Tampereen yliopisto

Auli Toikkonen

Aritmeettiset funktiot: kuuluisia matemaatikkoja ja keskeisiä käsitteitä

Informaatioteknologian ja viestinnän tiedekunta
Pro gradu -tutkielma
Heinäkuu 2021

Tiivistelmä

Auli Toikkonen: Aritmeettiset funktiot: kuuluisia matemaatikkoja ja keskeisiä käsitteitä
Pro gradu -tutkielma
Tampereen yliopisto
Matematiikan ja tilastotieteen tutkinto-ohjelma
Heinäkuu 2021

Tämän tutkielman aiheena ovat aritmeettiset funktiot. Aritmeettiset funktiot ovat kuvauksia, jotka määritellään positiivisille kokonaisluvuille ja jotka saavat arvoksi kompleksilukuja. Työssä tutustutaan aritmeettisten funktioiden keskeisiin käsitteisiin ja kuuluisiin matemaatikoihin. Aluksi määritellään Dirichlet'n tulo ja multiplikatiivinen funktio. Sen jälkeen esitetään Möbiuksen ja Eulerin funktiot, jotka ovat multiplikatiivisia. Seuraavaksi käsitellään täydellisesti multiplikatiivisia funktioita, joista esimerkkinä on Liouvillen funktio. Tämän jälkeen siirrytään modulaariseen aritmetiikkaan sekä määritellään täydellisen ja supistetun jäännössysteemin käsitteet. Lisäksi esitetään Ramanujanin summakaava. Sen jälkeen osoitetaan tekijäfunktioiden ominaisuuksia ja määritellään täydelliset luvut, Mersennen alkuluvut ja Fermat'n luvut. Lopuksi todistetaan tekijäfunktion keskiarvon kaava. Matemaattisen käsittelyn ohella tutkielmassa tarkastellaan myös teorioiden ja niiden keksijöiden historiaa.

Avainsanat: Dirichlet'n tulo, multiplikatiivinen funktio, Möbiuksen funktio, Eulerin funktio, Liouvillen funktio, täydellinen jäännössysteemi, Ramanujanin summa, tekijäfunktio, Mersennen alkuluku, täydellinen luku, Fermat'n luvut.

Sisällys

1 Johdanto **4**

2 Aritmeettisten funktioiden peruskäsitteitä **5**

2.1 Peter Gustav Lejeune Dirichlet 5

2.2 Dirichlet'n tulo 6

2.3 Multiplikatiiviset funktiot 8

2.4 August Ferdinand Möbius 11

2.5 Möbiuksen funktio 11

2.6 Leonhard Euler 14

2.7 Eulerin funktio 15

2.8 Täydellisesti multiplikatiiviset funktiot 18

2.9 Joseph Liouville 21

2.10 Liouvillen funktio 21

3 Modulaarinen aritmetiikka ja Ramanujanin summa **23**

3.1 Karl Friedrich Gauss 23

3.2 Täydellinen ja supistettu jäännössysteemi 24

3.3 Srinivasa Ramanujan 30

3.4 Ramanujanin summa 31

4 Tekijäfunktioiden ominaisuuksia **36**

4.1 Tekijäfunktio 36

4.2 Marin Mersenne 38

4.3 Mersennen alkuluku ja täydellinen luku 38

4.4 Pierre de Fermat 40

4.5 Fermat'n luvut 41

4.6 Tekijäfunktion keskiarvo 43

Lähteet **53**

1 Johdanto

Tässä tutkielmassa käsitellään lukuteorian alaan kuuluvia aritmeettisia funktiota. Aritmeettiset funktiot ovat kuvauksia, jotka määritellään positiivisille kokonaisluvuille ja jotka saavat arvoksi kompleksilukuja. Matemaattisen tarkastelun lisäksi tässä työssä syvennytään monen eri merkittävän matemaatikon historiaan ja heidän vaikutuksiinsa matematiikan ja erityisesti lukuteorian kehitykselle.

Luvussa 2 tutustutaan ensin matemaatikko Peter Gustav Lejeune Dirichlet'n saavutuksiin, määritellään Dirichlet'n tulo ja esitetään sen ominaisuuksia. Tämän jälkeen esitellään multiplikatiiviset funktiot ja osoitetaan Dirichlet'n tulon säilyttävän multiplikatiivisuuden. Sen jälkeen keskitytään August Ferdinand Möbiuksen historiaan, määritellään Möbiuksen funktio ja todistetaan Möbiuksen käänteiskaava. Sitten perehdytään Leonhard Eulerin elämän vaiheisiin ja tieteellisiin tuotoksiin sekä määritellään Eulerin funktio. Viimeisenä esitetään täydellisesti multiplikatiiviset funktiot, joista esimerkkinä on Joseph Liouvillen mukaan nimetty Liouvillen funktio.

Luvussa 3 käsitellään modulaarista aritmetiikkaa. Luvun alussa tarkastellaan kongruenssin kehittäjän Karl Friedrich Gaussin historiaa, jonka jälkeen todistetaan kongruenssiin liittyviä perustuloksia sekä määritellään täydellisen ja supistetun jäännössysteemin käsitteet. Tämän jälkeen perehdytään Srinivasa Ramanujaniin ja hänen kehittämäänsä summakaavaan.

Tutkielman viimeisessä luvussa käsitellään tekijäfunktioiden ominaisuuksia. Lukuun sisältyvät Marin Mersennen ja Pierre de Fermat'n historiaosuudet. Lisäksi määritellään Mersennen alkuluvut, täydelliset luvut ja Fermat'n luvut. Lopuksi syvennytään tekijäfunktion keskiarvon kaavan todistamiseen ja siihen läheisesti liittyvän Dirichlet'n tekijäprobleeman historiaan.

Lukijalta edellytetään lukuteorian perustuloksien hallintaa esimerkiksi yliopiston algebran kurssien pohjalta. Tässä tutkielmassa on pääosin käytetty lähdeteoksina A. Gioian kirjaa *The Theory of Numbers*, K. Rosenin teosta *Elementary Number Theory* ja T. Apostolin kirjaa *Introduction to Analytic Number Theory*.

2 Aritmeettisten funktioiden peruskäsitteitä

2.1 Peter Gustav Lejeune Dirichlet

Saksalainen Peter Gustav Lejeune Dirichlet (1805–1859) oli yksi 1800–luvun suurimmista lukuteoreetikoista. Dirichlet oli nuoresta pitäen kiinnostunut matematiikasta, joten hän suuntasi Pariisin yliopistoon opiskelemaan alaa. Pariisissa häntä opettivat esimerkiksi Jean-Baptiste Fourier, Jean Hachette, Pierre-Simon Laplace ja Siméon Poisson, jotka olivat aikansa tunnettuja tieteenharjoittajia. Dirichlet opiskeli myös itsenäisesti Carl Gaussin oppeja ja kuljetti aina mukanaan Gaussin teosta *Disquisitiones arithmeticae* (suomeksi Aritmeettisia tutkimuksia). [10, s. 237]

Ensimmäisessä tieteellisessä julkaisussaan Dirichlet todisti osan Fermat'n suuresta lauseesta, kun $n = 5$. Lauseessa esitetään, että yhtälöllä $x^n + y^n = z^n$ ei ole olemassa kokonaislukuratkaisuja x, y ja z, kun kokonaisluku $n > 2$. Ennestään Leonhard Euler ja Pierre de Fermat olivat todistaneet tapaukset, kun $n = 3$ ja $n = 4$. Tapaus $n = 5$ koostui kahdesta todistusosuudesta, joista Dirichlet onnistui ratkaisemaan toisen osuuden. Dirichlet'n julkaisun pohjalta Adrien-Marie Legendre jatkoi todistustyön loppuun ja koko ratkaisu julkaistiin vuonna 1825. Myöhemmin Dirichlet ratkaisi kyseisen yhtälön myös, kun $n = 14$. [10, s. 237–238]

Dirichlet kirjoitti habilitaatiotutkielmansa polynomien jaottomuudesta, aloitti opettamaan Breslaun yliopistossa ja jatkoi edelleen opettajauraansa Berliinissä sijaitsevassa sotakorkeakoulussa. Vuonna 1828 Dirichlet sai professorin viran Berliinin yliopistosta, joka oli yksi aikansa arvostetuimmista instituutioista. Gaussin menehdyttyä vuonna 1855 Dirichlet vastaanotti Gaussin kunnianarvoisen paikan Göttingenin yliopistossa Saksassa. Göttingenissä Dirichlet'n oppilaana oli muun muassa Bernhard Riemann. Dirichlet'n kuoltua Riemannista tuli hänen seuraajansa myötävaikuttaen funktioteoriaan, Fourier'n sarjoihin ja geometriaan. [10, s. 238–239]

Dirichlet'n vaikutus matematiikkaan on ollut valtava, erityisesti analyyttisen lukuteorian osalta. Fermat'n suuren lauseen lisäksi Dirichlet keskittyi tutkimuksissaan esimerkiksi neliöjäännöslauseeseen ja alkulukujen perustuloksiin aritmetiikassa. Hän loi analyyttisesta lukuteoriasta tutun Dirichlet'n sarjan, antoi oman tarkan määritelmän funktiolle, määritteli ensimmäisenä sarjojen suppenemisen ja loi pohjaa Fourier'n sarjalle ja monille muillekin teorioille. [10, s. 238–239]

2.2 Dirichlet'n tulo

Tässä alaluvussa keskitytään Dirichlet'n tuloon ja tutustutaan Dirichlet'n tulon perusominaisuuksiin.

Määritelmä 2.1. (Vrt. [9, s. 13]). *Aritmeettinen funktio* on kuvaus $f : \mathbb{Z}^+ \to \mathbb{C}$, eli se on määritelty positiivisille kokonaisluvuille ja se saa arvoksi kompleksilukuja.

Määritelmä 2.2 (Dirichlet'n tulo)**.** (Ks. [9, s. 13]). Aritmeettisten funktioiden f ja g *Dirichlet'n tulo* (eli *Dirichlet'n konvoluutio*) $f * g$ määritellään kaavalla

$$(f * g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big), \qquad d, n \in \mathbb{Z}^+.$$

Esimerkki 2.1. Lasketaan aritmeettiset funktioiden $f(n) = n$ ja $g(n) = n^2$ Dirichlet'n tulo, kun $n = 4$. Saadaan

$$\begin{aligned}(f * g)(4) = &\sum_{d|4} f(d)g\Big(\frac{4}{d}\Big)\\ =&f(1)g(4) + f(2)g(2) + f(4)g(1)\\ =&1 \cdot 16 + 2 \cdot 4 + 4 \cdot 1\\ =&28.\end{aligned}$$

Lause 2.1. *Dirichlet'n tulo on vaihdannainen ja liitännäinen. Toisin sanoen*

$$f * g = g * f \quad ja \quad (f * g) * h = f * (g * h)$$

kaikille aritmeettisille funktioille f, g ja h.

Todistus. (Ks. [1, s. 108]). Todistetaan ensin vaihdannaisuus. Olkoot f ja g aritmeettisia funktiota ja n positiivinen kokonaisluku. Silloin

$$(f * g)(n) = \sum_{d|n} f(d)g\Big(\frac{n}{d}\Big) = \sum_{c|n} f\Big(\frac{n}{c}\Big)g(c) = \sum_{c|n} g(c)f\Big(\frac{n}{c}\Big) = (g * f)(n),$$

sillä summassa luku $d = \frac{n}{c}$ käy läpi kaikki luvun n tekijät siten, että $n = dc$, samoin luku $c = \frac{n}{d}$. Siis $f * g = g * f$, mikä osoittaa vaihdannaisuuden.

Osoitetaan seuraavaksi liitännäisyys. Olkoot f, g ja h aritmeettisia funktiota. Tällöin huomataan, että

$$\begin{aligned}\big((f * g) * h\big)(n) &= \sum_{dc=n} (f * g)(d)h(c)\\ &= \sum_{dc=n} \Big(\sum_{ab=d} f(a)g(b)\Big)h(c)\\ &= \sum_{abc=n} f(a)g(b)h(c)\end{aligned}$$

ja

$$\begin{aligned}\big(f*(g*h)\big)(n) &= \sum_{ad=n} f(a)(g*h)(d)\\ &= \sum_{ad=n} f(a)\Big(\sum_{bc=d} g(b)h(c)\Big)\\ &= \sum_{abc=n} f(a)g(b)h(c).\end{aligned}$$

Siis $(f*g)*h = f*(g*h)$ eli Dirichlet'n tulo on liitännäinen. □

Lause 2.2. *Määritellään aritmeettinen funktio ε siten, että $\varepsilon(1) = 1$ ja $\varepsilon(n) = 0$, kun $n > 1$. Tällöin kaikille aritmeettisille funktioille f on voimassa*

$$f*\varepsilon = \varepsilon * f = f$$

eli funktio ε on neutraalialkio Dirichlet'n tulon suhteen.

Todistus. (Ks. [8, s. 164]). Olkoon f aritmeettinen funktio. Saadaan

$$(f*\varepsilon)(n) = \sum_{d|n} f(d)\varepsilon\Big(\frac{n}{d}\Big) = f(n)\varepsilon(1) = f(n)1 = f(n),$$

sillä $\varepsilon\big(\frac{n}{d}\big) = 0$, kun $d < n$. □

Lause 2.3. *Olkoon f aritmeettinen funktio. Jos $f(1) \neq 0$, niin on olemassa yksikäsitteinen aritmeettinen funktio g siten, että $f*g = \varepsilon$. Funktiota g sanotaan funktion f käänteisfunktioksi Dirichlet'n tulon suhteen ja sitä merkitään symbolilla f^{-1}.*

Todistus. (Ks. [1, s. 109]). Todistetaan induktiolla, että yhtälöllä $(f*g)(n) = \varepsilon(n)$ on yksikäsitteinen ratkaisu $g(1), g(2), \ldots, g(n)$ kaikilla $n \in \mathbb{Z}^+$.

1. Perusaskel. Osoitetaan, että väite on tosi, kun $n = 1$.

Saadaan $(f*g)(1) = f(1)g(1) = 1$ ja $g(1) = \frac{1}{f(1)}$, sillä $f(1) \neq 0$.

2. Induktioaskel. Olkoon $n > 1$ ja oletetaan, että funktion g arvot $g(1), \ldots, g(n-1)$ ovat yksikäsitteisesti määriteltyjä siten, että

$$(f*g)(n) = \varepsilon(n) \text{ kaikilla } n = 1, 2, \ldots, n-1.$$

Tällöin

$$(f*g)(n) = f(1)g(n) + \sum_{\substack{d|n\\ d>1}} f(d)g\Big(\frac{n}{d}\Big) = 0$$

ja edelleen

$$g(n) = -\frac{1}{f(1)} \sum_{\substack{d|n\\ d>1}} f(d)g\Big(\frac{n}{d}\Big), \qquad f(1) \neq 0.$$

Siis funktion g arvo luvulla n on yksikäsitteisesti määritelty.
3. Johtopäätös. Väite on tosi induktioperiaatteen nojalla ja lause on näin ollen todistettu. □

2.3 Multiplikatiiviset funktiot

Määritellään seuraavaksi multiplikatiivinen funktio ja todistetaan multiplikatiivisten funktioiden perusominaisuuksia. Lisäksi tässä alaluvussa osoitetaan, että Dirichlet'n tulo säilyttää multiplikatiivisuuden sekä Möbiuksen ja Eulerin funktiot ovat multiplikatiivisia.

1900-luvun alkupuolella multiplikatiivisia funktioita ovat erityisesti tutkineet matemaatikot Eric Temple Bell ja Ramaswamy Vaidyanathaswamy. Bell kirjoitti vuonna 1915 ensimmäisen merkittävän teoksen aritmeettisista funktioista. Washingtonin yliopiston julkaisemassa teoksessa *An arithmetical theory of certain numerical function* Bell esitti aritmeettisten funktioiden perustuloksia. Vuonna 1927 Vaidyanathaswamy julkaisi tutkimuksen *On the inversion of multiplicative arithmetic functions* lehdessä *Journal of the Indian Mathematical Society*. Kirjoituksessaan hän osoitti, että multiplikatiivisen funktion käänteisfunktio on multiplikatiivinen. Vaidyanathaswamy kirjoitti vuonna 1931 laajemman tutkimuksen *The theory of multiplicative arithmetic functions*, jossa hänen tuloksensa vastasivat läheisesti Bellin ideoita. [14, s. 579–580]

Määritelmä 2.3. (Vrt. [9, s. 18]). Aritmeettista funktiota f sanotaan *multiplikatiiviseksi*, jos funktio f ei ole nollafunktio ja $f(mn) = f(m)f(n)$ aina, kun $(m, n) = 1$.

Huomautus. Merkinnällä (m, n) tarkoitetaan lukujen m ja n suurinta yhteistä tekijää eli lukua $\text{syt}(m, n)$.

Huomautus. (Ks. [1, s. 105]). Jos aritmeettinen funktio f on multiplikatiivinen, niin $f(1) = 1$. Nimittäin jos $f(a) \neq 0$ $(a \in \mathbb{Z}^+)$, niin

$$f(a) = f(a \cdot 1) = f(a)f(1),$$

joten $f(1) = 1$.

Seuraavasta esimerkistä kuitenkin huomataan, että käänteinen implikaatio ei ole voimassa.

Esimerkki 2.2. ([9, s. 20], tehtävä 7-3.) Funktio $f(m) = 2m - 1$ ei ole multiplikatiivinen, vaikka $f(1) = 1$, sillä esimerkiksi $f(6) = 11 \neq f(2)f(3) = 15$.

Lause 2.4. *Jos funktiot f ja g ovat multiplikatiivisia, niin Dirichlet'n tulo $f * g$ on multiplikatiivinen.*

Todistus. (Ks. [1, s. 109]). Oletetaan, että funktiot f ja g ovat multiplikatiivisia. Olkoon $h = f * g$, ja oletetaan, että $(m, n) = 1$. Osoitetaan, että silloin

$$h(mn) = \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) = h(m)h(n).$$

Nyt $d|mn$ ja $(m, n) = 1$, joten luku d voidaan yksikäsitteisesti jakaa tekijöihinsä siten, että $d = ab$, missä $a|m$ ja $b|n$. Tällöin $(a, b) = 1$ ja $\left(\frac{m}{a}, \frac{n}{b}\right) = 1$. Täten

$$\begin{aligned}
h(mn) &= \sum_{d|mn} f(d)g\left(\frac{mn}{d}\right) \\
&= \sum_{a|m} \sum_{b|n} f(ab)g\left(\frac{mn}{ab}\right) \\
&= \sum_{a|m} \sum_{b|n} f(a)f(b)g\left(\frac{m}{a}\right)g\left(\frac{n}{b}\right) \\
&= \left(\sum_{a|m} f(a)g\left(\frac{m}{a}\right)\right)\left(\sum_{b|n} f(b)g\left(\frac{n}{b}\right)\right) \\
&= h(m)h(n).
\end{aligned}$$

Näin ollen Dirichlet'n tulo $f * g$ on multiplikatiivinen. □

Seuraus 2.1. *Jos funktio f on multiplikatiivinen ja*

$$g(n) = \sum_{d|n} f(d),$$

niin funktio g on multiplikatiivinen.

Todistus. (Ks. [1, s. 106]). Todistus suoritetaan vastaavalla tavalla kuin lauseen 2.4 todistus. □

Huomautus. Funktio g on funktion f *tekijäsummafunktio*.

Esimerkki 2.3. Olkoot f ja g multiplikatiivisia funktioita ja $h = f * g$. Tällöin

$$\begin{aligned}
h(10) =& (f * g)(10) \\
=& f(1)g(10) + f(2)g(5) + f(5)g(2) + f(10)g(1) \\
=& 1 \cdot g(10) + f(2)g(5) + f(5)g(2) + f(10) \cdot 1 \\
=& g(2)g(5) + f(2)g(5) + f(5)g(2) + f(2)f(5) \\
=& \big(g(2) + f(2)\big)g(5) + \big(g(2) + f(2)\big)f(5) \\
=& \big(g(2) + f(2)\big)\big(g(5) + f(5)\big) \\
=& (1 \cdot g(2) + f(2) \cdot 1)(1 \cdot g(5) + f(5) \cdot 1) \\
=& \big(f(1)g(2) + f(2)g(1)\big)\big(f(1)g(5) + f(5)g(1)\big) \\
=& h(2)h(5).
\end{aligned}$$

Lause 2.5. *Jos funktiot g ja $f * g$ on multiplikatiivisia, niin funktio f on multiplikatiivinen.*

Todistus. (Ks. [1, s. 110]). Olkoot funktiot g ja $f * g$ multiplikatiivisia. Tehdään vastaoletus, että funktio f ei ole multiplikatiivinen. Olkoon $h = f * g$. Vastaoletuksen nojalla funktio f ei ole multiplikatiivinen, joten on olemassa positiiviset kokonaisluvut m ja n siten, että $(m, n) = 1$, mutta $f(mn) \neq f(m)f(n)$. Valitaan luvut m ja n siten, että niiden tulo mn on mahdollisimman pieni.

Jos tulo $mn = 1$, niin tällöin $f(1) \neq f(1)f(1)$ eli $f(1) \neq 1$. Siis $h(1) = f(1)g(1) = f(1) \neq 1$ eli funktio h ei ole multiplikatiivinen ja päädytään ristiriitaan.

Jos tulo $mn > 1$, saadaan $f(ab) = f(a)f(b)$ kaikilla $ab < mn$ ja $(a, b) = 1$. Edelleen

$$\begin{aligned}
h(mn) =& \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(ab)g\Big(\frac{mn}{ab}\Big) + f(mn)g(1) \\
=& \sum_{\substack{a|m \\ b|n \\ ab<mn}} f(a)f(b)g\Big(\frac{m}{a}\Big)g\Big(\frac{n}{b}\Big) + f(mn) \\
=& h(m)h(n) - f(m)f(n) + f(mn).
\end{aligned}$$

Koska $f(mn) \neq f(m)f(n)$, niin $h(mn) \neq h(m)h(n)$. Siis funktio h ei ole multiplikatiivinen ja päädytään ristiriitaan. Siis funktio f on multiplikatiivinen. □

Lause 2.6. ([9, s. 20], tehtävä 7-1.) *Funktio ε on multiplikatiivinen.*

Todistus. Olkoon funktio f multiplikatiivinen funktio. (Multiplikatiivisia funktioita on olemassa: esimerkiksi funktio, joka on identtisesti 1.) Nyt lauseen 2.2 mukaan $f * \varepsilon = \varepsilon * f = f$. Näin ollen lauseen 2.5 nojalla funktio ε on multiplikatiivinen. □

Lause 2.7. *Jos funktio f on multiplikatiivinen, niin käänteisfunktio f^{-1} on multiplikatiivinen.*

Todistus. (Ks. [1, s. 110]). Tämä seuraa suoraan lauseesta 2.5, sillä $\varepsilon = f * f^{-1} = f^{-1} * f$, missä funktio ε on multiplikatiivinen. □

2.4 August Ferdinand Möbius

August Ferdinand Möbius (1790–1868) oli saksalainen matemaatikko ja tähtitieteilijä, joka erityisesti tunnetaan analyyttisen geometrian ja topologian tutkimuksistaan [15]. Möbius aloitti oikeustieteen opinnot Leipzigin yliopistossa vuonna 1809, mutta ensimmäisen opintovuoden jälkeen hän siirtyi opiskelemaan matematiikkaa, tähtitiedettä ja fysiikkaa. Vuonna 1813 hän matkusti jatko-opintoihin Göttingenin yliopistoon, jossa häntä opetti Carl Gauss antaen vankan taustan matematiikasta ja tähtitieteestä. Möbius kirjoitti väitöskirjansa tähtitieteen alalta vuonna 1815 ja sai tähtitieteen professorin viran Leipzigin yliopistosta vuonna 1816. [11, s. 186]

Möbiuksen matemaattiset julkaisut koskivat pääosin geometriaa. Hän käytti muun muassa homogeenisia koordinaatteja ja projektiivisia muunnoksia projektiivisessa geometriassa. Lisäksi hän käsitteli geometrisesti statiikkaa eli tasapaino-oppia mekaniikan alalta, joka tutkii esimerkiksi rakennuksiin ja siltoihin vaikuttavia voimia. [15]

Möbius oli edelläkävijä topologiassa. Hänen mukaansa on nimetty Möbiuksen nauha, joka saadaan aikaan kiertämällä nauhan toista päätä puoli kierrosta ennen nauhan päiden yhteen kiinnitystä. Tämän topologisen pinnan Möbius keksi vuonna 1858. [15]

2.5 Möbiuksen funktio

Möbiuksen mukaan on myös nimetty lukuteorian käsite Möbiuksen funktio, joka määritellään seuraavaksi. Lisäksi osoitetaan, että Möbiuksen funktio on multiplikatiivinen ja todistetaan Möbiuksen käänteiskaava.

Määritelmä 2.4. (Vrt. [1, s. 105]). *Möbiuksen funktio* μ on aritmeettinen funktio, joka määritellään seuraavasti:

$$\mu(n) = \begin{cases} 1, & \text{jos } n = 1, \\ (-1)^k, & \text{jos } n = p_1 \cdot p_2 \cdots p_k \text{ missä } p_1, p_2, \ldots, p_k \text{ ovat erisuuria alkuluja,} \\ 0, & \text{jos } p^2 | n \text{ jollakin alkuluvulla } p. \end{cases}$$

Esimerkki 2.4. Lasketaan Möbiuksen funktion arvot luvuille 26, 28 ja 30.
Jakamalla luvut alkulukutekijöihin saadaan
$\mu(26) = \mu(2 \cdot 13) = (-1)^2 = 1,$
$\mu(28) = \mu(2^2 \cdot 7) = 0$ ja
$\mu(30) = \mu(2 \cdot 3 \cdot 5) = (-1)^3 = -1.$

Lause 2.8. *Möbiuksen funktio* μ *on multiplikatiivinen.*

Todistus. (Ks. [1, s. 106]). Olkoot m ja n positiivisia kokonaislukuja siten, että $(m, n) = 1$. Jos $p^2|m$ tai $p^2|n$ jollakin alkuluvulla p, niin $p^2|mn$ ja edelleen $\mu(m) = \mu(mn) = 0 = \mu(m)\mu(n)$. Jos $m = p_1 \cdot p_2 \cdots p_k$ ja $n = q_1 \cdot q_2 \cdots q_h$, missä $p_1, p_2, \ldots, p_k$ ja $q_1, q_2, \ldots, q_h$ ovat erisuuria alkulukuja, niin $\mu(m) = (-1)^k$, $\mu(n) = (-1)^h$ ja $mn = p_1 \cdot p_2 \cdots p_k \cdot q_1 \cdot q_2 \cdots q_h$. Edelleen $\mu(mn) = (-1)^{k+h} = (-1)^k(-1)^h = \mu(m)\mu(n)$. Näin todistettiin, että Möbiuksen funktio μ on multiplikatiivinen. □

Lause 2.9. *Möbiuksen funktion tekijäsummafunktio on*

$$\sum_{d|n} \mu(d) = \begin{cases} 1, & \textit{jos } n = 1, \\ 0, & \textit{jos } n > 1, \end{cases} \qquad n \in \mathbb{Z}^+.$$

Todistus. (Vrt. [13, s. 272]). Merkitään $M(n) = \sum_{d|n} \mu(d)$. Oletetaan ensin, että $n = 1$. Silloin

$$M(1) = \sum_{d|1} \mu(d) = \mu(1) = 1.$$

Oletetaan sitten, että $n > 1$. Lauseen 2.8 nojalla Möbiuksen funktio μ on multiplikatiivinen. Edelleen seurauksen 2.1 nojalla Möbiuksen funktion tekijäsummafunktio $M(n)$ on multiplikatiivinen. Oletetaan, että $n = p^k$, missä p on alkuluku ja k on positiivinen kokonaisluku. Huomataan, että jos $k = 1$, niin $\mu(p) = -1$, ja jos $k \geq 2$, niin $\mu(p^k) = 0$. Siis

$$\begin{aligned} M(p^k) = \sum_{d|p^k} \mu(d) =& \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^k) \\ =& 1 + (-1) + 0 + \cdots + 0 = 0. \end{aligned}$$

Lopuksi oletetaan, että n on positiivinen kokonaisluku, jonka *kanoninen alkutekijähajotelma* on $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, missä $p_1, p_2, \ldots, p_k$ ovat erisuuria alkuluja, $\alpha_1, \alpha_2, \ldots, \alpha_k$ ovat positiivisia kokonaislukuja ja $p_1 < p_2 < \cdots < p_k$. Edelleen tekijäsummafunktio $M(n)$ on multiplikatiivinen, joten

$$M(n) = M(p_1^{\alpha_1}) M(p_2^{\alpha_2}) \cdots M(p_k^{\alpha_k}) = 0 \cdot 0 \cdots 0 = 0.$$

Näin ollen lause on todistettu. □

Määritelmä 2.5. (Vrt. [2, s. 31]). Määritellään *yksikköfunktio* u siten, että $u(n) = 1$ aina, kun $n \in \mathbb{Z}^+$.

Huomautus. (Vrt. [2, s. 31]). Lauseen 2.9 nojalla $\sum_{d|n} \mu(d) = \varepsilon(n)$. Siis $\mu * u = u * \mu = \varepsilon$, missä u ja μ ovat toistensa käänteisfunktioita Dirichlet'n tulon suhteen.

Huomautus. Yksikköfunktio u on multiplikatiivinen.

Lause 2.10 (Möbiuksen käänteiskaava)**.** *Olkoot f ja g aritmeettisia funktioita, ja olkoon $n \in \mathbb{Z}^+$. Tällöin*

$$g(n) = \sum_{d|n} f(d) \Leftrightarrow f(n) = \sum_{d|n} g(d) \mu\Big(\frac{n}{d}\Big).$$

Todistus. (Ks. [2, s. 32]). Yhtälö $g(n) = \sum_{d|n} f(d)$ voidaan kirjoittaa muodossa $g = f * u$, missä u on yksikköfunktio. Kertomalla yhtälö $g = f * u$ Möbiuksen funktiolla μ puolittain saadaan, että $g * \mu = (f * u) * \mu$. Dirichlet'n tulon liitännäisyyden ja edellisen huomautuksen nojalla $(f * u) * \mu = f * (u * \mu) = f * \varepsilon = f$. Siis $f = g * \mu$. Todistus suoritetaan toiseen suuntaan vastaavalla tavalla kertomalla yhtälöä $f = g * \mu$ yksikköfunktiolla u. □

Seuraus 2.2. *Jos funktio g on multiplikatiivinen ja*

$$g(n) = \sum_{d|n} f(d),$$

niin funktio f on multiplikatiivinen.

Todistus. (Ks. [9, s. 22]). Olkoon funktio g multiplikatiivinen. Kirjoitetaan $g = f * u$ ja kerrotaan yhtälö puolittain Möbiuksen funktiolla μ saaden $g * \mu = (f * u) * \mu = f * (u * \mu) = f * \varepsilon = f$. Nyt g ja μ ovat multiplikatiivisia, joten niiden Dirichlet'n tulo f on multiplikatiivinen. □

Huomautus. Seuraus 2.2 on seurauksen 2.1 tietynlainen käänteistulos.

2.6 Leonhard Euler

Sveitsiläinen Leonhard Euler (1707–1783) oli yksi kaikkien aikojen suurimmista ja tuotteliaimmista matemaatikoista. Elinaikanaan Euler julkaisi yli 500 kirjaa ja artikkelia sekä tuotti noin 800 sivua matemaattista tekstiä vuodessa. [5, s. 618, 620] Laplacea lainaten: ”Read Euler, read Euler, he is the master of us all” [6, s. 31]. Hän on myös merkittävästi myötävaikuttanut fysiikan alalla, erityisesti optiikassa, mekaniikassa, sähkössä ja magnetismissa [1, s. 118].

Euler oli papin poika ja isänsä toiveen mukaan Euler aloitti 13-vuotiaana opiskelunsa Baselin yliopistossa tähdätäkseen teologian uralle [13, s. 235]. Yliopiston matematiikan professori Johann Bernoulli kuitenkin huomasi Eulerin poikkeukselliset taidot matematiikassa ja fysiikassa. Näin ollen Eulerilla oli mahdollisuus saada lauantaisin yksityisopetusta Bernoullilta. Euler myös ystävystyi Johann Bernoullin kahden pojan Danielin ja Nicolauksen kanssa. Maisteritutkielmansa Euler kirjoitti vuonna 1724, missä hän vertasi René Descartesin ja Isaac Newtonin filosofisia ajatuksia. [6, s. 32–33] Eulerin kiinnostus matematiikkaa kohtaa sai hänet luopumaan suunnitelmistaan seurata isänsä jalanjälkiä [13, s. 235].

Vuonna 1727 Euler kutsuttiin Venäjälle lääketieteen ja fysiologian osaston jäseneksi Pietarin tiedeakatemiaan, jonka Katariina I oli perustanut. Euler oli saanut suositukset Daniel ja Nicolaus Bernoullilta, jotka toimivat Pietarin akatemian matematiikan tutkijoina. Myöhemmin vuonna 1733 Eulerista tuli Pietarin akatemian johtava matemaatikko ja akatemian aikakauskirjassa hän julkaisi runsaasti matemaattista tuotantoaan. Eulerin oikea silmä sokeutui vuonna 1735, mutta se ei Eulerin työtä hidastanut. Vuonna 1741 Euler vastasi myöntävästi Fredrik Suuren kutsuun saapua Berliinin akatemiaan. Euler asui Berliinissä 25 vuotta, mutta sai tältä ajalta palkkaa myös Pietarista, sillä hän levitti tutkimuksiaan sekä Berliinin että Pietarin akatemioiden julkaisuissa. Vuonna 1766 Euler palasi takaisin Venäjälle Pietarin akatemiaan Katariina Suuren hyväksynnällä, mutta alkoi sokeutumaan toisestakin silmästä samaisena vuotena. Tämäkään takaisku ei estänyt Euleria julkaisemasta tutkimuksiaan, vaan hän jatkoi töitään lastensa avustamana. Esimerkiksi suosittu algebran oppikirja *Elements of Algebra* julkaistiin vuonna 1770, jonka tekstin sokea Euler oli sanellut kotiapulaiselle. Eulerin kuoltua Pietarin akatemia jatkoi edelleen hänen tutkimuksiensa julkaisuja lähes 50 vuoden ajan. [5, s. 619–621, 644]

Eulerin merkitys matematiikan kehittymisessä on ollut valtava, sillä hän kehitti laaja-alaisesti puhtaan ja soveltuvan matematiikan tuntemusta. Hänen tutkimuksensa

koskivat pääosin nykyistä lukio- ja yliopistotason matematiikkaa sekä olivat kirjoitettu suurimmaksi osaksi nykykielellä ja -merkinnöillä. [5, s. 621]

Euler oli keskeinen matemaattisten merkintöjen kehittäjä, erityisesti monet merkintätavat geometriassa, algebrassa, trigonometriassa ja analyysissä ovat peräisin Eulerilta. Euler alkoi käyttämään kirjoituksissaan kirjainta e kuvaamaan luonnollisen logaritmin kantalukua. Ensimmäisen kerran kirjain e nähtiin painettuna teoksessa *Mechanica* vuonna 1736, jonka jälkeen merkintä vakiintui nopeasti. Kreikkalaista kirjainta π William Jones oli jo aikaisemminkin käyttänyt kuvaamaan ympyrän kehän ja halkaisijan suhdetta, mutta vuonna 1737 Euler otti merkinnän käyttöönsä tunnettuihin oppikirjoihinsa ja täten vakiinnutti laajasti kirjaimen π käytön. Lisäksi imaginääriyksikön merkitseminen kirjaimella i on peräisin Eulerilta vuodelta 1777, mikä yleistyi Gaussin käyttäessä sitä teoksessaan *Disquisitiones Arithmeticae* vuonna 1801. Käytämme edelleenkin monia muitakin Eulerin merkintätapoja, esimerkiksi merkitsemme kolmion sivuja pienillä kirjaimilla a, b, c, summaa merkinnällä $\sum$ ja muuttujan x funktiota merkinnällä $f(x)$. [5, s. 621–623]

Eulerin teokset sisälsivät tärkeitä käsitteitä ja teorioita, jotka ovat luoneet pohjaa nykyiselle matematiikan tietämykselle. Esimerkiksi Eulerin vuonna 1748 ilmestynyt latinankielinen teos *Introduction in Analysin Infinitorum* oli kaksiosainen tutkielma, joka käynnisti matemaattisen analyysin kehityksen. Teoksen myötä funktiosta tuli analyysin peruskäsite. Euler käsitteli teoksessaan alkeisfunktiota, trigonometrisia funktioita, trigonometristen funktioiden käänteisfunktioita, logaritmifunktioita ja eksponenttifunktioita lähes samalla tavalla kuin nykyäänkin. Hän myös todisti päättymättömiin sarjoihin liittyviä tuloksia, kuten että

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \cdots = \frac{\pi^2}{6}. \text{ [5, s. 623–626]}$$

Lukuteoriasta Euler ei julkaissut alan kirjoja, mutta hän kirjoitti lukuteorian oppeihin liittyviä artikkeleita ja kirjeitä. Muun muassa Euler todisti vuonna 1736 Fermat'n pienen lauseen. [5, s. 641–642]

2.7 Eulerin funktio

Tässä alaluvussa tutustutaan Eulerin mukaan nimettyyn aritmeettiseen funktioon.

Määritelmä 2.6. (Vrt. [7, s. 72]). *Eulerin funktio* φ määritellään kaikille positiivisille kokonaisluvuille kaavalla

$$\varphi(n) = |\{m \in \mathbb{Z}^+ : \ 1 \leq m \leq n \ \text{ja} \ (m, n) = 1\}|.$$

Esimerkki 2.5. Lasketaan Eulerin funktion $\varphi(n)$ arvot, kun $n = 7$ ja $n = 8$. Tällöin $\varphi(7) = 6$, sillä $(m, 7) = 1$, kun $m = 1, 2, 3, 4, 5, 6$. Huomataan, että $\varphi(p) = p - 1$, kun p on alkuluku, sillä kaikille $1 \leq m \leq p$ on voimassa $(m, p) = 1$, jos ja vain jos $m = 1, 2, \ldots, p - 1$. Vastaavasti $\varphi(8) = 4$, sillä $(m, 8) = 1$, kun $m = 1, 3, 5, 7$.

Lause 2.11. *Jos p on alkuluku ja $\alpha \in \mathbb{Z}^+$, niin*

$$\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\Big(1 - \frac{1}{p}\Big).$$

Todistus. (Ks. [13, s. 241]). Lasketaan niiden positiivisten kokonaislukujen määrä, jotka ovat pienempiä tai yhtä suuria kuin luku p^α ja joiden suurin yhteinen tekijä luvun p^α kanssa on erisuuri kuin yksi. Tällaisia ovat kokonaisluvut kp siten, että $1 \leq k \leq p^{\alpha-1}$. Nyt selvästi $(kp, p^\alpha) \neq 1$. Huomataan, että kyseisiä lukuja on siis $p^{\alpha-1}$ kappaletta. Näin ollen luvun p^α kanssa keskenään jaottomia kokonaislukuja on $p^\alpha - p^{\alpha-1}$ kappaletta. Siis $\varphi(p^\alpha) = p^\alpha - p^{\alpha-1} = p^\alpha\Big(1 - \frac{1}{p}\Big)$. □

Apulause 2.1. Jos a ja b ovat kokonaislukuja siten, että $(a, b) = d$, niin $(a/d, b/d) = 1$. Toisin sanoen luvut (a/d) ja (b/d) ovat keskenään jaottomia.

Todistus. (Ks. [13, s. 94]). Olkoot a ja b kokonaislukuja siten, että $(a, b) = d$. Osoitetaan, että luvuilla (a/d) ja (b/d) ei ole muuta yhteistä jakajaa kuin luku 1. Oletetaan, että e on kokonaisluku siten, että $e \mid (a/d)$ ja $e \mid (b/d)$. Tällöin on olemassa kokonaisluvut k ja l siten, että $a/d = ke$ ja $b/d = le$. Toisin sanoen $a = dek$ ja $b = del$. Näin ollen luku de on lukujen a ja b yhteinen tekijä. Mutta nyt oletuksen nojalla $(a, b) = d$ ja $de \leq d$, joten luku $e = 1$. Siis $(a/d, b/d) = 1$. □

Lause 2.12. *Kaikille kokonaisluvuille n on voimassa*

$$\sum_{d|n} \varphi(d) = n.$$

Todistus. (Ks. [1, s. 119]). Olkoon luku n jaollinen luvuilla $d_1, d_2, \ldots, d_k > 0$ (ja vain niillä) sekä määritellään joukko

$$S_i = \{m \in \mathbb{Z}^+ : \ m \leq n \ \text{ja} \ (m, n) = d_i\}, \qquad i = 1, 2, \ldots, k.$$

Jos $m \in S_i$, niin $m = d_i m'$ jollakin kokonaisluvulla m', missä $(m', \frac{n}{d_i}) = (\frac{m}{d_i}, \frac{n}{d_i}) = 1$ apulauseen 2.1 nojalla. Koska $0 \leq m' \leq \frac{n}{d_i}$, niin määritelmän 2.6 nojalla joukon S_i alkioiden lukumäärä $|S_i| = \varphi\Big(\frac{n}{d_i}\Big)$. Nyt joukot $S_1, S_2, \ldots, S_k$ ovat joukon $\{1, 2, \ldots, n\}$ ositus, jolloin

$$\sum_{i=1}^{k} \varphi\Big(\frac{n}{d_i}\Big) = \sum_{i=1}^{k} |S_i| = n.$$

Nyt oletuksen mukaan luku n on jaollinen luvuilla $d_1, d_2, \ldots, d_k$, joten

$$\left\{\frac{n}{d_1}, \frac{n}{d_2}, \ldots, \frac{n}{d_k}\right\} = \{d_1, d_2, \ldots, d_k\}.$$

Näin ollen $\sum_{d|n} \varphi(d) = n$. □

Apulause 2.2. Funktio $g(n) = n$ ($n \in \mathbb{Z}^+$) on multiplikatiivinen.

Todistus. Kaikille positiivisille kokonaisluvuille m ja n pätee, että $g(mn) = mn = g(m)g(n)$, joten funktio $g(n) = n$ on multiplikatiivinen. □

Lause 2.13. *Eulerin funktio φ on multiplikatiivinen.*

Todistus. (Ks. [1, s. 119]). Lauseen 2.12 mukaan $n = \sum_{d|n} \varphi(d)$. Koska apulauseen 2.2 nojalla funktio $g(n) = n$ on multiplikatiivinen, niin seurauksen 2.2 nojalla φ on multiplikatiivinen. □

Lause 2.14. *Olkoon kokonaisluvun $n > 1$ kanoninen alkutekijähajotelma $n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, missä $p_1, p_2, \ldots, p_k$ ovat erisuuria alkuluja, $\alpha_1, \alpha_2, \ldots, \alpha_k$ ovat positiivisia kokonaislukuja ja $p_1 < p_2 < \cdots < p_k$. Tällöin*

$$\varphi(n) = n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\cdots\Big(1 - \frac{1}{p_k}\Big) = n\prod_{i=1}^{k}\Big(1 - \frac{1}{p_i}\Big).$$

Todistus. (Ks. [1, s. 119]). Eulerin funktion φ multiplikatiivisuudesta seuraa, että

$$\varphi(n) = \varphi(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}) = \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k}).$$

Nyt lauseen 2.11 nojalla $\varphi(p^\alpha) = p^\alpha\Big(1 - \frac{1}{p}\Big)$. Siis

$$\begin{aligned}
\varphi(n) =& \varphi(p_1^{\alpha_1})\varphi(p_2^{\alpha_2})\cdots\varphi(p_k^{\alpha_k}) \\
=& p_1^{\alpha_1}\Big(1 - \frac{1}{p_1}\Big)p_2^{\alpha_2}\Big(1 - \frac{1}{p_2}\Big)\cdots p_k^{\alpha_k}\Big(1 - \frac{1}{p_k}\Big) \\
=& p_1^{\alpha_1} p_2^{\alpha_2}\cdots p_k^{\alpha_k}\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\cdots\Big(1 - \frac{1}{p_k}\Big) \\
=& n\Big(1 - \frac{1}{p_1}\Big)\Big(1 - \frac{1}{p_2}\Big)\cdots\Big(1 - \frac{1}{p_k}\Big) \\
=& n\prod_{i=1}^{k}\Big(1 - \frac{1}{p_i}\Big).
\end{aligned}$$

□

Esimerkki 2.6. Lasketaan Eulerin funktion $\varphi(n)$ arvo, kun $n = 360$. Nyt lausetta 2.14 soveltamalla ja jakamalla luku 360 alkulukutekijöihin saadaan

$$\varphi(360) = \varphi(2^3 \cdot 3^2 \cdot 5) = 360\Big(1 - \frac{1}{2}\Big)\Big(1 - \frac{1}{3}\Big)\Big(1 - \frac{1}{5}\Big) = 96.$$

2.8 Täydellisesti multiplikatiiviset funktiot

Esitetään täydellisesti multiplikatiivisten funktioiden määritelmä ja todistetaan välttämättömiä ja riittäviä ehtoja sille, että funktio on täydellisesti multiplikatiivinen.

Määritelmä 2.7. (Vrt. [2, s. 33]). Aritmeettista funktiota f sanotaan *täydellisesti multiplikatiiviseksi*, jos funktio f ei ole nollafunktio ja $f(mn) = f(m)f(n)$ aina, kun $m, n \in \mathbb{Z}^+$.

Huomautus. Täydellisesti multiplikatiivinen funktio on aina multiplikatiivinen.

Esimerkki 2.7. Lauseissa 2.8 ja 2.13 osoitettiin, että Möbiuksen ja Eulerin funktiot ovat multiplikatiivisia, mutta kyseiset funktiot eivät ole täydellisesti multiplikatiivisia. Nimittäin esimerkiksi $\mu(9) = 0$, mutta $\mu(3)\mu(3) = -1 \cdot (-1) = 1$. Lisäksi $\varphi(9) = 6$, mutta $\varphi(3)\varphi(3) = 2 \cdot 2 = 4$.

Lause 2.15. (Ks. [2, s. 34]). *Olkoon f multiplikatiivinen funktio. Tällöin funktio f on täydellisesti multiplikatiivinen, jos ja vain jos*

$$f(p^a) = f(p)^a$$

aina, kun p on alkuluku ja a on positiivinen kokonaisluku.

Todistus. Oletetaan, että f on täydellisesti multiplikatiivinen funktio. Olkoon p alkuluku ja a positiivinen kokonaisluku. Tällöin

$$f(p^a) = f(\underbrace{p \cdot p \cdots p}_{a \text{ kappaletta}}) = \underbrace{f(p)f(p)\cdots f(p)}_{a \text{ kappaletta}} = f(p)^a.$$

Oletetaan seuraavaksi, että $f(p^a) = f(p)^a$ jokaisella alkuluvulla p ja jokaisella positiivisella eksponentilla a. Olkoot m ja n positiivisia kokonaislukuja, ja olkoot niiden alkutekijähajotelmat muotoa $m = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$ ja $n = p_1^{b_1} \cdot p_2^{b_2} \cdots p_k^{b_k}$, missä $a_1, a_2, \ldots, a_k$ ja $b_1, b_2, \ldots, b_k$ ovat ei-negatiivisia kokonaislukuja. Silloin

$$\begin{aligned} f(mn) =& f(p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k} \cdot p_1^{b_1} \cdot p_2^{b_2} \cdots p_k^{b_k}) \\ =& f(p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdots p_k^{a_k+b_k}). \end{aligned}$$

Nyt funktio f on multiplikatiivinen, joten

$$f(p_1^{a_1+b_1} \cdot p_2^{a_2+b_2} \cdots p_k^{a_k+b_k}) = f(p_1^{a_1+b_1})f(p_2^{a_2+b_2}) \cdots f(p_k^{a_k+b_k}).$$

Oletuksen nojalla $f(p^a) = f(p)^a$, jolloin

$$f(p_1^{a_1+b_1})f(p_2^{a_2+b_2})\cdots f(p_k^{a_k+b_k}) = f(p_1)^{a_1+b_1}f(p_2)^{a_2+b_2}\cdots f(p_k)^{a_k+b_k}$$

$$\begin{aligned}
&= f(p_1)^{a_1}f(p_1)^{b_1}f(p_2)^{a_2}f(p_2)^{b_2}\cdots f(p_k)^{a_k}f(p_k)^{b_k} \\
&= f(p_1)^{a_1}f(p_2)^{a_2}\cdots f(p_k)^{a_k}f(p_1)^{b_1}f(p_2)^{b_2}\cdots f(p_k)^{b_k}.
\end{aligned}$$

Edelleen oletuksesta ja funktion f multiplikatiivisuudesta seuraa, että

$$f(p_1)^{a_1}f(p_2)^{a_2}\cdots f(p_k)^{a_k}f(p_1)^{b_1}f(p_2)^{b_2}\cdots f(p_k)^{b_k}$$

$$\begin{aligned}
&= f(p_1^{a_1})f(p_2^{a_2})\cdots f(p_k^{a_k})f(p_1^{b_1})f(p_2^{b_2})\cdots f(p_k^{b_k}) \\
&= f(p_1^{a_1}\cdot p_2^{a_2}\cdots p_k^{a_k})f(p_1^{b_1}\cdot p_2^{b_2}\cdots p_k^{b_k}) \\
&= f(m)f(n).
\end{aligned}$$

Täten lause on todistettu. □

Lause 2.16. *Olkoon f multiplikatiivinen funktio. Tällöin funktio f on täydellisesti multiplikatiivinen, jos ja vain jos*

$$f^{-1} = \mu f$$

aina, kun n on positiivinen kokonaisluku.

Todistus. (Ks. [2, s. 36]). Oletetaan, että f on täydellisesti multiplikatiivinen funktio. Nyt

$$(\mu f * f)(n) = \sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right).$$

Oletuksen nojalla f on täydellisesti multiplikatiivinen, joten

$$f(d)f\left(\frac{n}{d}\right) = f(n).$$

Siis

$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = f(n)\sum_{d|n}\mu(d) = f(n)\varepsilon(n) = \varepsilon(n),$$

sillä $f(1) = 1$ ja $\varepsilon(n) = 0$, kun $n > 1$. Näin ollen $f^{-1} = \mu f$.

Oletetaan sitten, että $f^{-1} = \mu f$. Tällöin

$$\sum_{d|n} \mu(d)f(d)f\left(\frac{n}{d}\right) = 0 \qquad \text{aina, kun } n > 1.$$

Silloin sijoittamalla summaan luku $n = p^a$ saadaan, että

$$\sum_{d|p^a} \mu(d) f(d) f\left(\frac{p^a}{d}\right) = 0.$$

Erityisesti

$$\mu(1) f(1) f(p^a) + \mu(p) f(p) f(p^{a-1}) = 0,$$

missä $\mu(1) = f(1) = 1$ ja $\mu(p) = -1$. Siis $f(p^a) = f(p) f(p^{a-1})$, joten induktiolla saadaan, että $f(p^a) = f(p)^a$, missä funktio f on multiplikatiivinen. Näin ollen lauseen 2.16 mukaan funktio f on täydellisesti multiplikatiivinen. □

Lause 2.17. ([13, s. 248], tehtävä 47.) *Jos funktiot f ja g ovat täydellisesti multiplikatiivisia, niin funktio fg on täydellisesti multiplikatiivinen.*

Todistus. Oletetaan, että funktiot f ja g ovat täydellisesti multiplikatiivisia. Olkoot m ja n positiivisia kokonaislukuja. Tällöin

$$(fg)(mn) = f(mn)g(mn) = f(m)f(n)g(m)g(n) = (fg)(m)(fg)(n),$$

joten funktio fg on täydellisesti multiplikatiivinen. □

Lause 2.18. ([2, s. 49], tehtävä 27.) *Jos funktio f on täydellisesti multiplikatiivinen, niin*

$$f(g * h) = (fg) * (fh)$$

aina, kun g ja h ovat aritmeettisia funktioita.

Todistus. Oletetaan, että funktio f on täydellisesti multiplikatiivinen. Nyt

$$\big((fg) * (fh)\big)(n) = \sum_{d|n} f(d)g(d) f\left(\frac{n}{d}\right) h\left(\frac{n}{d}\right).$$

Oletuksen nojalla f on täydellisesti multiplikatiivinen, joten

$$f(d) f\left(\frac{n}{d}\right) = f(n).$$

Täten

$$\sum_{d|n} f(d)g(d) f\left(\frac{n}{d}\right) h\left(\frac{n}{d}\right) = f(n) \sum_{d|n} g(d) h\left(\frac{n}{d}\right) = \big(f(g * h)\big)(n)$$

ja lause on saatu todistettua. □

2.9 Joseph Liouville

Ranskalainen matemaatikko Joseph Liouville (1809–1882) tunnetaan hänen tutkimuksistaan, kuten lukuteorian, analyysin, matemaattisen fysiikan ja tähtitieteen osa-alueilla. Ranskassa Liouville opiskeli vuodesta 1825 lähtien École Polytechniquen koulutuslaitoksessa ja jatkoi opintojaan Ecole des Ponts et Chausséessiin, missä hän opiskeli vuoteen 1830 asti. Opintojen aikana hän kirjoitti artikkeleita muun muassa elektrodynamiikasta, lämpöteoriasta ja osittaisdifferentiaaliyhtälöistä. [13, s. 248]

Vuonna 1831 Liouville sai assistentin viran École Polytechniquesissa ja aloitti opettamaan eri koulutuslaitoksissa. Liouville perusti samana vuonna aikakauslehden *Journal de Mathématiques Pures et Appliquées*, jolla oli tärkeä rooli 1800-luvun matematiikan kehitykselle Ranskassa. [13, s. 248] Liouville pysyi lehden päätoimittajana vuoteen 1874 saakka. Vuonna 1836 Liouville valmistui tohtoriksi soveltaessaan Fourier'n sarjaa matemaattisessa fysiikassa. Tämän jälkeen hän sai opettaa yliopistotasolla. [11, s. 175] Vuonna 1838 Liouville nimitettiin professoriksi École Polytechniquesiin. Liouville sai laitoksen johtajan viran vuonna 1851 Collége de Francen tutkimuslaitoksesta ja mekaniikan laitoksen johtajan viran vuonna 1857 Faculté des Science -instituutiosta. [13, s. 248]

Liouville tutki laaja-alaisesti eri matematiikan aloja. Esimerkiksi Liouville antoi ensimmäisenä täsmällisen esimerkin transsendenttiluvusta määrittäessään Liouvillen luvun. [11, s. 175] [13, s. 248] Hänen nimensä liitetään kompleksianalyysissä Liouvillen lauseeseen [5, s. 799]. Hänet myös tunnetaan Sturm-Liouvillen teoriasta, jota käytetään integraaliyhtälöiden ratkaisemiseen. Lisäksi hän myötävaikutti differentiaaligeometriaan. Yhteensä hänen matemaattisten tekstiensä kokonaistuotanto on yli 400 kappaletta, joista melkein puolet käsittelee lukuteoriaa. [13, s. 248]

2.10 Liouvillen funktio

Määritellään Joseph Liouville mukaan nimetty Liouvillen funktio λ, joka on tärkeä esimerkki täydellisesti multiplikatiivisesta funktiosta.

Määritelmä 2.8. (Vrt. [2, s. 37]). *Liouvillen funktio* λ määritellään siten, että $\lambda(1) = 1$ ja jos positiivisen kokonaisluvun n kanoninen alkutekijähajotelma on $n = p_1^{a_1} \cdot p_2^{a_2} \cdots p_k^{a_k}$, niin $\lambda(n) = (-1)^{a_1+a_2+\cdots+a_k}$.

Lause 2.19. *Liouvillen funktio* λ *on täydellisesti multiplikatiivinen.*

Todistus. Olkoot m ja n positiivisia kokonaislukuja, ja olkoot niiden alkutekijähajotelmat muotoa $m = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k}$ ja $n = p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}$, missä $\alpha_1, \alpha_2, \ldots, \alpha_k$ ja $\beta_1, \beta_2, \ldots, \beta_k$ ovat ei-negatiivisia kokonaislukuja. Silloin

$$\begin{aligned}
\lambda(mn) =& \lambda(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k} \cdot p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}) \\
=& (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k+\beta_1+\beta_2+\cdots+\beta_k} \\
=& (-1)^{\alpha_1+\alpha_2+\cdots+\alpha_k}(-1)^{\beta_1+\beta_2+\cdots+\beta_k} \\
=& \lambda(p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdots p_k^{\alpha_k})\lambda(p_1^{\beta_1} \cdot p_2^{\beta_2} \cdots p_k^{\beta_k}) \\
=& \lambda(m)\lambda(n).
\end{aligned}$$

Näin ollen funktio λ on täydellisesti multiplikatiivinen. □

Lause 2.20. *Olkoon $n \geq 1$. Tällöin*

$$\sum_{d|n} \lambda(d) = \begin{cases} 1, & \textit{jos luku } n \textit{ on neliö}, \\ 0, & \textit{muulloin.} \end{cases}$$

Lisäksi $\lambda^{-1}(n) = |\mu(n)|$ kaikille kokonaisluvuille n.

Todistus. (Ks. [2, s. 38]). Merkitään $g(n) = \sum_{d|n} \lambda(d)$. Tällöin funktio g on seurauksen 2.1 perusteella multiplikatiivinen. Nyt

$$\begin{aligned}
g(p^a) = \sum_{d|p^a} \lambda(d) =& 1 + \lambda(p) + \lambda(p^2) + \cdots + \lambda(p^a) \\
=& 1 - 1 + 1 - \cdots + (-1)^a \\
=& \begin{cases} 0, & \text{jos } a \text{ on pariton,} \\ 1, & \text{jos } a \text{ on parillinen.} \end{cases}
\end{aligned}$$

Jos $n = \prod_{i=1}^{k} p_i^{a_i}$, niin $g(n) = \prod_{i=1}^{k} g(p_i^{a_i})$. Jos jokin eksponentti a_i on pariton, niin $g(p_i^{a_i}) = 0$ ja $g(n) = 0$. Jos kaikki eksponentit a_i ovat parillisia, niin $g(p_i^{a_i}) = 1$ ja $g(n) = 1$. Näin ollen $g(n) = 1$, jos luku n on neliöllä jaollinen, ja $g(n) = 0$ muulloin. Lisäksi Möbiuksen funktion määritelmään 2.4 nojaten saadaan, että $\lambda^{-1}(n) = \mu(n)\lambda(n) = \mu^2(n) = |\mu(n)|$. □

3 Modulaarinen aritmetiikka ja Ramanujanin summa

3.1 Karl Friedrich Gauss

Karl Friedrich Gauss (1777–1855) oli saksalainen matemaatikko, tähtitieteilijä ja fyysikko, joka saavutuksillaan tuli tunnetuksi ja kunnioitetuksi ”matemaatikkojen ruhtinaaksi” [12, s. 184–185]. Hän oli matemaattisesti huippulahjakas pienestä pitäen. Sanotaan, että kolmevuotiaana Gauss korjasi virheen isänsä palkkakuitista. Toisen tarinan mukaan kahdeksanvuotias Gauss sai aritmetiikan oppitunnilla opettajaltaan haastavan ja aikaa vievän tehtävän, jossa piti laskea sadan ensimmäisen kokonaisluvun summa. Hetkessä Gauss sai oikeaksi vastaukseksi $50 \cdot 101 = 5050$, sillä hän jaotteli termit pareittain siten, että $1+100 = 101, 2+99 = 101, \ldots, 50+51 = 101$. [13, s. 146] Opettaja kertoi Gaussin poikkeuksellisista taidoista Braunschweigin herttualle Carl Wilhelm Friedrichille. Herttua alkoi tukemaan rahallisesti Gaussin opiskelua ja Gauss pääsi opiskelemaan Göttigenin yliopistoon vuonna 1795. [5, s. 696]

Vuonna 1796 Gauss ratkaisi 2000 vuotta vanhan matemaattisen ongelman ja konstruoi 17-sivuisen säännöllisen monikulmion käyttämällä vain viivoitinta ja harppia. Gauss vastaanotti tohtorin arvon vuonna 1799 ja väitöskirjassaan hän esitti ensimmäisen täsmällisen todistuksen keskeiselle algebran peruslauseelle, jonka mukaan jokaisella reaalikertoimisella astetta n olevalla polynomilla on täsmälleen n juurta. [13, s. 146] [5, s. 698]

Braunschweigin herttua tuki edelleen Gaussia taloudellisesti, joten Gaussin ei tarvinnut etsiä töitä tai käyttää aikaansa opettamiseen, vaan hänellä oli mahdollisuus keskittyä täysin tutkimustyötön [10, s. 170]. Vuonna 1801 Gauss julkaisi lukuteoriaa käsittelevän klassikkoteoksen *Disquisitiones Arithmeticae*, jossa muun muassa esitellään kongruenssin ja jäännösluokan käsite sekä todistetaan aritmetiikan peruslause ja neliönjäännöslause [12, s. 184] [5, s. 698]. Samaisena vuonna Gauss myötävaikutti tähtitieteen alalla laskiessaan asteroidi Cereksen liikeradan. Gaussin maine kasvoi Euroopassa ja vuonna 1802 hän sai työtarjouksen Pietarin akatemiasta, mutta Gauss jäi Braunschweigiin herttuan korottaessa stipendin suuruutta. Braunschweigin herttuan kuoltua sodassa vuonna 1806 Gauss tarvitsi uuden tulonlähteen. Vuonna 1807 Gaussista tuli Göttingenin yliopiston tähtitieteen professori ja observatorion johtaja

viettäen siellä loppuelämänsä. [12, s. 184–185]

Gauss tunnetaan monista tutkimuksistaan geometriassa, algebrassa, analyysissä, tähtitieteessä ja matemaattisessa fysiikassa. Erityisesti hän oli kiinnostunut lukuteoriasta. Hänen mukaansa ”matematiikka on tieteiden kuningatar ja lukuteoria on matematiikan kuningatar”. [13, s. 146] Matematiikan lisäksi Gauss tutki maanmittausta, magnetismia ja optiikkaa [12, s. 184].

3.2 Täydellinen ja supistettu jäännössysteemi

Tässä alaluvussa tarkastellaan kongruenssin perustuloksia ja määritellään täydellinen ja supistettu jäännössysteemi. Olkoot a, b kokonaislukuja ja olkoon m positiivinen kokonaisluku. Sanotaan, että luku a on *kongruentti* luvun b kanssa modulo m, jos $m \mid a - b$. Lukujen a ja b kongruenssia merkitään $a \equiv b \pmod{m}$.

Lause 3.1. *Olkoot luvut a, b kokonaislukuja siten, että* $a = mq_1 + r_1$ *ja* $b = mq_2 + r_2$, *missä* $0 \leq r_1, r_2 < m$. *Silloin* $a \equiv b \pmod{m}$, *jos ja vain jos* $r_1 = r_2$.

Todistus. (Ks. [1, s. 30]). Koska $a - b = mq_1 + r_1 - (mq_2 + r_2) = m(q_1 - q_2) + (r_1 - r_2)$, niin $m \mid a - b$, jos vain jos $m \mid r_1 - r_2$. Oletuksen nojalla $0 \leq r_1, r_2 < m$, joten $|r_1 - r_2| < m$, jolloin $m \mid r_1 - r_2$, jos ja vain jos $r_1 = r_2$. □

Lause 3.2. *Jos* $a \equiv b \pmod{m}$ *ja* $c \equiv d \pmod{m}$, *niin*

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

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

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

Todistus. (Vrt. [13, s. 149]). Oletetaan, että $a \equiv b \pmod{m}$ ja $c \equiv d \pmod{m}$. Silloin $m \mid (a - b)$ ja $m \mid (c - d)$, minkä seurauksena on olemassa kokonaisluvut k ja l siten, että $km = a - b$ ja $lm = c - d$.

Kohdassa (i) huomataan, että

$$(a + c) - (b + d) = (a - b) + (c - d) = km + lm = (k + l)m,$$

jolloin $m \mid [(a + c) - (b + d)]$. Siis $a + c \equiv b + d \pmod{m}$.

Kohta (ii) todistetaan vastaavalla tavalla siten, että

$$(a - c) - (b - d) = (a - b) - (c - d) = km - lm = (k - l)m,$$

jolloin $m \mid [(a-c)-(b-d)]$. Tällöin $a - c \equiv b - d \pmod{m}$.

Todistetaan kohta (iii). Nyt

$$ac - bd = ac - bc + bc - bd = c(a-b) + b(c-d) = ckm + blm = m(ck + bl).$$

Tällöin $m \mid (ac - bd)$, joten $ac \equiv bd \pmod{m}$. □

Seuraus 3.1. (Ks. [9, s. 33]). *Jos* $a \equiv b \pmod{m}$*, niin kaikilla* $k \in \mathbb{Z}$ *pätee* $ak \equiv bk \pmod{m}$.

Todistus. Oletetaan, että $a \equiv b \pmod{m}$ eli $m \mid (a-b)$. Huomataan, että $(a-b) \mid k(a-b)$. Tällöin jaollisuuden perusominaisuuksien nojalla $m \mid k(a-b)$ eli $m \mid (ak - bk)$. Näin ollen $ak \equiv bk \pmod{m}$. □

Seuraus 3.2. (Ks. [9, s. 33]). *Jos* $a \equiv b \pmod{m}$*, niin kaikilla* $k \in \mathbb{Z}^+$ *pätee* $a^k \equiv b^k \pmod{m}$.

Todistus. Oletetaan, että $a \equiv b \pmod{m}$. Todistetaan induktiolla, että kaikilla $k \in \mathbb{Z}^+$ pätee $a^k \equiv b^k \pmod{m}$.
1. Perusaskel. Osoitetaan, että väite on tosi, kun $k = 1$.
Nyt oletuksen nojalla $a \equiv b \pmod{m}$.
2. Induktioaskel. Oletetaan, että väite on tosi, kun $k = n$.
Silloin $a^n \equiv b^n \pmod{m}$ ja oletuksen nojalla edelleen $a \equiv b \pmod{m}$. Tällöin näiden kongruenssiyhtälöiden kertomisesta keskenään saadaan lauseen 3.2 nojalla $a^{n+1} \equiv b^{n+1} \pmod{m}$.
3. Johtopäätös. Induktioperiaatteen nojalla väite on tosi kaikilla $k \in \mathbb{Z}^+$ ja lause on näin ollen todistettu. □

Lause 3.3. *Oletetaan, että* $(k, m) = d$*. Silloin* $ka \equiv kb \pmod{m}$*, jos ja vain jos* $a \equiv b \pmod{m/d}$.

Todistus. (Ks. [9, s. 33]). Oletetaan, että $(k, m) = d$. Silloin $k = td$ ja $m = sd$ joillakin kokonaisluvuilla t ja s. Jos $m \mid (ka - kb)$, niin $k(a-b) = um$ jollakin kokonaisluvulla u. Sijoittamalla yhtälöön $k(a-b) = um$ luvut $k = td$ ja $m = sd$ saadaan

$$\begin{aligned} & td(a-b) = usd \\ \Leftrightarrow \quad & t(a-b) = us \\ \Leftrightarrow \quad & ta - tb = us, \end{aligned}$$

joten $ta \equiv tb \pmod{s}$. Nyt apulauseen 2.1 nojalla $(k/d, m/d) = (t, s) = 1$, joten $s \mid (a - b)$. Mutta $s = m/d$, jolloin $a \equiv b \pmod{m/d}$.

Jos $a \equiv b \pmod{m/d}$ eli $a \equiv b \pmod{s}$ niin $s \mid (a - b)$. Tällöin $a - b = vs$ jollakin kokonaisluvulla v. Sijoittamalla yhtälöön $ka - kb$ termit $(a - b) = vs$, $k = td$ ja $sd = m$ saadaan, että

$$ka - kb = k(a - b) = kvs = tdvs = (sd)tv = mtv.$$

Tällöin $m \mid (ka - kb)$, siis $ka \equiv kb \pmod{m}$. Näin ollen lause on todistettu molempiin suuntiin. □

Lause 3.4. ([9, s. 34], tehtävä 11-3.) *Jos* $a \equiv b \pmod{m}$ *ja* $0 < d \mid m$, *niin* $a \equiv b \pmod{d}$.

Todistus. Oletetaan, että $a \equiv b \pmod{m}$ ja $0 < d \mid m$. On siis olemassa kokonaisluvut k ja l siten, että $km = (a - b)$ ja $ld = m$. Näin ollen sijoittamalla saadaan, että $kld = (a - b)$, jolloin $d \mid (a - b)$. □

Määritelmä 3.1. Luvun a määräämä *jäännösluokka modulo m* on

$$[a] = \{k \in \mathbb{Z} \mid k \equiv a \pmod{m}\}.$$

Esimerkki 3.1. Olkoon luku $m = 3$. Tällöin luvun 0 määräämä jäännösluokka modulo 3 koostuu niistä kokonaisluvuista k, joille $k \equiv 0 \pmod{3}$, eli

$$[0] = \{\ldots, -6, -3, 0, 3, 6, \ldots\}.$$

Vastaavasti luvun 1 määräämä jäännösluokka modulo 3 koostuu niistä kokonaisluvuista k, joille $k \equiv 1 \pmod{3}$. Siis

$$[1] = \{\ldots, -5, -2, 1, 4, 7, \ldots\}.$$

Edelleen luvun 2 määräämäksi jäännösluokaksi saadaan

$$[2] = \{\ldots, -4, -1, 2, 5, 8, \ldots\}.$$

Huomataan, että $\mathbb{Z}_3 = \{[0], [1], [2]\}$.

Määritelmä 3.2. (Vrt. [9, s. 34]). *Täydelliseksi jäännössysteemiksi modulo m* sanotaan joukkoa, joka sisältää täsmälleen yhden edustajan kustakin jäännösluokastaan. Tätä merkitään myös lyhenteellä CRS $\pmod{m}$, joka tulee englannin kielen sanoista *complete residue system modulo m*.

Määritelmä 3.3. (Vrt. [9, s. 34]). Joukkoa $\{1, 2, \ldots, m\}$ kutsutaan *pienimmäksi positiiviseksi jäännössysteemiksi modulo m.*

Esimerkki 3.2. Joukko $\{21, 8, 16, -4, 11, 33, -1\}$ on täydellinen jäännössysteemi modulo 7, sillä

$$21 \equiv 0,\ 8 \equiv 1,\ 16 \equiv 2,\ -4 \equiv 3,\ 11 \equiv 4,\ 33 \equiv 5,\ -1 \equiv 6 \pmod 7.$$

Lause 3.5. *Jos joukko* $\{a_1, a_2, \ldots, a_m\}$ *on CRS* $\pmod m$ *ja* $(k, m) = 1$*, niin joukko* $\{ka_1, ka_2, \ldots, ka_m\}$ *on CRS* $\pmod m$.

Todistus. (Ks. [9, s. 34]). Oletetaan, että joukko $\{a_1, a_2, \ldots, a_m\}$ on CRS $\pmod m$ ja $(k, m) = 1$. Tehdään vastaoletus, että joillakin indekseillä $i \neq j$ on voimassa

$$ka_i \equiv ka_j \pmod m.$$

Nyt oletuksen nojalla $(k, m) = 1$, joten lauseen 3.3 mukaan $a_i \equiv a_j \pmod m$, mutta tämä on ristiriidassa oletuksen kanssa, jonka mukaan alkiot $\{a_1, a_2, \ldots, a_m\}$ eivät ole kongruentteja keskenään modulo m. Siis joukossa $\{ka_1, ka_2, \ldots, ka_m\}$ on m keskenään epäkongruenttia lukua modulo m eli joukko $\{ka_1, ka_2, \ldots, ka_m\}$ on CRS $\pmod m$. □

Määritelmä 3.4. (Vrt. [9, s. 34]). *Supistetuksi jäännössysteemiksi modulo m* sanotaan joukkoa, joka sisältää täsmälleen $\varphi(m)$ alkiota siten, että jokainen alkio on jaoton luvun m kanssa ja mitkään kaksi eri alkiota eivät ole kongruentteja keskenään modulo m. Tätä merkitään myös lyhenteellä RRS $\pmod m$ (englanniksi *reduced residue system modulo m*).

Määritelmä 3.5. (Vrt. [9, s. 34]). Joukkoa $\{a : 1 \leq a \leq m, (a, m) = 1\}$ kutsutaan *pienimmäksi positiiviseksi supistetuksi jäännössysteemiksi modulo m.*

Esimerkki 3.3. Joukko $\{1, 5, 7, 11\}$ on pienin supistettu jäännössysteemi modulo 12.

Lause 3.6. *Olkoon joukko* $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ *RRS* $\pmod m$*, ja olkoon k sellainen kokonaisluku, että* $(k, m) = 1$*. Tällöin* $\{ka_1, ka_2, \ldots, ka_{\varphi(m)}\}$ *on RRS* $\pmod m$.

Todistus. (Ks. [13, s. 235–236]). Todistetaan ensin, että jokainen kokonaisluku ka_i, missä $i \in \{1, 2, \ldots, \varphi(m)\}$, on jaoton luvun m kanssa. Tehdään vastaoletus, että joillakin indeksillä i on voimassa $(ka_i, m) > 1$. Tällöin on olemassa sellainen alkuluku

p, että $p \mid (ka_i, m)$. Silloin $p \mid ka_i$ ja $p \mid m$. Siis $p \mid k$ ja $p \mid m$ tai $p \mid a_i$ ja $p \mid m$. Nyt jos $p \mid k$ ja $p \mid m$, niin $(k, m) > 1$, mikä on ristiriidassa oletuksen $(k, m) = 1$ kanssa. Toisaalta jos $p \mid a_i$ ja $p \mid m$, niin $(a_i, m) > 1$, mikä on ristiriidassa oletuksen kanssa, että $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ on RRS $\pmod{m}$. Siis kokonaisluku ka_i on jaoton luvun m kanssa aina, kun $i \in \{1, 2, \ldots, \varphi(m)\}$.

Osoitetaan vielä, että mitkään kaksi eri kokonaislukua ka_i, missä $i \in \{1, 2, \ldots, \varphi(m)\}$, eivät ole kongruentteja keskenään modulo m. Tehdään vastaoletus, että $ka_i \equiv ka_j \pmod{m}$, missä $i \neq j$ siten, että $1 \leq i, j \leq \varphi(m)$. Koska oletuksen nojalla $(k, m) = 1$, niin lauseen 3.3 nojalla $a_i \equiv a_j \pmod{m}$. Tämä on ristiriidassa oletuksen kanssa, jonka mukaan $\{a_1, a_2, \ldots, a_{\varphi(m)}\}$ on RRS $\pmod{m}$. Siis kaikille $i \neq j$ pätee $ka_i \not\equiv ka_j \pmod{m}$ ja täten lause on todistettu. □

Lause 3.7 (Eulerin lause)**.** *Olkoon m positiivinen kokonaisluku ja k kokonaisluku. Jos $(k, m) = 1$, niin*

$$k^{\varphi(m)} \equiv 1 \pmod{m}.$$

Todistus. (Ks. [13, s. 236–237]). Olkoon joukko $A = \{a_1, a_2, \ldots, a_{\varphi(m)}\}$ RRS $\pmod{m}$. Oletetaan, että k sellainen kokonaisluku, että $(k, m) = 1$. Tällöin lauseen 3.6 nojalla joukko $kA = \{ka_1, ka_2, \ldots, ka_{\varphi(m)}\}$ on *RRS* $\pmod{m}$. Silloin joukon kA pienimmät positiiviset jäännökset modulo m ovat joukon A alkiot jossain järjestyksessä. Toisin sanoen jokainen joukon kA alkio on kongruentti jonkun joukon A alkion kanssa modulo m. Näin ollen soveltamalla lausetta 3.2 saadaan

$$ka_1 ka_2 \cdots ka_{\varphi(m)} \equiv a_1 a_2 \cdots a_{\varphi(m)} \pmod{m}$$

eli

$$k^{\varphi(m)} a_1 a_2 \cdots a_{\varphi(m)} \equiv a_1 a_2 \cdots a_{\varphi(m)} \pmod{m}.$$

Joukon A määrittelystä seuraa, että $(a_i, m) = 1$ aina, kun $i \in \{1, 2, \ldots, \varphi(m)\}$. Siis koska $(a_1 a_2 \cdots a_{\varphi(m)}, m) = 1$, niin lauseen 3.3 mukaan saadaan, että $k^{\varphi(m)} \equiv 1 \pmod{m}$. □

Seuraus 3.3 (Fermat'n pieni lause)**.** (Vrt. [13, s. 219]). *Jos p on alkuluku ja k on kokonaisluku siten, että $p \nmid k$, niin*

$$k^{p-1} \equiv 1 \pmod{p}.$$

Todistus. Tiedetään, että $\varphi(p) = p - 1$. Lisäksi jos $p \nmid k$, niin $(p, k) = 1$. Soveltamalla lausetta 3.7 saadaan $k^{\varphi(p)} \equiv 1 \pmod{p}$ eli $k^{p-1} \equiv 1 \pmod{p}$. □

Lause 3.8. *Oletetaan, että* $(m, n) = 1$. *Olkoon* $\mathcal{R}_1$ *RSS* $(\text{mod } m)$ *ja* $\mathcal{R}_2$ *RRS* $(\text{mod } n)$. *Tällöin joukko*

$$\mathcal{R} = \{km + jn \ : \ k \in \mathcal{R}_2, j \in \mathcal{R}_1\}$$

on RRS $(\text{mod } mn)$.

Todistus. (Ks. [9, s. 40–41]). Oletetaan, että $(m, n) = 1$. Osoitetaan ensin, että joukossa $\mathcal{R}$ on täsmälleen $\varphi(mn)$ alkiota. Oletetaan, että joillakin luvuilla $j_1, j_2 \in \mathcal{R}_1$ ja $k_1, k_2 \in \mathcal{R}_2$ $(k_1 \leq k_2)$ saadaan

$$k_1 m + j_1 n = k_2 m + j_2 n.$$

Tällöin

$$(j_1 - j_2)n = (k_2 - k_1)m.$$

Nyt koska oletuksen perusteella $(m, n) = 1$, niin $n \mid (k_2 - k_1)$. Mutta luvut k_1 ja k_2 kuuluvat joukkoon *RRS* $(\text{mod } n)$, joten $k_1 = k_2$. Tästä seuraa, että $j_1 = j_2$. Näin ollen joukossa $\mathcal{R}$ on täsmälleen $\varphi(m)\varphi(n)$ alkiota. Funktion φ multiplikatiivisuuden nojalla joukossa $\mathcal{R}$ on täsmälleen $\varphi(mn)$ alkiota.

Osoitetaan sitten, että mitkään kaksi joukon $\mathcal{R}$ alkiota eivät ole kongruentteja keskenään modulo mn. Oletetaan nyt, että joillakin luvuilla k_i ja j_i $(i = 1, 2)$ saadaan, että

$$k_1 m + j_1 n - (k_2 m + j_2 n) = qmn$$

jollakin kokonaisluvulla q. Tällöin

$$(k_1 - k_2)m = (qm - j_1 + j_2)n.$$

Vastaavalla tavalla koska $n \mid (k_1 - k_2)$, mutta luvut k_1 ja k_2 kuuluvat joukkoon *RRS* $(\text{mod } n)$, niin $k_1 = k_2$. Tästä seuraa, että $j_1 = j_2$. Näin ollen mitkään kaksi joukon $\mathcal{R}$ alkiota eivät ole kongruentteja keskenään modulo mn.

Viimeiseksi osoitetaan, että jokainen joukon $\mathcal{R}$ alkio on jaoton luvun mn kanssa. Oletetaan sitten, että $km + jn \in \mathcal{R}$. Olkoon d kokonaisluku siten, että $d = (km + jn, mn)$. Toisin sanoen luku d jakaa jokaisen lukujen $km + jn$ ja mn lineaarikombinaation. Huomataan, että

$$km^2 = m(km + jn) - j(mn),$$

joten $d \mid km^2$. Kirjoitetaan, että $d = ab$, missä $a \mid m$ ja $b \mid n$. Koska $b \mid d$, niin jaollisuuden perusominaisuuksien nojalla $b \mid km^2$. Mutta $(b, m) = 1$, joten $b \mid k$

ja $b \mid n$. Siis $b \mid (k, n) = 1$, jolloin $b = 1$. Vastaavalla tavalla saadaan, että $a = 1$. Tällöin $d = 1$, joten jokainen joukon $\mathcal{R}$ alkio on jaoton luvun mn kanssa. Näin ollen joukko $\mathcal{R}$ on $RRS \pmod{mn}$. □

3.3 Srinivasa Ramanujan

Intialainen matemaatikko Srinivasa Ramanujan (1887–1920) tunnetaan lukuteorian kehittäjänä. Ramanujan syntyi ja kasvoi Etelä-Intiassa opiskellen paikallisessa englanninkielisessä koulussa. [13, s. 254] 15-vuotiaana Ramanujan sai kopion George Shoobridge Carrin teoksesta *Synopsis of Elementary Results in Pure and Applied Mathematics*. Kirja on kokoelma tuhansista lauseista, joista monet esitetään vain lyhyillä todistuksilla. Ramanujan tarkasteli Carrin tuloksia kehittäen omia lauseitaan ja ideoitaan. [16] Vuonna 1904 Ramanujan aloitti apurahan tukemana opinnot Madrasin yliopistossa. Tähän saakka Ramanujan oli menestynyt hyvin kaikissa kouluaineissa, mutta yliopistossa hän uppoutui matematiikkaan laiminlyöden muita opintoja ja menettäen stipendinsä jatkumisen. [3, s. 1]

Korkeakoulututkinnon puuttuessa Ramanujanin oli haastavaa löytää kelvollinen työpaikka. Ramanujan jatkoi matemaattisia tutkimuksiaan eläen köyhissä olosuhteissa ilman työpaikkaa. Valtion virkamies Ramachandra Rao kuitenkin huomasi Ramanujanin lahjakkuuden ja tuki hänen matemaattisia tutkimuksiaan jonkin aikaa. Vuonna 1912 Ramanujan vastaanotti toimistotehtävän. [13, s. 254] [16]

Ramanujan julkaisi ensimmäisen tieteellisen julkaisun intialaisessa lehdessä *Journal of the Indian Mathematical Society* vuonna 1911. Hänen neroutensa sai vähitellen tunnustusta ja Ramanujan päätti aloittaa kirjeenvaihdon englantilaisen matemaatikon Godfrey Harold Hardyn kanssa. [16] Hardy oli ymmällään Ramanujanin esittämistä matemaattisista tuloksista. Ne eivät sisältäneet todistuksia, mutta osoittivat kuitenkin Ramanujanin älykkyyden. [13, s. 254] Hardy järjesti Ramanujanille stipendin Madrasin yliopistoon kahdeksi vuodeksi tuoden hänet lopulta Englantiin Cambridgen yliopistoon vuonna 1914 [3, s. 2]. Hardy opetti henkilökohtaisesti Ramanujania ja he tekivät yhteistyötä viiden vuoden ajan todistaen merkittäviä lauseita liittyen kokonaislukujen ominaisuuksiin [13, s. 254]. Ramanujan esimerkiksi tutki, kuinka monella eri tavalla positiivisen kokonaisluvun voi ilmaista positiivisten kokonaislukujen summana, kuten luku $4 = 3 + 1 = 2 + 2 = 2 + 1 + 1 = 1 + 1 + 1 + 1$. Hänen tutkimuksiansa julkaistiin englanniksi eurooppalaisissa lehdissä. [16] Ramanujanilla oli hämmästyttävän hyvä ymmärrys tietyn tyyppisistä funktioista ja sar-

joista. Ramanujan myötävaikutti merkittävästi lukuteoriaan ja työskenteli elliptisten funktioiden, äärettömien sarjojen ja ketjumurtolukujen parissa. Toisaalta Ramanujanilla oli epäselvä käsitys siitä, miten matemaattisesti todistetaan oikein. Esimerkiksi hänen esittämänsä lauseet alkuluvuista olivat usein vääriä. [13, s. 254]

Ramanujan oli yksi nuorimmista tiedeseura Royal Societyn jäsenistä. Valitettavasti vuonna 1917 Ramanujan sairastui vakavasti. Ensin Ramanujanin ajateltiin sairastuneen tuberkuloosiin, mutta nykyään hänen arvellaan kärsineen vitamiinin puutoksesta kasvissyöjänä ja sodan aiheuttamana pula-aikana. Hän palasi Intiaan vuonna 1919 jatkaen matemaattista työtään sänkypotilaana. Kuollessaan Ramanujanilta jäi julkaisemattomia muistiinpanoja ja tuloksia, joihin matemaatikot ovat omistautuneet monien vuosia ajan pyrkien niiden todistamiseen. [13, s. 254]

3.4 Ramanujanin summa

Esitellään seuraavaksi Ramanujanin kehittämä summakaava.

Merkintä. Merkitään kirjaimella $\mathcal{R}_n$ pienintä supistettua jäännössysteemiä modulo n.

Määritelmä 3.6. (Vrt. [9, s. 42]). Jos $s \in \mathbb{Z}^+$, niin aritmeettinen funktio c_s määritellään kaavalla

$$c_s(n) = \sum_{k \in \mathcal{R}_n} e^{2\pi isk/n}.$$

Funktiota c_s kutsutaan *Ramanujanin summaksi*.

Osoitetaan, että Ramanujanin summan $c_s(n)$ arvo ei muutu, jos summassa $\sum_{k \in \mathcal{R}_n} e^{2\pi isk/n}$ kokonaisluvut k ovat mistä tahansa supistetusta jäännössysteemistä modulo n.

Lause 3.9. *Jos joukko $\mathcal{T}$ on jokin RRS* $\pmod n$*, niin*

$$c_s(n) = \sum_{t \in \mathcal{T}} e^{2\pi ist/n}.$$

Todistus. (Ks. [9, s. 42]). Oletetaan, että joukko $\mathcal{T}$ on jokin *RRS* $\pmod n$. Lisäksi tiedetään, että joukko $\mathcal{R}_n$ pienin supistettu jäännössysteemi modulo n. Tällöin kaikille $t \in \mathcal{T}$ on olemassa yksikäsitteinen kokonaisluku $k \in \mathcal{R}_n$ siten, että $t \equiv k \pmod n$. Toisin sanoen kaikille $t \in \mathcal{T}$ on olemassa yksikäsitteinen k siten, että $t = k + nq(k)$

jollakin kokonaisluvulla $q(k)$. Tällöin

$$\begin{aligned}\sum_{t\in\mathcal{T}} e^{2\pi ist/n} &= \sum_{k\in\mathcal{R}_n} e^{2\pi is(k+nq(k))/n}\\ &= \sum_{k\in\mathcal{R}_n} e^{2\pi isk/n} e^{2\pi isq(k)}\\ &= \sum_{k\in\mathcal{R}_n} e^{2\pi isk/n}\cdot 1\\ &= c_s(n).\end{aligned}$$

Nimittäin jos $z \in \mathbb{R}$, niin Eulerin kaavan nojalla $e^{iz} = \cos z + i\sin z$ eli kaikille kokonaisluvuille $q(k)$ pätee, että $e^{2\pi isq(k)} = \cos 2\pi sq(k) + i\sin 2\pi sq(k) = 1 + i\cdot 0 = 1$. Lause on näin ollen todistettu. □

Lause 3.10. *Ramanujanin summa*

$$c_s(n) = \sum_{k\in\mathcal{R}_n} \cos\frac{2\pi sk}{n}, \qquad s \in \mathbb{Z}^+.$$

Todistus. (Ks. [9, s. 42–43]). Valitaan $\mathcal{T} = \{-k \ : \ k \in \mathcal{R}_n\}$. Osoitetaan ensin, että $\mathcal{T}$ on $RSS \pmod n$. Olkoon $\mathcal{R}_n = \{r_1, r_2, \ldots, r_{\varphi(n)}\}$ $RRS \pmod n$. Tällöin ensinnäkin $(r_i, n) = 1$ aina, kun $i \in \{1, 2, \ldots, \varphi(n)\}$, joten selvästi $(-r_i, n) = 1$ aina, kun $i \in \{1, 2, \ldots, \varphi(n)\}$. Lisäksi koska $r_i \not\equiv r_j \pmod n$ aina, kun $i \neq j$, niin vastaavasti seurausta 3.1 soveltamalla saadaan, että $-r_i \not\equiv -r_j \pmod n$ aina, kun $i \neq j$. Siis $\mathcal{T}$ on $RSS \pmod n$. Seuraavaksi lauseen 3.9 mukaan

$$\begin{aligned}&\sum_{k\in\mathcal{R}_n} e^{2\pi isk/n} = \sum_{k\in\mathcal{R}_n} e^{2\pi is(-k)/n}\\ \Leftrightarrow\ &\sum_{k\in\mathcal{R}_n}\left\{\cos\frac{2\pi sk}{n} + i\sin\frac{2\pi sk}{n}\right\} = \sum_{k\in\mathcal{R}_n}\left\{\cos\frac{2\pi s(-k)}{n} + i\sin\frac{2\pi s(-k)}{n}\right\}\\ \Leftrightarrow\ &\sum_{k\in\mathcal{R}_n}\cos\frac{2\pi sk}{n} + i\sum_{k\in\mathcal{R}_n}\sin\frac{2\pi sk}{n} = \sum_{k\in\mathcal{R}_n}\cos\frac{2\pi s(-k)}{n} + i\sum_{k\in\mathcal{R}_n}\sin\frac{2\pi s(-k)}{n}.\end{aligned}$$

Kosinin ja sinin ominaisuuksista tiedetään, että $\cos(-x) = \cos x$ ja $\sin(-x) = -\sin x$, joten saadaan

$$\sum_{k\in\mathcal{R}_n}\cos\frac{2\pi sk}{n} + i\sum_{k\in\mathcal{R}_n}\sin\frac{2\pi sk}{n} = \sum_{k\in\mathcal{R}_n}\cos\frac{2\pi sk}{n} - i\sum_{k\in\mathcal{R}_n}\sin\frac{2\pi sk}{n}.$$

Lisäksi yllä olevasta yhtälöstä seuraa, että

$$\sum_{k\in\mathcal{R}_n}\sin\frac{2\pi sk}{n} = 0,$$

joten Eulerin kaavaa soveltamalla saadaan

$$c_s(n) = \sum_{k \in \mathcal{R}_n} \cos \frac{2\pi sk}{n} - i \cdot 0 = \sum_{k \in \mathcal{R}_n} \cos \frac{2\pi sk}{n}.$$

Täten lause on todistettu. □

Seuraus 3.4. *Jos $n \mid s$, niin $c_s(n) = \varphi(n)$.*

Todistus. (Ks. [9, s. 43]). Oletetaan, että $n \mid s$. On siis olemassa kokonaisluku d siten, että $s = nd$. Näin ollen lauseen 3.10 nojalla ja sijoittamalla luku $s = nd$ saadaan

$$c_s(n) = \sum_{k \in \mathcal{R}_n} \cos \frac{2\pi sk}{n} = \sum_{k \in \mathcal{R}_n} \cos \frac{2\pi ndk}{n} = \sum_{k \in \mathcal{R}_n} \cos 2\pi dk = \sum_{k \in \mathcal{R}_n} 1.$$

Nyt summa $\sum_{k \in \mathcal{R}_n} 1$ yhteen laskee niiden positiivisten kokonaislukujen $k \in \mathcal{R}_n$ määrän, missä $k \leq n$ ja $(k, n) = 1$, joten Eulerin funktion määritelmää 2.6 soveltamalla saadaan, että

$$\sum_{k \in \mathcal{R}_n} 1 = \varphi(n).$$

Siis $c_s(n) = \varphi(n)$. □

Lause 3.11. *Ramanujanin summa $c_s(n)$ on multiplikatiivinen muuttujan n suhteen aina, kun $s \in \mathbb{Z}^+$.*

Todistus. (Ks. [9, s. 43]). Selvästi seurauksen 3.4 nojalla $c_s(1) = \varphi(1) = 1$, joten funktio c_s ei ole nollafunktio. Oletetaan, että $(m, n) = 1$. Silloin

$$\begin{aligned} c_s(m)c_s(n) &= \sum_{j \in \mathcal{R}_m} e^{2\pi isj/m} \sum_{k \in \mathcal{R}_n} e^{2\pi isk/n} \\ &= \sum_{\substack{j \in \mathcal{R}_m \\ k \in \mathcal{R}_n}} e^{2\pi is(j/m + k/n)} \\ &= \sum_{\substack{j \in \mathcal{R}_m \\ k \in \mathcal{R}_n}} e^{2\pi is(jn+km)/mn}. \end{aligned}$$

Nyt lauseen 3.8 mukaan joukko $\{jn + km\}$ on $RRS \pmod{mn}$, joten

$$\sum_{\substack{j \in \mathcal{R}_m \\ k \in \mathcal{R}_n}} e^{2\pi is(jn+km)/mn} = c_s(mn),$$

mikä todistaa lauseen. □

Tarkastellaan seuraavaksi geometristä sarjaa

$$\sum_{k=1}^{n} e^{2\pi isk/n} = \begin{cases} e^{2\pi is/n}\frac{(e^{2\pi is/n})^n-1}{e^{2\pi is/n}-1}, & \text{jos } e^{2\pi is/n} \neq 1, \\ n, & \text{jos } e^{2\pi is/n} = 1. \end{cases}$$

Tiedetään, että $e^{2\pi is/n} = \cos\frac{2\pi s}{n} + i\sin\frac{2\pi s}{n} = 1$, jos ja vain jos $n \mid s$. Vastaavasti $(e^{2\pi is/n})^n = e^{2\pi is} = 1$. Siis

$$\sum_{k=1}^{n} e^{2\pi isk/n} = \begin{cases} 0, & \text{jos } n \nmid s, \\ n, & \text{jos } n \mid s. \end{cases}$$

Lisäksi jos luku $n = p^b$, missä p on alkuluku ja b positiivinen kokonaisluku, niin

$$\mathcal{R}_{p^b} = \{k : 1 \leq k \leq p^b\} \setminus \{tp : 1 \leq t \leq p^{b-1}\}.$$

Toisin sanoen joukkoon $\mathcal{R}_{p^b}$ kuuluvat vain ne kokonaisluvut k, jotka kuuluvat välille $[1, p^b]$ ja joilla $(k, p^b) = 1$. Oletetaan, että $p^b||s$, mikä tarkoittaa, että $p^b \mid s$, mutta $p^{b+1} \nmid s$. Tällöin

$$\begin{aligned} c_s(p^b) &= \sum_{k\in\mathcal{R}_{p^b}} e^{2\pi isk/p^b} \\ &= \sum_{k=1}^{p^b} e^{2\pi isk/p^b} - \sum_{t=1}^{p^{b-1}} e^{2\pi istp/p^b} \\ &= \begin{cases} 0, & p^b \nmid s \\ p^b, & p^b \mid s \end{cases} - \begin{cases} 0, & p^{b-1} \nmid s \\ p^{b-1}, & p^{b-1} \mid s \end{cases} \\ &= \begin{cases} 0, & p^{b-1} \nmid s \\ -p^{b-1}, & p^{b-1}||s \\ p^b - p^{b-1}, & p^b \mid s. \end{cases} \qquad \text{[9, s. 43–44]} \end{aligned}$$

Tämän tuloksen avulla pystytään helposti todistamaan seuraava lause.

Lause 3.12. *Olkoot $n, s \in \mathbb{Z}^+$. Silloin*

$$\sum_{d|n} c_s(d) = \begin{cases} n, & \textit{jos } n \mid s, \\ 0, & \textit{jos } n \nmid s. \end{cases}$$

Todistus. (Ks. [9, s. 44]). Multiplikatiivisuuden perusteella lauseen todistamiseksi riittää tarkastella tapausta $n = p^b$, missä p on alkuluku ja b positiivinen kokonaisluku.

Jos $p^b \mid s$, niin seurauksen 3.4 nojalla $c_s(d) = \varphi(d)$ kaikille $d \mid p^b$. Tällöin lauseen 2.12 mukaan $\sum_{d|n} c_s(d) = p^b = n$. Oletetaan sitten, että $p^b \nmid s$, mutta $p^a || s$, missä $0 \leq a < b$. Tällöin

$$\begin{aligned}\sum_{d|p^b} c_s(d) =& c_s(1) + \sum_{j=1}^{a} c_s(p^j) + \sum_{j=a+1}^{b} c_s(p^j) \\ =& 1 + \sum_{j=1}^{a} (p^j - p^{j-1}) + (-p^{(a+1)-1}) \\ =& 1 + (p^1 - p^0 + p^2 - p^1 + \cdots + p^a - p^{a-1}) - p^a \\ =& 1 - p^0 + p^a - p^a \\ =& 0.\end{aligned}$$

Näin lause on todistettu. □

Seuraus 3.5. *Olkoot $n, s \in \mathbb{Z}^+$. Tällöin*

$$c_s(n) = \sum_{\substack{d|n \\ d|s}} \mu\Big(\frac{n}{d}\Big) d.$$

Todistus. (Ks. [9, s. 45]). Olkoon δ_s aritmeettinen funktio, joka määritellään kaavalla

$$\delta_s(n) = \begin{cases} n, \text{ jos } n \mid s \\ 0, \text{ jos } n \nmid s. \end{cases}$$

Lauseen 3.12 nojalla $c_s * u = \delta_s$, missä u on yksikköfunktio. Soveltamalla Möbiuksen käänteiskaavaa 2.10 saadaan $c_s = \delta_s * \mu$. Näin ollen

$$c_s(n) = \sum_{d|n} \delta_s(d) \mu\Big(\frac{n}{d}\Big) = \sum_{\substack{d|n \\ d|s}} \mu\Big(\frac{n}{d}\Big) d,$$

joten lause on todistettu. □

Esimerkki 3.4. ([9, s. 45], tehtävä 14-1.) Lasketaan Ramanujanin summa $c_1(n)$ kaikille $n \in \mathbb{Z}^+$. Nyt seurauksen 3.5 nojalla saadaan, että

$$c_1(n) = \sum_{\substack{d|n \\ d|1}} \mu\Big(\frac{n}{d}\Big) d = \mu\Big(\frac{n}{1}\Big) = \mu(n), \qquad n \in \mathbb{Z}^+.$$

Lause 3.13. ([9, s. 45], tehtävä 14-2.) *Funktio δ_s on multiplikatiivinen.*

Todistus. Tiedetään, että lauseen 3.11 nojalla Ramanujanin summa c_s on multiplikatiivinen. Näin ollen seurauksen 3.5 todistuksen ja seurauksen 2.1 mukaan funktio δ_s on multiplikatiivinen. □

4 Tekijäfunktioiden ominaisuuksia

4.1 Tekijäfunktio

Määritellään aritmeettinen funktio nimeltään tekijäfunktio ja osoitetaan, että tekijäfunktiot ovat multiplikatiivisia.

Määritelmä 4.1. (Vrt. [2, s. 38]). Olkoon $\alpha \in \mathbb{R}$. *Tekijäfunktio* σ_α on aritmeettinen funktio, joka määritellään kaavalla

$$\sigma_\alpha(n) = \sum_{d|n} d^\alpha.$$

Huomautus. Kun $\alpha = 0$, niin tekijäfunktio $\sigma_0(n)$ ilmaisee luvun n positiivisten tekijöiden lukumäärän ja sitä merkitään $\tau(n)$. Kun $\alpha = 1$, niin tekijäfunktio $\sigma_1(n)$ ilmaisee luvun n positiivisten tekijöiden summan ja tätä merkitään $\sigma(n)$.

Merkintä. Merkitään symbolilla N^α sellaista aritmeettista funktiota, että $N^\alpha = n^\alpha$, kun $n \in \mathbb{Z}^+$ ja $\alpha \in \mathbb{R}$ [2, s. 34].

Huomautus. Funktio N^α on multiplikatiivinen.

Lause 4.1. *Tekijäfunktio σ_α on multiplikatiivinen.*

Todistus. (Ks. [2, s. 38]). Kirjoitetaan $\sigma_\alpha = u * N^\alpha$, missä u on multiplikatiivinen yksikköfunktio. Siis lauseen 2.4 nojalla tekijäfunktio σ_α on multiplikatiivinen. □

Lause 4.2. *Olkoot p alkuluku ja a positiivinen kokonaisluku. Tällöin*

$$\sigma(p^a) = \frac{p^{a+1} - 1}{p - 1}$$

ja

$$\tau(p^a) = a + 1.$$

Todistus. (Ks. [13, s. 252]). Huomataan, että luvun p^a tekijät ovat $1, p, p^2, \ldots, p^a$ ja niitä on $a + 1$ kappaletta. Näin ollen $\sigma(p^a) = 1 + p + p^2 + \cdots + p^a = \frac{p^{a+1}-1}{p-1}$ ja $\tau(p^a) = a + 1$. □

Huomautus. Olkoot p alkuluku, $\alpha \in \mathbb{R}$ ja $a \in \mathbb{Z}^+$. Silloin

$$\sigma_\alpha(p^a) = 1^a + p^a + p^{2a} + \cdots + p^{a\alpha} = \begin{cases} \frac{p^{\alpha(a+1)}-1}{p^\alpha - 1}, & \text{jos } \alpha \neq 0, \\ a + 1, & \text{jos } \alpha = 0. \end{cases} \quad \text{[2, s. 38–39]}$$

Esimerkki 4.1. Lasketaan tekijäfunktioiden $\sigma_2(6)$ ja $\sigma_3(7)$ arvot. Nyt määritelmän 4.1 nojalla

$$\sigma_2(6) = \sum_{d|6} d^2 = 1^2 + 2^2 + 3^2 + 6^2 = 50.$$

Lisäksi saadaan

$$\sigma_3(7) = \sum_{d|7} d^3 = 1^3 + 7^3 = 344,$$

minkä vaihtoehtoinen ratkaisutapa on lauseen 4.2 huomautuksen nojalla

$$\sigma_3(7) = \frac{7^{3(1+1)} - 1}{7^3 - 1} = 344.$$

Lause 4.3. *Olkoon positiivisen kokonaisluvun n kanoninen alkutekijähajotelma $n = p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}$. Tällöin*

$$\sigma(n) = \prod_{j=1}^{s} \frac{p_j^{a_j+1} - 1}{p_j - 1}$$

ja

$$\tau(n) = \prod_{j=1}^{s} (a_j + 1).$$

Todistus. (Ks. [13, s. 252]). Lauseen 4.1 nojalla funktiot σ ja τ ovat multiplikatiivisia. Silloin lausetta 4.2 käyttämällä saadaan

$$\begin{aligned}
\sigma(n) =& \sigma(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}) \\
=& \sigma(p_1^{a_1}) \sigma(p_2^{a_2}) \cdots \sigma(p_s^{a_s}) \\
=& \frac{p_1^{a_1+1} - 1}{p_1 - 1} \cdot \frac{p_2^{a_2+1} - 1}{p_2 - 1} \cdots \frac{p_s^{a_s+1} - 1}{p_s - 1} \\
=& \prod_{j=1}^{s} \frac{p_j^{a_j+1} - 1}{p_j - 1}.
\end{aligned}$$

Vastaavalla tavalla

$$\begin{aligned}
\tau(n) =& \tau(p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s}) \\
=& \tau(p_1^{a_1}) \tau(p_2^{a_2}) \cdots (p_s^{a_s}) \\
=& (a_1 + 1)(a_2 + 1) \cdots (a_s + 1) \\
=& \prod_{j=1}^{s} (a_j + 1).
\end{aligned}$$

□

Esimerkki 4.2. Lasketaan lauseen 4.3 perusteella, että

$$\sigma(99) = \sigma(3^2 \cdot 11) = \frac{3^{2+1} - 1}{3 - 1} \cdot \frac{11^{1+1} - 1}{11 - 1} = 13 \cdot 12 = 156$$

ja

$$\tau(3^2 \cdot 11) = (2 + 1)(1 + 1) = 6.$$

4.2 Marin Mersenne

Marin Mersenne (1588–1648) oli ranskalainen teologi, filosofi ja matemaatikko. Mersenne opiskeli jesuiittojen oppilaitoksessa La Flèchessä ja jatkoi Pariisin yliopistoon opiskelemaan teologiaa. Vuonna 1611 Mersenne liittyi roomalaiskatoliseen ryhmään nimeltä *Minims*, joka tulee sanasta *minimi* tarkoittaen, että jokainen ryhmän jäsen pitää itseään pienimpänä tai vähäisimpänä. Mersenne vihittiin papiksi vuonna 1612 ja hän opetti filosofiaa vuosina 1614–1618 luostarissa Neversin kaupungissa. Vuonna 1619 Mersenne palasi Pariisiin, jossa hän järjesti kohtaamispaikan tiedemiehille, filosofeille ja matemaatikoille, kuten Pierre de Fermat'lle ja Blaise Pascalille. [13, s. 258]

Mersenne kirjoitti elämänsä aikana kirjoja matematiikasta, mekaniikasta, fysiikasta, musiikista ja akustiikasta. Hän tutki alkulukuja ja epäonnistuen yritti kehittää kaavan kaikkien alkulukujen esittämiseen. Vuonna 1644 hän väitti luetelleensa kaikki alkuluvut $p \leq 257$, missä $2^p - 1$ on alkuluku. Kyseinen tulos on kaukana nykyisestä tietämyksestä. [13, s. 258] Hänen mukaansa kuitenkin nimettiin Mersennen alkuluvut, joita käsitellään seuraavaksi.

4.3 Mersennen alkuluku ja täydellinen luku

Seuraavaksi tutkitaan täydellistä lukua, joka on itseään pienempien positiivisten tekijöiden summa. Tiettyjen mystisten uskomusten vuoksi jo antiikin kreikkalaiset olivat kiinnostuneita tämän kaltaisista luvuista ja tiesivät, kuinka määrittää kaikki parilliset täydelliset luvut. [13, s. 256] Esimerkiksi luku 6 on täydellinen luku, sillä sitä itseään pienemmät positiiviset tekijät ovat 1, 2 ja 3 ja niiden summa on 6.

Tässä alaluvussa osoitetaan, että kaikki parilliset täydelliset luvut voidaan laskea Mersennen alkulukujen avulla. Mersennen alkuluvut ovat muotoa $2^p - 1$, missä p on alkuluku. Mersennen alkulukujen etsintä on alkanut antiikin ajoilta ja uusia lukuja on löydetty kiihtyvällä tahdilla tehokkaiden tietokoneiden ja internetin kehittyessä

[13, s. 239]. Tähän päivään mennessä suurin Mersennen alkuluku on 51. Mersennen alkuluku $2^{82\,589\,933} - 1$, joka löydettiin 7.12.2018 [17].

Määritelmä 4.2. (Vrt. [13, s. 258]). Kokonaislukuja $M_n = 2^n - 1$, missä n on positiivinen kokonaisluku, kutsutaan *Mersennen luvuiksi*.

Määritelmä 4.3. (Vrt. [13, s. 258]). Alkulukuja $M_p = 2^p - 1$, missä p on alkuluku, kutsutaan *Mersennen alkuluvuiksi*.

Lause 4.4. *Jos $n \in \mathbb{Z}^+$ ja $2^n - 1$ on alkuluku, niin n on alkuluku.*

Todistus. (Ks. [13, s. 257–258]). Oletetaan, että $2^n - 1$ on alkuluku, missä $n \in \mathbb{Z}^+$. Tehdään vastaoletus, että n ei ole alkuluku. Silloin $n = ab$, missä $1 < a, b < n$. Tällöin luku $2^n - 1$ voidaan esittää muodossa

$$2^{ab} - 1 = (2^a - 1)(2^{a(b-1)} + 2^{a(b-2)} + \cdots + 2^a + 1).$$

Huomataan, että lausekkeen oikealla puolella molemmat tulon tekijät ovat suurempia kuin 1, joten $2^n - 1$ ei ole alkuluku, jos n ei ole alkuluku. Päädytään ristiriitaan, joten jos $2^n - 1$ on alkuluku, niin n on alkuluku. □

Määritelmä 4.4. (Vrt. [1, s. 179]). Kokonaislukua $n \geq 2$ sanotaan *täydelliseksi luvuksi*, jos sen tekijöiden summa on $2n$, toisin sanoen $\sigma(n) = 2n$.

Lause 4.5. *Jos M_p on Mersennen alkuluku, niin $n = 2^{p-1}M_p$ on täydellinen luku.*

Todistus. (Ks. [1, s. 179]). Oletetaan, että $M_p = 2^p - 1$ on Mersennen alkuluku. Nyt koska luku $2^p - 1$ on pariton, niin $(2^{p-1}, 2^p - 1) = 1$. Lauseen 4.1 mukaan tekijäfunktio σ on multiplikatiivinen. Tällöin lauseen 4.2 nojalla

$$\sigma(2^{p-1}) = \frac{2^{p-1+1} - 1}{2 - 1} = 2^p - 1$$

ja lisäksi määritelmän 4.1 mukaan

$$\sigma(2^p - 1) = \sum_{d|2^p-1} d = 1 + 2^p - 1 = 2^p,$$

joten saadaan

$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = (2^p - 1) \cdot 2^p = 2 \cdot 2^{p-1} \cdot (2^p - 1) = 2n.$$

Siis määritelmän 4.4 mukaan luku $n = 2^{p-1}M_p$ on täydellinen luku. □

Esimerkki 4.3. Luku 28 on täydellinen luku, sillä $\sigma(28) = 1+2+4+7+14+28 = 56 = 2\cdot 28$. Sama voidaan nähdä myös lauseen 4.5 perusteella, sillä $28 = 2^{3-1}\cdot(2^3-1)$ on täydellinen luku.

Lause 4.6. *Jos n on parillinen täydellinen luku, niin $n = 2^{p-1}M_p$, missä M_p on Mersennen alkuluku.*

Todistus. (Ks. [1, s. 179]). Oletetaan, että n on parillinen täydellinen luku. Olkoon $n = 2^r s$, missä $r \geq 1$ ja s on pariton. Koska n on täydellinen luku, niin $\sigma(n) = 2n$ eli $\sigma(2^r s) = 2\cdot 2^r s = 2^{r+1}s$. Koska $(2^r, s) = 1$, niin lauseiden 4.1 ja 4.2 nojalla saadaan

$$\sigma(2^r s) = \sigma(2^r)\sigma(s) = \frac{2^{r+1}-1}{2-1}\sigma(s) = (2^{r+1}-1)\sigma(s).$$

Tästä seuraa, että

$$(2^{r+1}-1)\sigma(s) = 2^{r+1}s.$$

Koska luku $2^{r+1}-1$ on pariton, niin $(2^{r+1}-1, 2^{r+1}) = 1$. Tällöin $2^{r+1} \mid \sigma(s)$, joten $\sigma(s) = 2^{r+1}t$ jollakin kokonaisluvulla t. Siis sijoittamalla funktion $\sigma(s) = 2^{r+1}t$ arvo yhtälöön $(2^{r+1}-1)\sigma(s) = 2^{r+1}s$ saadaan, että $2^{r+1}s = (2^{r+1}-1)2^{r+1}t$ eli $s = (2^{r+1}-1)t$. Osoitetaan seuraavaksi, että $t = 1$. Tehdään vastaoletus, että $t > 1$. Tällöin

$$\sigma(s) \geq 1 + t + (2^{r+1}-1)t > 2^{r+1}t = \sigma(s),$$

mikä johtaa ristiriitaan. Siis vastaoletus on väärin, eli $t = 1$. Näin ollen $s = 2^{r+1}-1 = M_{r+1}$ ja $\sigma(s) = 2^{r+1}$. Jos M_{r+1} ei ole alkuluku, niin $\sigma(s) > 2^{r+1} = \sigma(s)$, mikä on mahdotonta. Lopuksi saadaan siis, että $n = 2^{p-1}M_p$, missä $p = r+1$ ja M_p on Mersennen alkuluku. □

4.4 Pierre de Fermat

Kuuluisa ranskalainen lakimies Pierre de Fermat (1601–1665) oli yksi merkittävimmistä harrastelijamatemaatikoista. Hänen lapsuudestaan ja koulutuksestaan ei ole paljoa tietoa, mutta hän todennäköisesti sai perusopetuksensa paikallisessa ranskalaisessa koulussa. Fermat opiskeli ranskan kielen lisäksi espanjaa, italiaa, latinaa ja kreikkaa [12, s. 103]. 1620-luvulla Fermat asui Bordeaux'ssa, jossa hän aloitti ensimmäiset matemaattiset tutkimuksensa [10, s. 109]. Hän alkoi rekonstruoimaan eli selvittämään antiikin ajan matemaatikko Apollonioksen hävinneen teoksen sisältöä saatavilla olevan tiedon pohjalta [5, s. 489].

Fermat opiskeli oikeustiedettä Orléansin yliopistossa ja suoritti tutkinnon yksityisoikeudesta. Vuonna 1631 Fermat toimi lakimiehenä ja valtion virkamiehenä Tolousessa. [10, s. 109] Hänen tehtäviinsä kuului Ranskan kuninkaalle osoitettujen vetoomusten käsitteleminen. Fermat'n laki- ja parlamentaarinen ura kukoisti. Vuonna 1638 hänet valittiin rikostuomioistuimen jäseneksi ja vuonna 1648 hänet nimettiin kuninkaan neuvonantajaksi. [12, s. 104]

Kaiken aikaa Fermat oli kuitenkin omistautunut matematiikalle. Hän kehitti useita pääideoita differentiaali- ja integraalilaskennassa, kuten tangenttisuoran määrittämisen käyrän tiettyyn pisteeseen tai polynomifunktion maksimi- ja minimiarvon selvittämisen. Fermat oli matemaatikko René Descartesin rinnalla yksi analyyttisen geometrian keksijöistä ja Blaise Pascalin kanssa he loivat todennäköisyysteorian perusteet. Lukuteorian osalta hän esitti Fermat'n pienen lauseen 3.3, jolle Euler antoi myöhemmin todistuksen. Fermat tunnetaan myös Fermat'n suuresta lauseesta, jota käsiteltiin tutkielman toisessa luvussa. [12, s. 104]

Fermat ei juurikaan itse julkaissut matemaattisia löydöksiään [13, s. 128]. Hänellä oli tapana ratkaista ongelmia ja esittää tutkimuksensa matemaattiselle yhteisölleen [10, s. 110]. Fermat oli kirjeenvaihdossa muun muassa Descartesin ja Mersennen kanssa. Fermat'n kuoleman jälkeen hänen poikansa alkoi julkaisemaan Fermat'n muistiinpanoja ja teoksia hänen tuloksistaan. [12, s. 105] [13, s. 128]

4.5 Fermat'n luvut

Syvennytään seuraavaksi tarkemmin aritmeettiseen funktioon F_n eli Fermat'n lukuihin.

Määritelmä 4.5. (Vrt. [13, s. 131]). Kokonaislukuja $F_n = 2^{2^n} + 1$, missä n on positiivinen kokonaisluku, kutsutaan *Fermat'n luvuiksi*.

Fermat väitti Pascalille osoitetussa kirjeessään vuonna 1654, että kaikki luvut muotoa $F_n = 2^{2^n} + 1$ ovat alkulukuja, mutta Euler kumosi tämän väitteen vuonna 1732 osoittamalla, että $F_5 = 2^{2^5} + 1 = 4\ 294\ 967\ 297 = 641 \cdot 6\ 700\ 417$ onkin yhdistetty luku [12, s. 109]. Tämän jälkeen heräsi kysymys siitä, onko olemassa äärettömän monta alkulukua muotoa $2^{2^n} + 1$ ja asian selvittämiseen on käytetty valtavasti vaivannäköä. Tähän päivään mennessä tunnetaan vain viisi alkuluvullista Fermat'n lukua, jotka ovat $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ ja $F_4 = 65\ 537$. Monet matemaatikot uskovat, ettei muita Fermat'n alkulukuja ole olemassa. [13, s. 132]

Osoitetaan Fermat'n lukuihin liittyviä perustuloksia, joiden avulla pystytään todistamaan, että alkulukuja on ääretön määrä.

Lause 4.7. *Olkoon $n \in \mathbb{Z}^+$. Silloin $F_n = F_0F_1 \cdots F_{n-1} + 2$.*

Todistus. (Ks. [13, s. 133–134]). Todistetaan lause induktiolla.
1. Perusaskel. Osoitetaan, että väite on tosi, kun $n = 1$.
Saadaan $F_0 + 2 = 3 + 2 = 5 = F_1$.
2. Induktioaskel. Oletetaan, että väite on tosi, kun $n = k$ eli $F_k = F_0F_1 \cdots F_{k-1} + 2$.
Tällöin

$$\begin{aligned} F_0F_1 \cdots F_{k-1}F_k + 2 &= (F_0F_1 \cdots F_{k-1}) \cdot F_k + 2 \\ &= (F_k - 2) \cdot F_k + 2 && \text{(induktio-oletus)} \\ &= (2^{2^k} + 1 - 2) \cdot (2^{2^k} + 1) + 2 && \text{(määritelmä 4.5)} \\ &= (2^{2^k} - 1)(2^{2^k} + 1) + 2 \\ &= (2^{2^k})^2 - 1 + 2 \\ &= 2^{2^{k+1}} + 1 = F_{k+1}. \end{aligned}$$

3. Johtopäätös. Induktioperiaatteen nojalla lause on saatu todistettua. □

Lause 4.8. *Jos m ja n keskenään erisuuria positiivisia kokonaislukuja, niin tällöin $(F_m, F_n) = 1$.*

Todistus. (Ks. [13, s. 134]). Oletetaan, että m ja n keskenään erisuuria positiivisia kokonaislukuja siten, että $m < n$. Nyt lauseen 4.7 nojalla tiedetään, että

$$F_n = F_0F_1 \cdots F_m \cdots F_{n-1} + 2.$$

Oletetaan sitten, että luku d on lukujen F_m ja F_n yhteinen tekijä. Tällöin jaollisuuden perusominaisuuksien nojalla

$$d \mid (F_n - F_0F_1 \cdots F_m \cdots F_{n-1}) = 2.$$

Koska $d \mid 2$, niin joko $d = 1$ tai $d = 2$. Nyt koska Fermat'n lukujen määritelmän 4.5 nojalla luvut F_m ja F_n ovat parittomia, niin luku $d \neq 2$. Siis $d = 1$, jolloin $(F_m, F_n) = 1$. □

Lause 4.9. *Alkulukuja on ääretön määrä.*

Todistus. (Ks. [13, s. 134]). Tiedetään, että on olemassa äärettömän monta Fermat'n lukua F_n, joilla on aritmetiikan peruslauseen nojalla alkulukutekijä p_n. Koska lauseen 4.8 perusteella $(F_m, F_n) = 1$ aina, kun $m \neq n$, niin $p_m \neq p_n$. Näin ollen alkulukuja on oltava ääretön määrä. □

4.6 Tekijäfunktion keskiarvo

Tässä luvussa selvitetään, millaisia arvoja tekijäfunktio $\tau(n)$ saa suurilla luvun n arvoilla. Tämä luku perustuu lähteeseen [2, s. 52–59] merkittyä poikkeusta lukuun ottamatta. Tekijäfunktiolla $\tau(n)$ merkitään luvun n positiivisten tekijöiden lukumäärää. Tekijäfunktio $\tau(p) = 2$, kun p on alkuluku ja $\tau(p^k) = k+1$ ($k \in \mathbb{Z}^+$), jossa luku $k+1$ lähestyy ääretöntä, kun luku $n = p^k$ lähestyy ääretöntä. Näin ollen tekijäfunktion $\tau(n)$ arvot vaihtelevat suuresti luvun n kasvaessa.

Monien aritmeettisten funktioiden arvot vaihtelevat kyseisellä tavalla, joten on haastavaa arvioida niiden käyttäytymistä suurille luvun n arvoille. Joissakin tilanteissa on kannattavaa tarkastella aritmeettisen funktion keskiarvoa

$$\tilde{f}(n) = \frac{1}{n} \sum_{k=1}^{n} f(k),$$

sillä keskiarvon tutkiminen tasoittaa funktion arvon vaihtelua. Myöhemmin todistetaan, että tekijäfunktion keskiarvo $\tilde{\tau}(n)$ kasvaa yhtä nopeasti kuin logaritmifunktio $\log n$. Toisin sanoen

$$\lim_{n\to\infty} \frac{\tilde{\tau}(n)}{\log n} = 1.$$

Tällöin sanotaan, että funktion $\tau(n)$ *keskiarvo* on $\log n$.

Aloitetaan keskiarvon määrittäminen kiinnittämällä huomio aritmeettisen funktion osasummien merkintään.

Merkintä. Jos funktio f on aritmeettinen funktio, käytetään merkintää

$$\sum_{k\le x} f(k)$$

tarkoittamaan summaa

$$\sum_{k=1}^{[x]} f(k),$$

missä luku $[x]$ on suurin sellainen kokonaisluku, joka ei ylitä luvun x arvoa. Jos $0 < x < 1$, niin summa $\sum_{k=1}^{[x]} f(k)$ on tyhjä ja sen määritellään saavan arvoksi nolla.

Tavoitteena on määrittää summan $\sum_{k\le x} f(k)$ arvo erityisesti suurilla luvun x arvoilla. Tässä luvussa osoitetaan tekijäfunktioille Dirichlet'n keksimä kaava vuodelta 1849, jonka mukaan

$$\sum_{k\le x} \tau(k) = x \log x + (2C - 1)x + O(\sqrt{x}) \tag{4.1}$$

kaikille $x \geq 1$. Tässä luku C on *Eulerin vakio*, joka määritellään kaavalla

$$C = \lim_{n\to\infty}\Big(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} - \log n\Big).$$

Symbolilla $O(\sqrt{x})$ kuvataan muuttujan x funktiota, jonka arvo ei kasva nopeammin kuin jokin vakio kerrottuna luvulla $\sqrt{x}$. Tämä on yksi esimerkki iso O- notaatiosta, joka määritellään seuraavaksi.

Määritelmä 4.6. (Iso O- notaatio) Olkoon funktio $g(x) > 0$ kaikille luvuille $x \geq a$, missä a on jokin positiivinen reaaliluku. Merkitään

$$f(x) = O(g(x))$$

ilmaisemaan, että funktioiden osamäärä $\frac{f(x)}{g(x)}$ on rajoitettu kaikilla $x \geq a$. Toisin sanoen on olemassa sellaiset vakiot $M > 0$ ja a, että

$$\frac{|f(x)|}{g(x)} \leq M \qquad \text{kaikille } x \geq a.$$

Merkintä

$$f(x) = h(x) + O(g(x))$$

tarkoittaa, että

$$f(x) - h(x) = O(g(x)).$$

Jos

$$f(t) = O(g(t)), \text{ kun } t \geq a,$$

niin

$$\int_a^x f(t)dt = O\Big(\int_a^x g(t)dt\Big), \text{ kun } t \geq a.$$

Esimerkki 4.4. Nyt $\cos(x) = O(1)$, sillä on olemassa vakio $M = 2$ siten, että

$$\frac{|\cos x|}{1} \leq 2 \qquad \text{kaikille } x \geq 0.$$

Määritelmä 4.7. Jos

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1,$$

niin tällöin funktion $f(x)$ sanotaan *lähestyvän asymptoottisesti* funktiota $g(x)$, kun $x \to \infty$. Tätä merkitään

$$f(x) \sim g(x), \qquad \text{kun } x \to \infty.$$

Esimerkki 4.5. Yhtälö (4.1) tarkoittaa, että

$$\sum_{k\le x}\tau(k) \sim x\log x, \qquad \text{kun } x\to\infty.$$

Yhtälössä (4.1) termiä $x\log x$ kutsutaan osasumman $\sum_{k\le x}\tau(k)$ *asymptoottiseksi arvoksi*. Kaksi muuta termiä $(2C-1)x+O(\sqrt{x})$ edustavat *virhetermiä*, jota merkitään symbolilla $E(x)$. Siis yhtälössä (4.1)

$$E(x) = (2C-1)x + O(\sqrt{x}),$$

josta seuraa, että $E(x) = O(x)$. Vastaavasti funktion $E(x)$ asymptoottinen arvo on $(2C-1)x$.

Esitellään seuraavaksi Eulerin summakaava, joka antaa tarkan lausekkeen virhetermille.

Lause 4.10 (Eulerin summakaava)**.** *Jos funktio f on jatkuvasti derivoituva suljetulla välillä $[y,x]$, missä $0<y<x$, niin*

$$\sum_{y<n\le x} f(n) = \int_y^x f(t)dt + \int_y^x (t-[t])f'(t)dt + f(x)([x]-x) - f(y)([y]-y).$$

Todistus. Merkitään $m=[y]$ ja $k=[x]$. Olkoot kokonaisluvut $n, n-1 \in [y,x]$, ja olkoon luku $t\in[n-1,n]$, jolloin $[t]=n-1$. Tällöin

$$\begin{aligned}\int_{n-1}^{n}[t]f'(t)dt =& (n-1)\int_{n-1}^{n} f'(t)dt\\ =&(n-1)\big(f(n)-f(n-1)\big)\\ =&nf(n)-(n-1)f(n-1)-f(n).\end{aligned}$$

Lasketaan yllä olevan integraalin summa arvosta $n=m+2$ arvoon $n=k$. Saadaan

$$\begin{aligned}\sum_{n=m+2}^{k}\int_{n-1}^{n}[t]f'(t)dt &= \sum_{n=m+2}^{k}\big(nf(n)-(n-1)f(n-1)-f(n)\big)\\ \Leftrightarrow \int_{m+1}^{k}[t]f'(t)dt &= \sum_{n=m+2}^{k}\big(nf(n)-(n-1)f(n-1)\big) - \sum_{n=m+2}^{k} f(n)\\ &=(m+2)f(m+2)-(m+1)f(m+1)\\ &\quad +(m+3)f(m+3)-(m+2)f(m+2)+\cdots\end{aligned}$$

$$
\begin{aligned}
&+ kf(k) - (k-1)f(k-1) - \sum_{n=m+2}^{k} f(n) \\
=&kf(k) - (m+1)f(m+1) - \sum_{n=m+2}^{k} f(n) \\
=&kf(k) - mf(m+1) - \sum_{n=m+1}^{k} f(n) \\
=&kf(k) - mf(m+1) - \sum_{y<n\leq x} f(n).
\end{aligned}
$$

Tällöin

$$
\begin{aligned}
\sum_{y<n\leq x} f(n) &= -\int_{m+1}^{k} [t]f'(t)dt + kf(k) - mf(m+1) \\
&= -\int_{y}^{x} [t]f'(t)dt + \int_{k}^{x} [t]f'(t)dt + \int_{y}^{m+1} [t]f'(t)dt + kf(k) - mf(m+1) \\
&= -\int_{y}^{x} [t]f'(t)dt + kf(x) - kf(k) + mf(m+1) - mf(y) \\
&\quad + kf(k) - mf(m+1) \\
&= -\int_{y}^{x} [t]f'(t)dt + kf(x) - mf(y).
\end{aligned}
$$

Lasketaan seuraavaksi $\int_y^x f(t)dt$ osittaisintegrointisääntöä käyttämällä. Valitaan nyt $g(t) = t$, joten $g'(t) = 1$. Silloin

$$
\begin{aligned}
\int_{y}^{x} f(t)dt &= \Big|_{y}^{x} tf(t) - \int_{y}^{x} tf'(t)dt \\
&= xf(x) - yf(y) - \int_{y}^{x} tf'(t)dt.
\end{aligned}
$$

Nyt saadaan

$$
\begin{aligned}
\sum_{y<n\leq x} f(n) - \int_{y}^{x} f(t)dt &= -\int_{y}^{x} [t]f'(t)dt + kf(x) - mf(y) \\
&\quad -\left(xf(x) - yf(y) - \int_{y}^{x} tf'(t)dt\right)
\end{aligned}
$$

$$= \int_y^x (t - [t]) f'(t) dt + f(x)(k - x) - f(y)(m - y)$$
$$= \int_y^x (t - [t]) f'(t) dt + f(x)([x] - x) - f(y)([y] - y),$$

sillä oli merkitty, että $m = [y]$ ja $k = [x]$. Näin on saatu todistettua, että

$$\sum_{y<n<x} f(n) = \int_y^x f(t) dt + \int_y^x (t - [t]) f'(t) dt + f(x)([x] - x) - f(y)([y] - y).$$

□

Lause 4.11. *Jos $x \geq 1$, niin*

$$\sum_{n \leq x} \frac{1}{n} = \log x + C + O\left(\frac{1}{x}\right),$$

missä C on Eulerin vakio.

Todistus. Oletetaan, että $x \geq 1$ ja $y = 1$. Merkitään $f(t) = \frac{1}{t}$, jolloin $f'(t) = -\frac{1}{t^2}$. Lauseen 4.10 nojalla saadaan, että

$$\sum_{y<n\leq x} \frac{1}{n} = \int_1^x \frac{dt}{t} - \int_1^x \frac{t - [t]}{t^2} dt - \frac{x - [x]}{x} - \frac{[y] - y}{y}.$$

Lisätään yhtälön molemmille puolille luku 1. Lisäksi havaitaan, että

$$\frac{x - [x]}{x} \leq \frac{1}{x}$$

ja $[y] - y = 0$. Tällöin

$$\sum_{y<n\leq x} \frac{1}{n} + 1 = \int_1^x \log t - \int_1^x \frac{t - [t]}{t^2} dt + O\left(\frac{1}{x}\right) - 0 + 1$$
$$\Leftrightarrow \sum_{n \leq x} \frac{1}{n} = \log x - 0 - \int_1^x \frac{t - [t]}{t^2} dt + O\left(\frac{1}{x}\right) + 1$$
$$= \log x + 1 - \int_1^\infty \frac{t - [t]}{t^2} dt + \int_x^\infty \frac{t - [t]}{t^2} dt + O\left(\frac{1}{x}\right).$$

Tässä majoranttiperiaatteen nojalla

$$0 \leq \int_x^\infty \frac{t - [t]}{t^2} dt \leq \int_x^\infty \frac{1}{t^2} dt = \frac{1}{x},$$

sillä

$$\int_x^R \frac{1}{t^2}dt = \Big/_x^R -\frac{1}{t} = \frac{1}{x} - \frac{1}{R} \to \frac{1}{x},$$

kun $R \to \infty$, ja näin ollen epäoleellinen integraali suppenee ja

$$\int_x^\infty \frac{1}{t^2}dt = \frac{1}{x}.$$

Täten

$$\sum_{n\le x} \frac{1}{n} = \log x + 1 - \int_1^\infty \frac{t-[t]}{t^2}dt + O\Big(\frac{1}{x}\Big).$$

Huomataan, että

$$1 - \int_1^\infty \frac{t-[t]}{t^2}dt = \lim_{x\to\infty}\Big(\sum_{n\le x}\frac{1}{n} - \log x\Big) = \lim_{x\to\infty}\Big(1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{x} - \log x\Big) = C.$$

Siis lause on täten todistettu. □

Lause 4.12. *Jos $x \ge 1$, niin*

$$\sum_{n\le x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O\big(x^\alpha\big), \qquad \textit{missä } \alpha \ge 0.$$

Todistus. Oletetaan, että $x \ge 1$ ja $y = 1$. Merkitään $f(t) = t^\alpha$ $(t \ge 1)$, jolloin $f'(t) = \alpha t^{\alpha-1}$, $\alpha \ge 0$. Lausetta 4.10 soveltamalla saadaan

$$\sum_{n\le x} n^\alpha = \int_1^x t^\alpha dt + \alpha \int_1^x t^{\alpha-1}(t-[t])dt - x^\alpha(x-[x]) - 0 + 1.$$

Tässä

$$0 \le \alpha \int_1^x t^{\alpha-1}(t-[t])dt \le \alpha \int_1^x t^{\alpha-1}dt = \alpha \Big/_1^x \frac{t^\alpha}{\alpha} = \alpha\frac{x^\alpha - 1}{\alpha} \le x^\alpha$$

ja selvästi $x^\alpha(x-[x]) \le x^\alpha$ ja $1 \le x^\alpha$. Näin ollen

$$\sum_{n\le x} n^\alpha = \Big/_1^x \frac{t^{\alpha+1}}{\alpha+1} + O\big(x^\alpha\big) = \frac{x^{\alpha+1}}{\alpha+1} - \frac{1}{\alpha+1} + O\big(x^\alpha\big),$$

missä edelleen $\frac{1}{\alpha+1} \le x^\alpha$. Näin ollen lause on todistettu ja saadaan

$$\sum_{n\le x} n^\alpha = \frac{x^{\alpha+1}}{\alpha+1} + O\big(x^\alpha\big).$$

□

Lause 4.13 (Tekijäfunktion keskiarvo)**.** *Kaikille $x \geq 1$ on voimassa kaava*

$$\sum_{n \leq x} \tau(n) = x \log x + (2C - 1)x + O(\sqrt{x}), \tag{4.2}$$

missä C on Eulerin vakio.

Todistus. Tiedetään, että $\tau(n) = \sum_{d|n} 1$, joten

$$\sum_{n \leq x} \tau(n) = \sum_{n \leq x} \sum_{d|n} 1.$$

Nyt $d \mid n$, joten kirjoitetaan $n = qd$, jolloin yllä oleva summa on yli kaikkien sellaisten positiivisten kokonaislukuparien q ja d, että $qd \leq x$. Silloin

$$\sum_{n \leq x} \tau(n) = \sum_{\substack{q,d \\ qd \leq x}} 1. \tag{4.3}$$

Tällä tarkoitetaan summaa, joka käy tiettyjen hilapisteiden yli qd-koordinaatistossa. Hilapisteellä tarkoitetaan koordinaatiston pistettä, jonka koordinaatit ovat kokonaislukuja. Yhtälön $qd = n$ määräämät hilapisteet sijaitsevat hyperbelillä, joten summa (4.3) laskee niiden hilapisteiden lukumäärän, jotka sijaitsevat arvoja $n = 1, 2, \ldots, [x]$ vastaavilla hyperbeleillä. Jokaiselle kiinnitetylle positiiviselle kokonaisluvulle $d \leq x$ voidaan ensin laskea ne hilapisteet, jotka sijaitsevat välillä $1 \leq q \leq x/d$, ja summata ne yli kaikilla $d \leq x$.

Tällöin kuvaa 4.1 mukaillen saadaan, että

$$\sum_{n \leq x} \tau(n) = \sum_{d \leq x} \sum_{q \leq x/d} 1.$$

Nyt lauseen 4.12 nojalla, kun $\alpha = 0$, saadaan

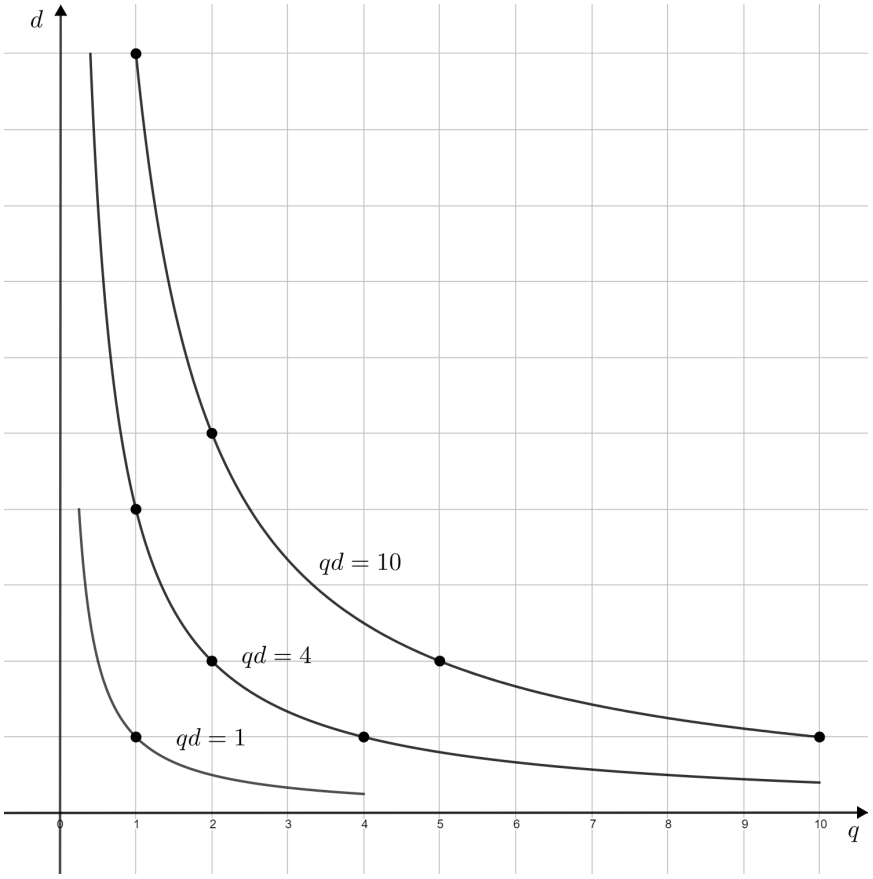
$$\sum_{q \leq x/d} 1 = \frac{x}{d} + O(1).$$

Siis

$$\sum_{d \leq x} \tau(n) = \sum_{d \leq x} \left(\frac{x}{d} + O(1) \right) = x \sum_{d \leq x} \frac{1}{d} + O(x).$$

Käyttämällä seuraavaksi lausetta 4.11 havaitaan, että

$$\begin{aligned} \sum_{d \leq x} \tau(n) &= x \sum_{d \leq x} \frac{1}{d} + O(x) \\ &= x \left(\log x + C + O\left(\frac{1}{x} \right) \right) + O(x) \\ &= x \log x + O(x). \end{aligned}$$



Kuva 4.1

Tämä on lauseessa esitetyn kaavan (4.2) heikompi versio, joka ilmaisee, että

$$\sum_{n \le x} \tau(n) \sim x \log x, \qquad \text{kun } x \to \infty.$$

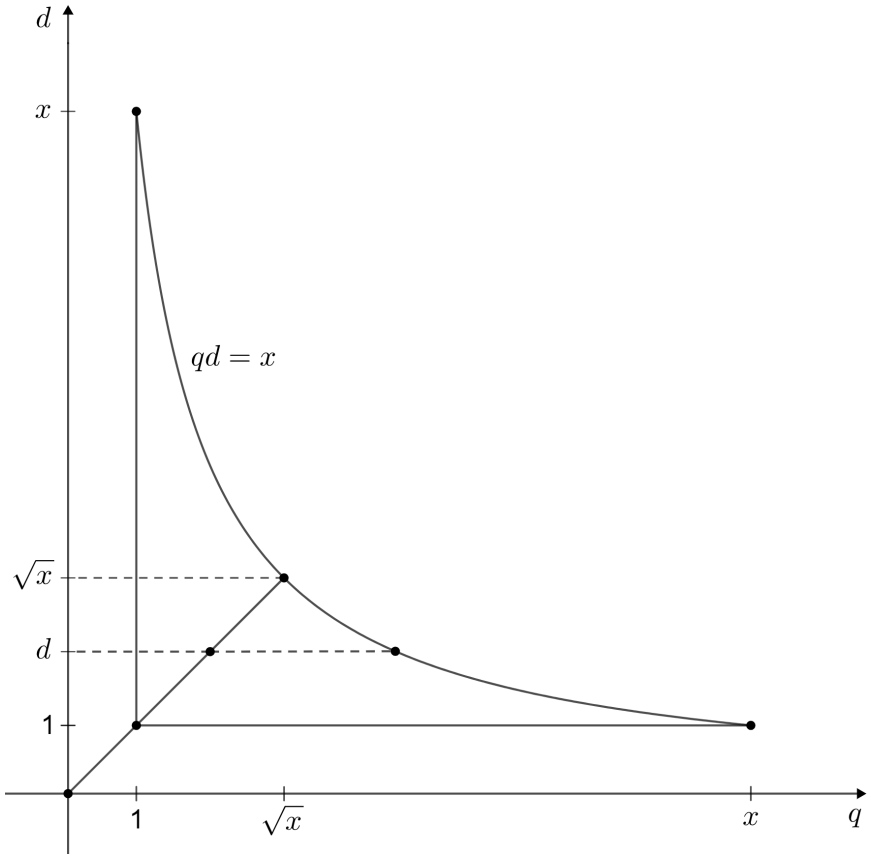
Siis tekijäfunktion $\tau(n)$ keskiarvo on $\log n$.

Todistetaan lauseen kaava (4.2) palaamalla summaan (4.3). Lasketaan niiden hilapisteiden lukumäärä, jotka sijaitsevat hyperbelin $qd = x$ ja suorien $q = 1$ ja $d = 1$ rajaamalla alueella. Suora $q = d$ jakaa kyseisen alueen symmetrisesti kahteen yhtä suureen osaan. Hilapisteiden kokonaislukumäärä saadaan kertomalla kahdella suoran $q = d$ alapuolelle rajaaman alueen hilapisteet ja lisäämällä puolittavan suoran $q = d$ kohdalla olevat hilapisteet.

Tällöin kuvasta 4.2 huomataan, että

$$\sum_{d \le x} \tau(n) = 2 \sum_{d \le \sqrt{x}} \left(\left[\frac{x}{d} \right] - d \right) + [\sqrt{x}].$$

Hyödynnetään seuraavaksi relaatiota $[x] = x + O(1)$ sekä lauseita 4.11 ja 4.12.



Kuva 4.2

Lasketaan

$$\begin{aligned}\sum_{d\le x}\tau(n) =& 2\sum_{d\le\sqrt{x}}\Big(\frac{x}{d}-d+O(1)\Big)+O(\sqrt{x})\\ =& 2x\sum_{d\le\sqrt{x}}\frac{1}{d}-2\sum_{d\le\sqrt{x}}d+O(\sqrt{x})\\ =& 2x\left(\log\sqrt{x}+C+O\Big(\frac{1}{\sqrt{x}}\Big)\right)-2\Big(\frac{(\sqrt{x})^2}{2}+O(\sqrt{x})\Big)+O(\sqrt{x})\\ =& x\log x+(2C-1)x+O(\sqrt{x}).\end{aligned}$$

Näin ollen kaava (4.2) on saatu todistettua. □

Historian aikana kaavan (4.2) virhetermiä $O(\sqrt{x})$ on tarkennettu. Godfrey Harold Hardy ja Edmund Landau osoittivat vuonna 1915, että $\inf\theta \ge 1/4$. Vuonna 1903 Georgy Voronoy todisti, että virhetermi on $O(x^{1/3}\log x)$, vuonna 1922 Johannes van der Corput osoitti virhetermin olevan $O(x^{33/100})$ ja vuonna 1969 Grigori Kolesnik arvioi virhetermiksi $O(x^{(12/37)+\varepsilon})$ kaikille $\varepsilon > 0$. Pienimmän luvun θ määrittäminen, millä virhetermiksi saadaan $O(x^{\theta})$, on ratkaisematon *Dirichlet'n tekijäprobleema*.

Viimeisin tulos on vuodelta 2003, missä Martin Huxley väittää, että $\theta = 131/416$. Tiedetään myös, että Ramanujan oli kiinnostunut Dirichlet'n tekijäprobleemasta. Hän ei parantanut virhetermiä vaan antoi aputuloksia, joita on käytetty virhetermin tarkentamiseen. [4, s. 106]

Lähteet

[1] Andreescu, T. ja Andrica, D. *Number Theory: Structures, Examples, and Problems*. Springer Science & Business Media, Boston, 2009.

[2] Apostol, T. M. *Introduction to Analytic Number Theory*. Springer Science & Business Media, New York, 1976.

[3] Berndt, B. C. ja Rankin, R. A. *Ramanujan: Letters and Commentary (History of Mathematics, Vol 9)*. American Mathematical Society, Rhode Island, 1995.

[4] Berndt, B. C., Sun, K. ja Zaharescu, A. *The circle problem of Gauss and the divisor problem of Dirichlet—Still unsolved*. The American Mathematical Monthly, 125:2, 99-114, 2018.

[5] Boyer, C. *Tieteiden kuningatar: matematiikan historia*. Art House Oy, Helsinki, 1968 (3. painos). Kääntänyt Pietiläinen, K., 2000.

[6] Debnath, L. *The Legacy Of Leonhard Euler: A Tricentennial Tribute*. Imperial College Press, London, 2010.

[7] Erickson, M. ja Vazzana, A. *Introduction to Number Theory*. Chapman & Hall/CRC, Boca Raton, 2008.

[8] Everest, G. ja Ward, T. *An Introduction to Number Theory*. Springer-Verlag, London, 2005.

[9] Gioia, A. A. *The Theory of Numbers*. Markham Publishing Company, Chicago, 1970.

[10] Krantz, S. G. *An Episodic History of Mathematics: Mathematical Culture Through Problem Solving*. Mathematical Association of America, Washington, 2010.

[11] McElroy, T. *A to Z of Mathematicians*. Facts on File, New York, 2005.

[12] Robbins, N. *Beginning Number Theory*. Jones and Bartlett Publishers, Sudbury, 2006 (2. painos).

[13] Rosen, K. H. *Elementary Number Theory*. Sixth edition, Pearson, Harlow, 2014.

[14] Vaidyanathaswamy, R. *The theory of multiplicative arithmetic functions*. Transactions of the American Mathematical Society, Vol. 33, No. 2, 1931.

[15] Britannica, The Editors of Encyclopaedia. *August Ferdinand Möbius*. [Verkkodokumentti, viitattu 2.2.2021]
https://www.britannica.com/biography/August-Ferdinand-Mobius

[16] Britannica, The Editors of Encyclopaedia. *Srinivasa Ramanujan*. [Verkkodokumentti, viitattu 9.3.2021]
https://www.britannica.com/biography/Srinivasa-Ramanujan

[17] GIMPS - Great Internet Mersenne Prime Search, Mersenne Research, Inc. [Verkkodokumentti, viitattu 16.3.2021]
https://www.mersenne.org/primes/?press=M82589933