e\left(-\frac{\ell}{c(x+i\mu)}\right)\right| \le \sum_\ell |b(\ell)|e^{-2\pi\mu\ell/(c(x^2+\mu^2))} \ll \sum_\ell |b(\ell)| \left(\frac{2\pi\mu\ell}{c(x^2+\mu^2)}\right)^{-(2\kappa+3)/4}$$
$$\ll \left(\frac{c(x^2+\mu^2)}{\mu}\right)^{(2\kappa+3)/4} \sum_\ell \frac{|b(\ell)|}{\ell^{(2\kappa+3)/4}} \ll \left(\frac{c(x^2+\mu^2)}{\mu}\right)^{(2\kappa+3)/4)}.$$

Täten summa ja integraali ovat itseisesti suppenevia, ja voimme ensin integroida. Huomataan, että

$$\int_{-\infty}^{\infty} \bar{h}(x)(x+i\mu)^{-\kappa} e\left(-\frac{1}{c(x+i\mu)}\right) dx = \int_M^{M_2}(u) \int_{-\infty}^{\infty} (x+i\mu)^{-\kappa} e\left(-\frac{1}{z(x+i\mu)} - ux\right) dxdu$$
$$= \int_M^{M_2} g(u) \int_{-\infty+i\mu}^{\infty+i\mu} e\left(-\frac{\ell}{cz} - uz\right)\frac{dz}{z^\kappa}du.$$

Integraalilla on singulariteetti pisteessä $z = 0$. Käyttäkäämme residylausetta. Muodostetaan integrointitie siten, että integroidaan reaaliakselin suuntaisesti pisteestä $-T + i\mu$ pisteeseen $T + i\mu$, sitten pisteestä $T + i\mu$ alas pisteeseen $T - iT$, tämän jälkeen pisteestä $T - iT$ pisteeseen $\varepsilon - iT$, josta noustaan origon ympäristöön, kierretään origo, laskeudutaan suoraa $\Re z = -\varepsilon$ pisteeseen $-\varepsilon - iT$, josta jatketaan pisteeseen $-T - iT$, josta noustaan pisteeseen $-T + i\mu$.

Imaginääriakselin suuntaiset integraalit väleillä $[T+i\mu, T-iT]$ ja $[-T-iT, -T+i\mu]$ ovat pienet, samoin reaaliakselin suuntaiset integraalit suoralla $\Im z = -T$. Imaginääriakselin viereiset integraalit (suorilla $\Re z = \varepsilon$ ja $\Re z = -\varepsilon$) kumoavat toisensa. Lopulta jäljelle jää vain origon kierto. Ryhdymme nyt tarkastelemaan tätä.

Tehdään muuttujanvaihto:

$$v = -iz\sqrt{\frac{cu}{\ell}}.$$

Tämä kääntää integroinnin origon ympäri lähtien negatiiviselta reaaliakselta ja päätyen negatiiviselle reaaliakselille vastapäivään. Saadaan

$$\begin{aligned}\int e\left(-\frac{\ell}{cz}-uz\right)\frac{dz}{z^\kappa} &= \int e\left(-\frac{\ell}{c\cdot\frac{v}{-i}\sqrt{\frac{\ell}{cu}}}-\frac{uv}{(-i)}\sqrt{\frac{\ell}{cu}}\right)\left(i\sqrt{\frac{\ell}{cu}}\right)^{1-\kappa}v^{-\kappa}dv\\ &= (-1)^{k-1}\left(\frac{cu}{\ell}\right)^{(\kappa-1)/2}\int e\left(-\frac{i\ell}{v\sqrt{\frac{\ell}{cu}}}-iv\sqrt{\frac{\ell u}{c}}\right)v^{-\kappa}dv\\ &= (-1)^{k-1}\left(\frac{cu}{\ell}\right)^{(\kappa-1)/2}\int e\left(-i\sqrt{\frac{\ell u}{c}}\left(\frac{1}{v}-v\right)\right)v^{-\kappa}dv\\ &= (-i)^{\kappa-1}\left(\frac{cu}{\ell}\right)^{(\kappa-1)/2}\int \exp\left(\frac{t}{2}\left(v-\frac{1}{v}\right)\right)v^{-\kappa}dv.\end{aligned}$$

Tässä on huomioitava, että

$$J_\nu(x) = \frac{1}{2\pi i}\int_C e^{1/2t(v-v^{-1})}v^{-\nu-1}dv,$$

missä C on integrointitie origon ympäri myötäpäivään negatiiviselta reaaliakselilta aloittaen. Sijoittaen tähän

$$t = 4\pi\sqrt{\frac{\ell u}{c}}$$

sekä $\nu = \kappa - 1$ saadaan

$$J_{\kappa-1}\left(4\pi\sqrt{\frac{\ell u}{c}}\right) = \frac{1}{2\pi i}\int_C e^{1/2\cdot 4\pi\sqrt{\frac{\ell u}{c}}(v-v^{-1})}v^{-\kappa}dv,$$

kuten vaadittu. □

Lause 75. *Olkoot $a(n)$ painoa $\kappa \in 2\mathbb{Z}$ olevan holomorfisen täyden moduliryhmän $SL(2,\mathbb{Z})$ suhteen olevan kärkimuodon $F(z)$ Fourier-kertoimet. Olkoon $g(x)$ välillä $[M, M_2]$ tuettu funktio, joka on kahdesti jatkuvasti derivoituva ja olkoon a/k rationaaliluku ($a, k \in \mathbb{Z}$). Nyt*

$$\sum_{M\le m\le M_2} a(m)e\left(\frac{am}{k}\right)g(m) = (-1)^{\kappa/2}2\pi\sum_{n=1}^{\infty}a(n)n^{(\kappa-1)/2}e\left(-\frac{\bar{a}n}{k}\right)\int_M^{M_2}x^{(\kappa-1)/2}J_{\kappa-1}\left(4\pi\frac{\sqrt{nx}}{k}\right)g(x)dx.$$

Todistus. Käytetään edellä todistettua lausetta. Nyt

$$F\left(z+\frac{a}{k}\right) = F \mid \begin{pmatrix}1 & a/k\\ 0 & 1\end{pmatrix} = F \mid \begin{pmatrix}\bar{a} & \bar{k}\\ -k & a\end{pmatrix}\begin{pmatrix}1 & a/k\\ 0 & 1\end{pmatrix} = F \mid \begin{pmatrix}\bar{a} & 1/k\\ -k & 0\end{pmatrix},$$

missä $a\bar{a} + k\bar{k} = 1$. Modulimuoto, G, jolla

$$G \mid \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = F \mid \begin{pmatrix} 1 & a/k \\ 0 & 1 \end{pmatrix}$$

saadaan asettamalla

$$G = F \mid \begin{pmatrix} \bar{a} & 1/k \\ -k & 0 \end{pmatrix} \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} = F \mid \begin{pmatrix} 1/k & -\bar{a} \\ 0 & k \end{pmatrix},$$

eli

$$G(z) = k^{-\kappa} F\left(\frac{z}{k^2} - \frac{\bar{a}}{k}\right).$$

Käytetään nyt edellä todistettua kaavaa valinnoilla $c = q^2$, ja kertoimet $a(m)$ ja $b(\ell)$ korvattuna kertoimilla $a(m)e\left(\frac{am}{k}\right)$ ja $k^{-\kappa}a(\ell)e\left(-\frac{\bar{a}\ell}{k}\right)$. □

On myös mahdollista muotoilla toisenlainen, niin sanottu katkaistu Voronoi-tyyppinen summakaava.

Lause 76. *Olkoon $x \geq 1$, $k \leq x$, $h \in \mathbb{Z}$ ja $1 \leq N \ll x$, ja olkoot $a(n)$ holomorfisen kärkimuodon Fourier-kertoimet. Nyt*

$$\sum_{n \leq x} a(n)e\left(\frac{h}{k}n\right) = \left(\pi\sqrt{2}\right)^{-1} k^{1/2}x^{-1/4+\kappa/2} \sum_{n \leq N} a(n)e_k\left(-n\bar{h}\right) n^{-1/4-\kappa/2} \cos\left(\frac{4\pi\sqrt{nx}}{k} - \frac{\pi}{4}\right) + O\left(kx^{\kappa/2+\varepsilon}N^{-1/2}\right).$$

Todistus. Todistuksen yksityiskohdat sivuutetaan, mutta hahmotelma käydään läpi luennoilla. (Siltä varalta, ettei lukija ehdi luennoille: tämä ei ole kurssin tärkein asia – minulta voi myös pyytää kopiota todistuksesta.) □

Osittaissummausta käyttäen saamme varsin käyttökelpoisen muotoilun normeeratuille Fourier-kertoimille ($a(n) = b(n)n^{(\kappa-1)/2}$):

$$\sum_{n \leq x} b(n)e\left(\frac{h}{k}n\right) = \left(\pi\sqrt{2}\right)^{-1} k^{1/2}x^{1/4} \sum_{n \leq N} b(n)e_k\left(-n\bar{h}\right) n^{-3/4} \cos\left(\frac{4\pi\sqrt{nx}}{k} - \frac{\pi}{4}\right) + O\left(kx^{1/2+\varepsilon}N^{-1/2}\right).$$

Katkaistun Voronoi-tyyppisen summakaavan avulla voidaan todistaa seuraava keskiarvotulos (huomiotava, että tässä tarkastellaan neliön keskiarvoa, mikä itse asiassa on hyvin yleinen tarkasteltava lukuteoriassa). Merkitään $A\left(x, \frac{h}{k}\right) = \sum_{n \leq x} a(n)e\left(\frac{h}{k}n\right)$

Lause 77. *Kun $X \geq 1$, pätee*

$$\int_1^X \left|A\left(x, \frac{h}{k}\right)\right|^2 dx = c(\kappa)kX^{\kappa+1/2} + O\left(k^2X^{\kappa+\varepsilon}\right) + O\left(k^{3/2}X^{\kappa+1/4+\varepsilon}\right),$$

missä

$$c(\kappa) = \left((4\kappa+2)\pi^2\right)^{-1} \sum_{n=1}^{\infty} |a(n)|^2 n^{-\kappa-1/2}.$$

Todistus. Tarkastellaan integraalia välillä $[X/2, X]$. Halutaan osoittaa, että

$$\int_{X/2}^{X} \left| A\left(x, \frac{h}{k}\right)\right|^2 dx = c(\kappa)k\left(X^{\kappa+1/2} - \left(\frac{X}{2}\right)^{\kappa+1/2}\right) + O\left(k^2X^{\kappa+\varepsilon}\right) + O\left(k^{3/2}X^{\kappa+1/4+\varepsilon}\right),$$

kun $k \leq X/2$ sillä vaadittu tulos ilmeisesti seuraa tästä tällä oletuksella. Kun taas $X \ll k$, niin todetaan, että

$$\left|\sum_{n\leq x} a(n)e\left(\frac{h}{k}n\right)\right| \leq \sum_{n\leq x}|a(n)| \ll \sum_{n\leq x} d(n)n^{(\kappa-1)/2} \ll \sum_{n\leq x} n^{(\kappa-1)/2+\varepsilon} \ll x^{(\kappa+1)/2+\varepsilon},$$

Ja tämän arvon neliön yli integrointi:

$$\int_1^X x^{(\kappa+1)+\varepsilon}dx \ll X^{\kappa+2+\varepsilon} \ll k^2X^{\kappa+\varepsilon},$$

eli tämä saadaan hävitettyä toiseen virhetermiin. Riittää siis tarkastella tapausta $k \leq X/2$. Olkoon nyt $\frac{X}{2} \leq k \leq X$. Otetaan käyttöön katkaistu Voronoi-tyyppinen summakaava:

$$\sum_{n\leq x} a(n)e\left(\frac{h}{k}n\right) = \left(\pi\sqrt{2}\right)^{-1} k^{1/2}x^{-1/4+\kappa/2}\sum_{n\leq N} a(n)e_k\left(-n\bar{h}\right)n^{-1/4-\kappa/2}\cos\left(\frac{4\pi\sqrt{nx}}{k} - \frac{\pi}{4}\right) + O\left(kx^{\kappa/2+\varepsilon}N^{-1/2}\right).$$

Sijoitetaan kaavaan $N = X$. Nyt

$$\sum_{n\leq x} a(n)e\left(\frac{h}{k}n\right) = \left(\pi\sqrt{2}\right)^{-1} k^{1/2}x^{-1/4+\kappa/2}\sum_{n\leq X} a(n)e_k\left(-n\bar{h}\right)n^{-1/4-\kappa/2}\cos\left(\frac{4\pi\sqrt{nx}}{k} - \frac{\pi}{4}\right) + O\left(kX^{(\kappa-1)/2+\varepsilon}\right) = S\left(x, \frac{h}{k}\right) + O\left(kX^{(\kappa-1)/2+\varepsilon}\right).$$

Keskitytään nyt tarkastelemaan termin $S\left(x, \frac{h}{k}\right)$ neliön integraalia. Ongelmaa lähestytään hyvin yksinkertaisesti: kerrotaan neliöinti auki ja integroidaan termi termiltä. Kirjoitetaan kuitenkin aluksi

$$\cos\left(\frac{4\pi\sqrt{nx}}{k} - \frac{\pi}{4}\right) = \frac{1}{2}\left(e\left(2\frac{\sqrt{nx}}{k} - \frac{1}{8}\right) + e\left(-2\frac{\sqrt{nx}}{k} + \frac{1}{8}\right)\right)$$

Saadaan

$$\int_{X/2}^{X}\left|S\left(x, \frac{h}{k}\right)\right|dx = S_0 + O\left((k|S_1| + s_2|)\right),$$

missä

$$\begin{aligned} S_0 &= \left(4\pi^2\right)^{-1} k\sum_{n\leq X}|a(n)|^2n^{-\kappa-1/2}\int_{X/2}^{X} x^{-1/2+\kappa}dx \\ &= \left((4\kappa+2)\pi\right)^{-1} k\sum_{n=1}^{\infty}|a(n)|^2n^{-\kappa-1/2}\left(X^{\kappa+1/2} - \left(\frac{X}{2}\right)^{\kappa+1/2}\right) + O\left(kX^{\kappa+\varepsilon}\right) \end{aligned}$$

(tästä muodostuu päätermi) ja

$$S_1 = \sum_{m,n\le X, m\neq n} a(n)\overline{a(m)}(mn)^{-1/4-\kappa/2}\int_{X/2}^{X} x^{-1/2+\kappa}e\left(2\frac{(\sqrt{m}-\sqrt{n})\sqrt{x}}{k}\right)dx$$

$$S_2 = \sum_{m,n\le X} a(n)\overline{a(m)}(mn)^{-1/4-\kappa/2}\int_{X/2}^{X} x^{-1/2+\kappa}e\left(2\frac{(\sqrt{m}+\sqrt{n})\sqrt{x}}{k}\right)dx$$

Summat S_2 ja S_1 voidaan arvioida samalla tavalla, ja itse asiassa S_2 on ehkä jopa hitusen helpompi. Keskitytään siis summan S_1 arviointiin. Arvioidaan ensin integraali ensimmäisen derivaatan testillä. Saadaan

$$\int_{X/2}^{X} x^{\kappa-1/2}e\left(2\frac{(\sqrt{m}-\sqrt{n})\sqrt{x}}{k}\right)dx \ll \frac{X^\kappa k}{|\sqrt{m}-\sqrt{n}|}.$$

Summataan

$$\begin{aligned}
S_1 &= kX^\kappa \sum_{1\le n<m\le X} a(n)\overline{a(m)}(mn)^{-1/4-\kappa/2}(\sqrt{m}-\sqrt{n})^{-1} \\
&= kX^\kappa \sum_{1\le n<m\le X} |a(n)||a(m)|(nm)^{-1/4-\kappa/2}(m-n)^{-1}(\sqrt{m}+\sqrt{n}) \\
&\ll kX^\kappa \sum_{1\le n<m\le X} n^{\varepsilon-3/4}m^{\varepsilon-1/4}(m-n)^{-1} \ll kX^\kappa \sum n^{\varepsilon-1/4}\ell^{-1}(n+\ell)^{\varepsilon-3/4} \\
&\ll kX^{\kappa+\varepsilon}\sum_{\ell\le X}\ell^{-1} \ll kX^{\kappa+\varepsilon}.
\end{aligned}$$

Summa S_2 voidaan arvioida samoin. Olemme siis saaneet arvioksi

$$\int_{X/2}^{X}\left|S\left(x,\frac{h}{k}\right)\right|dx = ((4\kappa+2)\pi)^{-1}k\sum_{n=1}^{\infty}|a(n)|^2n^{-\kappa-1/2}\left(X^{\kappa+1/2}-\left(\frac{X}{2}\right)^{\kappa+1/2}\right) + O\left(k^2X^{\kappa+\varepsilon}\right).$$

Koska

$$A\left(x,\frac{h}{k}\right) = S\left(x,\frac{h}{k}\right) + O\left(kX^{(\kappa-1)/2+\varepsilon}\right),$$

niin Hölderin (valinnalla $p=q=2$) nojalla saadaan

$$\int_{X/2}^{X}\left|A\left(x,\frac{h}{k}\right)\right|^2dx = ((4\kappa+2)\pi)^{-1}k\sum_{n=1}^{\infty}|a(n)|^2n^{-\kappa-1/2}\left(X^{\kappa+1/2}-\left(\frac{X}{2}\right)^{\kappa+1/2}\right) + O\left(k^2X^{\kappa+\varepsilon}\right) + O\left(k^{3/2}X^{\kappa+1/4+\varepsilon}\right).$$

□

Esimerkki 78. Todettakoon nyt, että Jutila on todistanut, että

$$\sum_{n\le M} b(n)e(n\alpha) \ll \sqrt{M},$$

kun $\alpha \in \mathbb{R}$ ja $a(n) = n^{(\kappa-1)/2}$. Rankinin lauseen ja Parsevalin kaavan nojalla tämä arvio on itse asiassa paras mahdollinen:

$$\int_0^1 \left| \sum_{n \leq M} b(n) e(n\alpha) \right|^2 d\alpha = \sum_{n \leq M} |a(n)|^2 \asymp M.$$

Todistus perustuu approksimatiivisen funktionaaliyhtälön kehittämiseen ja käyttöön.

Mielenkiintoista kyllä, seuraava lause voidaan todistaa varsin vähällä vaivalla:

Lause 79. *Olkoot $b(n)$ holomorfisen kärkimuodon normeeratut Fourier-kertoimet. Nyt*

$$\sum_{n \leq M} b(n) \ll M^{1/3+\varepsilon}.$$

Todistus. Käytetään normeeratuille kertoimille katkaistua Voronoi-tyyppistä summakaavaa:

$$\sum_{n \leq M} b(n) e\left(\frac{h}{k} n\right) = \left(\pi\sqrt{2}\right)^{-1} k^{1/2} M^{1/4} \sum_{n \leq N} b(n) e_k\left(-n\bar{h}\right) n^{-3/4} \cos\left(\frac{4\pi\sqrt{nM}}{k} - \frac{\pi}{4}\right) + O\left(kM^{1/2+\varepsilon} N^{-1/2}\right).$$

Koska eksponenttitermiä ei ole, niin $k = 1$, $h = 0$. Täten

$$\sum_{n \leq M} b(n) = \left(\pi\sqrt{2}\right)^{-1} M^{1/4} \sum_{n \leq N} b(n) n^{-3/4} \cos\left(4\pi\sqrt{nM} - \frac{\pi}{4}\right) + O\left(M^{1/2+\varepsilon} N^{-1/2}\right)$$

Valitaan nyt $N = M^{1/3+\varepsilon}$. Tällöin

$$\begin{aligned} \left| \sum_{n \leq M} b(n) \right| &\leq \left| \left(\pi\sqrt{2}\right)^{-1} M^{1/4} \sum_{n \leq M^{1/3}} b(n) n^{-3/4} \cos\left(4\pi\sqrt{nM} - \frac{\pi}{4}\right) \right| + O\left(M^{1/2+\varepsilon} M^{-1/6}\right) \\ &\leq M^{1/4} \sum_{n \leq} |b(n)| n^{-3/4} + O\left(M^{1/3+\varepsilon}\right) \leq M^{1/4} \sum_{n \leq M^{1/3}} n^{\varepsilon - 3/4} + O\left(M^{1/3+\varepsilon}\right) \ll M^{1/3+\varepsilon}. \end{aligned}$$

□

Tämän summan arvion on konjekturoitu olevan $\ll M^{1/4+\varepsilon}$. Tämän konjektuurin yllättävyys, samoin kuin ylläolevan arvion, on siinä, että neliöjuurikumoutuminen on varsin tyypillinen ilmiö, mutta neliöjuuren alle ei ole läheskään aina pääsyä.

Voronoi-tyyppisiä summakaavoja voidaan todistaa myös eksponenttisummille, joissa on Fourier-kertoimien tilalla tekijäfunktion arvot. Summan muoto muuttuu hieman, mutta ei paljon (ja muutos selittyy menetelmällisesti eräällä residyllä), ja filosofisesti sillä, että koska tekijäfunktion arvot ovat positiivisia, on eksponenttisumman joskus saatava isoja arvoja. Termi, joka on samanlainen kuin kärkimuototapauksessa, on taas puolestaan pieni, joten se ei voi riittää yksinään.

Lause 80. *Kun $x \geq 1$, $k \leq x$, $h \in \mathbb{Z}$ ja $1 \leq N \ll x$, niin*

$$\sum_{n \leq M} d(n) e\left(\frac{h}{k} n\right) = k^{-1}(\log x + 2\gamma - 1 - 2\log k)x + E\left(0, \frac{h}{k}\right) + \left(\pi\sqrt{2}\right)^{-1} k^{1/2} x^{1/4} \sum_{n \leq N} d(n) e_k\left(-n\bar{h}\right) n^{-3/4} \cos\left(\frac{4\pi\sqrt{nx}}{k} - \frac{\pi}{4}\right) + O\left(k x^{1/2+\varepsilon} N^{-1/2}\right),$$

missä $E\left(0, \frac{h}{k}\right)$ on Estermannin zeta-funktion arvo pisteessä $\left(0, \frac{h}{k}\right)$.

Estermannin zeta-funktio on määritelty sarjana:

$$E(s, r) = \sum_{n=1}^{\infty} d(n) e(nr) n^{-s},$$

missä $r = \frac{h}{k}$. Sarja suppenee, kun $\Re s > 1$. Sillä on funktionaaliyhtälö ja meromorfinen jatke koko tasoon. Kriittistä on tietää, että

$$E\left(0, \frac{h}{k}\right) \ll k \log 2k.$$

Lause 81. *Pätee*

$$\sum_{n \leq M} d(n) = M \log M + (2\gamma - 1)M + O\left(M^{1/3+\varepsilon}\right).$$

Todistus. Harjoitustehtävä 5.1. □

Luku 6

Linnikin ongelma

6.1 Ongelman kuvaus

Tarkastellaan pisteitä $\alpha \in \mathbb{Z}^3$, eli $|\alpha|^2 = x_1^2 + x_2^2 + x_3^2$, kun $\alpha = (x_1, x_2, x_3)$. Joukko

$$\Omega_n = \left\{ x = \frac{\alpha}{|\alpha|} : \alpha \in \mathbb{Z}^3, |\alpha|^2 = n \right\}$$

on yksikköpallolla. Legendren mukaan Ω_n on epätyhjä jos ja vain jos $n \neq 4^a(8b+7)$, kun a ja b ovat kokonaislukuja, $a \geq 0$.

Linnik kysyi onko joukko Ω_n tasaisesti jakautunut normalisoidun Lebesguen mitan $d\sigma$suhteen yksikköpallolle S^2, kun $a = 0$, eli jos tarkastellaan jotain yksikköympyrän järkevää osajoukkoa, niin lähestyykö tälle osajoukolle sijoittuneiden pisteiden osuus kaikista joukon Ω_n pisteistä osajoukon mittaa. Vastaus tähän kysymykseen on myönteinen, eli seuraava lause pätee (rajoitutaan yksinkertaisuuden vuoksi kuitenkin vain neliövapaisiin n):

Lause 82. *Olkoon $f \in C^\infty(S^2)$. Kun $n \to \infty$, n on neliövapaa ja $n \neq 7$ (mod 8), niin*

$$\frac{1}{|\Omega_n|} \sum_{x \in \Omega_n} f(x) \to \int_{S^2} f d\sigma.$$

Todistetaan tämä lause, joskin osa teknisistä yksityiskohdista jätetään puhtaasti uskon tai aktiivisuuden varaan. Ennen kuin pääsemme lauseen todistukseen, joudumme kuitenkin käymään läpi hieman teoriaa ja lemmoja.

6.2 Konveksisuusrajoista

Tarkastellaan Dirichlet'n sarjaa

$$\sum_{n=1}^{\infty} c(n) n^{-s}.$$

Oletetaan, että sarja suppenee itseisesti, kun $\Re s > 1$. Oletetaan, että sillä on funktionaaliyhtälö funktionaaliyhtälöä muotoa $s \to 1 - s$. Funktionaalioyhtälön avulla saadaan johdettua sarjan analyyttisen jatkon käytös suoralla $\Re s = 0$, ja Phragmen-Lindelöfin konveksisuusperiaattesta saadaan käytös suoralla $\Re s = \frac{1}{2}$. Tätä rajaa kutsutaan konveksisuusrajaksi, ja jossain

mielessä se on triviaali. Valitettavasti tämä arvio ei yleensä ole riittävän hyvä, vaan tarvitaan parempi raja, englanniksi *sub-convexity bound*, konveksisuuden rikkova raja.

Aloitetaan klassisella esimerkillä.

Esimerkki 83. Olkoon $L(s,\chi) = \sum_{n=1}^{\infty} \chi(n)n^{-s}$ Dirichlet'n L-funktio. Tässä χ on primitiivinen karakteri moduli q. Nyt

$$\left(\frac{q}{\pi}\right)^{s/2} \Gamma\left(\frac{s+a}{2}\right) L(s,\chi) = \varepsilon_\chi i^{(1-s)/2} \Gamma\left(\frac{1-s+a}{2}\right) L(1-s,\bar{\chi}),$$

missä $a = \frac{\chi(1)-\chi(-1)}{2}$, $\varepsilon_\chi = G(1,\chi)q^{-1/2}$ ja $G(1,\chi) = \sum_{b(\bmod q)} \chi(b)e\left(\frac{b}{q}\right)$ (Gaussin summa, eli $|\varepsilon_\chi| = 1$. Tästä funktionaaliyhtälöstä ja Phragmen-Lindelöfistä seuraa

$$L(s,\chi) = q^{1/4}\log q$$

suoralla $\Re s = \frac{1}{2}$. Ensimmäisenä tämän rajan rikkoi Burgess, joka tiputti eksponentin luvusta $\frac{1}{4}$ lukuun $\frac{3}{16}$.

Linnikin ongelmakin ratkeaa rikkomalla konveksisuusraja. Todistamme siis seuraavan lauseen:

Lause 84. *Olkoon χ primitiivinen karakteri modulo q, ja olkoon $\Re s = \frac{1}{2}$. Tällöin*

$$L_f(s,\chi) \ll |s|^2 q^{5/11} d(q)^2 \log q,$$

missä $L_f(s,\chi) = \sum_{n=1}^{\infty} b(n)\chi(n)n^{-s}$, missä $b(n)$ ovat painoa κ olevan holomorfisen kärkimuodon Fourier-kertoimet.

Huomattava on, että konveksisuusraja olisi $L(s,\chi) \ll q^{1/2}(\log q)^2$. Muiden lukujen kuin q eksponentteja ei ole edes yritetty optimoida, koska niillä ei ole väliä. Tämän lauseen todistus vaatii kuitenkin erään keskiarvon arviointia. Arvioidaan se ensin. Tarvitsemme δ-symbolin määrittelyn, ja tavan paloittaa δ osasiin.

Määritelmä 85. Määritellään δ-symboli seuraavasti:

$$\delta(n) = \begin{cases} 1 & \text{jos } n = 0 \\ 0 & \text{muuten.} \end{cases}$$

Olkoon nyt ω välillä $\frac{K}{2} < |t| < K$ tuettu funktio, joka on parillinen, ja jonka derivaatat toteuttavat ehdot

$$\omega^{(j)}(t) \ll K^{-j-1}.$$

Oletetaan lisäksi, että

$$\sum_{k=1}^{\infty} \omega(k) = 1.$$

Asetetaan

$$\delta_k(n) = \omega(k) - \omega\left(\frac{n}{k}\right).$$

Nyt

$$\delta(n) = \sum_{k|n} \delta_k(n),$$

joten

$$\delta(n) = \sum_k k^{-1} \sum_{h(\bmod k)} e\left(\frac{hn}{k}\right) \delta_k(n).$$

Kirjoitetaan nyt

$$\Delta_c(n) = \sum_r r^{-1} \delta_{cr}(n),$$

jolloin

$$\delta(n) = \sum_c c^{-1} \sum_{a(\bmod c)}^{\star} e\left(\frac{an}{c}\right) \Delta_c(n),$$

kun $r = (h,k)$, $a = \frac{h}{r}$ ja $c = \frac{k}{r}$.

Muistellaan vielä Kloostermanin summien määritelmää ja ominaisuuksia.

Määritelmä 86. Kloostermanin summa on

$$S(m,n;k) = \sum_{h(\bmod k),(h,k)=1} e_k\left(mh + n\bar{h}\right).$$

Weil on todistanut, että

$$S(m,n;p^c) \ll 2p^{c/2},$$

kun p on alkuluku, paitsi jos sekä m että n ovat luvun p monikertoja. Yleisemmin:

$$S(m,n;c) \leq d(c)\sqrt{\mathrm{syt}(m,n,c)}c^{1/2}$$

Todistetaan nyt ensin lemma, jota tarvitaan L-funktion arvion todistamiseen.

Lemma 87. *Olkoot λ_ℓ ovat mielivaltaisia kompleksilukuja, kun $1 \leq \ell \leq L$, g kahdesti jatkuvasti derivoituva funktio, joka on tuettu välillä $[M, 2M]$, ja joka toteutaa ehdon $|g^{(j)}(m)| \leq M^{-j}$, kun $j = 0, 1, 2$. Kirjoitetaan*

$$S = \sum_{\chi(\bmod q)}^{\star} \left|\sum_n b_m \chi(m) g(m)\right|^2 \left|\sum_\ell \lambda_\ell \chi(\ell)\right|^2.$$

Nyt

$$S \ll \varphi(q) M (\log M) \sum_\ell |\lambda_\ell|^2 d(\ell) + d(q)(LM)^{7/4} (\log LM)^2 \left(\sum_\ell |\lambda_\ell|\right)^2,$$

missä implikoidut vakiot riippuvat vain funktiosta f.

Todistus. Huomataan, että summa voidaan kirjoittaa muodossa

$$S = \sum_{\chi(\bmod q)}^{\star} \left|\sum a_n \chi(n)\right|^2,$$

missä $a_n = \sum_{\ell m = n} \lambda_\ell b_m g(m)$. Kirjoitetaan

$$G(n,\chi) = \sum_{m(\bmod k)} \chi(m) e\left(\frac{mn}{q}\right)$$

Gaussin summille. Nyt

$$\chi(m) = \frac{1}{q}\sum_{n=1}^{q} G(-n,\chi)e\left(\frac{mn}{q}\right).$$

Tämän avulla voidaan arvioida

$$S \le \frac{\varphi(q)}{q}\sideset{}{^\star}\sum_{a(\bmod q)}\left|a_n e\left(\frac{an}{q}\right)\right|^2.$$

Laajentaen summaus kaikkiin jäännösluokkiin saadaan

$$S \le \varphi(q)\sum_{h\equiv 0(\bmod q)} S_h,$$

missä $S_h = \sum_{n_1-n_2=h} a_{n_1}\overline{a_{n_2}}$. Kun $h=0$, saamme diagonaalitermin $\varphi(q)S_0$, missä

$$S_0 = \sum |a_n|^2.$$

Merkitään loppukontribuutiota ($h\neq 0$) $S_\star$. Kun $h=0$, kirjoitetaan

$$S_h = \sum_c c^{-1}S_{hc},$$

missä

$$S_{hc} = \sideset{}{^\star}\sum_{a(\bmod c)}\sum_{n_1,n_2} a_{n_1}\overline{a_{n_2}}e\left(\frac{a}{c}(n_1-n_2-h)\right)\Delta_c(n_1-n_2-h).$$

Ottaen käyttöön lukujen a_n konvoluutioesitys, voidaan kirjoittaa

$$S_{hc} = \sum_{\ell_1,\ell_2}\lambda_{\ell_1}\overline{\lambda_{\ell_2}}T_{\ell_1\ell_2}(c),$$

missä

$$T_{\ell_1\ell_2}(c) = \sideset{}{^\star}\sum_{a(\bmod c)} e\left(-\frac{ah}{c}\right)\sum_{m_1,m_2} b_{m_1}\overline{b_{m_2}}e\left(\frac{a}{c}(\ell_1 m_1-\ell_2 m_2)\right)F(m_1,m_2),$$

missä edelleen

$$F(m_1,m_2) = g(m_1)\bar{g}(m_2)\Delta_c)\ell_1 m_1-\ell_2 m_2-h).$$

Valitsemalla $K = N^{1/2} = (LM)^{1/2}$ (jälkimmäinen yhtäsuuruus suoraan määritelmistä) pätee arvio

$$F^{(i,j)} \ll K^{-1}\left(\frac{cM}{K}\right)^{-i-j},$$

kun $0\le i,j\le 2$. Käyttämällä Voronoi-tyyppistä summakaavaa muuttujien m_1 ja m_2 suhteen saadaan

$$T_{\ell_1\ell_2}(c) = \sideset{}{^\star}\sum_{a(\bmod c)} e\left(\frac{ah}{c}\right)\sum_{r_1,r_2} b_{r_1}\overline{b_{r_2}}e\left(\frac{\overline{a\ell'}}{c_1}r_1-\frac{\overline{a\ell''}}{c_2}r_2\right)F_v(r_1,r_2),$$

missä $\ell' = \frac{\ell_1}{(\ell_1,c)}$, $\ell'' = \frac{\ell_2}{(\ell_2,c)}$, $c_1 = \frac{c}{(\ell_1,c)}$, $c_2 = \frac{c}{(\ell_2,c)}$ ja

$$F_v(r_1,r_2) = \frac{4\pi^2}{c_1c_2}\int_0^\infty\int_0^\infty F(x_1,x_2)J_{\kappa-1}\left(\frac{4\pi\sqrt{x_1r_1}}{c_1}\right)J_{\kappa-1}\left(\frac{4\pi\sqrt{x_2r_2}}{c_2}\right)dx_1dx_2.$$

Käyttäen osittaisintegrointia, rekursiivista kaavaa

$$\frac{d}{dz}\left(z^\nu J_\nu(z)\right) = z^\nu J_{\nu-1}(z),$$

rajaa

$$J_\nu(z) \ll (1+z)^{-1/2}$$

sekä funktion F derivaattojen rajoja, saadaan

$$F_v(r_1,r_2) \ll \frac{M^2}{c_1c_2K}\left(1+\frac{cMr_1}{c_1^2K}\right)^{-5/4}\left(1+\frac{cMr_2}{c_2^2K}\right)^{-5/4}.$$

Käytetään arviota $\sum_{r\le x}|b_r|^2 \ll x$, jolloin saadaan

$$\sum_{r_1,r_2} b_{r_1}\overline{r_2}\,|F_v(r_1,r_2)| \ll K.$$

Summa yli luvun a palasen $T_{\ell_1\ell_2}$ lausekkeessa on Kloostermanin summa $S(h,\star;c)$. Sovelletaan siihen Weilin rajaa ja saadaan

$$T_{\ell_1\ell_2}(c) = \sum_{r_1,r_2} b_{r_1}\overline{b_{r_2}}F_v(r_1,r_2)S(h,\star;c) \ll (h,c)^{1/2}c^{1/2}d(c)(LM)^{1/2}.$$

Täten

$$S_{hc} \ll (h,c)^{1/2}c^{1/2}d(c)(LM)^{1/2}\left(\sum|\lambda_\ell|\right)^2.$$

Summataan seuraavaksi luvun c yli, kun $c < 2(LM)^{1/2}$. Saadaan

$$S_h \ll d(h)(LM)^{3/4}(\log LM)\left(\sum|\lambda_\ell|\right)^2.$$

Summataan lukujen $h \equiv 0 \pmod q$ yli, kun $0 < |h| \le LM$, ja sadaan

$$S_\star \ll d(q)(LM)^{7/4}(\log LM)^2\left(\sum|\lambda_\ell|\right)^2.$$

Lukujen a_n konvoluutioesityksestä saadaan vielä

$$S_0 \ll M(\log M)\sum_\ell |\lambda_{/ell}|^2 d(\ell).$$

Huomataan nyt, että

$$S \ll S_0 + S_\star,$$

jolloin todistus on valmis. □

Ylläolevaa lemma itse asiassa tullaan tarvitsemaan seuraavan näppärän korollaarin muodossa:

Korollaari 88. *Olkoon χ primitiivinen karakteri modulo q, ja olkoon $g(m)$ määritetty kuten lemmassa. Nyt*

$$B_\chi = \sum_m b_m \chi(m) g(m) \ll \left(q^{7/22} M^{7/11} + M^{7/8} \right) d(q)^2 \log M.$$

Todistus. Selkeyden vuoksi merkitään lemman karakteria χ_1 Valitaan $\lambda_\ell = \overline{\chi_1}(\ell)$. Nyt

$$\begin{aligned} S &= \sum_{\chi(\bmod q)}^{\star} \left| \sum_m b_m \chi(m) g(m) \right|^2 \left| \sum_\ell \overline{\chi_1}(\ell) \chi(\ell) \right|^2 \\ &\gg |b_m \chi_1(m) g(m)|^2 \left| \sum_\ell \overline{\chi_1}(\ell) \chi_1(\ell) \right|^2 = |B_\chi|^2 \left| \{ \ell \leq L : (\ell, q) = 1 \} \right|^2. \end{aligned}$$

Valitaan

$$L = q^{4/11} M^{-3/11} + 2qd(q)\varphi(q)^{-1},$$

mistä arvio seuraakin. □

Muotoillaan nyt Voronoi-tyyppisen summakaavan karakteriversio:

Lemma 89. *Olkoon F sileä ja kompaktisti tuettu positiivisilla reaaliluvuilla määritelty funktio ja olkoon χ karakteri modulo q. Kun $q \geq 1$ kokonaisluku ja $(a, q) = 1$, pätee*

$$\sum_m b_m \chi(m) F(m) = \varepsilon_\chi^2 \sum_r \overline{\chi}(r) F_v(r),$$

missä $\varepsilon_\chi = G(1, \chi) q^{-1/2}$ ja

$$F_v(y) = 2\pi i^\kappa q^{-1} \int_0^\infty F(x) J_{\kappa - 1} \left(\frac{4\pi \sqrt{xy}}{q} \right) dx.$$

Todistus. Koska sekä

$$\chi(m) = \frac{1}{G(1, \bar{\chi})} \sum_{a(\bmod q)} \overline{\chi}(a) e\left(\frac{am}{q} \right)$$

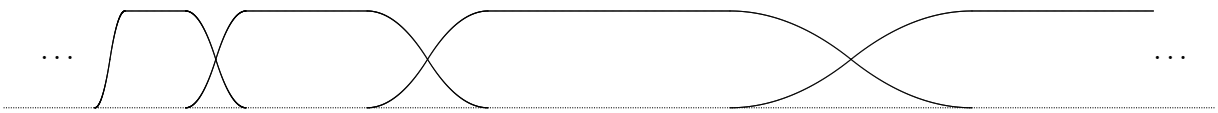
että

$$\frac{1}{G(1, \chi)} \sum_{a(\bmod q)} \overline{\chi}(a) e\left(-\frac{\bar{a} r}{q} \right) = \bar{\chi}(-r)$$

pätee, väite seuraa suoraan tavallisesta Voronoi-tyypisestä summakaavasta. □

Nyt voimme siirtyä varsinaisen L-funktion arviointiin.

Todistus. Käyttäen sileää dyadista ositusta, eli oheisen kuvan kuvaamaa tilannetta (esimerkiksi): riittää arvioida summia tyyppiä



$$H = \sum_m b_m \chi(m) m^{-s} h(m),$$

missä h on sileä funktio, joka on tuettu välillä $M, 2M$, $h^{(j)}(m) \ll M^{-j}$. Jos $M \ll q$, käytetään korollaaria valiten $g(m) = m^{-s}h(m)$, ja saadaan

$$H \ll |s|^2 \left(q^{7/22} M^{3/22} + M^{3/8}\right) d(q)^2 \log q.$$

Tällaisten osasummien yhteiskontribuutio, kun $M \ll q$ on siis

$$O\left(|s|^2 q^{5/11} d(q)^2 \log q\right).$$

Kun $M \gg q$, käytetään Voronoi-tyyppistä summakaavaa karaktereille, jolloin

$$H = \sum_m b_m \chi(m) m^{-s} h(m) = 2\pi i^\kappa q^{-1} \varepsilon_\chi^2 \sum_r b_r \bar{\chi}(r) \int_0^\infty h(x) x^{-s} J_{\kappa-1}\left(\frac{4\pi\sqrt{xr}}{q}\right) dx.$$

Osittaisintegroidaan seuraavaksi ($h(x)x^{-s}$ on derivoitava palikka, J-Bessel integroitava). Saadaan

$$2\pi i^\kappa q^{-1} \varepsilon_\chi^2 \int_0^\infty h(x) x^{-s} J_{\kappa-1}\left(\frac{4\pi\sqrt{xr}}{q}\right) dx \ll |s|^2 M^{1/2} q^{-1} \left(1 + q^{-2} M r\right)^{-5/4}.$$

Tehdään nyt dyadinen jako r:n suhteen, eli summaus suunnilleen välin $[R, 2R]$, ja sovelletaan korollaaria. Korollaari antaa dyadisen välin arvioksi

$$H \ll |s|^2 \left(q^{7/22} R^{7/11} + R^{7/8}\right) M^{1/2} q^{-1} \left(1 + q^{-2} M R\right)^{-5/4} d(q)^2 \log q.$$

Maksimoidaan nyt tämä arvio. Asetetaan $R = q^2 M^{-1}$. Tällöin

$$\begin{aligned} H &\ll |s|^2 \left(q^{7/22+14/11} M^{-7/11} + q^{7/4} M^{-7/8}\right) M^{1/2} q^{-1} d(q)^2 \log q \\ &= |s|^2 \left(q^{13/22} M^{-3/22} + q^{3/4} M^{-3/8}\right) d(q)^2 \log q \end{aligned}$$

Koska kyseessä on muuttujan M laskeva funktio, saavuttaa se suurimman arvonsa, kun M on mahdollisimman pieni, eli $M \asymp q$. Tällöin

$$H \ll |s|^2 \left(q^{13/22-3/22} + q^{3/4-3/8}\right) d(q)^2 \log q \asymp |s|^2 q^{5/11} d(q)^2 \log q,$$

kuten toivottu. □

6.3 Linnikin ongelman ratkaisu

Modulimuodot saadaan sotkettua mukaan Linnikin ongelman ratkaisuun Weylin summien kautta. Yksiulotteinen versio tilanteesta olisi tämä: Jos pitää osoittaa, että äärellinen pistejoukko X_n on jakautunut tasaisesti joukolle $S^1 = \mathbb{R}/\mathbb{Z}$. Weylin kriteeri joukon X_n tasaisesti jakautumiselle Lebesguen mitan suhteen, kun $n \to \infty$ on:

$$\frac{1}{|X_n|} \sum_{\theta \in X_n} e(m\theta) \to 0$$

kaikilla $m \in \mathbb{Z}$, $m \neq 0$.

Kaksiulotteinen tilanne (eli esimerkiksi pallonpinta avaruudessa $\mathbb{R}^3$) jossain mielessä vastaava. Weylin kriteeri pinnalla S^2 tasaiselle jakautumiselle on, että

$$\frac{1}{|\Omega_n|} \sum_{X \in \not\leqslant_\kappa} P(X) \to 0,$$

kun $n \to \infty$ kaikilla kolmen reaalimuuttujan homogeenisilla harmonisilla polynomeilla $P(x)$, joiden aste on positiivinen.

Tämä on yhtäpitävää sen kanssa, että vaaditaan

$$\sum_{\alpha \in \mathbb{Z}^3, |\alpha|^2 = n} P\left(\frac{\alpha}{|\alpha|}\right) = o_3(r_3(n)),$$

missä $r_3(n) = |\{\alpha \in \mathbb{Z}^3 : |\alpha|^2 = n\}|$. Muodostetaan polynomin P arvoista thetasarja:

$$\vartheta(z, P) = \sum_{\alpha \in \mathbb{Z}} P(\alpha) e\left(|\alpha|^2 z\right) = \sum_n r(n; P) e(nz).$$

Tämä on holomorfinen modulimuoto painoa $\frac{3}{2} + \ell$ ryhmän $\Gamma_0(4)$ suhteen, kun P on astetta ℓ, ja tämä on kärkimuoto, kun $\ell > 0$. Todistus sivuutetaan, mutta sen löytää Shimuran vuoden 1973 Annals-paperista.

Kun $\ell = 0 = \deg P$, on käsissämme hyvin tavanomainen theta-sarja:

$$\vartheta(z, 1) = \vartheta^3(z) = \sum_{n \geq 0} r_3(n) e(nz).$$

Kun n on neliövapaa positiivinen kokonaisluku, $n \neq 8b + 7$, tarvitsemme kaksi asiaa:

1. $r_3(n) \gg_\varepsilon n^{1/2-\varepsilon}$
2. $|r(n, P)| \ll n^{\kappa/2 - 1/4 - \delta}$ jollekin kiinteälle $\delta > 0$, kun $\ell > 0$.

Jälkimmäinen ehto tarkoittaa normeeratuille kertoimille, että niiden on oltava $\ll n^{1/4-\delta}$ jollakin kiinteällä $\delta > 0$.

Nyt tarvitsemme hyviä arvioita ryhmän $\Gamma_0(4)$ holomorfisten kärkimuotojen Fourier-kertoimille. Jossain mielessä triviaali arvio saadaan, kun hyödynnetään kärkimuotojen ominaisuutta:

$$y^{\kappa/2} |f(z)| \ll 1.$$

kaikilla $z \in \mathbb{H}$. Merkitään $F(z) = y^{\kappa/2}|f(z)|$. Tällöin

$$a(n) e^{-2\pi n y} = \int_0^1 e(-nx) f(x + iy) dx,$$

joten

$$|a(n)| \leq e^{2\pi n y} y^{-\kappa/2} \int_0^1 F(x + iy) dx \ll e^{2\pi n y} y^{\kappa/2}.$$

Valitaan ny $y = \frac{1}{n}$, jolloin saadaan

$$|a(n)| \ll e^{2\pi} n^{\kappa/2} |lln^{\kappa/2}.$$

Tämä arvio ei kuitenkaan valitettavasti tarkoituksiimme riitä.

Sen sijaan ylläoleva arvio L-funktion suuruudelle antaa Waldspurgerin lauseen avulla puolipainoisten kärkimuotojen ryhmän $\Gamma_0(4)$ suhteen kertoimille arvion

$$c(q) \ll q^{5/22}\tau(q)\log q.$$

Tämä on selkeästi pienempi kuin $\frac{1}{4}$. Kohta 2 on todistuksesta siis valmis.

Voimme siirtyä kohtaan 1. Tätä varten tarvitsemme luokkalukukaavaa. Olkoon d neliökunnan $Q(\sqrt{-n})$ diskriminantti (eli mikäli $n \equiv 1(\mathrm{mod}4)$, niin $d = n$ ja muulloin $d = 4n$). Kun n on neliövapaa, Gauss on todistanut

$$r_3(n) = 12h(d)\left(1 - \left(\frac{d}{2}\right)\right),$$

missä $\left(\frac{d}{2}\right)$ on Kroneckerin symboli ja $h(d)$ on niin kutsuttu *luokkaluku*. Toisaalta luokkalukukaava kertoo, että

$$h(d) = c|d|^{1/2}L(1,\chi_d).$$

Tämän avulla Siegel on todistanut, että $h(d) \gg_\varepsilon |d|^{1/2-\varepsilon}$, eli $r_3(n) \gg n^{1/2-\varepsilon}$.

Luku 7

Lehmerin konjektuurista

Lehmerin konjektuurin mukaan Ramanujanin τ-funktion arvot ovat nollasta poikkeavia. On hyvin helppo nähdä, että ne ovat kaikki kokonaislukuja. Toisaalta Delignen arvio antaa niille suuruusrajoja. Valitettavasti tätä enemmän on hyvin hankala sanoa.

Rankinin ja Selbergin keskiarvotuloksen mukaan Ramanujanin τ-funktion on pakko saavuttaa ainakin yksi nollasta poikkeava arvo välillä $[M, M + M^{3/5}]$. Parempiakin arvioita on mahdollista saada. Osoitetaan nyt seuraava väite todeksi:

Lause 90. *Välillä* $[M, M + 2\sqrt{46}M^{1/4} + 24]$ *Ramanujanin* τ*-funktiolla on vähintään yksi nollasta poikkeava arvo.*

Tätä ennen tarvitsemme kuitenkin seuraavan lauseen sekä muutaman lemman.

Lause 91. *Olkoon* p *alkuluku. Jos* p *on neliönepäjäännös modulo* 23*, niin* $\tau(p) \equiv 0 \pmod{23}$*. Jos taas* p *on neliönjäännös, niin jos* p *voidaan esittää muodossa* $p = a^2 + 23b^2$*, niin* $\tau(p) \equiv 2 \pmod{23}$*, ja jos lukua* p *ei tässä muodossa voida esittää, niin* $\tau(p) \equiv -1 \pmod{23}$*.*

Todistus. Kirjoitetaan

$$\phi(x) = (1-x)\left(1-x^2\right)\left(1-x^3\right)\cdots.$$

Nyt

$$\phi(x) = 1 + \sum_{n=1}^{\infty}(-1)^n\left(x^{n(3n-1)/2} + x^{n(3n+1)/2}\right),$$

ja lisäksi $\Delta(x) = x\phi(x)^{24} \equiv x\phi(x)\phi\left(x^{23}\right)$, missä $\Delta(x)$ on diskriminanttifunktio. Voidaan lisäksi kirjoittaa

$$x\phi(x)\phi\left(x^{23}\right) = x\left(\sum_{m=0}^{\infty}a_m x^m\right)\left(\sum_{m=0}^{\infty}a_m x^{23m}\right) = \sum_{n=1}^{\infty}c_n x^n,$$

joten $\tau(n) \equiv c_n \pmod{23}$. Tässä siis $a_n = (-1)^m$, jos $n = \frac{1}{2}m(3m \pm 1)$, ja muulloin $a_0 = 0$. Voidaan lisäksi kirjoittaa

$$c_n = a_{n-1} + a_1 a_{n-24} + a_2 a_{n-47} + \cdots + a_h a_{n-1-23h},$$

missä $h = \left\lfloor \frac{n-1}{23} \right\rfloor$. Kirjoitetaan nyt $n = 23k + \ell$. Nyt $a_{n-1} = 0$, paitsi jos

$$23k + \ell - 1 = \frac{1}{2}m\left(3m \pm 1\right),$$

eli $36m^2 \pm 12m = 552k + 24\ell - 24$, eli $(6m \pm 1)^2 \equiv \ell \equiv n \pmod{23}$, eli $c_n = 0$, jos n on neliön epäjäännösmodulo 23 (sillä tämä sama päättely voidaan toistaa kaikille kertoimille $a_{n-1-23t}$, eli ne kaikki häviävät. Ensimmäinen osa väitettä on nyt siis todistettu.

Voimme nyt siis olettaa, että p on neliönjäännös modulossa 23. Tällöin

$$c_p = \sum a_{m(3m\pm1)/2} a_{p-1-23/2(3m\pm1)} = \sum (-1)^{m+n},$$

missä summaus tapahtuu niiden lukujen m ja n arvojen yli, joilla

$$p - 1 - \frac{23}{2} m\,(3m \pm 1) = \frac{1}{2} n\,(3n \pm 1)\,,$$

eli $(6n \pm 1)^2 + 23\,(6m \pm 1)^2 = 24p$, jolloin luvun c_p arvo riippuu niistä luvuista u ja v, jotka toteuttavat Diofantoksen yhtälön $u^2 + 23v^2 = 24p$. Kirjoitetaan $\omega = \sqrt{-23}$. Nyt p hajoaa renkaassa $K(\omega)$ kahdeksi alkuideaaliksi

$$\pi, \pi' = \left(p, \frac{2r + 23 \pm \omega}{2}\right),$$

missä r on kongruenssin $(2r + 23)^2 \equiv -23 \pmod{4p}$ ratkaisu. Renkaassa $K(\omega)$ on kolme luokkaa ideaaleja: pääideaali, ja kaksi muuta, jotka voidaan tyypittää luvun 2 tekijöinä:

$$\pi_2 = \left(2, \frac{1}{2} + \frac{\omega}{2}\right), \quad \pi_2' = \left(2, \frac{1}{2} - \frac{1}{2}\omega\right).$$

Tarvitaan lisäksi luvun 3 tekijöitä, eli ideaaleja

$$\pi_3 = \left(3, \frac{1}{2} - \frac{\omega}{2}\right), \quad \pi_3' = \left(3, \frac{1}{2} + \frac{1}{2}\omega\right).$$

Tässä merkinnät on valittu niin, että π_2 ja π_3 kuuluvat samaan luokkaa ideaaleja, $\pi_2 \sim \pi_3$. Nyt ideaaleilla π ja π' on kaksi vaihtoehtoa: joko ne molemmat ovat pääideaaleja tai sitten ne eivät ole pääideaaleja kuuluen eri ideaaliluokkiin.

Tarkastellaan aluksi tilannetta, joss π on pääideaali, eli $\pi = \left(\frac{1}{2}a + \frac{1}{2}b\omega\right)$, missä $a - b$ on parillinen. Nyt $4p = \pi\pi' = a^2 + 23b^2$, elin $a^2 - b^2 = 4(p - 6b^2)$, eli lukujen a ja b pitää molempien olla parillisia, sillä jos ne olisivat parittomia, olisi vasen puoik jaollinen kahdeksalla. Täten $p = h^2 + 23k^2$, ja koska jako alkuideaaleiksi on yksikäsitteinen, on tällä vain yksi ratkaisu positiivisten kokonaislukujen joukossa. Tässä tapauksessa siis

$$24p = (1 + \omega)(1 - \omega)(h + k\omega)(h - k\omega),$$

ja tarkastelemallamme yhtälöllä $24p = u^2 + 23v^2$ on kaksi ratkaisua

$$u = h + 23k,\ v = |h - k| \quad \text{sekä} \quad u = |h - 23k|,\ v = h + k.$$

Molemmissa tapauksissa yksi kahdesta kongruenssista

$$u + v \equiv 0 \pmod{24} \quad \text{ja} \quad u - v \equiv 0 \pmod{24}$$

pätee, joten sekä u että v ovat joko molemmat parillisia tai parittomia, joten $c_p = 2$. Tämäkin tapaus on nyt saatu päätökseen.

On vielä käsiteltävä se tilanne, joss π ja π' eivät ole pääideaaleja. Voimme valita ratkaisut r niin, että $\pi_2 \sim \pi_3 \sim \pi$ ja $\pi_2' \sim \pi_3' \sim \pi'$, josta seuraa, että $\pi_2'\pi$, $\pi_3'\pi$ ja $\pi_2\pi_3\pi$ ovat pääidealeja, eli $8p$, $12p$ ja $24p$ on esitettävissä muodossa $u^2 + 23v^2$ vain yhdellä tavalla. Mielenkiintoinen tapaus on

$$\pi_2\pi_3\pi = \left(\frac{3+3\omega}{2}, 1-\omega\right)\left(p, \frac{2r+23+\omega}{2}\right) = \left(\frac{u+vomega}{2}\right),$$

missä u ja v toteuttavat yhtälön $24p = u^2+23v^2$. Tästä seuraa, että on plemassa kokonaisluvut h, h', k ja k', joilla

$$\frac{3p+3p\omega}{2} = \frac{h+k\omega}{2} \cdot \frac{u+v\omega}{2}$$

ja

$$p - p\omega = \frac{h'-k'\omega}{2} \cdot \frac{u+v\omega}{2},$$

ja täten, käyttäen yhtälöä $24p = u^2 + 23v^2$ saadaan

$$(u - v\omega)(1+\omega) = 4(h+k\omega)$$

ja

$$(u - v\omega)(1-\omega) = 6(h'-k'\omega),$$

mistä seuraa, että $u - v = 4k$ ja $u + k = 6k'$, ja koska $u^2 - v^2 = 24(p - v^2)$, saadaan joko

$$u = 6n+1, \quad v = 6m-1$$

tai

$$u = 6n-1, \quad 6m+1.$$

Täten $m+n$ on pariton, ja $c_p = -1$. □

Lemma 92. *Mikäli $\tau(p) = 0$, kun p on alkuluku, niin $\tau\left(p^k\right) = 0$, kun k on pariton ja $\tau\left(p^k\right) = (-1)^{k/2}p^{11k/2}$, kun k parillinen.*

Todistus. Todistetaan väite induktiolla. Selvästi

$$\tau\left(p^2\right) = \tau(p)^2 - p^{11}\tau(1) = -p^{11}.$$

Voimme nyt olettaa väitteen olevan todistettu, kun $k \leq m$. Nyt

$$\tau\left(p^{m+1}\right) = \tau(p)\tau\left(p^m\right) - p^{11}\tau\left(p^{m-1}\right) = -p^{11}\tau\left(p^{m-1}\right),$$

mikä todistaa väitteen. □

Lemma 93. *Olkoon $\tau(p) \neq 0$, ja olkoon $p^\ell \mid\mid \tau(p)$. Tällöin*

$$p^{\ell m} \mid\mid \tau\left(p^m\right).$$

Todistus. Todistetaan väite induktiolla. Oletetaan, että väite pätee, kun $m \leq n$. Nyt

$$\tau\left(p^{n+1}\right) = \tau(p)\tau\left(p^n\right) - p^{11}\tau\left(p^{n-1}\right).$$

Tarkastellaan yhtälön oikean puolen jaollisuutta luvulla p. Ilmeisesti

$$p^{n+1} \mid\mid \tau(p)\tau\left(p^n\right)$$

sekä

$$p^{11+(n-1)\ell} \mid\mid p^{11}\tau\left(p^{(n-1)}\right).$$

Delignen arvion nojalla $0 \leq \ell \leq 5$. Täten

$$(n+1)\ell < 11 + (n-1)\ell.$$

Täten

$$p^{(n+1)\ell} \mid\mid \tau\left(p^{\ell}\right),$$

ja lemma on todistettu. □

Lemma 94. *Kun $a, b \in \mathbb{Z}$, niin*

$$\tau(a^2 + 23b^2) \neq 0.$$

Todistus. Kirjoitetaan aluksi luvun $a^2 + 23b^2$ alkutekijähajotelma:

$$a^2 + 23b^2 = \prod_{j=1}^{s} p_j^{k_j},$$

jolloin

$$\tau(a^2 + 23b^2) = \prod_{j=1}^{s} \tau\left(p_j^{k_j}\right).$$

Osoitetaan seuraavaksi, että tulontekijät ovat nollasta poikkeavia. Edellisestä lemmasta seuraa, että mikäli $\tau(p_j) \neq 0$, niin myös $\tau\left(p_j^{k_j}\right) \neq 0$. Riittää siis keskittyä tilanteeseen, jossa $\tau(p_j) = 0$ jollakin j. Mikäli k_j on parillinen, on $\tau\left(p_j^{k_j}\right)$ nollasta poikkeava. Siispä riittää tarkastella parittomia eksponentteja. Ramanujanin ja Wiltonin lauseen mukaan $\tau(p) \equiv 0 \pmod{23}$ vain, jos $\left(\frac{p}{23}\right) = -1$. Siispä p_j ei ole neliönjäännös modulossa 23. Resiprookkilain mukaan

$$\left(\frac{p}{23}\right)\left(\frac{23}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{23-1}{2}},$$

joten $\left(\frac{23}{p}\right) = (-1)^{(p-1)/2}\left(\frac{p}{23}\right)$, eli $\left(\frac{-23}{p}\right) = \left(\frac{-1}{p}\right)(-1)^{(p-1)/2}\left(\frac{p}{23}\right) = \left(\frac{p}{23}\right) = -1$. Siispä -23 ei ole neliönjäännös modulossa p. Kuitenkin $p \mid \left(a^2 + 23b^2\right)$, eli $-23 \equiv \frac{a^2}{b^2} \pmod{23}$, mikä on ristiriita. □

Vihdoinkin voimme siirtyä varsinaisen lauseen todistukseen.

Todistus. Olkoon kokonaisluku n annettu. Tavoitteemme on löytää toinen kokonaisluku, joka on suurempi kuin n, mutta mahdollisimman lähellä lukua n sekä muotoa a^2+23b^2. Kirjoitetaan $a = \lfloor\sqrt{n}\rfloor$. Asetetaan lisäksi $h = n - a^2$. Selvästi $(a+1)^2 > n$, ja $h \leq 2a \leq 2\sqrt{n}$. Asetetaan $b = \left\lfloor\sqrt{\frac{h}{23}}\right\rfloor + 1$, jolloin $23b^2 > h$, ja $a^2 + 23b^2 > n$. Lisäksi

$$23b^2 \leq 23\left(\sqrt{\frac{h}{23}} + 1\right)^2 = h + 2\sqrt{23h} + 23.$$

Tästä seuraa, että $a^2+23b^2 \leq n+2\sqrt{23h}+23 \leq n+2\sqrt{46}n^{1/4}+23$, mikä todistaa väitteen. □

Luku 8

Rankinin arvio Fourier-kertoimien itseisarvojen summille

Tässä luvussa varsinainen tavoitteemme on todistaa arvio

$$x(\log x)^{-\delta_1} \ll \sum_{n\leq x} |b(n)| \ll x(\log x)^{-\delta_2},$$

kun $b(n)$ ovat normeeratut Fourier-kertoimet. Lisäksi määritämme kelvolliset arvot vakioille δ_1 ja δ_2. Todistamme itse asiassa hieman yleisemmän väitteen, eli seuraavan lauseen:

Lause 95. *Olkoon* $F(\beta) = \frac{2^{\beta-1}}{5}\left(2^\beta + 3^{2-\beta}\right) - 1$ *ja* $G(\beta) = 2^{\beta-1} - 1$, *kun* $\beta \geq 0$. *Nyt*

$$x\left(\log x\right)^{G(\beta)} \ll \sum_{n\leq x} |b(n)|^{2\beta} \ll x\left(\log x\right)^{F(\beta)}, \textit{kun}$$

$0 \leq \beta \leq 1$.

Tämän todistaminen vaatii melkoisen kasan lemmoja (mikä ei varmastikaan kenellekään tule yllätyksenä). Kiinnitetään ensin hieman notaatiota. Kirjoitetaan

$$B_\beta(s) = \sum_{n=1}^{\infty} |b(n)|^{2\beta} n^{-s},$$

kun $\beta \geq 0$. Sarja suppenee itseisesti, kun $\sigma = \Re s > 1$. Kirjoitetaan

$$b(p) = 2\cos\theta_p,$$

missä $0 \leq \theta_p \leq \pi$ kaikille alkuluvuile p ja kirjoitetaan kaikille kokonaisluvuille r

$$\psi_r(s) = \prod_p \left(1 - 2p^{-s}\cos r\theta_p + p^{-2s}\right)^{-1}.$$

Nyt pääsemme lemmoihin. Aloitetaan lemmalla, jonka todistus sivuutetaan:

Lemma 96. *Kun* $\sigma > 1$, *voidaan kirjoittaa*

$$A_1(s) = \zeta^2(s)\psi_2(s)H_1(s)$$

ja

$$A_2(s) = \zeta^6(s)\psi_2^4(s)\psi_4(s)H_2(s),$$

missä $\zeta(s)\psi_2(s)$, $\psi_4(s)$, $H_1(s)$ ja $H_2(s)$ ovat itseisesti suppenevia, kun $\sigma > 1$ ja holomorfisia funktioita, kun $\sigma \geq 1$. Lisäksi funktioilla $\zeta(s)\psi_2(s)$ ja $\psi_4(s)$ ei ole nollakohtia, kun $\sigma \geq 1$

Todistus. Sivuutetaan. □

Kirjoitetaan nyt $f_\beta(x) = f_\beta(x; b, c) = x^\beta - bx - cx^2$, kun $\beta > 0$, $0/leqx \leq 1$ ja b ja c ovat reaalisia. (Näille tullaan valitsemaan sopivat arvot myöhemmin. Selvästi f_β on jatkuva välillä $[0, \infty[$ ja derivoituva välillä $]0, \infty[$.

Lemma 97. *Mikäli joillekin arvoille a, b, c ja $\beta > 0$ pätee*

$$f_\beta(x; b, c) \leq a$$

kaikilla $x \in [0, 1]$, niin silloin kaikille $\theta \in [0, \pi]$ pätee

$$|2\cos\theta|^{2\beta} \leq 2^{2\beta-3}\left(8a + 4b + 3c + 4(b + c)\cos 2\theta + c\cos 4\theta\right).$$

Toisaalta, jos $f_\beta(x; b, c) \geq a$ kaikilla $x \in [0, 1]$, niin silloin kaikille $\theta \in [0, \pi]$ pätee

$$|2\cos\theta|^{2\beta} \geq 2^{2\beta-3}\left(8a + 4b + 3c + 4(b + c)\cos 2\theta + c\cos 4\theta\right).$$

Todistus. Nämä arviot saadaan, kun kirjoitetaan $x = \cos^2\theta$, ja huomataan, että

$$8\left(a + bx + cx^2\right)^2 = 8\left(a + b\cos^2\theta + c\cos 4\theta\right)^2 = 8a + 4b + 3c + 4(b + c)\cos 2\theta + c\cos 4\theta.$$

□

Voimme jatkaa funktion f_β tarkastelua.

Lemma 98. *Mikäli funktio f_β on sellainen, että*

$$f'_\beta\left(\frac{1}{6}; b, c\right) = 0 \quad ja \quad f_\beta\left(\frac{1}{6}; b, c\right) = f_\beta(1; b, c),$$

niin silloin

$$b = b_1 := \frac{(35\beta + 2)6^{1-\beta} - 12}{25}$$

ja

$$c = c_1 := \frac{36 - (5\beta + 1)6^{2-\beta}}{25}$$

Todistus. Väite seuraa suoraan kirjoittamalla ehdot auki ja manipuloimalla lausekkeita. □

Samoin voidaan myös todistaa seuraava lemma:

Lemma 99. *Mikäli funktio f_β toteuttaa ehdot*

$$f'_\beta\left(\frac{1}{2}; b, c\right) = f_\beta\left(\frac{1}{2}; b, c\right) = 0,$$

niin $b = b_2 := (2 - \beta)2^{1-\beta}$ ja $c = c_2 := (\beta - 1)2^{2-\beta}$, ja $2b_2 + c_2 = 2^{2-\beta}$.

Kirjoitetaan nyt $g_\beta(x) = f_\beta(x; b_1, c_1)$ ja $h_\beta(x) = f_\beta(x; b_2, c_2)$. Ja voimmekin nyt muotoilla lemman näiden suuruudelle.

Lemma 100. *Kun* $0 \le x \le 1$*, niin*

$$g_\beta(x) \le g_\beta(1) \quad ja \quad h_\beta(x) \ge 0,$$

kun $0 \le \beta \le 1$.

Todistus. Huomataan, että

$$f''_\beta(x; b, c) = \beta(\beta - 1)x^{\beta-2} - 2c.$$

täten funktiolla f''_β on korkeintaan yksi nollakohta, kun $x > 0$, ja siispä funktiolla f'_β on korkeintaan kaksi nollakohtaa, kun $x > 0$. Koska $g_\beta\left(\frac{1}{6}\right) = g_\beta(1)$, niin $g'_\beta(x') = 0$ jollekin yksikäsitteiselle $\frac{1}{6} < x' < 1$, ja $\frac{1}{6}$ ja x' ovat funktion g'_β ainoat nollakohdat välillä $]0, 1[$. Vastaavasti voidaan myös todeta, että $\frac{1}{2}$ ja jokin y' välillä $\left]0, \frac{1}{2}\right[$ ovat funktion h'_β ainoat nollakohdat välillä $]0, 1[$. Nyt

$$g''_\beta\left(\frac{1}{6}\right) = \frac{36}{25}\left(6^{-\beta}(5\beta - 1)(5\beta - 2) - 2\right) = D(\beta),$$

ja nyt $D(0) = D(1) = 0$ ja $D(\beta) < 0$ for $\beta \in]0, 1[$. Täten g_β saavuttaa maksiminsa pisteissä $\frac{1}{6}$ ja 1, ja funktiolla g_β on lokaali minimi pisteessä x'. Vastaavasti

$$h''_\beta\left(\frac{1}{2}\right) = (\beta - 1)(\beta - 2)2^{2-\beta},$$

ja tämä on positiivinen, kun $\beta \in]0, 1[$. Täten h_β saavuttaa miniminsä välillä $[0, 1]$ pisteissä 0 ja $\frac{1}{2}$, kun $\beta \in]0, 1[$. Pisteessä y' funktiolla h_β on lokaali maksimi. Jatkuvuuden nojalla lemma pätee myös reunapisteissä 0 ja 1. □

Aikaisempien lemmojen avulla olemme johtaneet seuraavan tuloksen:

Lemma 101. *Jos* $0 \le \beta \le 1$*, niin*

$$2^{2\beta-3}\left(4b_2 + 3c_2 + 4(b_2 + c_2)\cos 2\theta + c_2 \cos 4\theta\right) \le |2\cos\theta|^{2\beta} \le 2^{2\beta-3}\left(8 - 4b_1 - 5c_1 + 4(b_1 + c_1)\cos 2\theta + c_1 \cos 4\theta\right).$$

Pääsemme vihdoin varsinaisen lauseen todistukseen.

Todistus. Kirjoitetaan

$$A_\beta(s) = \prod_p A_\beta(s, p),$$

missä

$$A_\beta(s, p) = 1 + |2\cos\theta_p|^{2\beta} p^{-s} + \sum_{\nu=2}^{\infty} \left|\frac{\sin(\nu + 1)\theta_p}{\sin\theta_p}\right|^{2\beta} p^{\nu s}.$$

Majoroidaan tätä summalla

$$A^+(s, p) = 1 + u^+(\theta_p)p^{-s} + \sum_{\nu=2}^{\infty}(\nu + 1)^{2\beta} p^{-\nu s},$$

ja minoroidaan summalla

$$A^-(s,p) = 1 + u^-(\theta_p)p^{-s},$$

missä $u^+(\theta)$ ja $u^-(\theta)$ ovat edellisen lemman antamat ylä- ja alarajat funktiolle $|2\cos\theta|^{2\beta}$ (nämä luonnollisestikin riippuvat luvusta β). Kirjoitetaan nyt

$$A_\beta^+(s) = \prod_p A_\beta^+(s,p) = \sum_{n=1}^{\infty} a^+(n)n^{-s}$$

ja vastaavasti funktiolle A_β^-. Nämä sarjat ovat selvästi itseisesti suppenevia, kun $\sigma > 1$. Kirjoitetaan yksinkertaisuuden vuoksi

$$u^+(\theta) = K + 2L\cos 2\theta + 2M\cos 4\theta$$

ja

$$u^- = k + 2k\ell\cos 2\theta + 2m\cos 4\theta.$$

Nyt funktiot A_β^+ ja A_β^{-1} voidaan kirjoittaa tuloina

$$A_\beta^+ = \zeta^K \psi_2^L \psi_4^M H_3$$

ja

$$A_\beta^- = \zeta^k \psi_2^\ell \psi_4^m H_4,$$

missä H_3 ja H_4 ovat itseisesti suppenevia, kun $\sigma > 1$ ja holomorfisia, kun $\sigma \geq 1$. Funktiot A_β^+ ja A_β^- ovat holomorfisia, kun $\sigma \geq 1$ lukuunottamatta singulariteettejä pisteessä $s = 1$. Tässä pisteessä funktiot käyttäytyvät kuin funktioiden $(s-1)^{L+K}$ ja $(s-1)^{\ell+k}$ vakiomonikerrat. Delangen ja Ikeharan lauseen mukaan pätee

$$\sum_{n\leq x} a^+(n) \sim C^+ x\,(\log x)^{K-L-1}$$

ja

$$\sum_{n\leq x} a^- \sim C^- x\,(\log x)^{k-\ell-1},$$

missä C^+ ja C^- ovat positiivisia vakioita. Kun $0 \leq \beta \leq 1$, pätee

$$K - L = 2^{2\beta-3}(8 - 6b_1 - 7c_1) = F(\beta) + 1$$

ja

$$k - \ell = 2^{2\beta-3}(2b_2 + c_2) = G(\beta) + 1,$$

ja väite seuraakin tästä, sillä

$$\sum_{n\leq x} a^-(n) \leq S(x, 2\beta) \leq \sum_{n\leq x} a^+(n).$$

□