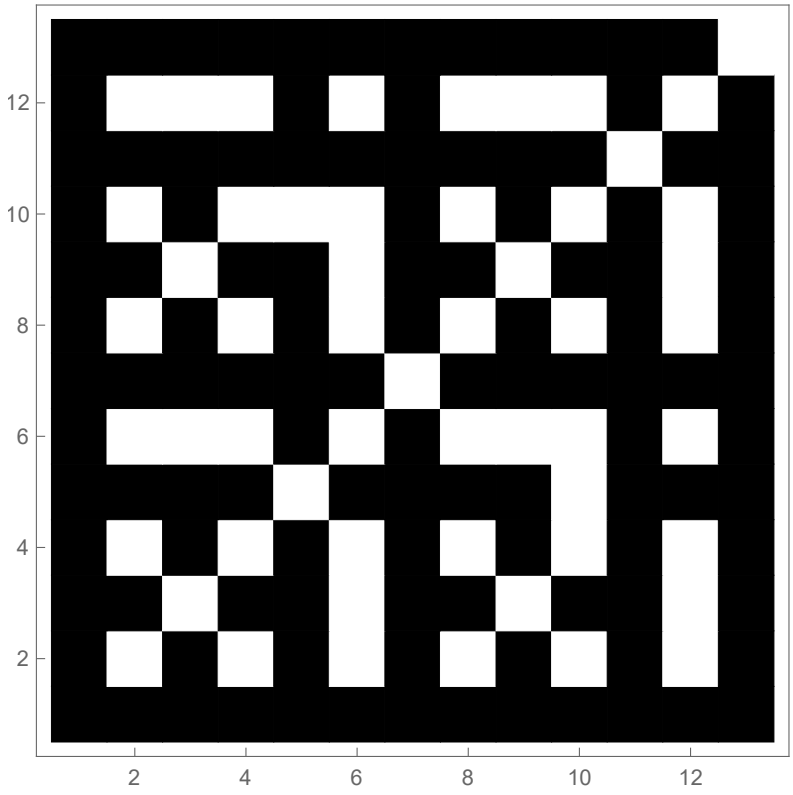
Suhteellisten alkulukuparien todennäköisyys



Kati Kosonen

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos

Kevät 2020

Tiivistelmä: Kati Kosonen, *Suhteellisten alkulukuparien todennäköisyys* (engl. *Probability that two numbers are coprime*), matematiikan pro gradu -tutkielma, 58 sivua, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, kevät 2020.

Tässä tutkielmassa osoitetaan, että kaksi satunnaisesti valittua kokonaislukua ovat keskenään suhteellisia alkulukuja 61% todennäköisyydellä. Tulosta lähestytään lukuteorian näkökulmasta erilaisten funktioiden ja niiden ominaisuuksien avulla. Eulerin φ-funktio on merkittävässä roolissa, sillä tutkielman päätulos on Eulerin funktion keskimääräisen kasvunopeuden näyttäminen. Tämän tuloksen sovelluksena pystytään klassisen todennäköisyyden avulla osoittamaan alkulukuparien todennäköisyys. Tulos keskimääräiselle kasvunopeudelle on merkittävä sen monipuolisten sovellusmahdollisuuksien takia.

Tutkielmassa perehdytään lukuteorian kahteen keskeiseen multiplikatiiviseen funktioon, Eulerin φ-funktioon ja Möbiuksen μ-funktioon. Käydään molempien funktioiden huomionarvoiset tulokset läpi ja osoitetaan, miten funktiot ovat yhteydessä toisiinsa. Möbiuksen funktio on tutkielman tärkeimpiä työkaluja, koska sen yhteydet muihin tutkielmassa esiteltäviin funktioihin ovat päätuloksen kannalta olennaisia.

Analyyttiseen lukuteoriaan syvennytään tutkielman edetessä, kun käsitellään funktiota ζ reaalisten arvojen tapauksessa. Eulerin ζ-funktio määritellään sarjana, mutta se voidaan esittää myös päättymättömänä tulona. Päättymättömät tulot ovat tutkielman käytetyimpiä työkaluja, joten perehdytään niiden teoriaan tarkemmin. Funktioon ζ liittyy myös tunnettu lukuteorian tulos, Baselin ongelma, jolle annetaan kaksi erilaista todistusta.

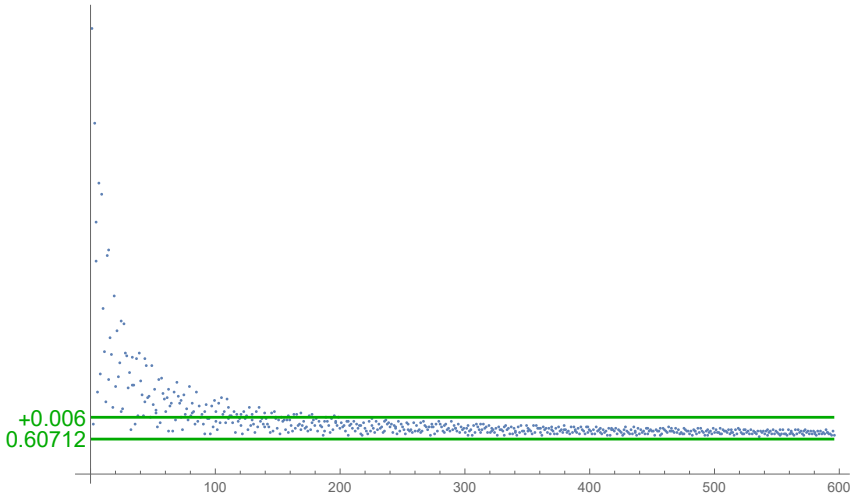
Tutkielmassa tarkastellaan myös toista Eulerin funktion nopeuden sovellusta. Toinen sovellus liittyy Fareyn jonoiksi kutsuttujen murtolukujonojen teoriaan, johon perehdytään vuonna 1747 esitetyn kysymyksen saattelemana. Keskimääräisen kasvunopeuden tuloksen avulla pystytään osoittamaan Fareyn jonojen asymptoottinen pituus.

Tutkielman lopuksi käsitellään suppeasti kompleksianalyysin tuloksia sarjoille, jotta saadaan pohja esitellä kompleksinen ζ-funktio ja sen nollakohdat. Kompleksisen ζ-funktion nollakohtien tarkasteluun liittyy vahvasti tunnetuin lukuteorian avoin ongelma, Riemannin hypoteesi. Käydään läpi millaisia lähestymistapoja matemaatikoilla on ollut vuosien varrella hypoteesin todistamiseksi.

Sisältö

Johdanto

Suhteellisia alkulukuja ovat luvut, joiden suurin yhteinen tekijä on yksi. Tutkiessa lukupareja $(1,1)$, $(1,2)$, $(2,1)$ ja $(2,2)$ huomataan, että neljästä lukuparista kolmessa parissa luvut ovat keskenään suhteellisia alkulukuja, kun tarkastellaan 2×2-ruudukkoa. Ruudukossa 5×5 lukupareja, joissa lukujen suurin yhteinen tekijä on yksi, on 19 paria 25 parista. Todennäköisyys saada satunnaisesti suhteellinen alkulukupari on noin 75%. Todennäköisyys on hyvin korkea näissä tapauksissa. Mitä todennäköisyydelle tapahtuu, kun tarkastellaan ruudukkoa $N \times N$, missä luku N lähestyy ääretöntä? Seuraava kuva 0.1 avaa kysymyksessä olevaa tilannetta.



Kuva 0.1: Suhteellisten alkulukuparien tiheys

Kysymys on muotoiltu tutkielmassa lauseeksi:

Lause 0.1. *Olkoon $N \in \mathbb{N}$. Merkitään suhteellisten alkulukuparien joukkoa*

$$T_N = \{(n, n') \in \mathbb{N} : 1 \leq n, n' \leq N, \mathrm{syt}(n, n') = 1\}$$

ruudukossa $N \times N$. Tällöin

$$\lim_{N \to \infty} \frac{\#T_N}{N^2} = \frac{6}{\pi^2} + \mathrm{O}\left(\frac{\log(N)}{N}\right) \approx 61\%.$$

Todistuksessa sovelletaan klassista todennäköisyyttä ja Eulerin funktion keskimääräistä kasvunopeutta. Yllä muotoiltu lause on suora sovellus Eulerin funktion kasvunopeudesta, mikä on tutkielman päätulos. Päätuloksen todistaminen vaatii monia yksityiskohtaisia tarkasteluja, jotta se olisi mahdollisimman lyhyt ja ytimekäs. Tutkielman merkittävin tulos on muotoiltu lauseeksi:

Lause 0.2. $\Phi(n) = \frac{3n^2}{\pi^2} + \mathrm{O}(n\log(n))$.

Tuloksen todistamiseen tarvittavien yksityiskohtien tarkastelu aloitetaan tutkielman ensimmäisestä luvusta, missä määritellään Eulerin φ-funktio, jonka summafunktio on Φ. Funktio φ on lukuteorian monikäyttöinen funktio monien alkulukuihin liittyvien ominaisuuksien takia. Samassa luvussa tarkastellaan myös Möbiuksen μ-funktiota, jonka tärkeys tutkielmassa on se, että sen avulla voidaan esittää tutkielman muut funktiot. Möbiuksen funktiolle näytetään yhteys Eulerin φ-funktioon ja seuraavassa luvussa huomataan, että μ-funktiolla on yhteys myös Eulerin ζ-funktion kanssa.

Toisessa luvussa tutustutaan Eulerin toiseen tutkielman kannalta merkittävään funktioon, ζ-funktioon. Eulerin ζ-funktio esitetään usein sarjamuodossa ja mielenkiintoisen funktiosta tekee sen, että sen voi esittää myös päättymättömänä tulona. Luvun päätulos on Baselin ongelmaksi kutsuttu tulos, missä tutkitaan ζ-funktion arvoa kiinnitetyssä pisteessä. Tämä tulos on suuri yksityiskohta, mitä tarvitaan keskimääräisen kasvunopeuden todistamisessa. Baselin ongelmalle esitetään kaksi todistusta, joista ensimmäinen seuraa Eulerin alkuperäistä todistusta ja toinen on Tom M. Apostolin tekemä todistus 2-ulotteisen integraalin avulla.

Kolmannen luvun alussa käydään läpi, mitä merkintä $\mathrm{O}(n\log(n))$ tarkoittaa lauseessa, ja mikä yhteys merkinnällä on funktion asymptoottisen käyttäytymisen kanssa. Tämän jälkeen on todistukseen tarvittavat tulokset kerätty kokoon. Tästä saadaan suoraan suhteellisten alkulukuparien todennäköisyys todistettua, kun tiedetään Eulerin funktion keskimääräinen kasvunopeus. Luvun loppuun tutustutaan toiseen hyvin erilaiseen sovellukseen kasvunopeudelle. Fareyn jonoiksi kutsuttu lukuteorian osa-alue soveltaa kasvunopeutta osoittamaan yksittäisen Fareyn jonon pituutta.

Tutkielman viimeisessä luvussa tehdään lyhyt vilkaisu kompleksianalyysin maailmaan, ja laajennetaan Eulerin ζ-funktio kuuluisammaksi Riemannin ζ-funktioksi. Bernhard Riemann oli ensimmäinen matemaatikko, joka näytti ζ-funktion ominaisuuksien pätevän myös kompleksitasossa tietyin ehdoin. Luvussa käsitellään hyvin pintapuolisesti, millaisia tuloksia kompleksisella ζ-funktiolla on ja mitä sen nollakohdista tiedetään. Luvussa puhutaan lyhyesti funktion analyyttisestä jatkamisesta koko kompleksitasoon lukuunottamatta napaa. Tutkielma loppuu Riemannin hypoteesin historiakatsaukseen, jonka avulla pyritään näyttämään, miten matemaatikot ovat hypoteesia pyrkineet vuosien varrella lähestymään, ja millainen vaikutus suomalaisella matemaatikolla on ollut hypoteesin tutkimiseen.

Tutkielman merkittävin lähde on [12], sillä sieltä löytyvät tutkielman päätulokset todistuksineen. Kyseisessä lähteessä on monia sovelluksia Eulerin funktion kasvunopeudelle. Muilla lähteillä on pyritty täydentämään ja tuomaan tutkielmaan mahdollisimman laaja kokonaisuus tarvittavista yksityiskohdista. Tutkielman kuvat ovat kirjoittajan tekemiä Wolfram Mathematicalla tai GeoGebralla.

Merkintöjä

Aloitetaan käymällä läpi joukkomerkinnät, joita tutkielmassa tullaan käyttämään. Tässä työssä luonnollisten lukujen joukkoon, $\{1, 2, 3, \dots\} = \mathbb{N}$, ei kuulu luku nolla. Merkintä $\mathbb{R}_+$ tarkoittaa aidosti positiivisia reaalilukuja eli $\mathbb{R}_+ = \{x \in \mathbb{R} : x > 0\}$, ja merkintä $\mathbb{R}_-$ aidosti negatiivisia reaalilukuja. Merkinnällä $\mathbb{P}$ tarkoitetaan alkulukujen muodostamaa joukkoa, $\mathbb{P} = \{p_j\}_{j\in\mathbb{N}} = \{p_1, p_2, p_3, p_4, \dots\} = \{2, 3, 5, 7, \dots\}$. Tällöin kirjaimella p_i tarkoitetaan joukon $\mathbb{P}$ i. alkioita.

Kokonaisosan ja kongruenssiluokan merkintöjen kanssa pitää olla tarkkana, ettei sotke niitä samankaltaisen merkinnän takia keskenään.

- Luvulle $a \in \mathbb{R}$ merkintä $\lfloor a \rfloor$ tarkoittaa luvun a *kokonaisosaa* eli

$$\lfloor a \rfloor = \max\{k \in \mathbb{Z} : k \leq a\}.$$

- *Kongruenssiluokkia* merkitään:

$$[a]_i = \{b \in \mathbb{Z} : a \equiv b \pmod{i}\}.$$

- Jos joukko B on äärellinen, niin silloin merkinnällä $\#B$ tarkoitetaan joukon B *alkioiden lukumäärää.*

Luku 1

Multiplikatiivisia funktioita

Tässä luvussa perehdytään analyyttisen lukuteorian kannalta olennaisiin funktioihin ja niiden ominaisuuksiin. Määritellään aluksi aritmeettinen funktio, jonka pääasiallinen ominaisuus tämän tutkielman kannalta on multiplikatiivisuus. Tämä funktion ominaisuus toimii työkaluna useissa todistuksissa. Osassa lukuteorian kirjallisuutta puhutaan lukuteoreettisista funktioista, kun tarkoitetaan aritmeettisia funktioita.

Määritelmä 1.1. *Aritmeettiseksi funktioksi* kutsutaan funktiota f, jos se on määritelty seuraavasti:

$$f : \mathbb{N} \to \mathbb{R} \text{ tai } f : \mathbb{N} \to \mathbb{C}.$$

Määritelmä 1.2. Jos aritmeettiselle funktiolle $f : \mathbb{N} \to \mathbb{C}$ pätee, että $f(lk) = f(l)f(k)$ aina, kun $\text{syt}(l, k) = 1$, niin funktiota f sanotaan *multiplikatiiviseksi*. Funktio f on *täydellisesti multiplikatiivinen*, jos $f(lk) = f(l)f(k)$ kaikille $l, k \in \mathbb{N}$.

Täydellisesti multiplikatiivisia funktioita ovat esimerkiksi vakiofunktio $f = 1$ ja potenssifunktio $f(l) = l^n$, missä $n \in \mathbb{N}$. Lukuteorian kannalta tärkeitä täydellisesti multiplikatiivisia funktioita ovat Legendren symboli ja Liouvillen funktio [3]. Tässä tutkielmassa perehdytään kahteen multiplikatiiviseen funktioon, joista kumpikaan ei ole täydellisesti multiplikatiivinen.

Esitellään seuraavaksi nämä funktiot, Eulerin φ ja Möbiuksen μ.

1.1 Eulerin funktio φ

Eulerin φ-funktio on lukuteorian tunnetuimpia funktioita. Eulerin funktiota voidaan soveltaa algebran puolella ja toisaalta jotkin salakirjoitusmenetelmät käyttävät sen ominaisuuksia salauksen vahvistamiseen, eli φ-funktiolla on laajat sovellusmahdollisuudet monella eri matematiikan osa-alueella. Funktio φ on aritmeettinen funktio, jonka Euler kehitti samalla, kun rakensi todistusta Fermat'n pienelle lauseelle [24].

Määritelmä 1.3. (Eulerin funktio). Olkoon funktio $\varphi : \mathbb{N} \to \mathbb{N}$,

$$\varphi(n) = \#\{m \in \mathbb{N} : m \leqslant n \text{ ja } \text{syt}(n, m) = 1\}.$$

Määritelmässä φ-funktion arvo on niiden positiivisten kokonaislukujen määrä n, jotka ovat suhteellisia alkulukuja luvun m kanssa. Tarkastellaan φ-funktiota vielä numeerisen esimerkin kautta.

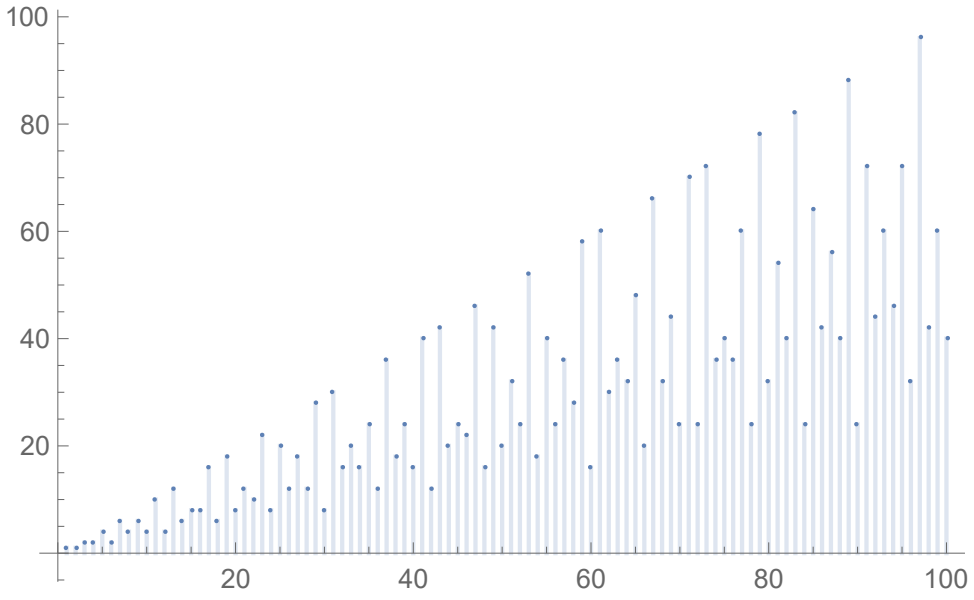
Esimerkki 1.4.

$\varphi(6) = 2,$ koska luvun 6 kanssa suhteelliset alkuluvut ovat ainoastaan luvut 1 ja 5, kun tarkastellaan kokonaislukuväliä 1 - 6.

$\varphi(15) = 8,$ sillä ehto suurimmasta yhteisestä tekijästä toteutuu lukujen 1, 2, 4, 7, 8, 11, 13 ja 14 kanssa välillä 1 - 15.

$\varphi(17) = 16,$ koska alkulukujen kanssa pätee kaava $\varphi(p) = p - 1,$ kaikille $p \in \mathbb{P}$.

Eulerin φ-funktion arvojen laskeminen käsin on työlästä jo suhteellisen pienillä luvuilla, jos ei tiedetä annetun luvun olevan alkuluku. Funktion arvojen laskemiseen on monia muitakin tapoja kuin kokeileminen. Työkaluja arvojen laskemiselle saadaan lisää, kun tutustutaan syvemmin φ-funktion muihin esitysmuotoihin.



Kuva 1.1: Funktion φ arvot välillä $[1, 100]$.

Kuvasta 1.1 huomataan, että Eulerin φ-funktion arvojen vaihtelu on hyvin voimakasta. Kappaleen loppupuolella tarkastellaan, millaisten ylä- ja alarajojen sisälle φ-funktion arvojen vaihtelu osuu.

Seuraavaa lemmaa tullaan tarvitsemaan Eulerin funktion multiplikatiivisuuden todistuksessa. Lemma ja sen todistus on muotoiltu kiinalaisen jäännöslauseen pohjalta.

Lemma 1.5. *(Kiinalainen jäännöslause). Olkoot* $l, k \in \mathbb{N}$ *ja* $\text{syt}(l, k) = 1$. *Asetetaan* $H = \{[h]_l : \text{syt}(h, l) = 1\}$, $I = \{[i]_k : \text{syt}(i, k) = 1\}$ *ja* $J = \{[j]_{lk} : \text{syt}(j, lk) = 1\}$. *Tällöin kuvaus*

$$H \times L \mapsto J, \quad ([h]_l, [i]_k) \mapsto [hk + il]_{lk} \tag{1.1}$$

on bijektio.

Todistus. Kongruenssiluokkien laskusääntöihin nojaten kuvaus (1.1) on hyvin määritelty, sillä se ei riipu edustajien valinnasta. Osoitetaan aluksi kuvauksen surjektiivisuus. Valitaan mielivaltainen $[j]_{lk} \in J$. Nyt tarvitsee löytää $[h]_l \in H$ ja $[i]_k \in I$ siten, että

$$[j]_{lk} = [hk + il]_{lk}. \tag{1.2}$$

Oletuksesta $\text{syt}(l, k) = 1$ ja Bézout'n lemmasta seuraa, että on olemassa $y, x \in \mathbb{Z}$ siten, että

$$yk + xl = 1. \tag{1.3}$$

Bézout'n lemma löytyy lähteestä [6, s. 91]. Kerrotaan yhtälöä (1.3) puolittain luvulla j, jolloin yhtälöstä $jyk + jxl = j$ voidaan poimia yhtälön (1.2) muuttujat h ja i seuraavasti:

$$h = jy \text{ ja } \ i = jx, \text{ jolloin } \ [jy]_l \in H \text{ ja } \ [jx]_k \in I.$$

Joukkojen määritelmien mukaisesti riittää osoittaa, että $\text{syt}(jy, l) = 1$ ja $\text{syt}(jx, k) = 1$.

Todistetaan tapaus $\text{syt}(jy, l) = 1$. Tapauksen $\text{syt}(jx, k) = 1$ todistus menee vastaavasti. Merkitään $c = \text{syt}(jy, l)$, jolloin luku c on lukujen jy ja l tekijä, joten $c \mid jy$ ja $c \mid l$. Oletuksesta $\text{syt}(l, k) = 1$ ja joukon J määritelmästä seuraa suoraan, että $\text{syt}(j, l) = 1$, ja tästä havaitaan $c \mid y$. Nyt tarkastellaan yhtälöä (1.3), jolloin huomataan, että $c \mid yk$ ja $c \mid xl$. Näin ollen $c \mid 1$ eli $c = 1$. Näin on saatu todistettua $\text{syt}(jy, l) = 1$.

Injektiivisyyden todistamiseen riittää todeta, että joukot $H \times L$ ja J ovat äärellisiä ja keskenään yhtä mahtavia, eli molemmissa joukoissa on sama määrä alkioita. Kuvaus $H \times I \mapsto J$ on surjektio ja injektio eli silloin se on bijektio. □

Lemman 1.5 avulla on helppoa osoittaa φ-funktion multiplikatiivisuus.

Lause 1.6. *Eulerin φ-funktio on multiplikatiivinen.*

Todistus. Olkoot $l, k \in \mathbb{N}$ ja $\text{syt}(l, k) = 1$. Tarvitsee osoittaa, että

$$\varphi(lk) = \varphi(l)\varphi(k).$$

Kirjoitetaan väite Eulerin funktion määritelmän 1.3 avulla:

$$\#\{a \leqslant lk : \text{syt}(a, lk) = 1\} = \#\{a \leqslant l : \text{syt}(a, l) = 1\} \cdot \#\{a \leqslant k : \text{syt}(a, k) = 1\}.$$

Merkitään joukot lemman 1.5 tavalla. Huomataan joukkojen samankaltaisuus, joten valitaan ne seuraavasti:

$$\begin{aligned} \#H &= \#\{a \leqslant l : \text{syt}(a, l) = 1\}, \\ \#I &= \#\{a \leqslant k : \text{syt}(a, k) = 1\} \text{ ja} \\ \#J &= \#\{a \leqslant lk : \text{syt}(a, lk) = 1\}. \end{aligned}$$

Muotoillaan väite asetettujen joukkojen avulla:

$$\#J = \#H \cdot \#I.$$

Lemman (1.5) todistuksessa näytettiin, että $\#(H \times I) = \#J$. Väite seuraa. □

Eulerin φ-funktion multipikatiivisuutta hyödynnetään mm. RSA-salauksen kanssa. RSA-salauksen yksi selvitettävistä kaavoista salakirjoituksen purkamiseen on

$$\varphi(m) = (p-1)(q-1).$$

Luku m on kahden todella suuren alkuluvun tulo, jolloin salakirjoitus on vahva, koska tietokoneidenkin on täysin mahdotonta selvittää lukua m, jos tiedossa ei ole alkulukuja p ja q [9, s. 241-243].

Huomautus 1.7. Funktio φ on multiplikatiivinen, mutta se ei ole täydellisesti multiplikatiivinen. Esimerkiksi $\varphi(4) = 2 \neq 1 = 1 \cdot 1 = \varphi(2) \cdot \varphi(2)$.

Seuraavaksi osoitetaan yksi tärkeistä lukuteorian lauseista, jonka Euler todisti vuonna 1760. Eulerin lause on erikoistapaus Lagrangen ryhmäteoriaa koskevasta lauseesta [6].

Lause 1.8. *(Eulerin Lause). Jos* $\text{syt}(a,n) = 1$*, niin* $a^{\varphi(n)} \equiv 1 \pmod{n}$.

Todistus. Tarkastellaan positiivisten kokonaislukujen joukkoa $\{1, 2, 3, \ldots, n\}$. Muodostetaan joukko A joukon $\{1, 2, 3, \ldots, n\}$ alkioista, jotka ovat suhteellisia alkulukuja luvun n kanssa. Joukko

$$A = \{b_1, b_2, \ldots, b_{\varphi(n)}\} = \{b \in \{1, 2, \ldots, \varphi(n)\} : \text{syt}(b, n) = 1\},$$

missä $b_i \not\equiv b_j \pmod{n}$, kun $i \neq j$. Oletuksesta $\text{syt}(a,n) = 1$ ja joukon A alkioista määrätään uusi joukko B siten, että

$$B = \{ab_1, ab_2, \ldots, ab_{\varphi(n)}\},$$

missä $\text{syt}(ab_i, n) = 1$ kaikilla $i \in \{1, 2, \ldots, \varphi(n)\}$. Lisäksi joukolle B pätee, että $ab_i \not\equiv ab_j \pmod{n}$ eli $n \nmid (b_i - b_j)a$, kun $i \neq j$, mikä seuraa oletuksesta $\text{syt}(a,n) = 1$ ja tiedosta, että $b_i \not\equiv b_j \pmod{n}$, kun $i \neq j$ eli $n \nmid b_i - b_j$. Joukot A ja B ovat kongruentteja luvun n suhteen, joten tästä seuraa, että joukkojen alkioiden tulot ovat keskenään kongruentteja modulo n. Nyt lasketaan kongruenssien laskusäännöillä todistus loppuun:

$$\begin{aligned} b_1 \cdot b_2 \cdots b_{\varphi(n)} &\equiv (ab_1) \cdot (ab_2) \cdots (ab_{\varphi(n)}) \pmod{n} \\ b_1 \cdot b_2 \cdots b_{\varphi(n)} &\equiv a^{\varphi(n)}(b_1 \cdot b_2 \cdots b_{\varphi(n)}) \pmod{n} \\ a^{\varphi(n)} &\equiv 1 \pmod{n}. \end{aligned}$$

□

Eulerin lauseen todistus avautuu nopeasti, kun sitä havainnollistaa konkreettisilla luvuilla. Tällöin nähdään, miten joukko B saadaan konstruoitua helposti joukosta A. Eulerin lauseesta saadaan muodostettua Fermat'n pieni lause, kun muistetaan funktion φ arvo alkuluvuille. Samojen oletusten ollessa voimassa Fermat'n pieni lause muuttuu vain luvun a potenssin osalta:

$$a^{p-1} \equiv 1 \pmod{n}.$$

Käydään läpi, millaista hyötyä Eulerin funktion multiplikatiivisuudesta on, kun käsitellään alkulukujen monikertoja.

Lause 1.9. *Jos* p *on alkuluku ja* $c \in \mathbb{N}$*, niin*

$$\varphi(p^c) = p^c - p^{c-1} = p^c\left(1 - \frac{1}{p}\right).$$

Todistus. Tutkitaan lukuja $\{1, 2, 3, \ldots, p^c - 1, p^c\}$. Kuinka moni näistä luvuista ei ole suhteellinen alkuluku luvun p^c kanssa? Vastaus löytyy luvuista, joille pätee ehdot:

$$1 \leq m \leq p^c \quad \text{ja} \quad p \mid m.$$

Tällöin luvut m ovat muotoa:

$$m = ph, \text{ missä } 1 \leq ph \leq p^c, \text{ jolloin } 1 \leq h \leq p^{c-1}.$$

Nähdään selvästi, että lukuja, jotka eivät ole suhteellisia alkulukuja luvun p^c kanssa, on p^{c-1} kappaletta. Tästä seuraa suoraan, että suhteellisia alkulukuja täytyy silloin olla

$$\varphi(p^c) = p^c - p^{c-1} = p^c\left(1 - \frac{1}{p}\right). \qquad \square$$

Seuraavan lauseen ja sen todistuksen ymmärtämistä varten käydään läpi, mitä merkintä $\prod_{p|n}$ tarkoittaa. Merkinnällä tarkoitetaan niitä tulontekijöitä p, jotka jakavat annetun luvun n. Seuraava esimerkki selventää merkinnän tarkoitusta.

Esimerkki 1.10. Olkoon $n = 30$, ja $\prod_{p|n} \frac{p^2 + p}{n}$. Luvun n alkulukuesityksestä saadaan tuloon vaadittavat alkuluvut: $n = 30 = 2 \cdot 3 \cdot 5$. Tällöin

$$\prod_{p|30} \frac{p^2 + p}{n} = \frac{2^2 + 2}{30} \cdot \frac{3^2 + 3}{30} \cdot \frac{5^2 + 5}{30} = \frac{2}{25}.$$

Nyt voidaan siirtyä muotoilemaan Eulerin φ-funktion esitys tulomuodossa ja todistamaan kyseinen tulos.

Lause 1.11. $\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$.

Todistus. Olkoon $n = \prod_{i=1}^{k} p_i^{c_i}$, missä $c \in \mathbb{N}$. Lauseen 1.9 avulla todistus on melko suoraviivainen lasku, kun muistetaan φ-funktion multiplikatiivisuus.

$$\begin{aligned}
\varphi(n) = \varphi\left(\prod_{i=1}^{k} p_i^{c_i}\right) &\overset{\text{multipli.}}{=} \varphi(p_1^{c_1})\varphi(p_2^{c_2}) \cdots \varphi(p_k^{c_k}) \\
&\overset{\text{L.1.9}}{=} p_1^{c_1}\left(1 - \frac{1}{p_1}\right) p_2^{c_2}\left(1 - \frac{1}{p_2}\right) \cdots p_k^{c_k}\left(1 - \frac{1}{p_k}\right) \\
&= p_1^{c_1} p_2^{c_2} \cdots p_k^{c_k}\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= \left(\prod_{i=1}^{k} p_i^{c_i}\right)\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right) \cdots \left(1 - \frac{1}{p_k}\right) \\
&= n \prod_{p|n} \left(1 - \frac{1}{p}\right). \qquad \square
\end{aligned}$$

Funktion φ esittäminen tulon avulla on tämän tutkielman kannalta yksi tärkeimmistä työkaluista, mitä tullaan hyödyntämään tutkielman edetessä. Tulomuodosta on hyötyä myös tarkistaessa funktion arvoja, kuten seuraavasta esimerkistä huomataan.

Esimerkki 1.12. Lausetta 1.11 hyödyntäen lasketaan arvot:

$$\varphi(9) = 9 \cdot \prod_{p|9} \left(1 - \frac{1}{p}\right) = 9 \cdot \left(1 - \frac{1}{3}\right) = 9 \cdot \frac{2}{3} = 6$$

$$\varphi(24) = 24 \cdot \prod_{p|24} \left(1 - \frac{1}{p}\right) = 24 \cdot \left(1 - \frac{1}{2}\right)\left(1 - \frac{1}{3}\right) = 24 \cdot \frac{1}{2} \cdot \frac{2}{3} = 8$$

Tarkastellaan summaa $\sum_{a|n} \varphi(a) = n$ funktion φ arvoille ja huomataan mielenkiintoinen ilmiö. Esimerkiksi edellä olleelle luvulle $n = 24$ havaitaan, että

$$24 = 1+1+2+2+2+4+4+8 = \varphi(1)+\varphi(2)+\varphi(3)+\varphi(4)+\varphi(6)+\varphi(8)+\varphi(12)+\varphi(24).$$

Esimerkissä 1.12 tehty havainto pätee yleisesti, joten todistetaan se seuraavaksi. Tulos on Johann Carl Friedrich Gaussin kehittelemä [6].

Lause 1.13. *Jokaiselle $n \in \mathbb{N}$ pätee, että* $\sum_{a|n} \varphi(a) = n$.

Todistus. Todistus mukailee lähteessä [19, s. 59-60] esitettyä todistusta. Jaetaan todistus kahteen tapaukseen.

Ensimmäisenä käydään läpi tapaus, kun $n = p^c$, missä $c \in \mathbb{N}$. Luku n on alkuluvun p jokin c. monikerta. Luvun n jakajina ovat luvut $\{1, p, p^2, \ldots, p^c\}$, jolloin summa voidaan kirjoittaa muodossa

$$\sum_{a|n} \varphi(a) = \sum_{a|p^c} \varphi(a) = \sum_{d=0}^{c} \varphi\big(p^d\big).$$

Nyt voidaan soveltaa lausetta 1.9:

$$\sum_{d=0}^{c} \varphi\big(p^d\big) = 1 + \sum_{d=1}^{c} p^d - p^{d-1}.$$

Kirjoitetaan summa $1 + \sum_{d=1}^{c} p^d - p^{d-1}$ auki:

$$1 + (p-1) + \big(p^2 - p\big) + \big(p^3 - p^2\big) + \cdots + \big(p^{c-1} - p^{c-2}\big) + \big(p^c - p^{c-1}\big) = p^c.$$

Huomataan, että termit kumoavat toisensa, joten jäljelle jää

$$\sum_{a|n} \varphi(a) = p^c = n.$$

Ensimmäinen tapaus on todistettu.

Todistetaan seuraavaksi tapaus, kun luvun n alkulukuesityksessä on useampi alkuluku. Tällöin $n = p_1^{c_1} p_2^{c_2} \cdots p_h^{c_h}$, missä kaikki luvut $p_1, p_2, \ldots, p_h$ ovat eri alkulukuja ja $c_1, c_2, \ldots, c_h \in \mathbb{N}$. Jakajien huomataan olevan muotoa $a = p_1^{t_1} p_2^{t_2} \cdots p_h^{t_h}$, missä
$0 \leq t_j \leq c_j$, kun $j = 1, \ldots, h$.

Nyt voidaan viedä todistus näillä tiedoilla loppuun: Lauseesta 1.6 seuraa, että

$$\varphi(a) = \varphi\left(p_1^{t_1}\right)\varphi\left(p_2^{t_2}\right)\cdots\varphi\left(p_h^{t_h}\right),$$

jota käytetään heti toisen yhtäsuuruuden jälkeen:

$$\begin{aligned}\sum_{a|n}\varphi(a) &= \sum_{t_1=0}^{c_1}\cdots\sum_{t_h=0}^{c_h}\varphi\left(p_1^{t_1}p_2^{t_2}\cdots p_h^{t_h}\right)\\ &= \sum_{t_1=0}^{c_1}\cdots\sum_{t_h=0}^{c_h}\varphi\left(p_1^{t_1}\right)\varphi\left(p_2^{t_2}\right)\cdots\varphi\left(p_h^{t_h}\right)\\ &= \prod_{j=1}^{h}\sum_{t_j=0}^{c_j}\varphi\left(p_j^{t_j}\right)\\ &= \prod_{j=1}^{h}\varphi(1)+\varphi(p_j)+\varphi\left(p_j^2\right)+\cdots+\varphi\left(p_j^{c_j}\right).\end{aligned}$$

Ensimmäisen tapauksen nojalla saadaan, että

$$\prod_{j=1}^{h}\varphi(1)+\varphi(p_j)+\varphi\left(p_j^2\right)+\cdots+\varphi\left(p_j^{c_j}\right) = \prod_{j=1}^{h}p_j^{c_j} = n,$$

mistä väite seuraa. □

Esitellään seuraavaksi kombinatoriikan tulos, seulaperiaate. Tuloksen löytää todistuksineen lähteestä [25, s. 156].

Lause 1.14. *(Seulaperiaate). Jos $B_1, B_2, B_3, \ldots, B_n$ ovat perusjoukon A äärellisiä osajoukkoja, niin on voimassa*

$$\#\left(\bigcup_{j=1}^{n}B_j\right) = \sum_{j=1}^{n}\#(B_j) - \sum_{1\le j<i\le n}\#(B_j\cap B_i)+\cdots+(-1)^{n-1}\#(B_1\cap\cdots\cap B_n).$$

Seulaperiaatetta voidaan soveltaa Eulerin φ-funktioon. Olkoon joukko $A=\{1,2,3,\ldots,n\}$, ja luvun n alkulukuesitys $n = p_1^{e_1}p_2^{e_2}\cdots p_m^{e_m}$. Tällöin funktio φ voidaan esittää muodossa

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right) = n - \sum_{i=1}^{m}\frac{n}{p_i} + \sum_{1\le i\le j\le m}\frac{n}{p_ip_j} - \cdots.$$

Seuraavaksi perehdytään φ-funktion ylä- ja alarajoihin, joista mainittiin kuvan 1.1 yhteydessä. Määritelmästä 1.3 voidaan päätellä, että $\varphi(n)\le n$ kaikille luvuille $n\in\mathbb{N}$. Kuvassa 1.1 näkyvän ylärajan saa muotoiltua yhtälöstä

$$\limsup_{n\to\infty}\frac{\varphi(n)}{n} = 1.$$

Tiedetään lauseen 1.11 nojalla, että

$$\frac{\varphi(n)}{n} = \prod_{p|n}\left(1-\frac{1}{p}\right).$$

Pienin yläraja tästä saadaan vaihtamalla luvun n tilalle alkuluku p, koska alkuluvuilla on aina suhteellisia alkulukuja luvun $p-1$ verran. Ylärajaksi saadaan, että

$$\lim_{n\to\infty} \sup \frac{\varphi(n)}{n} = \lim_{p\to\infty} \frac{\varphi(p)}{p} = \lim_{p\to\infty} 1 - \frac{1}{p} = 1.$$

Alarajan arvioiminen on kuvasta katsottuna hankalampaa, koska funktion arvot heilahtelevat enemmän.

Olkoon $n_k = 2 \cdot 3 \cdot 5 \cdot 7 \cdots p_k$, ja käännetään lause 1.11 ympäri, jolloin

$$\frac{n_k}{\varphi(n_k)} = \prod_{l=1}^{k} \left(1 - \frac{1}{p_l}\right)^{-1}.$$

Avataan tulon sisällä oleva termi $\frac{1}{1-\frac{1}{p_l}}$ geometriseksi sarjaksi, joten

$$\prod_{l=1}^{k} \left(1 - \frac{1}{p_l}\right)^{-1} = \prod_{l=1}^{k} \left(1 + p_l^{-1} + p_l^{-2} + \cdots\right). \tag{1.4}$$

Geometristen sarjojen tulosta saadaan Cauchyn tulon nojalla sarja, jossa esiintyy jokainen murtoluku $\frac{1}{n}$. Cauchyn tulo löytyy lähteestä [4, s.204-205]. Luvun n alkulukutekijät sisältyvät joukkoon $p_1, p_2, \ldots, p_k$ ja erityisesti lukujen $1, 2, \ldots, k$ alkutekijät kuuluvat samaan joukkoon. Nyt yhtälössä (1.4) olevaa tuloa voidaan arvioida harmonisen sarjan osasummalla, jolloin

$$\frac{n_k}{\varphi(n_k)} \geq \sum_{h=1}^{k} \frac{1}{h}. \tag{1.5}$$

Seuraavaksi arvioidaan osasummaa logaritmin avulla:

$$\sum_{h=1}^{k} \frac{1}{h} \geq \log(k). \tag{1.6}$$

Arviolle tarkka todistus löytyy lauseesta 3.5.

Yhdistämällä epäyhtälöt (1.5) ja (1.6) saadaan arvio:

$$\frac{n_k}{\varphi(n_k)} \geq \log(k). \tag{1.7}$$

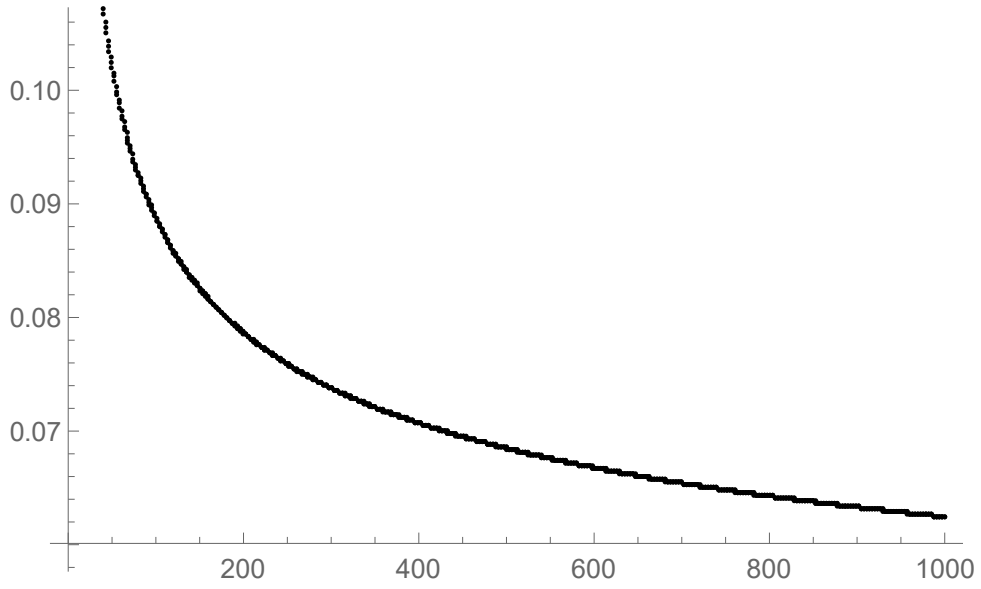
Epäyhtälöä (1.7) kääntämällä saadaan, että

$$0 \leq \frac{\varphi(n_k)}{n_k} \leq \frac{1}{\log(k)}.$$

Siis

$$\lim_{k\to\infty} \inf \frac{\varphi(n_k)}{n_k} = \lim_{k\to\infty} \frac{1}{\log(k)} = 0,$$

eli funktion $\frac{\varphi(n_k)}{n_k}$ asymptoottinen alaraja on nolla.



Kuva 1.2: Funktion $f(k) = \frac{\varphi(n_k)}{n_k}$ kuvaaja, kun luku k on suuri.

Kuvasta 1.2 nähdään, miten funktion $\frac{\varphi(n_k)}{n_k}$ arvot lähestyvät nollaa, kun luku k kasvaa suureksi. Kuvassa 1.2 luvun k arvot ovat vaaka-akselilla.

Todistetaan kappaleen loppuun vielä kaava, jolla Eulerin φ-funktion arvon saa lasketttua tulolle, jonka termit eivät ole keskenään suhteellisia alkulukuja.

Lause 1.15. *Olkoon* $c = \text{syt}(n, n')$, *missä* $c \in \mathbb{N}$ *ja* $c \neq 1$. *Tällöin*

$$\varphi(nn') = \varphi(n) \cdot \varphi(n') \cdot \frac{c}{\varphi(c)}.$$

Kaavasta huomataan helposti, mistä funktion φ multiplikatiivisuus tulee, kun $c = 1$.

Todistus. Olkoon $n, n' \in \mathbb{N}$. Oletuksesta $c = \text{syt}(n, n')$ seuraa, että luvuilla n ja n' on yksi tai useampi yhteinen alkulukutekijä. Kirjoitetaan $\varphi(nn')$ lauseen 1.11 avulla, mistä saadaan

$$\varphi(nn') = nn' \prod_{p|nn'} \left(1 - \frac{1}{p}\right).$$

Kirjoitetaan seuraavaksi tulo $\prod_{p|nn'}$ luvuille n ja n' erikseen ja jaetaan useamman kerran tulevilla termeillä:

$$nn' \prod_{p|nn'} \left(1 - \frac{1}{p}\right) = nn' \cdot \frac{\prod_{p|n} \left(1 - \frac{1}{p}\right) \prod_{p|n'} \left(1 - \frac{1}{p}\right)}{\prod_{p|n \text{ ja } p|n'} \left(1 - \frac{1}{p}\right)}. \tag{1.8}$$

Huomataan, että nimittäjässä oleva tulo voidaan kirjoittaa luvun c avulla, jolloin

$$\prod_{p|n \text{ ja } p|n'} \left(1 - \frac{1}{p}\right) = \prod_{p|c} \left(1 - \frac{1}{p}\right).$$

Sijoitetaan luvun c avulla kirjoitettu tulo yhtälöön (1.8), ja käytetään jokaiseen tuloon lausetta 1.11 uudelleen, jolloin

$$nn' \cdot \frac{\prod\limits_{p|n}\left(1-\frac{1}{p}\right)\prod\limits_{p|n'}\left(1-\frac{1}{p}\right)}{\prod\limits_{p|c}\left(1-\frac{1}{p}\right)} = \frac{\frac{n\cdot\varphi(n)}{n}\cdot\frac{n'\cdot\varphi(n')}{n'}}{\frac{\varphi(c)}{c}}.$$

Tästä saadaan haluttu tulos,

$$\varphi(nn') = \varphi(n)\cdot\varphi(n')\cdot\frac{c}{\varphi(c)}. \qquad \square$$

1.2 Möbiuksen μ-funktio

Toinen tärkeä lukuteoreettinen funktio on Möbiuksen μ-funktio. Ensimmäisen kerran funktiota käytti Euler todistuksissaan vuonna 1748, mutta tarkemman määritelmän ja perustelut antoi Möbius vasta vuonna 1832. Funktio μ on laajasti lukuteoriassa käytetty funktio, koska sillä on yhteys alkulukujen jakautumiseen ja Riemannin hypoteesiin [6]. Tutkielmassa Möbiuksen funktio toimii olennaisena työkaluna tutkittaessa Eulerin funktion keskimääräistä kasvunopeutta.

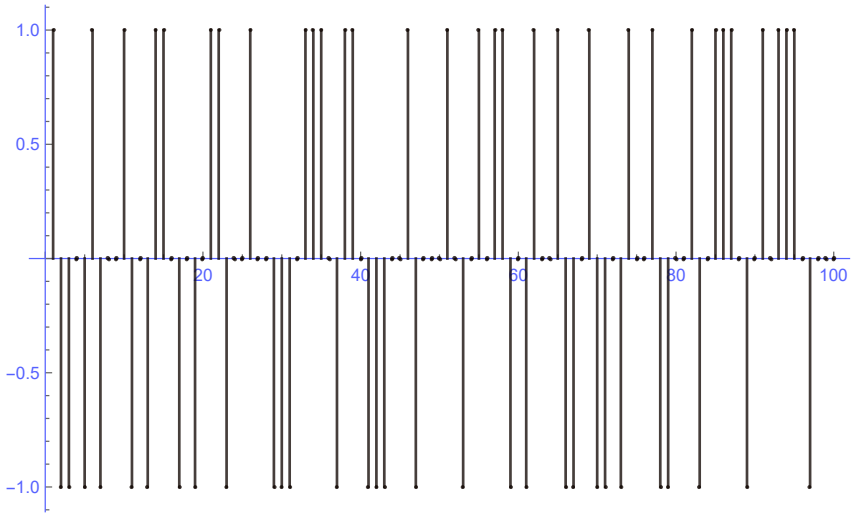
Määritellään Möbiuksen funktio ja tarkastellaan arvojen jakautumista.

Määritelmä 1.16. *Möbiuksen funktio* $\mu : \mathbb{N} \to \{-1, 0, 1\} \subset \mathbb{R}$ määritellä seuraavasti:

(1) $\mu(1) = 1$,

(2) $\mu(n) = 0$, jos luku n on neliöllä jaollinen,

(3) $\mu(p_1, p_2, \ldots, p_k) = (-1)^k$, missä kaikki alkuluvut $p_1, p_2, \ldots, p_k$ ovat eri lukuja.



Kuva 1.3: Funktion μ arvot välillä $[1, 100]$.

Esimerkki 1.17. Funktio μ saa arvoja:

$$\mu(1) = 1,\ \mu(2) = (-1)^1 = -1,\ \mu(3) = (-1)^1 = -1,$$
$$\mu(4) = \mu(2^2) = 0,\ \mu(5) = -1,\ \mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1,\ \text{jne.}$$

Kuvasta 1.3 nähdään, että μ-funktio saa 31 kertaa arvon 1, 30 kertaa arvon -1 ja arvon 0 funktio saa 39 kertaa joukossa $\{1, 2, \ldots, 100\}$. Funktion arvot lähestyvät asymptoottisesti kohti nollaa. Luvun 3 alussa tarkastellaan funktioiden asymptoottista käyttäytymistä ja muutamalla sanalla mainitaan funktion μ keskimääräisestä kasvunopeudesta.

Osoitetaan seuraavaksi μ-funktion multiplikatiivisuus.

Lause 1.18. *Möbiuksen funktio μ on multiplikatiivinen.*

Todistus. Olkoot $n, m \in \mathbb{Z}$ ja $\text{syt}(n, m) = 1$ eli n ja m ovat suhteellisia alkulukuja. Täytyy osoittaa, että

$$\mu(nm) = \mu(n)\mu(m).$$

Käydään todistus läpi tapaus kerrallaan: Jos $n = m = 1$, niin $\mu(1 \cdot 1) = 1 = \mu(1)\mu(1)$. Jos $n = 1$ ja $m \in \mathbb{Z}$, niin $\mu(1 \cdot m) = m = \mu(1)\mu(m)$. Vastaavasti, kun $m = 1$ ja $n \in \mathbb{Z}$. Jos toisella luvuista n tai m on neliöllinen tekijä, niin tällöin $\mu(nm) = 0 = \mu(n)\mu(m)$. Lopuksi tarvitsee todistaa tilanne, jos $n = p_1 p_2 \cdots p_k$ ja $m = q_1 q_2 \cdots q_h$. Alkuluvut ovat kummassakin eri lukuja ja oletuksesta $\text{syt}(n, m) = 1$ seuraa, että $p_i \neq q_j$. Nyt $\mu(n) = \mu(p_1 p_2 \cdots p_k) = (-1)^k$ ja $\mu(m) = \mu(q_1 q_2 \cdots q_h) = (-1)^h$, kun nämä yhdistetään saadaan

$$\mu(n)\mu(m) = (-1)^k \cdot (-1)^h = (-1)^{k+h} = \mu(p_1 p_2 \cdots p_k q_1 q_2 \cdots q_h) = \mu(nm).$$

Möbiuksen μ-funktio on multiplikatiivinen. □

Huomautus 1.19. Möbiuksen funktio, samoin kuin Eulerin funktio, ei ole täydellisesti multiplikatiivinen. Esimerkiksi $\mu(4) = 0 \neq 1 = (-1) \cdot (-1) = \mu(2)\mu(2)$.

Möbiuksen μ-funktiolle voidaan todistaa samankaltainen summakaava kuin φ-funktiolle. Tulos on toinen tärkeä Möbiuksen funktion ominaisuus.

Lause 1.20. *Olkoon $m \in \mathbb{N}$. Tällöin*

$$\sum_{a|m} \mu(a) = \begin{cases} 1, & \text{kun } m = 1 \\ 0, & \text{kun } m \geq 2. \end{cases}$$

Todistus. Todistus seuraa lähteen [17, s. 122-123] todistusta. Tilanteessa $m = 1$ väite saadaan suoraan.

Olkoon $m \geq 2$. Luku m voidaan esittää alkuluvun monikertana $m = p^h$, jollekin $h \geq 1$. Möbiuksen funktion määritelmän avulla avataan summa:

$$\sum_{a|m} \mu(a) = \mu(1) + \mu(p) + \mu(p^2) + \cdots + \mu(p^h) = 1 - 1 + 0 + 0 + \cdots + 0 = 0.$$

Väite seuraa tässä tapauksessa.

Jos lukua m ei voida esittää pelkästään alkuluvun monikertana, tällöin luku m on muotoa jollain alkuluvulla p :

$$m = p^h k,\ \text{missä } h \geq 1, k \geq 2 \text{ ja } \text{syt}(p, k) = 1.$$

Muistetaan, että luku a on luvun m tekijä, eli $a \mid m$. Aritmetiikan peruslauseesta ja ehdosta $\text{syt}(p,k) = 1$ seuraa, että luku a voidaan esittää muodossa

$$a = p^j l, \text{ missä } 0 \leq j \leq h \text{ ja } l \mid k.$$

Ehto $\text{syt}(p,k) = 1$ takaa sen, että luvun m tekijät ovat kuin luku a yllä. Muotoillaan väite uudestaan:

$$\sum_{a|m} \mu(a) = \sum_{l|k} \sum_{j=0}^{h} \mu(p^j l).$$

Ehdosta $\text{syt}(p,k) = 1$ seuraa myös, että $\text{syt}(p,l) = 1$ kaikille l siten, että $l \mid k$. Käytetään seuraavaksi Möbiuksen funktion multiplikatiivisuutta:

$$\sum_{a|m} \mu(a) = \sum_{l|k} \sum_{j=0}^{h} \mu(p^j)\mu(l).$$

Siirretään termit $\mu(l)$ sisemmästä summasta ulos:

$$\sum_{l|k} \mu(l) \sum_{j=0}^{h} \mu(p^j) = \sum_{l|k} \mu(l)(1 - 1 + 0 + 0 + \cdots + 0) = \sum_{l|k} \mu(l) \cdot 0 = 0.$$

Väite seuraa. □

Esimerkki 1.21. Valitaan, että $n = 12$ ja lasketaan summa $n \sum_{a|n} \frac{\mu(a)}{a}$:

$$\begin{aligned} 12 \cdot \sum_{a|12} \frac{\mu(a)}{a} &= 12\left(\frac{\mu(1)}{1} + \frac{\mu(2)}{2} + \frac{\mu(3)}{3} + \frac{\mu(4)}{4} + \frac{\mu(6)}{6} + \frac{\mu(12)}{12}\right) \\ &= 12\left(1 + \left(\frac{-1}{2}\right) + \left(\frac{-1}{3}\right) + \frac{0}{4} + \frac{1}{6} + \frac{0}{12}\right) \\ &= 12\left(1 - \frac{1}{2} - \frac{1}{3} + \frac{1}{6}\right) = 4. \end{aligned}$$

Lasketaan seuraavaksi Eulerin funktion arvo, kun $n = 12$:

$$\varphi(12) = 12 \cdot \prod_{p|12} \left(1 - \frac{1}{p}\right) = 12\left(\frac{1}{2}\right)\left(\frac{2}{3}\right) = 4.$$

Huomataan vastauksien olevan samat, joten Möbiuksen funktiolla on jonkinlainen yhteys φ-funktion kanssa.

Todistetaan edellisessä esimerkissä 1.21 tehty havainto Eulerin ja Möbiuksen funktioiden välillä. Kun aritmetiikan peruslauseen kanssa sovelletaan huomautusta 1.14, niin funktioiden φ ja μ yhteys on helpommin nähtävissä.

Seuraus 1.22.

$$\varphi(n) = \sum_{aa'=n} a' \mu(a).$$

Todistus. Muistetaan, että $\varphi(n)$ voidaan kirjoittaa lausen 1.11 nojalla tulomuodossa ja siihen sovelletaan seulaperiaatetta huomautuksen 1.14 mukaisesti, niin saadaan tulo muotoiltua uudelleen:

$$\varphi(n) = n\prod_{p|n}\left(1-\frac{1}{p}\right) = n\left(1-\sum_{p|n}\frac{1}{p}+\sum_{p<p'|n}\frac{1}{pp'}-\sum_{p<p'<p''|n}\frac{1}{pp'p''}+\dots\right). \tag{1.9}$$

Huomataan, että lausekkeessa olevat ykköset noudattavat tuttua kaavaa, kun tarkastellaan niitä Möbiuksen funktion näkökulmasta. Sulkeiden sisällä olevat termit, kun kirjoitetaan jokainen μ-funktion avulla erikseen saadaan, että

$$\mu(1) = 1,\ \mu\left(\frac{1}{p}\right) = (-1)^1,\ \mu\left(\frac{1}{pp'}\right) = (-1)^2....$$

Tästä huomataan, että μ-funktio löytyy yhtälöstä, kun tarpeeksi muokkaa. Seuraavaksi päästään lähemmäs haluttua tulosta, kun kirjoitetaan Eulerin φ Möbiuksen μ-funktion avulla:

$$\varphi(n) = n\sum_{a|n}\frac{\mu(a)}{a} = \sum_{a|n}\frac{n}{a}\mu(a) \tag{1.10}$$

$$= \sum_{a|n}a\mu\left(\frac{n}{a}\right) = \sum_{aa'=n}a\mu\left(\frac{aa'}{a}\right) = \sum_{aa'=n}a'\mu(a). \tag{1.11}$$

Möbiuksen μ-funktion määritelmässä neliöllä jaolliset luvut ovat nollaa, sillä merkintä $p \mid n$ kadottaa neliöllä jaolliset termit pois. Esimerkiksi tapauksessa, kun $n = 4$, niin silloin $\mu(4) = \mu(2^2) = 0$. Seuraavassa summamerkinnässä, kun tarkastellaan yhtälöä (1.9), on $p < p' \mid n$, jolloin tähänkään summaan ei tule neliöllisiä termejä, koska alkuluvut ovat erisuuria. Tästä johtuen neliöllä jaolliset luvut häviävät. Nämä nollat ovat mukana yhtälön (1.10) kohdalla, mutta tarkastellessa yhtälöä (1.9) huomataan, että sieltä ne tipahtavat nätisti pois. Nollien ongelmattomuus on helppoa huomata edellä olleen esimerkin nojalla.

Rivillä (1.11) muuttujanvaihto ensimmäisen yhtäsuuruuden kohdalla voidaan tehdä jaollisuuden takia. Möbiuksen funktion näkökulmasta on sama, että onko muuttujana luvun n jakava luku a, vai lukujen n ja a osamäärä. Rivin (1.11) toisen yhtäsuuruuden kohdalla on ajateltu, että kun $a \mid n$, niin $n = a' \cdot a$ jollakin $a' \in \mathbb{Z}$. Tästä sieventämällä ja samanlaisella muuttujanvaihdolla kuin edellä saadaan väite todistettua. □

Luku 2

Reaalinen ζ-funktio

Luku kaksi alkaa tutustumisella päättymättömien tulojen teoriaan. Päättymättömät tulot ovat olennainen osa Eulerin ζ-funktiota, koska tulojen avulla saadaan liitettyä alkuluvut funktion ζ kanssa. Eulerin ζ-funktiosta on luontevaa siirtyä yhteen lukuteorian tunnetuimmista ongelmista eli Baselin ongelmaa. Baselin ongelmalle on olemassa monia ratkaisutapoja, joten tässä tutkielmassa perehdytään tarkemmin kahteen erilaiseen ratkaisutapaan.

2.1 Päättymättömät tulot

Sarjat ovat tuttu käsite eli lukujonon ääretön yhteenlasku. Tässä kappaleessa tutustutaan tuloihin, jotka jatkuvat äärettömyyteen sarjojen kaltaisesti. Tällaisia tuloja kutsutaan päättymättömiksi tuloiksi. Käydään läpi kaksi määritelmää päättymättömille tuloille ja todistetaan muutamia perustuloksia, jotta tutkielmaa lukiessa olisi selvää, miten tulot käyttäytyvät. Päättymättömät tulot ovat tärkeä työkalu matematiikassa. Tässä kappaleessa esiteltävät tulokset ja niiden todistukset mukailevat lähteessä [4, s. 206-209] esiteltyjä tuloksia.

Päättymättömistä tuloista mainitsi ensimmäisiä kertoja François Viéte vuonna 1593 [7]. Hän osoitti, että

$$\frac{2}{\pi} = \sqrt{\frac{1}{2}} \cdot \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}} \cdot \sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2} + \frac{1}{2}\sqrt{\frac{1}{2}}}} \cdots .$$

Ensimmäiset havainnot päättymättömistä tuloista linkittyvät vahvasti luvun π erilaisiin esitysmuotoihin.

Määritellään ensin, mistä päättymätön tulo rakentuu, ja tarkastellaan määritelmää vielä numeerisen esimerkin avulla.

Määritelmä 2.1. Olkoon jono $(a_n)_{n=1}^{\infty}$ reaalisia tai kompleksisia lukuja, ja olkoot

$$t_1 = a_1,\ t_2 = a_1 \cdot a_2,\ \ldots\ , t_n = a_1 \cdot a_2 \cdot a_3 \cdots a_n = \prod_{k=1}^{n} a_k.$$

Järjestettyä paria $((a_n)_{n=1}^{\infty}, (t_n)_{n=1}^{\infty})$ kutsutaan *päättymättömäksi tuloksi*. Luvut t_n ovat osatuloja ja luvut a_n ovat tulon tekijöitä.

Huomautus 2.2. Merkintöjen helpottamiseksi tutkielmassa käytetään kahta erilaista tapaa merkitä päättymätöntä tuloa:

$$a_1 a_2 \cdots a_n \cdots, \text{ tai } \prod_{n=1}^{\infty} a_n. \tag{2.1}$$

Päättymättömään tuloon $\prod_{k=1}^{\infty} f(p_k)$, missä $\mathbb{P} = \{p_i : i \in \mathbb{N}\}$ on alkulukujen joukko suuruusjärjestyksessä, viitataan tutkielmassa merkinnällä $\prod_{p\in\mathbb{P}} f(p)$, missä $f : \mathbb{N} \to \mathbb{C}$.

Esimerkki 2.3. Yksinkertaisin esimerkki päättymättömästä tulosta on:

$$\prod_{n=1}^{\infty} n,$$

jolloin

$$t_1 = 1,\ t_2 = 1 \cdot 2 = 2,\ t_3 = 1 \cdot 2 \cdot 3 = 6, \ldots,$$
$$t_{12} = 1 \cdot 2 \cdots 12 = \prod_{n=1}^{12} n = 479001600, \ldots.$$

Osatulot $(t_n)_{n=1}^{\infty}$ ovat luvun n kertomia.

Mitä tapahtuu kohti ääretöntä mentäessä? Miten päättymättömät tulot suppenevat ja hajaantuvat? Muistellessa sarjoja voisi ajatella, että tulo (2.1) suppenee, jos osatulojen jono $(t_n)_{n=1}^{\infty}$ suppenee. Tällainen määritelmä voi johtaa harhaan, jos tulon tekijänä on yksikin nolla, sillä silloin tulo suppenee nollaan riippumatta muista tulon tekijöistä. Hämmentäviltä johtopäätöksiltä vältytään, kun määritellään päättymättömän tulo tarkemmin vielä suppenemisen ja hajaantumisen osalta. Päättymättömien tulojen kohdalla puhutaan harvemmin nollaan suppenemisesta, kuten seuraava määritelmä sen osoittaa.

Määritelmä 2.4. Olkoon päättymätön tulo $\prod_{n=1}^{\infty} a_n$ ja sen osatulo $t_n = \prod_{k=1}^{n} a_k$.

(1) Jos äärettömän moni tulontekijä a_n on nolla, niin silloin tulo *hajaantuu nollaan*.

(2) Jos $a_n \neq 0$ kaikilla $n \in \mathbb{N}$ ja $(t_n)_{n=1}^{\infty}$ suppenee nollaan, niin silloin päättymätön tulo *hajaantuu nollaan*.

(3) Jos yksikään tulontekijä a_n ei ole nolla, niin tulo *suppenee*, jos on olemassa luku $t \neq 0$ siten, että osatulojen $(t_n)_{n=1}^{\infty}$ jono suppenee tähän lukuun t. Tässä tapauksessa lukua t kutsutaan tulon *arvoksi* ja merkitään $t = \prod_{n=1}^{\infty} a_n$.

(4) Jos on olemassa luku N siten, että $a_n \neq 0$ kaikilla $n > N$, niin tulo $\prod_{n=1}^{\infty} a_n$, *suppenee*, jos $\prod_{n=N+1}^{\infty} a_n$ suppenee (3) kohdan mukaisesti. Tässä tapauksessa tulon $\prod_{n=1}^{\infty} a_n$ arvo on $a_1 a_2 a_3 \cdots a_N \cdot \prod_{n=N+1}^{\infty} a_n$.

(5) Tulo $\prod_{n=1}^{\infty} a_n$ *hajaantuu*, jos se ei suppene (3) tai (4) kohdan mukaisesti.

Määritelmän 2.4 kahdessa ensimmäisessä kohdassa todetaan päättymättömän tulon "hajaantuvan nollaan". Avataan tilannetta esimerkin avulla.

Esimerkki 2.5. Päättymättömän tulon arvon löytämiseen voidaan käyttää logaritmisarjoja, kun muistetaan tarkistaa, että $a_N > 0$. Osatuloille on totta, että

$$\log\left(\prod_{n=1}^{N} a_n\right) = \sum_{n=1}^{N} \log(a_n), \text{ jokaiselle äärelliselle luvulle } N \in \mathbb{N}.$$

Muistetaan, että logaritmi on määrittelyjoukossaan jatkuva, joten sen voi viedä rajaarvojen sisäpuolelle. Seuraavaksi voidaan tutkia rajankäyntiä samassa tilanteessa kuin yllä:

$$\log\left(\lim_{N\to\infty}\prod_{n=0}^{N} a_n\right) = \lim_{N\to\infty}\log\left(\prod_{n=1}^{N} a_n\right) = \lim_{N\to\infty}\sum_{n=1}^{N}\log(a_n). \tag{2.2}$$

Tarkastellaan tuloa $\prod_{n=1}^{\infty}\frac{1}{n}$ ja sijoitetaan se yhtälöön (2.2), joten

$$\log\left(\prod_{n=1}^{\infty}\frac{1}{n}\right) = \sum_{n=1}^{\infty}\log\left(\frac{1}{n}\right) = \sum_{n=1}^{\infty} -\log(n) = -\infty.$$

Sarja $-\log(n)$ hajaantuu. Tarkastellessa osatulojen käyttäytymistä huomataan niiden suppenevan nollaan. Tästä seuraa sanonta, että päättymätön tulo hajaantuu nollaan.

Huomataan määritelmän 2.4 nojalla, että nolla voi olla päättymättömän suppenevan tulon arvo. Mutta tämä on mahdollista, jos ja vain jos äärellinen määrä tulontekijöistä on nollia. Päättymättömän tulon suppenemiseen ei vaikuta tekijöiden lisääminen tai poistaminen, kun tämä tehdään äärellisellä määrällä alkioita.

Tarkastellaan Cauchyn ehtoa tuloille.

Lause 2.6. *(Cauchyn ehto tuloille). Päättymätön tulo* $\prod_{n=1}^{\infty} a_n$ *suppenee, jos ja vain jos jokaiselle* $\varepsilon > 0$ *on olemassa luku* N *siten, että* $n > N$*, niin seuraa*

$$|a_{n+1}a_{n+2}\cdots a_{n+k} - 1| < \varepsilon, \text{ jokaiselle } k = 1, 2, 3, \ldots. \tag{2.3}$$

Todistus. Katso [4, s. 207-208]. □

Todistetaan lopuksi päättymättömän tulon ja sarjan suppenemisen yhteys toisiinsa.

Lause 2.7. *Olkoon* $b_n > 0$*, missä* $n \in \mathbb{N}$*. Tulo* $\prod_{n=1}^{\infty}(1 + b_n)$ *suppenee, jos ja vain jos sarja* $\sum_{n=1}^{\infty} b_n$ *suppenee.*

Todistus. Merkitään

$$g_n = b_1 + b_2 + b_3 + \cdots + b_n, \text{ ja } \; t_n = (1 + b_1)(1 + b_2)(1 + b_3) \cdots (1 + b_n).$$

Jonot $(g_n)_{n=1}^{\infty}$ ja $(t_n)_{n=1}^{\infty}$ ovat kasvavia, jolloin halutun tuloksen todistamiseen tarvitsee osoittaa, että $(g_n)_{n=1}^{\infty}$ on rajoitettu, jos ja vain jos $(t_n)_{n=1}^{\infty}$ on rajoitettu. Selvästi $t_n > g_n$, joten jono $(t_n)_{n=1}^{\infty}$ on rajoitettu alhaalta jonolla $(g_n)_{n=1}^{\infty}$.

Näytetään vielä, että jono t_n on rajoitettu ylhäältä jonolla e^{g_n}, missä $(g_n)_{n=1}^{\infty}$. Eksponenttifunktion $f(x) = e^x$ sarjaesityksen nojalla

$$1 + y \leq e^y. \tag{2.4}$$

Differentiaalilaskennan väliarvolauseesta saadaan, että $e^y \geq 1$. Siis

$$(1 + b_1)(1 + b_2) \cdots (1 + b_n) \leq e^{b_1 + b_2 + \cdots + b_n},$$

joten $t_n \leq e^{g_n}$. Tällöin t_n on rajoitettu ylhäältä jonolla $e^{b_1 + b_2 + \cdots + b_n} = e^{g_n}$.

Mainitaan vielä, että $(t_n)_{n=1}^{\infty}$ ei voi supeta nollaan, koska jokainen $t_n \geq 1$ ja

$$t_n \to +\infty, \text{ jos } g_n \to +\infty.$$

Nyt on näytetty, että $(g_n)_{n=1}^{\infty}$ on rajoitettu, jos ja vain jos $(t_n)_{n=1}^{\infty}$ on rajoitettu. Tästä seuraa haluttu väite. □

2.2 Eulerin ζ-funktio

Leonhard Euler oli kiinnostunut analyyttisesta lukuteoriasta, ja varsinkin alkulukuihin liittyvistä tuloksista. Euler todisti sarjateorian avulla vuonna 1737, että alkulukuja on olemassa äärettömän monta, ja samalla hän tutustui sarjaan

$$\sum_{n=1}^{\infty} \frac{1}{n^s},$$

missä luku $s \in \mathbb{R}$ ja $s > 1$ [24]. Tästä sarjasta tuli yksi kuuluisimmista analyyttisen lukuteorian aiheista. Euler todisti sarjan suppenevan, mutta pystyi todistamaan sarjalle vahvemman tuloksen. Sarja suppenee tasaisesti puolisuoralla $s_0 \leq x < \infty$, kun $s_0 > 1$. Sarja hajaantuu, kun $s \leq 1$. Euler määritteli sarjan avulla jatkuvan ja differentioituvan funktion $\zeta :]1, \infty[\to \mathbb{R}$,

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \text{ missä } 1 < s < \infty.$$

Funktio nimettiin löytäjänsä mukaan *Eulerin ζ-funktioksi.*

Samana vuonna Euler todisti, että alkulukujen ja ζ-funktion välillä on yhteys. Muotoillaan tästä seuraava tulos ja todistetaan se päättymättömien tulojen ja Eulerin tulokaavan avulla.

Lause 2.8. *Olkoon $s \in \mathbb{R}$ ja $s > 1$, niin*

$$\zeta(s) = \prod_{h=1}^{\infty} \frac{1}{1 - p_h^{-s}}.$$

Todistus. Todistus jäljittelee lähteessä [4, s. 209-210] olevaa todistusta ζ-funktion tulomuodolle.

Olkoon $T_k(s) = \prod_{h=1}^{k} \frac{1}{1-p_h^{-s}}$ osatulo. Todistuksessa riittää osoittaa, että

$$T_k(s) \to \zeta(s), \text{ kun } k \to \infty.$$

Aloitetaan avaamalla osatulo T_k auki, ja kirjoittamalla termit geometrisena sarjana:

$$\begin{aligned} T_k = \prod_{h=1}^{k} \frac{1}{1-p_h^{-s}} &= \frac{1}{1-p_1^s} \cdot \frac{1}{1-p_2^s} \cdots \frac{1}{1-p_k^s} \\ &= \left(\sum_{a=0}^{\infty} \left(\frac{1}{p_1^s} \right)^a \right) \cdot \left(\sum_{a=0}^{\infty} \left(\frac{1}{p_2^s} \right)^a \right) \cdots \left(\sum_{a=0}^{\infty} \left(\frac{1}{p_k^s} \right)^a \right) \\ &= \left(1 + \frac{1}{p_1^s} + \frac{1}{p_1^{2s}} + \dots \right) \left(1 + \frac{1}{p_2^s} + \frac{1}{p_2^{2s}} + \cdots \right) \cdots \left(1 + \frac{1}{p_k^s} + \frac{1}{p_k^{2s}} + \dots \right) \\ &= \prod_{h=1}^{k} \left(1 + \frac{1}{p_h^s} + \frac{1}{p_h^{2s}} + \dots \right). \end{aligned}$$

Huomataan, että osatulo T_k muodostuu äärellisestä määrästä itseisesti suppenevia sarjoja.

Seuraavaksi kerrotaan nämä sarjat keskenään yhteen ja järjestellään jakajana olevat alkuluvut p_h suuruusjärjestykseen, jolloin saadaan tutun näköinen itseisesti suppeneva sarja:

$$\frac{1}{p_1^{c_1 s} p_2^{c_2 s} \cdots p_k^{c_k s}} = \frac{1}{n^s}, \text{ missä } n = p_1^{c_1 s} p_2^{c_2 s} \cdots p_k^{c_k s} \text{ ja jokainen } c_j \geq 0.$$

Näin ollen $T_k = \sum_{I_1} \frac{1}{n^s}$, missä summaus käy yli lukujen n, joiden alkulukutekijät $p_h \leq p_k$. Aritmetiikan peruslause takaa, että summauksessa olevat luvut n ovat siellä vain kerran. Vähentämällä summan T_k funktiosta ζ saadaan, että

$$\zeta(s) - T_k = \sum_{n=1}^{\infty} \frac{1}{n^s} - \sum_{I_1} \frac{1}{n^s} = \sum_{I_2} \frac{1}{n^s},$$

missä summaus I_2 käy yli niiden lukujen n, joiden jokin alkulukutekijä $p_h > p_k$. Tällöin $n > p_k$, joten saadaan

$$|\zeta(s) - T_k| \leq \sum_{n > p_k} \frac{1}{n^s}.$$

Tällöin summa $\sum_{n>p_k} \frac{1}{n^s}$ lähestyy nollaa, kun $k \to \infty$, koska sarja $\sum_{n=1}^{\infty} \frac{1}{n^s}$ suppenee, joten väite saadaan todistettua $T_k \to \zeta(s)$. □

Lausetta 2.8 pidetään aritmetiikan peruslauseen analyyttisena esitystapana [12]. Seuraava tulos osoittaa, että jos Eulerin ζ-funktion sarjaesitys suppenee itseisesti, niin silloin funktion ζ esitys päättymättömänä tulona suppenee itseisesti.

Lause 2.9. *Jos sarja* $\sum_{n=1}^{\infty} \frac{1}{n^s}$ *suppenee itseisesti, niin tulo* $\prod_{h=1}^{\infty} \frac{1}{1-p_h^{-s}}$ *suppenee myös itseisesti.*

Todistus. Esitetään päättymätön tulo lauseen 2.7 avulla:

$$\prod_{h=1}^{\infty} \frac{1}{1-p_h^{-s}} = \prod_{h=1}^{\infty}(1+t_h),$$

missä $t_h = \frac{1}{p_h^s} + \frac{1}{p_h^{2s}} + \cdots$. Avataan sarja t_h geometrisen summan kaavalla:

$$\sum_{k=1}^{\infty}\left(\frac{1}{p_h^s}\right)^k = \frac{\frac{1}{p_h^s}}{1-\frac{1}{p_h^s}}.$$

Arvioidaan termiä $\frac{\frac{1}{p_h^s}}{1-\frac{1}{p_h^s}}$ ylöspäin, jolloin saadaan, että

$$\frac{\frac{1}{p_h^s}}{1-\frac{1}{p_h^s}} \leq \frac{2}{p_h^s},$$

kun $s > 1$ ja $p_h \geq 2$.

Näin ollen sarja $\sum_{h=1}^{\infty} t_h$ suppenee itseisesti majoranttiperiaatteen nojalla. Lauseen 2.6 nojalla päättymätön tulo $\prod_{h=1}^{\infty}(1+t_h)$ suppenee itseisesti. □

Lauseessa 1.9 osoitettiin, että φ-funktion ja Möbiuksen funktion välillä on yhteys. Möbiuksen funktiolla on yhteys myös Eulerin ζ-funktion kanssa.

Lause 2.10. *Olkoon $s \in \mathbb{R}$ ja $s > 1$, niin*

$$\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}.$$

Todistus. Todistus mukailee lähteessä [19, s. 221] tehtyä todistusta.

Sarja $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ suppenee itseisesti yliharmonisena sarjana. Valitaan toinen sarja $C(s) = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$, joka suppenee itseisesti majoranttiperiaatteen nojalla, koska $|\mu(n)| \leq 1$ kaikilla $n \in \mathbb{N}$. Itseisesti suppenevien sarjojen tulo suppenee myöskin itseisesti Cauchyn tulon nojalla, katso [4, s. 204-205]. Tämän perusteella saadaan, että

$$\zeta(s)C(s) = \sum_{b=1}^{\infty}\frac{1}{b^s}\sum_{a=1}^{\infty}\frac{\mu(a)}{a^s} = \sum_{b=1}^{\infty}\sum_{a=1}^{\infty}\frac{\mu(a)}{(ba)^s}.$$

Seuraavaksi kirjoitetaan termit $\mu(a)$ ja $\frac{1}{(ba)^s}$ omina sarjoinaan siten, että

$$\sum_{b=1}^{\infty}\sum_{a=1}^{\infty}\frac{\mu(a)}{(ba)^s} = \sum_{ba=1}^{\infty}\frac{1}{(ba)^s}\sum_{a|ba}\mu(a). \tag{2.5}$$

Merkitään $n = ba$, ja sijoitetaan se yhtälöön (2.5):

$$\sum_{ba=1}^{\infty}\frac{1}{(ba)^s}\sum_{a|ba}\mu(a) = \sum_{n=1}^{\infty}\frac{1}{(n)^s}\sum_{a|n}\mu(a) = 1,$$

koska lauseesta 1.20 muistetaan, että $\sum_{a|n} \mu(a) = 1$, kun $n = 1$ ja muulloin se on nollaa.

Nyt on osoitettu, että $\zeta(s)C(s) = 1$, josta seuraa haluttu väite:

$$\frac{1}{\zeta(n)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}, \text{ kun } s > 1. \qquad \square$$

Möbiuksen μ-funktiolla on kytkös alkulukuihin ζ-funktion kautta, kuten juuri osoitettiin. Tämän tuloksen myötä funktion μ käyttäytyminen on yhteydessä alkulukujen jakautumiseen [6, s. 390-392].

2.3 Baselin ongelma

Pysytään vielä Eulerin ζ-funktiossa, mutta tarkastellaan sitä seuraavaksi kiinnitetyn arvon $s = 2$ kautta. Tätä tulosta kutsutaan Baselin ongelmaksi Bernoullin veljesten ja Eulerin kotikaupungin Baselin mukaan. Baselin ongelmasta kirjoitettiin ensimmäiset julkiset havainnot noin 1700-luvun alussa. Bernoullin veljekset olivat perehtyneet ahkerasti Eulerin ζ-funktioon tapauksessa, kun $s = 2$:

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \frac{1}{5^2} + \cdots = ?$$

He eivät kuitenkaan saaneet laskettua sarjalle arvoa, joten he pyysivät apua muilta matemaatikoilta. Euler kuuli ongelmasta ja alkoi työstämään funktiolleen todistusta. Vuonna 1740 Euler esitteli siihen aikaan kauniiksi ja elegantiksi luonnehditun tuloksensa maailmalle [10].

Tutustutaan Eulerin todistukseen, josta kaikki aikoinaan lähti liikkeelle, ja tarkastellaan todistuksessa olevia epäkohtia ja olettamuksia, jotka heikentävät todistuksen validiutta.

Lause 2.11.

$$\zeta(2) = \sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}.$$

Leonhard Euler todisti sinifunktiolle esityksen päättymättömänä tulona [10]. Tämä on tärkeä tulos käydä läpi ennen lauseen 2.11 todistusta.

Lemma 2.12.

$$\sin(\pi x) = \pi x \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2}\right), \text{ } \textit{missä } x \in \mathbb{R}$$

Todistus. Katso [14]. $\square$

Lemmasta 2.6 seuraa, että sinifunktio voidaan esittää päättymättömänä tulona

$$\sin(x) = x \prod_{k=1}^{\infty} \left(1 - \frac{x^2}{k^2\pi^2}\right) = x\left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{4\pi^2}\right)\cdots, \text{ missä } x \in \mathbb{R}. \tag{2.6}$$

Sinifunktion tekijöihin jaolla on tärkeä rooli Eulerin todistuksessa lauseelle 2.11, koska ilman lemman 2.6 todistusta olisi Eulerin alkuperäinen todistus Baselin ongelmalle hyvin puutteellinen. Tulos tekee Eulerin todistuksesta perustellumman, muttei täydellistä.

Todistus. (Lause 2.11). Todistus mukailee lähdettä [10, s. 62-63]. Euler aloitti todistuksensa k-asteisesta polynomifunktiosta

$$f(x) = 1 + a_1x + a_2x^2 + a_3x^3 + \cdots + a_kx^k,$$

jolla on k kappaletta nollasta eroavia nollakohtia. Merkitään niitä $b_1, b_2, \ldots, b_k$. Seuraavaksi kirjoitetaan polynomi f tulomuotoon nollakohtiensa avulla:

$$f(x) = \left(1 - \frac{x}{a_1}\right)\left(1 - \frac{x}{a_2}\right)\cdots\left(1 - \frac{x}{a_k}\right).$$

Seuraavaksi Euler käytti todistuksessaan sinifunktion sarjakehitelmää

$$\sin(x) = x - \frac{x^3}{3!} + \frac{x^5}{5!} - \frac{x^7}{7!} + \cdots = x\left(1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \ldots\right), \tag{2.7}$$

Euler merkitsi sarjakehitelmää funktiolla $q(x)$, jolloin hän sai yhtälön (2.7) muotoon

$$\frac{\sin(x)}{x} = q(x).$$

Sinifunktion nollakohdat löytyvät luvun π monikerroista: $0, \pm\pi, \pm 2\pi, \pm 3\pi, \ldots$. Huomataan, että funktion $q(x) = 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \ldots$ nollakohdat ovat samat lukuunottamatta arvoa $x = 0$.

Seuraava vaihe Eulerin alkuperäisessä todistuksessa on kyseenalainen, koska Euler tulkitsi polynomin $q(x)$ ∞-asteiseksi polynomiksi. Päättymättömän potenssisarjan esitys tulomuodossa nollakohtien avulla ei ole itsestään selvyys ja polynomin aste on aina äärellistä. Oletetaan epäkohdat perustelluiksi ja jatketaan todistusta.

Euler kirjoitti "polynomifunktion" $q(x)$ nollakohtien avulla, jolloin funktio $q(x)$ muodostuu päättymättömästä tulosta

$$\begin{aligned} q(x) &= 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \ldots \\ &= \left(1 + \frac{x}{\pi}\right)\left(1 - \frac{x}{\pi}\right)\left(1 + \frac{x}{2\pi}\right)\left(1 - \frac{x}{2\pi}\right)\left(1 + \frac{x}{3\pi}\right)\left(1 - \frac{x}{3\pi}\right)\cdots. \end{aligned}$$

Seuraavaksi Euler yhdisti peräkkäiset termit keskenään saadakseen yhteisiä tekijöitä samalla tavalla kuin yhtälössä (2.6):

$$\begin{aligned} 1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \ldots &= \left(1 - \frac{x^2}{\pi^2}\right)\left(1 - \frac{x^2}{2^2\pi^2}\right)\left(1 - \frac{x^2}{3^2\pi^2}\right)\cdots \\ &= 1 - \left(\frac{1}{\pi^2} + \frac{1}{2^2\pi^2} + \frac{1}{3^2\pi^2}\right)x^2 + (\ldots)x^4 - \ldots. \end{aligned}$$

Lopuksi Euler vertaili luvun x^2 kertoimia yhtälöstä

$$1 - \frac{x^2}{3!} + \frac{x^4}{5!} - \frac{x^6}{7!} + \cdots = 1 - \left(\frac{1}{\pi^2} + \frac{1}{2^2\pi^2} + \frac{1}{3^2\pi^2} + \ldots\right)x^2 + \ldots,$$

josta pääsi muutaman laskutoimituksen päähän haluamastaan ratkaisusta.

$$-\frac{1}{3!} = -\left(\frac{1}{\pi^2} + \frac{1}{2^2\pi^2} + \frac{1}{3^2\pi^2} + \dots\right)$$

Euler kertoi yhtälöä puolittain luvulla $-\pi^2$, jolloin

$$\frac{\pi^2}{3!} = 1 + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \dots.$$

Euler viimeisteli todistuksensa vastaukseen

$$\sum_{n=1}^{\infty} \frac{1}{n^2} = \frac{\pi^2}{6}. \qquad \square$$

Eulerin todistusta voidaan pitää alkusysäyksenä Baselin ongelman ratkaisemiseen, koska nykyään Baselin ongelmaan on monia erilaisia todistuksia. Matemaatikot huomasivat, että ongelmaa voidaan lähestyä eri matematiikan osa-alueilta, kuten Fourier-analyysin, todennäköisyysteorian, kompleksianalyysin, jne. näkökulmista.

Todistetaan lause 2.11 uudestaan täysin toisenlaisen lähestymistavan kautta. Vuonna 1978 Frits Beukers todisti 2-ulotteisella Riemann integraalilla $\int_0^1 \int_0^1 \frac{1}{1-xy}$, että arvo $\zeta(3)$ on irrationaaliluku. Tästä todistuksesta huomattiin, että samanlaisella lähestymistavalla pystyttiin laskemaan funktion $\zeta(2)$ tarkka arvo.

Todistus. (Lause 2.11). Todistus seuraa lähdettä [2]. Todistus perustuu yllä esitetyn Riemann integraalin ja arvon $\zeta(2)$ väliseen yhteyteen laajentamalla integroitava osa geometriseksi sarjaksi, jota voidaan integroida termeittäin.

Geometrisestä sarjasta muistetaan, että

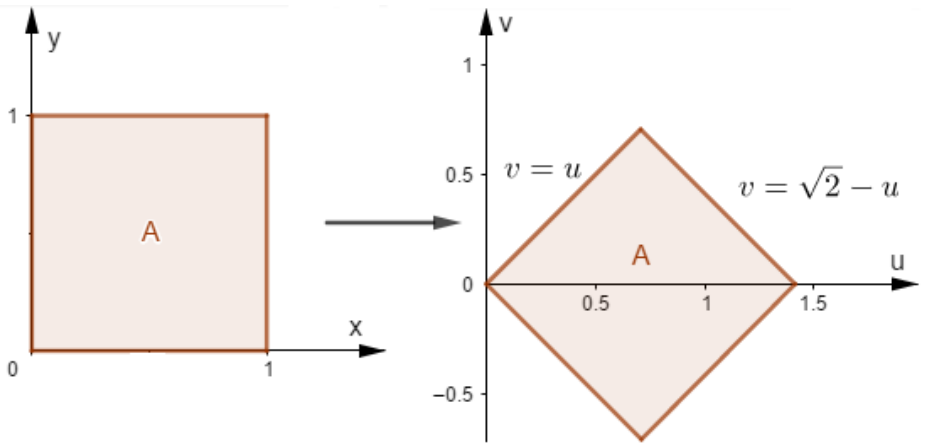
$$\frac{1}{1-xy} = 1 + xy + (xy)^2 + (xy)^3 + \dots = \sum_{n=0}^{\infty} (xy)^n, \text{ kun } |xy| < 1.$$

Seuraavaksi integroidaan yllä olevaa geometristä sarjaa termeittäin:

$$I = \int_0^1 \int_0^1 \frac{1}{1-xy} = \int_0^1 \int_0^1 \sum_{n=0}^{\infty} x^n y^n \, dxdy \overset{x^n \geq 0}{=} \int_0^1 \sum_{n=0}^{\infty} y^n \cdot \frac{1}{n+1} \, dy$$
$$\overset{\frac{y^n}{n+1} \geq 0}{=} \sum_{n=0}^{\infty} \frac{1}{(n+1)^2} = \sum_{n=1}^{\infty} \frac{1}{n^2} = \zeta(2).$$

Integroiminen sarjan yli onnistuu, koska funktiot x^n ja y^n ovat aidosti positiivisia ja integroituvia koko suljetulla välillä $[0, 1]$. Täytyy siis osoittaa, että $I = \frac{\pi^2}{6}$.

Integraalin kulkema alue xy-tasossa on neliö, jonka vastakkaiset kulmat ovat $(0, 0)$ ja $(1, 1)$. Tehdään muuttujanvaihto kääntämällä koordinaattiakselit myötäpäivään $\frac{\pi}{4}$ radiaanikulman verran. Tällöin neliö kääntyy kuvan 2.1 osoittamalla tavalla.



Kuva 2.1: Todistuksessa tehtävä koordinaatiston muutos.

Koordinaatiston muutosta voidaan kuvata muuttujien vaihdolla seuraavasti:

$$x = \frac{u-v}{\sqrt{2}} \text{ ja } y = \frac{u+v}{\sqrt{2}}, \text{ joten } \frac{1}{1-xy} = \frac{2}{2-u^2+v^2}.$$

$$u = v + \sqrt{2}x \text{ ja } v = -u + \sqrt{2}y.$$

Muuttujanvaihto tehdään muuttujanvaihtolauseen nojalla, koska Jacobin determinantti on positiivista. Alkuperäisessä koordinaatistossa piste $(1,0)$ vastaa käännetyn koordinaatiston pistettä $\left(\sqrt{2},0\right)$, katso kuva 2.1. Neliön symmetrian avulla voidaan lähteä laskemaan integraalia kahdessa osassa:

$$I = 2\int_0^{\frac{1}{\sqrt{2}}} \left(\int_0^u \frac{2}{2-u^2+v^2} dv \right) du + 2\int_{\frac{1}{\sqrt{2}}}^{\sqrt{2}} \left(\int_0^{\sqrt{2}-u} \frac{2}{2-u^2+v^2} dv \right) du \tag{2.8}$$

$$= 4\int_0^{\frac{1}{\sqrt{2}}} \left(\int_0^u \frac{1}{2-u^2+v^2} dv \right) du + 4\int_{\frac{1}{\sqrt{2}}}^{\sqrt{2}} \left(\int_0^{\sqrt{2}-u} \frac{1}{2-u^2+v^2} dv \right) du. \tag{2.9}$$

Integraaleihin pystyy soveltamaan tuttua integrointikaavaa

$$\int_0^x \frac{1}{b^2+t^2}\, dt = \frac{1}{b} \arctan\left(\frac{x}{b}\right), b < 0.$$

Käytetään edellistä integrointikaavaa yllä olevan yhtälön (2.9) sisempiin integraaleihin:

$$\int_0^u \frac{1}{2-u^2+v^2}\, dv = \frac{1}{\sqrt{2-u^2}} \arctan\left(\frac{u}{\sqrt{2-u^2}}\right) \text{ ja}$$

$$\int_0^{\sqrt{2}-u} \frac{1}{2-u^2+v^2}\, dv = \frac{1}{\sqrt{2-u^2}} \arctan\left(\frac{\sqrt{2}-u}{\sqrt{2-u^2}}\right).$$

Nyt voidaan jatkaa laskemista sijoittamalla sievennetyt muodot alkuperäiseen yhtälöön (2.9):

$$I = 4\int_0^{\frac{1}{\sqrt{2}}} \frac{1}{\sqrt{2-u^2}} \arctan\left(\frac{u}{\sqrt{2-u^2}}\right) du + 4\int_{\frac{1}{\sqrt{2}}}^{\sqrt{2}} \frac{1}{\sqrt{2-u^2}} \arctan\left(\frac{\sqrt{2}-u}{\sqrt{2-u^2}}\right) du.$$

Merkintöjen helpottamiseksi asetetaan, että

$$I_1 = 4\int_0^{\frac{1}{\sqrt{2}}} \frac{1}{\sqrt{2-u^2}} \arctan\left(\frac{u}{\sqrt{2-u^2}}\right)\, du \text{ ja}$$
$$I_2 = 4\int_{\frac{1}{\sqrt{2}}}^{\sqrt{2}} \frac{1}{\sqrt{2-u^2}} \arctan\left(\frac{\sqrt{2}-u}{\sqrt{2-u^2}}\right)\, du.$$

Lasketaan ensin integraalin I_1 arvo kiinnittämällä $u = \sqrt{2}\sin(\theta)$. Lasketaan termi du kiinnitetyn arvon avulla, jolloin $du = \sqrt{2}\cos(\theta)\, d\theta = \sqrt{2-u^2}\, d\theta$. Lasketaan uudet rajat integraalille, $\frac{1}{\sqrt{2}} = \sqrt{2}\sin(\theta)$, jolloin $\theta = \frac{\pi}{6}$. Huomataan, että

$$\tan(\theta) = \frac{u}{\sqrt{2-u^2}}.$$

Tällöin kaikki termit, joissa on tangentin käänteisfunktiota, kumoutuvat pois ja jäljelle jää vain integraali

$$I_1 = 4\int_0^{\frac{\pi}{6}} \theta\, d\theta = 2\left(\frac{\pi}{6}\right)^2.$$

Lasketaan integraali I_2 muuttujanvaihdolla $u = \sqrt{2}\cos(2\theta)$, jolloin

$$du = -2\sqrt{2}\sin(2\theta)\, d\theta = -2\sqrt{2}\sqrt{1-\cos^2(2\theta)}\, d\theta$$
$$= -2\sqrt{2}\sqrt{1-\frac{u^2}{2}}\, d\theta = -2\sqrt{2-u^2}\, d\theta.$$

Huomataan, että termi $\left(\frac{\sqrt{2}-u}{\sqrt{2-u^2}}\right)$ saadaan supistettua tutumpaan muotoon trigonometristen funktioiden laskusäännöillä:

$$\frac{\sqrt{2}-u}{\sqrt{2-u^2}} = \frac{\sqrt{2}-\sqrt{2}\cos(2\theta)}{\sqrt{2-(\sqrt{2}\cos(2\theta))^2}} = \frac{\sqrt{2}(1-\cos(2\theta))}{\sqrt{2(1-\cos^2(2\theta))}} = \frac{1-\cos(2\theta)}{\sqrt{1-\cos^2 2\theta}}$$
$$= \frac{2\sin^2(\theta)}{\sin(2\theta)} = \frac{2\sin^2(\theta)}{2\sin(\theta)\cos(\theta)} = \frac{\sin(\theta)}{\cos(\theta)} = \tan(\theta).$$

Integraalin uudet rajat lasketaan muuttujanvaihdolla $\sqrt{2} = \sqrt{2}\cos(2\theta)$, jolloin $\theta = 0$ ja $\frac{1}{\sqrt{2}} = \sqrt{2}\cos(2\theta)$, joten $\theta = \frac{\pi}{6}$. Tällöin integraalin I_2 arvo on

$$I_2 = 8\int_0^{\frac{\pi}{6}} \theta\, d\theta = 4\left(\frac{\pi}{6}\right)^2.$$

Lopulta saadaan laskettua koko integraalin arvo,

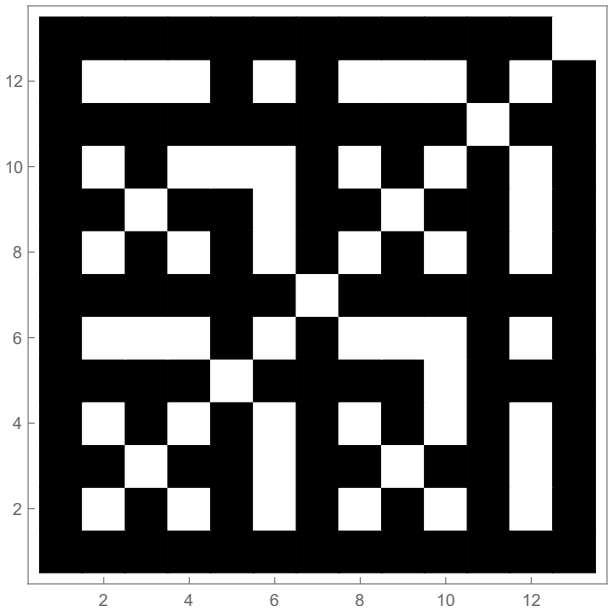
$$I = I_1 + I_2 = 2\left(\frac{\pi}{6}\right)^2 + 4\left(\frac{\pi}{6}\right)^2 = 6\left(\frac{\pi}{6}\right)^2 = \frac{\pi^2}{6}. \qquad \square$$

Baselin ongelman ratkaisu on hieno tulos, jota voidaan lähestyä monella erilaisella tavalla. Matemaatikot ovat tutkineet Eulerin ζ-funktion arvoja, ja huomanneet parillisten lukujen olevan helpompia laskea kuin parittomien. Roger Apéry sai todistettua vuonna 1978, että $\zeta(3)$ on irrationaaliluku, mutta tarkemmin funktion ζ parittomista luvun s arvoista ei tiedetä [11].

Luku 3

Suhteellisten alkulukuparien todennäköisyys

Tässä luvussa todistetaan tutkielman päätulos lauseena 3.9. Tulosta soveltaen todistetaan todennäköisyys suhteellisille alkulukupareille. Johdatellaan luvun aiheeseen tarkastelemalla tutkielman kansikuvaa tarkemmin.



Kuva 3.1: Tutkielman kansikuva.

Kuvassa 3.1 on 13×13-ruudukko, missä ruutu kuvastaa lukuparia. Mustilla ruuduilla kuvataan tilannetta, jolloin lukujen suurin yhteinen tekijä on yksi ja valkoisten ruutujen kohdalla lukujen suurin yhteinen on jotain muuta kuin yksi. Ennen kappaletta 3.3 tarkastellaan funktioiden asymptoottista käyttäytymistä, funktioiden keskimääräisen kas-

vunopeuden arvioimista yleisessä tilanteessa ja tarkemmin Eulerin funktion tapauksessa. Luvun loppussa perehdytään vielä Fareyn jonoihin päätuloksen eräänä sovelluksena.

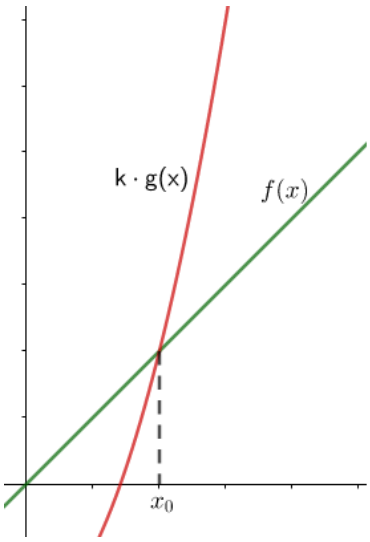
3.1 Funktioiden asymptoottinen käyttäytyminen

Paul Bachmann esitteli vuonna 1894 julkaisemassaan analyyttisen lukuteorian kirjassa merkinnän O kuvaamaan funktioiden asymptoottista käyttäytymistä. Edmund Landau piti tätä merkintää järkevänä ja käytti O-merkintää omassa kirjassaan vuonna 1909. Landaun julkaisema kirja saavutti suuremman lukijajoukon, jolloin O-merkintä sai nimen *Landaun symboli*. Merkintä O on olennainen työkalu, kun kuvataan funktioiden asymptoottista kasvunopetta, ja merkinnällä saadaan yksinkertaistettua sotkuisia ja pitkiä merkintöjä.

Määritellään O-merkintä formaalisti.

Määritelmä 3.1. Olkoot $f, g : A \to \mathbb{R}$, kun $A \subseteq \mathbb{R}$. Merkitään $f = \mathrm{O}(g(x))$ suurille x, jos ja vain jos on olemassa vakiot $k, x_0 \in \mathbb{R}$ siten, että

$$|f(x)| \leq k \cdot |g(x)|\,, \text{ kaikille } x > x_0.$$



Kuva 3.2: Funktio kg on funktion f asymptoottinen yläraja.

Määritelmän mukaan f ei kasva nopeammin kuin $\mathrm{O}(g(x))$ arvon x_0 jälkeen. Kuvasta 3.2 nähdään, miten funktion f kuvaaja pysyy funktion $k \cdot g$ kuvaajan alapuolella pisteen x_0 jälkeen.

Merkintää käytetään kuvaamaan funktion raja-arvokäyttäytymistä kohti jotain tiettyä arvoa tai ääretöntä mentäessä. Tässä tutkielmassa perehdytään tarkemmin funktion asymptoottiseen käyttäytymiseen kohti ääretöntä mentäessä, joten esimerkit on valittu tästä näkökulmasta.

Esimerkki 3.2. Jos $f(x) = x^4 - 5x^3 + 7x^2 - 381x + 4092$, niin määritelmän 3.1 mukaan funktio voidaan kirjoittaa lyhyempään muotoon johtavan termin avulla. Tässä tapauksessa johtava termi on x^4, koska luvun x lähestyessä ääretöntä termi x^4 "päättää" funktion

asymptoottisen käyttäytymisen. Funktion loppuosa muotoillaan O-merkinnän ja jäljelle jääneiden termien johtavan termin x^3 avulla. Funktio saadaan muotoon $f(x) = x^4 + \mathrm{O}(x^3)$.

Määritelmä 3.3. Olkoot $f, g : \mathbb{N} \to \mathbb{R}$ tai $f, g : \mathbb{R} \to \mathbb{R}$ siten, että $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$. Tällöin funktiot f ja g ovat *asymptoottisesti ekvivalentit*. Merkitään $f \sim g$.

Esimerkki 3.4. Tarkastellaan funktiota $f(x) = 2^x + x^2$. Funktio f voidaan määritelmän 3.1 nojalla siistiä muotoon $f(x) = 2^x + \mathrm{O}(x^2)$, koska termi 2^x on tässä tapauksessa funktion nopeuden määräävä termi. Seuraavaksi voidaan jakaa termillä 2^x, jolloin

$$\frac{f(x)}{2^x} = 1 + \frac{\mathrm{O}(x^2)}{2^x}.$$

Nyt viedään luku x kohti ääretöntä:

$$\frac{f(x)}{2^x} \to 1, \text{ kun } x \to \infty,$$

koska termi $\frac{\mathrm{O}(x^2)}{2^x}$ menee nollaan, niin virhetermi kutistuu hyvin pieneksi ja funktio saadaan arvioitua. Funktio f on asymptoottisesti ekvivalentti funktion $h(x) = 2^x$ kanssa, merkitään $f \sim 2^x$.

Merkinnällä O pyritään karsimaan epäoleellinen osa funktiosta pois ja jättämään jäljelle tärkein osa, funktion keskimääräisen kasvunopeuden määräämä termi. Tällä ominaisuudella saadaan arvioitua epäyhtälöt suoraan yhtälöiksi, koska O-merkintä pitää kaiken informaation mukana korostaen todistuksen kannalta tärkeintä osaa. Tätä ominaisuutta tarvitaan heti seuraavan lauseen todistuksen loppupuolella.

Tarkastellaan seuraavaksi harmonisen sarjan osasummien arviointia, sillä siinä sovelletaan O-merkintää ja tulosta tullaan tarvitsemaan tutkielman päätuloksen todistamisessa. Harmoninen sarja hajaantuu hyvin hitaasti, koska sen osummia voidaan arvioida logaritmien avulla seuraavan lauseen mukaisesti.

Lause 3.5. *Olkoot $m \geq 1$ ja $0 < \gamma < 1$. Tällöin*

$$\sum_{h=1}^{m} \frac{1}{h} = \log(m) + \gamma + \mathrm{O}\left(\frac{1}{m}\right),$$

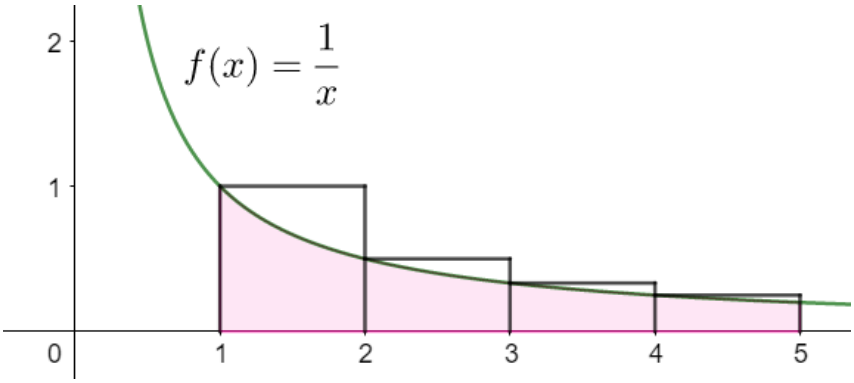
missä γ on Eulerin vakio.

Huomautus 3.6. Eulerin vakiolla on numeerinen arvo, $\gamma = 0,577215665\ldots$. Tästä numeerisesta arvosta huolimatta matemaatikot eivät ole pystyneet osoittamaan, onko γ rationaaliluku vai irrationaaliluku [12, s. 46].

Lause 3.5 todistetaan suppenemistestin erikoistapauksena.

Todistus. Olkoot

$$t_m = \sum_{h=1}^{m} \frac{1}{h}, \quad s_m = \int_1^m \frac{1}{x}\, dx = \log(m) \quad \text{ja} \quad b_m = t_m - s_m.$$



Kuva 3.3: Yläsumma t_m integraalille s_m.

Kuvasta 3.3 nähdään, että yläsumman t_m palkit ovat integraalin s_m yläpuolella, joten

$$\int_1^m \frac{dx}{x} \leq \sum_{h=1}^{m} \frac{1}{h},$$

ja tällöin $b_m \geq 0$ kaikilla $m \in \mathbb{N}$. Erotus b_m on alhaalta rajoitettu.

Kuvan avulla 3.3 huomataan $\log(m+1) - \log(m) \geq \frac{1}{m+1}$, joten

$$b_m - b_{m+1} = -\frac{1}{m+1} + \int_m^{m+1} \frac{dx}{x} \geq 0.$$

Siis lukujono $(b_m)_{m=1}^{\infty}$ on vähenevä. Tällöin on olemassa raja-arvo

$$\lim_{m\to\infty} b_m = \lim_{m\to\infty} \sum_{h=1}^{m} \frac{1}{h} - \log(m) = \gamma. \tag{3.1}$$

Edellisten vaiheiden nojalla tiedetään, että

$$0 \leq b_m - b_{m+1} = \int_m^{m+1} \frac{dx}{x} - \frac{1}{m+1} \leq \frac{1}{m} - \frac{1}{m+1} = \frac{1}{m(m+1)},$$

koska $\frac{1}{x} \leq \frac{1}{m}$, kun $m \leq x \leq m+1$. Sarja $\sum_{m=1}^{\infty} \frac{1}{m(m+1)}$ suppenee kohti lukua 1, joten

$$b_h - \lim_{m\to\infty} b_m = \sum_{m=h}^{\infty} b_m - b_{m+1} \leq \sum_{m=h}^{\infty} \left(\frac{1}{m} - \frac{1}{m+1}\right) = \frac{1}{h}. \tag{3.2}$$

Arvioimalla epäyhtälö (3.2) yhtälöksi O -merkinnän avulla ja yhdistämällä sen yhtälön (3.1) kanssa saadaan, että

$$\sum_{h=1}^{m} \frac{1}{h} - \log(m) - \gamma = \mathrm{O}\left(\frac{1}{m}\right).$$

Termit uudelleen järjestämällä saadaan haluttu väite.

$$\sum_{h=1}^{m} \frac{1}{h} = \log(m) + \gamma + \mathrm{O}\left(\frac{1}{m}\right). \qquad \square$$

Huomataan, että harmonisen sarjan osasummat $\sum_{h=1}^{m} \frac{1}{h}$ ovat asymptoottisesti ekvivalentit termin $\log(m)$ kanssa.

Palataan vielä Möbiuksen funktioon ennen kuin siirrytään tutkimaan Eulerin funktion keskimääräistä kasvunopeutta. Funktion μ saa arvon 0 useimmin verrattuna arvoihin 1 ja -1. Funktion asymptoottista käyttäytymistä voidaan tarkastella keskimääräisen kasvunopeuden avulla. Möbiuksen funktion keskimääräistä kasvunopeutta kuvataan *Mertensin funktiolla*

$$M(x) = \sum_{1 \leq n \leq x} \mu(n)$$

kaikille $n \in \mathbb{N}$. Mertensin funktiolle pätee, kun $|\mu(n)| \leq 1$, niin selvästi $|M(x)| \leq \lfloor x \rfloor$ luvuille $x > 0$. Keskimääräinen kasvunopeus Möbiuksen funktiolle saadaan näyttämällä raja-arvo

$$\lim_{x \to \infty} \frac{M(x)}{x} = 0.$$

Tarkka todistus löytyy lähteestä [6, s. 350-351].

3.2 Eulerin funktion keskimääräinen kasvunopeus

Määritellään seuraavaksi Eulerin φ-funktiosta muotoiltu summafunktio, jonka keskimääräisen kasvunopeuden näyttäminen on tutkielman päätulos.

Määritelmä 3.7. Olkoon $\Phi : \mathbb{N} \to \mathbb{R}$,

$$\Phi(n) = \sum_{h=1}^{n} \varphi(h), n \in \mathbb{N}.$$

Esimerkki 3.8. Summafunktio Φ saa arvoja

$$\Phi(5) = \sum_{h=1}^{5} \varphi(h) = \varphi(1) + \varphi(2) + \varphi(3) + \varphi(4) + \varphi(5) = 1 + 1 + 2 + 2 + 4 = 10.$$

$$\Phi(16) = \sum_{h=1}^{16} \varphi(h) = 80.$$

Seuraava lause osoittaa summafunktion keskimääräisen kasvunopeuden. Tuloksella on monia sovelluksia, joista kaksi esitetään tässä tutkielmassa. Lisää sovelluksista voi lukea lähteestä [12].

Lause 3.9. $\Phi(n) = \frac{3n^2}{\pi^2} + \mathrm{O}(n \log n)$.

Todistus. Todistus mukailee lähteestä [12, s. 353-354] löytyvää todistusta. Aloitetaan avaamalla $\Phi(n)$ ja sovelletaan siihen seurausta 1.22:

$$\Phi(n) = \varphi(1) + \varphi(2) + \cdots + \varphi(n) = \sum_{aa' \leq n} a'\mu(a).$$

Tulo $a'\mu(a)$ voidaan avata kahdeksi summaksi, kun muistetaan huomioida edellisen summauksen ehto $aa' \leq n$, jolloin

$$\sum_{aa' \leq n} a'\mu(a) = \sum_{a=1}^{n} \mu(a) \sum_{a'=1}^{\lfloor \frac{n}{a} \rfloor} a'. \tag{3.3}$$

Merkinnällä $\left\lfloor \frac{n}{a} \right\rfloor$ tarkoitetaan murtoluvun $\frac{n}{a}$ kokonaisosaa. Merkinnän tarkempi määritelmä löytyy tutkielman johdannon merkintöjä -osiosta. Huomataan, että summassa $\sum_{a'=1}^{\lfloor \frac{n}{a} \rfloor} a'$ lasketaan kokonaisluvuilla, jolloin se voidaan ilmaista aritmeettisen keskiarvon avulla:

$$\sum_{a'=1}^{\lfloor \frac{n}{a} \rfloor} a' = \frac{\left\lfloor \frac{n}{a} \right\rfloor \left(\left\lfloor \frac{n}{a} \right\rfloor + 1 \right)}{2}.$$

Sijoitetaan aritmeettinen keskiarvo yhtälöön (3.3):

$$\sum_{a=1}^{n} \mu(a) \left(\frac{\left\lfloor \frac{n}{a} \right\rfloor \left(\left\lfloor \frac{n}{a} \right\rfloor + 1 \right)}{2} \right) = \frac{1}{2} \sum_{a=1}^{n} \mu(a) \left(\left\lfloor \frac{n}{a} \right\rfloor^2 + \left\lfloor \frac{n}{a} \right\rfloor \right). \tag{3.4}$$

Tarkastellaan sulkeissa olevaa osaa $\left(\left\lfloor \frac{n}{a} \right\rfloor^2 + \left\lfloor \frac{n}{a} \right\rfloor \right)$. Tiedetään, että

$$\left\lfloor \frac{n}{a} \right\rfloor \leq \frac{n}{a} \leq \left\lfloor \frac{n}{a} \right\rfloor + 1,$$

joten

$$\left\lfloor \frac{n}{a} \right\rfloor^2 \leq \left(\frac{n}{a} \right)^2 \leq \left\lfloor \frac{n}{a} \right\rfloor^2 + 2 \left\lfloor \frac{n}{a} \right\rfloor + 1.$$

Termin $\left\lfloor \frac{n}{a} \right\rfloor^2 + 2\left\lfloor \frac{n}{a} \right\rfloor + 1$ keskimääräinen kasvunopeus on $\left\lfloor \frac{n}{a} \right\rfloor^2$, joten loppuosa arvioidaan O-merkinnän avulla, jolloin sen käsitteleminen helpottuu todistuksessa. Saadaan yhtälö

$$\left\lfloor \frac{n}{a} \right\rfloor^2 + 2 \left\lfloor \frac{n}{a} \right\rfloor + 1 = \left\lfloor \frac{n}{a} \right\rfloor^2 + \mathrm{O}\left(\frac{n}{a} \right),$$

joten alkuperäisen termin saa kirjoitettua muotoon

$$\left(\left\lfloor \frac{n}{a} \right\rfloor^2 + \left\lfloor \frac{n}{a} \right\rfloor \right) = \left(\frac{n^2}{a^2} \right) + \mathrm{O}\left(\frac{n}{a} \right).$$

Sijoitetaan arvio yhtälöön (3.4) ja avataan tulo funktion μ summan kanssa:

$$\frac{1}{2} \sum_{a=1}^{n} \mu(a) \left(\frac{n^2}{a^2} + \mathrm{O}\left(\frac{n}{a} \right) \right) = \frac{1}{2} \left(\sum_{a=1}^{n} \mu(a) \cdot \frac{n^2}{a^2} + \sum_{a=1}^{n} \mathrm{O}\left(\frac{n}{a} \right) \right) \tag{3.5}$$

$$= \frac{n^2}{2} \sum_{a=1}^{n} \frac{\mu(a)}{a^2} + \mathrm{O}\left(n \sum_{a=1}^{n} \frac{1}{a} \right). \tag{3.6}$$

Viimeisestä summasta häviää μ-funktio, koska se saa arvoja $-1, 0$ ja 1, joten μ ei vaikuta arviointiin. Kirjoitetaan summa $\sum_{a=1}^{n} \frac{1}{a}$ lauseen 3.5 avulla, jolloin yhtälöön saadaan haluttu logaritmi näkyviin:

$$\sum_{a=1}^{n} \frac{1}{a} = \log(n) + \gamma + \mathrm{O}\left(\frac{1}{n}\right) = \log(n) + \mathrm{O}(1).$$

Sijoitetaan tulos yhtälöön (3.6) ja saadaan, että

$$\frac{n^2}{2} \sum_{a=1}^{n} \frac{\mu(a)}{a^2} + \mathrm{O}(n \log(n) + \mathrm{O}(1)).$$

Merkintä $\mathrm{O}(1)$ yhdistyy sulkeiden ulkopuolella olevaan O-merkintään.

Vaihdetaan osasummat sarjoiksi, jolloin lisäksi tuleva termi arvioidaan merkinnällä O, koska sen kasvunopeus on hitaampi muihin verrattuna:

$$\frac{n^2}{2} \sum_{a=1}^{n} \frac{\mu(a)}{a^2} + \mathrm{O}(n \log(n)) = \frac{n^2}{2} \sum_{a=1}^{\infty} \frac{\mu(a)}{a^2} + \mathrm{O}(n \log(n)) + \mathrm{O}\left(n^2 \sum_{a=n+1}^{\infty} \frac{1}{a^2}\right). \tag{3.7}$$

Arvioidaan yhtälön (3.7) viimeistä termiä $\sum_{a=n+1}^{\infty} \frac{1}{a^2}$ integraalin avulla:

$$\sum_{a=n+1}^{\infty} \frac{1}{a^2} \leq \int_n^{\infty} \frac{1}{a^2} da = \frac{1}{n}.$$

Sijoitetaan arvio yhtälöön (3.7), jolloin saadaan

$$\frac{n^2}{2} \sum_{a=1}^{\infty} \frac{\mu(a)}{a^2} + \mathrm{O}(n \log(n)) + \mathrm{O}\left(n^2 \cdot \frac{1}{n}\right) = \frac{n^2}{2} \sum_{a=1}^{\infty} \frac{\mu(a)}{a^2} + \mathrm{O}(n \log(n)) + \mathrm{O}(n).$$

Nyt ollaan saatu funktion Φ keskimääräinen kasvunopeus siihen vaiheeseen, että sijoitetaan tutkielmassa aiemmin todistettujen lauseiden tulokset paikalleen. Lauseen 2.10 nojalla saadaan Eulerin funktion arvo $\zeta(2)$, johon sovelletaan Baselin ongelman ratkaisua $\zeta(2) = \frac{\pi^2}{6}$. Siis

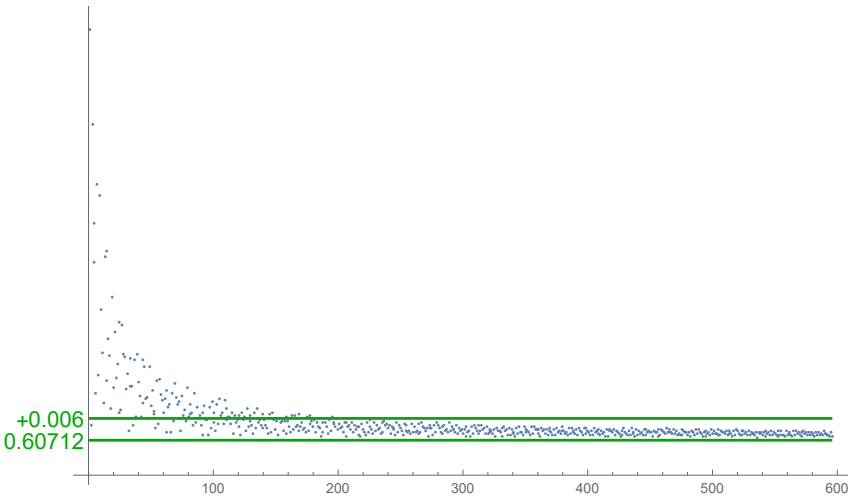
$$\begin{aligned} \Phi(n) = \frac{n^2}{2} \sum_{a=1}^{\infty} \frac{\mu(a)}{a^2} + \mathrm{O}(n \log(n)) + \mathrm{O}(n) &= \frac{n^2}{2} \cdot \frac{1}{\zeta(2)} + \mathrm{O}(n \log(n)) \\ &= \frac{n^2}{2} \cdot \frac{6}{\pi^2} + \mathrm{O}(n \log(n)) \\ &= \frac{3n^2}{\pi^2} + \mathrm{O}(n \log(n)). \end{aligned}$$

□

3.3 Suhteellisten alkulukuparien tiheys

Tähän mennessä on tutkittu Eulerin φ ja ζ -funktioita, Möbiuksen funktiota, tarkasteltu funktioiden keskimääräisten kasvunopeuksien arvioimista ja todistettu Φ-funktion keskimääräinen kasvunopeus. Funktion Φ kasvun sovelluksena pystytään todistamaan tutkielman toinen päätulos. Mikä on todennäköisyys, että kaksi satunnaisesti valittua kokonaislukua joukosta $\{1, 2, 3, \ldots, N\}^2$ ovat keskenään suhteellisia alkulukuja? Kysymystä

täytyy lähestyä ensin äärellisestä tilanteesta ja tämän jälkeen tutkia, mitä tapahtuu luvun N kasvaessa suureksi. Tarkastellaan tutkielman kansikuvaa ja huomataan, että 169 lukuparista 115 paria on suhteellisia alkulukuja keskenään, jolloin todennäköisyys saada satunnaisesti valittuna suhteelliset alkuluvut on 68%. Todennäköisyys on hieman suurempi, kun lukuja on vähän. Suuremmalla määrällä kokonaislukuja todennäköisyys saada suhteelliset alkuluvut on noin 61%.



Kuva 3.4: Suhteellisten alkulukuparien tiheys.

Kuvassa 3.4 nähdään suhteellisten alkulukuparien joukon asymptoottinen tiheys. Tiheyden heilahtelu on suurta, kun lukupareja on vähän. Tästä johtuen kansikuvassa olevien alkulukuparien määrä on suhteessa suuri kaikkiin lukupareihin kyseisessä ruudukossa. Virhe pienenee alle prosenttiin, kun ylitetään 200 kokonaislukuparin raja. Asymptoottinen tiheys lähestyy seuraavan lauseen osoittamaa arvoa.

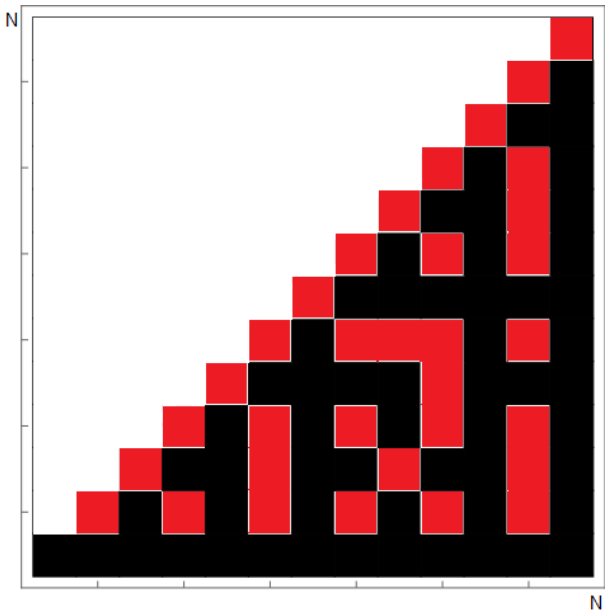
Lause 3.10. *Olkoon $N \in \mathbb{N}$. Merkitään suhteellisten alkulukuparien joukkoa*

$$T_N = \{(n, n') \in \mathbb{N} : 1 \leq n, n' \leq N, \mathrm{syt}(n, n') = 1\}$$

ruudukossa $N \times N$. Tällöin

$$\lim_{N \to \infty} \frac{\#T_N}{N^2} = \frac{6}{\pi^2} + \mathrm{O}\left(\frac{\log(N)}{N}\right) \approx 61\%.$$

Todistus. Tarkastellaan aluksi kuvaa 3.5.



Kuva 3.5: Puolikas $N \times N$-ruudukko ja sen diagonaali.

Kuvassa 3.5 nähdään puolet joukosta $\{1, 2, 3, \ldots, N\} \times \{1, 2, 3, \ldots, N\}$ ja ruudukon diagonaali. Punaiset ruudut kuvastavat tilannetta, kun $\text{syt}(n, n') \neq 1$ ja mustilla ruuduilla on merkitty tilanne, jossa $\text{syt}(n, n') = 1$. Todistuksessa osoitetaan, että mustia ruutuja on $N \times N$-ruudukossa noin 61%.

Olkoon $N \geq 1$, jolloin ruudukossa on N^2 kappaletta lukupareja. Kiinnitetään toinen lukuparin luvuista, jolloin näistä N^2 lukuparista Eulerin φ-funktio antaa meille niiden lukujen lukumäärän, jotka ovat suhteellisia alkulukuja kiinnitetyn luvun kanssa. Kuvan 3.5 tilanteessa φ-funktiosta muodostuu summa $\sum_{n=1}^{N} \varphi(n)$, jolloin koko ruudukosta $N \times N$ muodostettu summa on

$$2 \cdot \sum_{n=1}^{N} \varphi(n) - 1.$$

Summasta vähennetään yksi, koska diagonaalin ainut musta ruutu on pari $(1, 1)$, ja se tulee laskuun kahdesti mukaan molempien puolikkaiden mukana. Lauseen 3.9 nojalla tiedetään, että φ-funktioiden summa on funktion Φ keskimääräinen kasvunopeus:

$$2 \cdot \sum_{n=1}^{N} \varphi(n) - 1 = 2 \cdot \Phi(N) - 1 = 2 \cdot \left(\frac{3N^2}{\pi^2} + \mathrm{O}(N \log(N)) \right) - 1. \tag{3.8}$$

Yhtälöstä (3.8) saadaan lukuparien lukumäärä, jotka ovat keskenään suhteellisia alkulukuja ruudukossa $N \times N$.

Seuraavaksi lasketaan klassisen todennäköisyyden avulla, paljonko suhteellisia alkulukupareja on suhteessa kaikkiin ruudukossa oleviin lukupareihin. Saadaan suhde $N \times N$-

ruudukon lukupareista

$$\begin{aligned}\frac{2\cdot\left(\frac{3N^2}{\pi^2}+\mathrm{O}(N\log(N)\right)-1}{N^2} &= \frac{6}{\pi^2}+\frac{\mathrm{O}(N\log(N))}{N^2}-\frac{1}{N^2}\\ &= \frac{6}{\pi^2}+\mathrm{O}\left(\frac{\log(N)}{N}\right)-\frac{1}{N^2}\\ &= \frac{6}{\pi^2}+\mathrm{O}\left(\frac{\log(N)}{N}\right).\end{aligned}$$

Termi $-\frac{1}{N^2}$ kasvaa keskimääräisesti hitaammin termiin $\frac{\log(N)}{N}$ verrattuna, joten se voidaan arvioida O-merkinnän alle.

Kun luku N lähestyy kohti ääretöntä, termi $\mathrm{O}\left(\frac{\log(N)}{N}\right)$ menee nollaan. Tällöin suhteellisten alkulukuparien todennäköisyys on $\frac{6}{\pi^2}\approx 0.61$. □

Tulos voidaan yleistää tapaukseen, missä valitaan m kappaletta luonnollisia lukuja, ja tarkastellaan todennäköisyyttä, että näillä luvuilla m ei ole yhteisiä tekijöitä, jotka ovat suurempia kuin yksi. Tämän tapauksen todennäköisyys pystytään laskemaan suoraan Riemannin ζ-funktion arvolle $\frac{1}{\zeta(m)}$. Tilanteessa, missä tarkastellaan useampaa kuin kahta luonnollista lukua, tarvitaan lisäehto luvuille $(n_1, n_2, \ldots, n_m)$ siten, että
$\mathrm{syt}(n_i, n_j) = 1$ kaikille $i \neq j$. Tämän lisäehdon kanssa on onnistuttu laskemaan vain tilanne, missä on kolme satunnaisesti valittua lukua. Tässä tapauksessa todennäköisyys tippuu alle 30 prosentin [1].

3.4 Fareyn jonot

Tarkastellaan tutkielman lopuksi Fareyn jonoja, mikä on eräs lukuteorian osa-alue. Tässä kappaleessa osoitetaan, että Fareyn jonoilla on yhteys summafunktion Φ keskimääräisen kasvunopeuden kanssa. Kappaleessa tutustutaan Fareyn jonoihin pintapuolisesti yksittäisten ominaisuuksien kautta lähteen [21, s. 141-144] mukaisessa järjestyksessä. Lähteestä [12] löytyy lisää Fareyn jonojen tuloksia ja sovelluksia.

Almanakassa "Ladies Diary" esitettiin vuonna 1747 kysymys: "Kuinka monta erilaista murtolukua on olemassa, mitkä ovat pienempiä kuin yksi siten, että suurin nimittäjä on alle 100?" [18, s. 34]. Kysymys herätti mielenkiintoa ja oli haastava, koska vuonna 1747 kukaan ei ollut vielä määritellyt käsitettä Fareyn jonoille. Kysymys ratkaistiin seuraavan vuoden Ladies Diary -almanakassa. Vastaukseksi oli laskettu vuonna 1748, että ehdot täyttäviä murtolukuja olisi olemassa 3055 [13, s. 23].

Määritellään Fareyn jonot ja todistetaan niille muutamia perustuloksia, jotta voidaan Fareyn jonojen avulla antaa kysymykselle vastaus ja tarkistaa, onko se laskettu oikein vuonna 1748. Fareyn jonot voidaan määritellä eri tavoilla lähteen lähestymistavasta riippuen, kuten lähteitä [12] ja [21] vertaamalla huomaa.

Määritelmä 3.11. Määritellään *Fareyn jonot* induktion avulla. Merkitään termit $\frac{0}{1}$ ja $\frac{1}{1}$ ensimmäiselle riville. Seuraavien rivien $n = 2, 3, 4, \ldots$ termit rakentuvat säännöllä, missä n. rivi syntyy $(n-1)$. rivin termien järjestyksestä, mihin tulee uusi termi rivillä $(n-1)$ olevien vierekkäisten termien $\frac{q}{h}$ ja $\frac{k}{l}$ väliin, jos ehto $h + l \leq n$ pätee. Uusi termi on aina muotoa $\frac{q+k}{h+l}$.

Määritelmän 3.11 mukaan toisella rivillä ovat edellisen rivin termit $\frac{0}{1}$ ja $\frac{1}{1}$. Uusi termi $\frac{0+1}{1+1}$ tulee termien $\frac{0}{1}$ ja $\frac{1}{1}$ väliin, koska ehto $1+1 \leq 2$ täyttyy. Kolmannelle riville tulevat uudet termit $\frac{1}{3}$ ja $\frac{2}{3}$ toisen rivin termien väleihin. Neljännelle riville uusiksi termeiksi käyvät murtoluvut $\frac{1}{4}$ ja $\frac{3}{4}$, mutta termit $\frac{2}{5}$ ja $\frac{3}{5}$ eivät käy, koska $5 > 4$.

$$
\begin{array}{ccccccccccc}
\frac{0}{1} & & & & & & & & & & \frac{1}{1} \\
\frac{0}{1} & & & & & \frac{1}{2} & & & & & \frac{1}{1} \\
\frac{0}{1} & & & \frac{1}{3} & & \frac{1}{2} & & \frac{2}{3} & & & \frac{1}{1} \\
\frac{0}{1} & & \frac{1}{4} & \frac{1}{3} & & \frac{1}{2} & & \frac{2}{3} & \frac{3}{4} & & \frac{1}{1} \\
\frac{0}{1} & \frac{1}{5} & \frac{1}{4} & \frac{1}{3} & \frac{2}{5} & \frac{1}{2} & \frac{3}{5} & \frac{2}{3} & \frac{3}{4} & \frac{4}{5} & \frac{1}{1}
\end{array}
$$

Kuva 3.6: Viisi ensimmäistä Fareyn jonoa määritelmän 3.11 mukaan.

Kuvassa 3.6 nähdään, miten uudet rivit säilyttävät edellisten rivien järjestyksen, ja mihin uudet termit sijoittuvat määritelmän 3.11 mukaisesti.

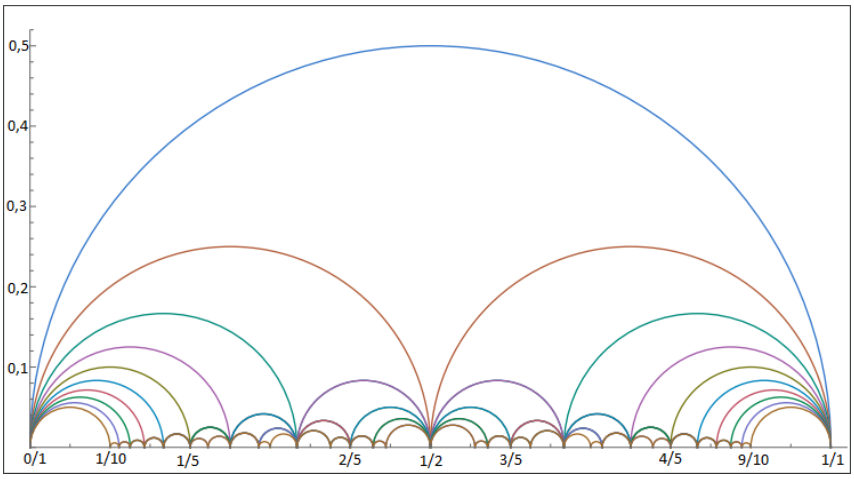
Esimerkki 3.12. Kirjoitetaan kuvan 3.6 viisi ensimmäistä Fareyn jonoa auki:

$$
\begin{aligned}
\mathscr{F}_1 &= \left\{\frac{0}{1}, \frac{1}{1}\right\} \\
\mathscr{F}_2 &= \left\{\frac{0}{1}, \frac{1}{2}, \frac{1}{1}\right\} \\
\mathscr{F}_3 &= \left\{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\right\} \\
\mathscr{F}_4 &= \left\{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\right\} \\
\mathscr{F}_5 &= \left\{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\right\}.
\end{aligned}
$$

Fareyn jonon pituus lasketaan termien lukumäärän mukaan, eli

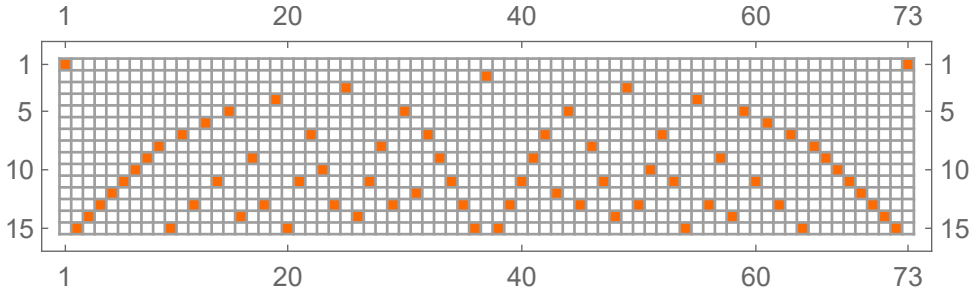
$$\#\mathscr{F}_1 = 2,\ \#\mathscr{F}_2 = 3,\ \#\mathscr{F}_3 = 5,\ \#\mathscr{F}_4 = 7 \ \text{ ja } \ \#\mathscr{F}_5 = 11.$$

Fareyn jonoissa termien lukumäärä kasvaa nopeasti suureksi, jolloin pituuden määrittäminen tietylle Fareyn jonolle muuttuu työlääksi.



Kuva 3.7: Fareyn kaaviolla esitettynä $\mathscr{F}_{10}$.

Ensimmäisessä kuvassa 3.7 on Fareyn kaavion avulla esitetty Fareyn jono $\mathscr{F}_{10}$. Fareyn kaavio muodostuu ympyrän kaarista, jotka yhdistävät Fareyn jonojen termit toisiinsa. Kaaviossa pisin ja korkein kaari kuvaa jonoa $\mathscr{F}_1$, eli se lähtee termistä $\frac{0}{1}$ ja päättyy termiin $\frac{1}{1}$. Seuraavat kaksi kaarta kuvaavat jonoa $\mathscr{F}_2$, koska siinä on kolme termiä, jotka yhdistetään toisiinsa. Näin jatketaan jonoon $\mathscr{F}_{10}$ asti, jolloin valmiiseen kuvaan on muodostunut Fareyn jono $\mathscr{F}_{10}$.



Kuva 3.8: Fareyn jono $\mathscr{F}_{15}$.

Toisessa kuvassa 3.8 on esitetty Fareyn jono $\mathscr{F}_{15}$ nimittäjien avulla. Väritetyt ruudut ovat jonon $\mathscr{F}_{15}$ nimittäjiä luvusta 1 lukuun 15. Väritetyt ruudut laskemalla saadaan termien lukumäärä kyseissä jonossa eli jonon $\mathscr{F}_{15}$ pituus on 73.

Kuvista 3.6, 3.7 ja 3.8 nähdään, että Fareyn jonojen termit käyttäytyvät symmetrisesti. Symmetrisen käyttäytymisen lisäksi Fareyn jonoilla on muitakin mielenkiintoisia ominaisuuksia, kuten termit $\frac{q}{h}$ ovat supistetussa muodossa siten, että $0 \leq \frac{q}{h} \leq 1$.

Seuraavassa lauseessa tarkastellaan kahta Fareyn jonon termiä $\frac{q}{h}$ ja $\frac{k}{l}$ ja osoitetaan niiden olevan vierekkäisiä, mikäli ne toteuttavat kaavan $kh - ql = 1$.

Lause 3.13. *Jos termit $\frac{q}{h}$ ja $\frac{k}{l}$ ovat vierekkäisiä Fareyn jonossa $\mathscr{F}_n$ siten, että termi $\frac{q}{h}$ on termin $\frac{k}{l}$ vasemmalla puolella, niin $kh - ql = 1$.*

Todistus. Todistus seuraa lähteessä [21, s. 142] esitettyä todistusta. Todistetaan väite induktion avulla. Tapaus on selvä, kun $n = 1$.

Tehdään induktio-oletus. Oletetaan, että väite pätee Fareyn jonolle $\mathscr{F}_{n-1}$, jolloin $kh - ql = 1$.

Osoitetaan, että väite pätee Fareyn jonolle $\mathscr{F}_n$. Fareyn jonossa $\mathscr{F}_n$ vierekkäisiä termejä ovat joko $\frac{q}{h}, \frac{k}{l}$ tai $\frac{q}{h}, \frac{q+k}{h+l}$ tai $\frac{q+k}{h+l}, \frac{k}{l}$, missä termit $\frac{q}{h}$ ja $\frac{k}{l}$ olivat vierekkäisiä jonossa $\mathscr{F}_{n-1}$. Nyt saadaan, että

$$\begin{aligned} kh - ql &= 1 \text{ tai} \\ (q+k)h - q(h+l) &= qh + kh - qh - ql = 1 \text{ tai} \\ k(h+l) - (q+k)l &= kh + kl - ql - kl = 1. \end{aligned}$$

Väite on osoitettu induktion avulla. □

Lauseen 3.13 avulla saadaan kaksi lisäehtoa Fareyn jonojen termeille.

Seuraus 3.14. *Fareyn jonojen termit ovat aina suuruusjärjestyksessä.*

Todistus. Olkoon termi $\frac{q}{h}$ Fareyn jonossa $\mathscr{F}_n$, missä $n \in \mathbb{N}$. Valitaan samasta Fareyn jonosta termi $\frac{k}{l}$, joka on termin $\frac{q}{h}$ viereinen termi oikealta puolelta. Todistus menee vastaavasti vasemmalta puolelta valitulle termille. Tällöin lauseen 3.13 nojalla pätee:

$$kh - ql = 1. \tag{3.9}$$

Jaetaan yhtälöä (3.9) puolittain nimittäjien tulolla:

$$\begin{aligned} \frac{kh}{hl} - \frac{ql}{hl} &= \frac{1}{hl} \\ \frac{k}{l} - \frac{q}{h} &= \frac{1}{hl} \geq 0. \end{aligned}$$

Väite seuraa. □

Seuraus 3.15. *Fareyn jonon termi $\frac{q}{h}$ on supistetussa muodossa, eli* $\operatorname{syt}(q, h) = 1$.

Todistus. Olkoon $n \in \mathbb{N}$. Olkoon Fareyn jonon $\mathscr{F}_n$ termi $\frac{q}{h}$, jolle halutaan osoittaa, että $\operatorname{syt}(q, h) = 1$. Valitaan samasta jonosta termi $\frac{k}{l}$ siten, että se on termin $\frac{q}{h}$ vierekkäinen termi vasemmalta puolelta. Todistus menee vastaavasti, jos valinta tehdään termin $\frac{q}{h}$ oikealta puolelta. Termeille $\frac{k}{l}$ ja $\frac{q}{h}$ pätee lauseen 3.13 nojalla yhtälö:

$$ql - kh = 1. \tag{3.10}$$

Muistetaan, että luvut $l, k \in \mathbb{N}$, jolloin yhtälöstä (3.10) ja Bézout'n lemmasta seuraa, että $\operatorname{syt}(q, h) = 1$. Bézout'n lemma löytyy lähteestä [6, s. 91]. □

Osoitetaan, että tämä vierekkäisten termien väliin tuleva uusi termi on yksikäsitteinen pienimmällä nimittäjällä.

Lause 3.16. *Olkoot termit $\frac{q}{h}$ ja $\frac{k}{l}$ vierekkäisiä missä tahansa Fareyn jonossa. Tällöin kaikista mahdollisista murtoluvuista termien $\frac{q}{h}$ ja $\frac{k}{l}$ välissä, murtoluku $\frac{q+k}{h+l}$ on yksikäsitteinen pienimmällä mahdollisella nimittäjällä.*

Todistus. Todistuksen idea seuraa lähdettä [21, s. 142-143]. Aluksi tarkastellaan termiä $\frac{q+k}{h+l}$. Termi esiintyy ensimmäisen kerran Fareyn jonossa $\mathscr{F}_{h+l}$ ja suuruusjärjestystä noudattaen se löytyy termien $\frac{q}{h}$ ja $\frac{k}{l}$ välistä,

$$\frac{q}{h} < \frac{q+k}{h+l} < \frac{k}{l}.$$

Oletetaan seuraavaksi, että termien välissä on mikä tahansa murtoluku $\frac{a}{b}$ siten, että

$$\frac{q}{h} < \frac{a}{b} < \frac{k}{l}.$$

Tällöin

$$\frac{k}{l} - \frac{q}{h} = \left(\frac{k}{l} - \frac{a}{b}\right) + \left(\frac{a}{b} - \frac{q}{h}\right) = \frac{kb-al}{lb} + \frac{ah-qb}{bh}. \tag{3.11}$$

Oletuksesta $\frac{a}{b} < \frac{k}{l}$ seuraa, että $kb - al > 0$. Koska $kb - al$ on kokonaisluku, tällöin $kb - al \geq 1$. Samanlaisilla perusteluilla saadaan, että $ah - qb \geq 1$. Siis

$$\frac{kb-al}{lb} + \frac{ah-qb}{bh} \geq \frac{1}{lb} + \frac{1}{bh} = \frac{h+l}{lbh}. \tag{3.12}$$

Yhdistetään yhtälöt (3.11) ja (3.12), jolloin

$$\frac{k}{l} - \frac{q}{h} = \frac{kb-al}{lb} + \frac{ah-qb}{bh} \geq \frac{h+l}{lbh}. \tag{3.13}$$

Seuraavaksi käytetään lausetta 3.13 yhtälöön (3.13), jolloin

$$\frac{h+l}{lbh} \leq \frac{k}{l} - \frac{q}{h} = \frac{kh-ql}{lh} = \frac{1}{lh}. \tag{3.14}$$

Yhtälöstä (3.14) seuraa, että $b \geq h + l$.

Jos $b > h + l$, niin termin $\frac{a}{b}$ nimittäjä ei ole pienin mahdollinen kaikista termien $\frac{q}{h}$ ja $\frac{k}{l}$ välisistä murtoluvuista. Tarkastellaan tilannetta, kun $b = h + l$. Sijoitetaan $b = h + l$ epäyhtälöön (3.12),

$$\frac{k(h+l)-al}{l(h+l)} + \frac{ah-q(h+l)}{(h+l)h} \geq \frac{1}{l(h+l)} + \frac{1}{(h+l)h} = \frac{1}{hl}. \tag{3.15}$$

Epäyhtälöitä (3.14) ja (3.15) tarkastelemalla huomataan, että epäyhtälöt voidaan muuttaa yhdeksi yhtälöksi, koska molempien epäyhtälöiden viimeinen termi on $\frac{1}{hl}$. Siis

$$\frac{k(h+l)-al}{l(h+l)} + \frac{ah-q(h+l)}{(h+l)h} = \frac{1}{l(h+l)} + \frac{1}{(h+l)h}. \tag{3.16}$$

Oletuksen avulla, että termit $\frac{q}{h}$ ja $\frac{k}{l}$ vierekkäisiä, voidaan lopuksi ratkaista luku a yhtälöiden $k(h + l) - al = 1$ ja $ah - q(h + l) = 1$ avulla. Yhtälöparista saadaan, että $a = q+k$. Näin on osoitettu, että termi $\frac{q+k}{h+l}$ on yksikäsitteisesti termien $\frac{q}{h}$ ja $\frac{k}{l}$ välissä. □

Palataan kappaleen ensimmäiseen esimerkkiin, jossa avattiin viisi ensimmäistä Fareyn jonoa. Tarkastellaan näiden jonojen termien lukumääriä:

$$\begin{aligned}
\#\mathscr{F}_1 &= 2,\\
\#\mathscr{F}_2 &= 3 = 2 + 1,\\
\#\mathscr{F}_3 &= 5 = 3 + 2,\\
\#\mathscr{F}_4 &= 7 = 5 + 2,\\
\#\mathscr{F}_5 &= 11 = 7 + 4
\end{aligned}$$

Huomataan, että termien lukumäärä koostuu edellisen jonon termeistä, johon lisätään jokin luku. Tämä jokin luku on koko tutkielman läpi käynyt Eulerin φ-funktion arvo kysytyssä jonossa. Termien lukumäärä lisääntyy kaavan

$$\#\mathscr{F}_n = \#\mathscr{F}_{n-1} + \varphi(n)$$

mukaisesti, missä Eulerin φ-funktio yhdistyy Fareyn jonoihin. Tämä kaava kertoo täsmällisesti Fareyn jonon pituuden. Esimerkiksi jonon $\mathscr{F}_{27}$ pituus on

$$\#\mathscr{F}_{27} = \#\mathscr{F}_{26} + \varphi(27) = 213 + 18 = 231.$$

Fareyn jonojen pituus käyttäytyy asymptoottisesta näkökulmasta seuraavan lauseen mukaisesti. Lause on yleistys edellisestä tuloksesta.

Lause 3.17. *Fareyn jonon $\mathscr{F}_n$ pituus on $\#\mathscr{F}_n = \frac{3n^2}{\pi^2} + \mathrm{O}(n\log(n))$.*

Todistus. Jonossa $\mathscr{F}_n$ esiintyvät termit muodostuvat jonon $\mathscr{F}_{n-1}$ termeistä ja uusista termeistä, jotka ovat määritelmän 3.11 mukaan muotoa $\frac{q}{h}$. Jos q ja h eivät ole keskenään suhteellisia alkulukuja, pystytään niiden muodostamaa termiä $\frac{q}{h}$ sieventämään. Tämä sievennetty muoto löytyy joistain edellisistä jonoista. Tästä seuraa suoraan, että $\mathrm{syt}(q,h) = 1$. Muotoillaan Fareyn jonon pituudelle kaava

$$\#\mathscr{F}_n = \#\mathscr{F}_{n-1} + \varphi(n).$$

Toisaalta $\mathscr{F}_1 = 1$, niin

$$\#\mathscr{F}_n = 1 + \sum_{m=1}^{n} \varphi(m) = 1 + \Phi(n).$$

Lauseen 3.9 nojalla

$$\#\mathscr{F}_n = \frac{3n^2}{\pi^2} + \mathrm{O}(n\log(n)). \qquad \square$$

Lause yhdisti summafunktion $\Phi(n)$ arvon Fareyn jonojen asymptoottiseen pituuteen. Fareyn jonot on eräs sovellus, johon $\Phi(n)$ arvoa voidaan käyttää suhteellisten alkulukuparien todennäköisyyden lisäksi.

Tässä vaiheessa on hyvä palauttaa mieleen kysymys aivan kappaleen alusta: "Kuinka monta erilaista murtolukua on olemassa, mitkä ovat pienempiä kuin yksi siten, että suurin nimittäjä on alle 100?" Kysymys on helpottunut huomattavasti Fareyn jonojen määrittelyn jälkeen.

Murtolukujen pitää olla aidosti pienempiä kuin yksi, ja kaikissa Fareyn jonoissa viimeinen termi on yksi, jolloin muistetaan vähentää lopputuloksesta yksi pois. Suurimman

nimittäjän pitää olla alle 100, niin silloin napataan edellinen Fareyn jono $\mathscr{F}_{99}$. Kysymyksessä haetaan tarkalleen lukumäärää $\#\mathscr{F}_{99} - 1$.

Termien $\mathscr{F}_{99} - 1$ lukumäärä on

$$\#\mathscr{F}_{99} - 1 = 3005 - 1 = 3004.$$

Vuonna 1747 esitettyyn kysymykseen saadaan vastaukseksi, että on olemassa 3004 erilaista ehdot täyttävää murtolukua. Huomataan tämän eroavan alkuperäisestä vastauksesta 51 murtoluvun verran, joten tällöin on tapahtunut käsin laskiessa jokin virhe.

Jos tarkastellaan asymptoottisen pituuden kaavan kautta termien lukumäärää jonossa $\mathscr{F}_{99}$, niin saadaan jonon pituudeksi

$$\#\mathscr{F}_{99} \approx \frac{3 \cdot 99^2}{\pi^2} = 2979.$$

Jos verrataan yllä laskettuun 3004 murtolukuun, niin vastauksesta puuttuu noin 24 murtolukua, jolloin virhe on hieman alle prosentin luokkaa. Asymptoottisen pituuden tarkkuus on todella täsmällinen jo jonon $\mathscr{F}_{99}$ kohdalla. Virhe pienenee, mitä pidemmälle Fareyn jonoissa mennään.

Luku 4

Kompleksinen ζ-funktio

Luvussa kaksi tarkasteltiin Eulerin ζ-funktiota ja sen ominaisuuksia reaaliluvuilla. Palataan samaan funktioon, mutta laajennetaan sen määrittelyjoukko kompleksilukuihin. Kompleksinen ζ-funktio, eli Riemannin ζ-funktio, määritellään myös sarjana, joten luvun neljä alkuun määritellään kompleksiset sarjat ja niiden suppeneminen. Tästä siirrytään määrittelemään Riemannin ζ-funktio ja tarkastelemaan sen nollakohtia. Tutkielman viimeisenä aiheena tutustutaan Riemannin hypoteesiin, koska se liittyy ζ-funktion eräiden nollakohtien sijaintiin. Luvussa käydään hyvin kevyesti läpi kompleksianalyysin tuloksia, koska tarkoitus on esitellä Riemannin ζ-funktio ja sen nollakohdat mahdollisimman kattavasti ilman tarkkoja yksityiskohtia.

4.1 Kompleksiset sarjat

Seuraavaksi perehdytään kompleksisen sarjan käsitteeseen. Kompleksitermiset sarjat käyttäytyvät samankaltaisesti kuin reaaliset sarjat, koska termin ollessa kompleksinen tutkitaan sen reaaliosan ja imaginaariosan reaalisen kertoimen käyttäytymistä. Tämän kaltainen tarkastelu mahdollistaa kompleksisten sarjojen suppenemisen ja hajaantumisen määrittelyn samoin kuin reaalisten sarjojen tapauksessa.

Määritelmä 4.1. Olkoon $(z_m)_{m=1}^{\infty}$ kompleksilukujen muodostama jono, ja määritellään tämän avulla jono $(c_m)_{m=1}^{\infty}$ siten, että $c_1 = z_1,\ c_2 = z_1 + z_2,\ c_3 = z_1 + z_2 + z_3, \ldots$. Tällöin *kompleksinen osasummien jono* on muotoa

$$c_m = z_1 + z_2 + z_3 + \cdots + z_m$$

ja *kompleksinen sarja* on muotoa

$$\sum_{m=1}^{\infty} z_m,$$

jokaiselle $m \in \{1, 2, 3, \ldots\}$. Sarjan termit ovat kompleksilukuja $z_m = x_m + iy_m$, ja $m \in \mathbb{N}$.

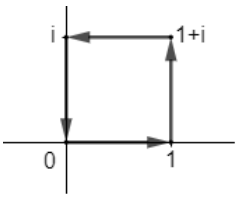
Muotoillaan tästä seuraavaksi tarkempi lause, jossa kompleksisen sarjan suppeneminen on verrattavissa reaalisen sarjan suppenemiseen.

Lause 4.2. *Kompleksinen sarja suppenee, jos ja vain jos termien reaali- ja imaginaariosista muodostetut sarjat suppenevat.*

Todistus. Todistus seuraa kompleksisen jonon $(c_m)_{m=1}^{\infty}$ raja-arvon olemassaolosta. □

Esimerkki 4.3. Sarja $\sum_{n=0}^{\infty} i^n$ hajaantuu, koska osasummien jonolla ei ole raja-arvoa ja se käyttäytyy jaksollisesti:

$$1,\ 1+i,\ 1+i+i^2=i,\ 1+i+i^2+i^3=0,\ 1+i+i^2+i^3+i^4=1,\ \ldots.$$



Kuva 4.1: Esimerkin 4.3 osasummien jaksollisen käyttäytymisen tulos

Määritellään seuraavaksi funktiojonon ja funktiosarjan tasainen suppeneminen.

Määritelmä 4.4. Funktiojono $(g_n)_{n=1}^{\infty}$ *suppenee tasaisesti* joukossa $F \subset \mathbb{C}$ funktioon $g : F \to \mathbb{C}$, jos jokaiselle $\varepsilon > 0$ on olemassa luku N siten, että

$$|g_n(z) - g(z)| \leq \varepsilon \text{ kaikille } z \in F \text{ ja kaikille } n \geq N, n \in \mathbb{N}.$$

Funktiosarja $\sum_{n=0}^{\infty} f_n$ muodostuu funktiojonoista $(g_m)_{m=0}^{\infty}$, missä $g_m : F \to \mathbb{C}$ ja määritellään, että $f_0 = g_0$ ja $f_n = g_m - g_{m-1},\ n \in \mathbb{N}$. Osasumma muodostuu siten, että

$$g_m = g_0 + (g_1 - g_0) + \cdots + (g_m - g_{m-1}) = \sum_{n=0}^{m} f_n.$$

Määritelmä 4.5. Funktiosarja $\sum_{n=0}^{\infty} f_n$ funktioista $f_n : F \to \mathbb{C}$ *suppenee itseisesti ja tasaisesti* joukossa F, jos sarja $\sum_{n=0}^{\infty} |f_n|$ suppenee tasaisesti joukossa F.

Tämä tapahtuu, jos funktiojono $(k_n)_{n=0}^{\infty}$ termeineen $k_n = |f_1| + \cdots + |f_n|$ suppenee tasaisesti joukossa F.

Huomautus 4.6. Itseisesti ja tasaisesti kompakteissa joukoissa suppenevan funktiosarjan sanotaan suppenevan *normaalisti*.

Lause 4.7. *Jos funktiosarja suppenee normaalisti, niin se suppenee tasaisesti kompakteilla joukoilla.*

Todistus. Olkoot sarja $\sum_{n=0}^{\infty} f_n$ kuten yllä ja

$$g_n = f_1 + f_2 + \cdots + f_n \text{ ja } k_n = |f_1| + |f_2| + \cdots + |f_n|.$$

Aloitetaan todistus epäyhtälö tarkastelulla

$$|g_m(z) - g_n(z)| \leq |f_{n+1}(z)| + \cdots + |f_m(z)| = k_m(z) - k_n(z),$$

mikä on totta kaikilla $z \in F$ ja $m \geq n$. Määritelmästä 4.5 seuraa, että funktiojono k_n suppenee tasaisesti funktioon k joukossa F jollekin $k : F \to \mathbb{C}$.

Todistetaan, että funktiojono g_n on tasainen Cauchy-jono eli se suppenee tasaisesti. Olkoon $\varepsilon > 0$ ja olkoon luku N siten, että $|k_n(z) - k(z)| \leq \varepsilon$ kaikilla $n \in \mathbb{N}$. Silloin kaikilla $z \in F, n, m \in \mathbb{N}$ seuraa, että

$$k_m(z) - k_n(z) = |k_m(z) - k_n(z)| \leq |k_m(z) - k(z)| + |k(z) - k_n(z)| \leq 2\varepsilon$$

kaikilla $z \in F, m \geq n \geq N$. Tällöin funktiojono $(g_n)_{n=0}^{\infty}$ on tasainen Cauchy, jolloin funktiojono g_n suppenee tasaisesti funktioon g joukossa F jollekin $g : F \to \mathbb{C}$. □

4.2 Riemannin ζ-funktio

Bernhard Riemann tutustui Eulerin ζ-funktioon, ja näytti 1800-luvulla, että ζ-funktion voi laajentaa koskemaan kompleksilukuja, joiden reaaliosa on aidosti suurempaa kuin 1 [16]. Tämän johdosta Eulerin ζ-funktio tunnetaan paremmin Riemannin ζ-funktiona. Riemannin työskentely lukuteorian osa-alueella painottuikin suurimmalta osin ζ-funktion ominaisuuksien tutkimiseen ja Riemannin hypoteesin muotoilemiseen.

Määritelmä 4.8. *Riemannin funktio* määritellään kompleksisena sarjana

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z},$$

missä $\zeta : \{z \in \mathbb{C} : \mathrm{Re}(z) > 1\} \to \mathbb{C}$.

Sarjaa olivat käsitelleet Eulerin lisäksi Chebyshev ja Dirichlet, mutta Riemann oli ensimmäinen, joka tutki sarjan käyttäytymistä luvuille $z \in \mathbb{C}$. Vuonna 1837 Dirichlet julkaisi kuuluisan tuloksensa alkuluvuista aritmeettisissa lukujonoissa, joita hän tutki Dirichlet'n sarjaksi kutsutulla työkalulla [3]. Sarjan Dirichlet määritteli seuraavasti:

$$D(z) = \sum_{n=1}^{\infty} \frac{a_n}{n^z},$$

missä kertoimet $a_n \in \mathbb{C}$, ja luku z on kompleksimuuttuja. Yksi tunnetuimmista Dirichlet'n sarjoista on Riemannin funktio ζ.

Euler todisti ζ-funktion suppenevan puolisuoralla $1 < s < \infty$. Tämä todistus voidaan laajentaa koskemaan kompleksitasoa, jolloin tarkastellaan lukuja $z \in \mathbb{C}$, joiden $\mathrm{Re}(z) > 1$.

Lause 4.9. *Sarja* $\sum_{n=1}^{\infty} \frac{1}{n^z}$ *suppenee normaalisti joukossa* $\{z \in \mathbb{C} : \mathrm{Re}(z) \geq c\}$, *missä* $c \in \mathbb{R}$ *ja* $\mathrm{Re}(z) \geq c > 1$.

Todistus. Merkitään, että $\mathrm{Re}(z) = \alpha > 1$. Tällöin $\frac{1}{n^\alpha} \leq \frac{1}{n^c}$. Kompleksianalyysin laskusäännöistä muistetaan, että $|w^z| = w^{\mathrm{Re}(z)}$. Yliharmoninen sarja $\sum_{n=1}^{\infty} \frac{1}{n^c}$ suppenee itseisesti, joten majoranttiperiaatteen nojalla sarja $\sum_{n=1}^{\infty} \left|\frac{1}{n^z}\right|$ ja funktio ζ suppenevat myös itseisesti. Väite seuraa eli sarja $\sum_{n=1}^{\infty} \frac{1}{n^z}$ suppenee normaalisti. □

Huomautus 4.10. Riemannin ζ-funktio hajaantuu harmonisena sarjana, kun $z = 1$.

Määritellään seuraavaksi analyyttiset funktiot.

Määritelmä 4.11. Olkoon avoin $C \subset \mathbb{C}$ ja $C \neq \emptyset$. Olkoon $f : C \to \mathbb{C}$ jokaisessa joukon C pisteessä kompleksisesti differentioituva funktio. Tällöin f on *analyyttinen funktio* joukossa C.

Osassa kompleksianalyysin kirjallisuutta käytetään holomorfisuus -termiä kuvaamaan analyyttisyyttä, vaikka ne määritellään hyvin eri tavoilla. Kompleksisesta differentioituvuudesta ja analyyttisistä funktioista voi lukea lisää Bruce Palkan kompleksianalyysin teoksesta [23, s. 62-68 & 256-269].

Seuraavaksi esitellään ζ-funktion analyyttisyys, jolloin se pystytään jatkamaan analyyttisesti koko kompleksitasoon lukuunottamatta pistettä $z = 1$, koska tässä kohdassa ζ-funktiolla on ensimmäisen kertaluvun napa.

Lause 4.12. *Riemannin ζ-funktio, $\zeta : \{z \in \mathbb{C} : \mathrm{Re}(z) > 1\} \to \mathbb{C}$, on analyyttinen.*

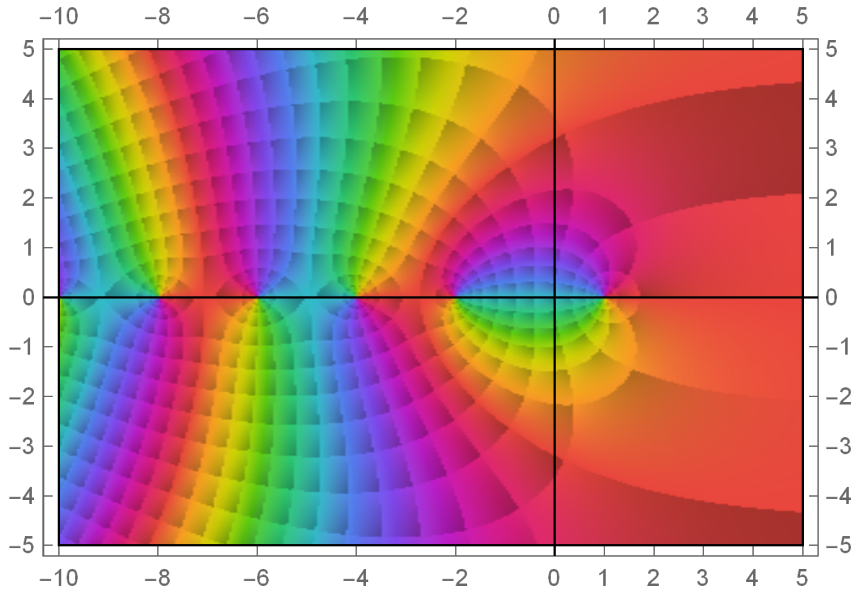
Todistus. Tuloksen todistamiseen tarvittava ydinkohta on funktion itseinen ja tasainen suppeneminen kompakteilla joukoilla. Lauseessa 4.9 osoitettiin, että funktio ζ suppenee itseisesti ja tasaisesti. Tämä määrää ζ-funktion analyyttisyyden muutaman lisätuloksen kanssa. Tulosta ei todisteta tarkemmin, koska vaadittavat lisätulokset eivät ole tutkielman kannalta oleellisia. Tarkka todistus löytyy lähteestä [23, s. 256-258]. □

Lause 4.13. *(ζ-funktion analyyttinen jatkaminen). On olemassa analyyttinen funktio $\zeta : \mathbb{C} - \{1\} \to \mathbb{C}$ siten, että*

$$\zeta(z) = \sum_{n=1}^{\infty} \frac{1}{n^z},$$

kaikille $z \in \mathbb{C}$, joiden $\mathrm{Re}(z) > 1$.

Todistus. Katso [20, s. 319-321] □



Kuva 4.2: Analyyttisesti jatketun ζ-funktion triviaaleja nollakohtia.

Kuvassa 4.2 nähdään analyyttisesti jatketun Riemannin ζ-funktion viisi ensimmäistä triviaalia nollakohtaa ja napa kohdassa $z = 1$. Värityksestä nähdään, miten ζ-funktio käyttäytyy erilaisilla arvoilla. Kappaleen alussa todistettiin, että funktio ζ suppenee joukossa, missä $\mathrm{Re}(z) > 1$. Tämä alue on kuvassa väritetty punaisen sävyillä. Kohdassa $z = 1$ funktio hajaantuu, jota on kuvassa merkitty pyörteellä. Kuvassa käytettyjen värien tarkempi selitys löytyy lähteestä [26, s. 248-249].

Huomautus 4.14. Luonnollisten lukujen sarjan tiedetään hajaantuvan positiiviseen ääretömään:

$$1 + 2 + 3 + 4 + \cdots = \infty.$$

Kirjoitetaan luonnolliset luvut tutun sarjan muotoon:

$$1 + 2 + 3 + 4 + \cdots = \sum_{n=1}^{\infty} \frac{1}{n^{-1}}. \tag{4.1}$$

Luonnollisten lukujen sarja voidaan esittää Riemannin ζ-funktion arvolla $z = -1$. Muistetaan, että Riemannin funktio on määritelty, kun $\mathrm{Re}(z) > 1$, joten nyt ollaan funktion määrittelyjoukon ulkopuolella. Matemaatikot ovat osoittaneet, että arvo $\zeta(-1)$ voidaan laskea, ja että kyseinen arvo olisi

$$\zeta(-1) = -\frac{1}{12}. \tag{4.2}$$

Yhtälöiden (4.1) ja (4.2) voidaan ajatella väittävän, että hajaantuvalla sarjalla olisi arvo. Tässä tapauksessa se tarkoittaisi, että kaikkien positiivisten kokonaislukujen summa olisi negatiivinen murtoluku.

Tilannetta kutsutaan ζ-funktion *regularisoinniksi*. Teoreettisessa fysiikassa ja matematiikassa ζ-funktion regularisointi on menetelmä, jonka avulla pystytään antamaan äärellisiä arvoja päättymättömille tuloille ja hajaantuville sarjoille. Tämä normalisointimenetelmä antaa mahdollisuuden käsitellä hajaantuvia sarjoja lukuteoriassa jollain konkreettisilla

arvoilla, kuten yhtälö (4.2) osoitti. Nykyään ζ-funktion regularisointia käytetään fysiikan puolella, koska säieteorian tuloksien pohjalla vaikuttaa luonnollisten lukujen summan tulos. Lähteestä [8] voi lukea lisää ζ-funktion erilaisista sovelluksista fysiikassa ja lähteessä [3, s. 265-266] käsitellään ζ-funktion arvoja negatiivisilla kokonaisluvuilla.

4.3 Funktion ζ nollakohdat ja Riemannin hypoteesi

Riemann tutki nollakohtien olemassaoloa ja sijaintia analyyttisesti jatketulle ζ-funktiolle. Osan nollakohdista Riemann sai selville suoraan mukaansa nimetyn funktionaaliyhtälön avulla. Lopuista nollakohdista keskustellaan vielä tänäkin päivänä ja yritetään todistaa tuloksia niille. Tarkastellaan ensin aluetta, missä Riemannin funktiolla ei ole nollakohtia.

Lause 4.15. $\zeta(z) \neq 0$ *kaikilla* $z \in \mathbb{C}$, *joiden* $\mathrm{Re}(z) > 1$.

Todistus. Lauseesta 2.7 muistetaan, että tulo $\prod_{n=1}^{\infty}(1 + b_n)$ suppenee, jos ja vain jos sarja $\sum_{n=1}^{\infty} b_n$ suppenee.

Kirjoitetaan funktio ζ tuloesityksensä avulla:

$$\zeta(z) = \prod_{n=1}^{\infty} \frac{1}{1 - p_n^{-z}}. \tag{4.3}$$

Nyt voidaan muokata yhtälössä (4.3) tulon sisällä olevaa termiä:

$$\frac{1}{1 - p_n^{-z}} = \frac{p_n^z}{p_n^z - 1} = 1 + \frac{1}{p_n^z - 1}.$$

Merkitään $b_n = \frac{1}{p_n^z - 1}$. Arvioidaan lukua b_n ylöspäin, jolloin

$$\frac{1}{p_n^z - 1} \leq \frac{1}{p_n^z}. \tag{4.4}$$

Sarja $\sum_{n=1}^{\infty} \frac{1}{p_n^z - 1}$ suppenee itseisesti majoranttiperiaatteen nojalla, jolloin tulo $\prod_{n=1}^{\infty}(1 + b_n)$ suppenee, kun $\mathrm{Re}(z) > 1$.

Jos Riemannin ζ-funktiolla olisi nollakohtia, täytyisi päättymättömän tulon määritelmän 2.4 nojalla jokin tulon $\prod_{n=1}^{\infty}(1 + b_n)$ tekijöistä olla nolla. Tämä ei kuitenkaan ole mahdollista, koska termi $\frac{1}{p_n^z - 1} \neq 0$ kaikilla $p_n \in \mathbb{P}$, missä $n \in \mathbb{N}$. Tulontekijöillä ei ole nollakohtia, joten väite seuraa. □

Lause 4.16. *Riemannin funktiolla* ζ *ei ole nollakohtia suoralla* $\mathrm{Re}(z) = 1$.

Todistus. Katso [9, s. 171]. □

Lauseista 4.15 ja 4.16 seuraa, että Riemannin ζ-funktiolla ei ole nollakohtia joukossa

$$\{z \in \mathbb{C} : \mathrm{Re}(z) \geq 1\}.$$

Tätä aluetta kutsutaan *nollakohtavapaaksi alueeksi.*

Jotta päästään käsiksi ζ-funktion nollakohtiin, tarvitsee ensin määritellä funktionaaliyhtälö.

Lause 4.17. *(Riemannin funktionaaliyhtälö). Olkoon* $z \in \mathbb{C}$, *niin*

$$\zeta(z) = 2(2\pi)^{z-1} \sin\Big(\frac{\pi z}{2}\Big)\Gamma(1-z)\zeta(1-z).$$

Todistus. Katso [6, s. 380-381]. □

Riemannin funktionaaliyhtälössä esiintyvä gammafunktio Γ on matematiikan tunnetuimpia ja tärkeimpiä funktioita sen laajojen sovellusmahdollisuuksien vuoksi. Gammafunktio on Eulerin kehittelemä funktio 1750-luvulta [16]. Funktiolla on tärkeä rooli Riemannin ζ-funktion kanssa työskennellessä. Käydään aluksi läpi gammafunktion eräs määritelmä. Lisäksi huomataan, että gammafunktiolla on hyvin paljon samankaltaisia ominaisuuksia ζ-funktion kanssa.

Määritelmä 4.18. *Gammafunktio* $\Gamma(z)$ määritellään Eulerin integraalina:

$$\Gamma(z) = \int_0^\infty e^{-t}t^{z-1}\, dt,\ \mathrm{Re}(z) > 0 \tag{4.5}$$

Lause 4.19. *Gammafunktio* Γ *on analyyttinen funktio puolitasossa* $\mathrm{Re}(z) > 0$.

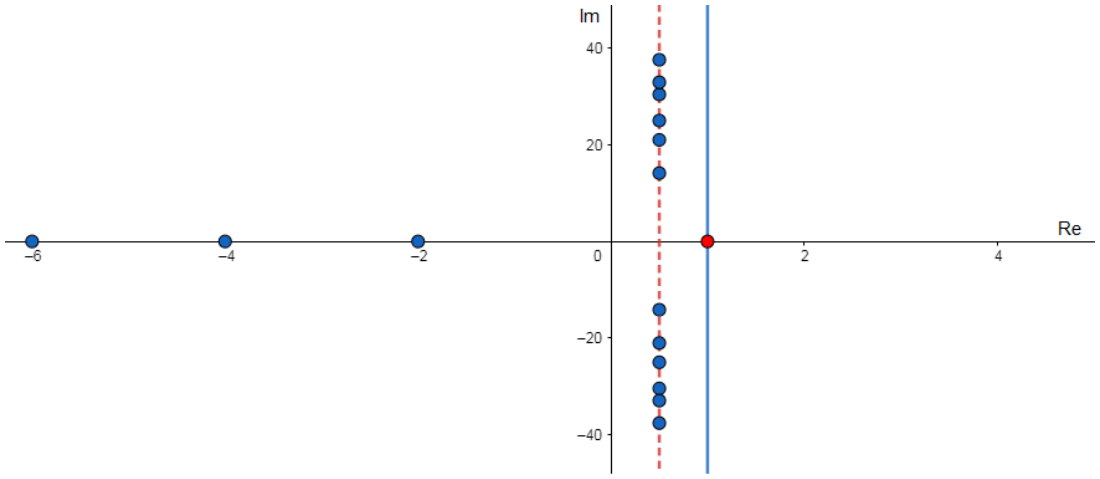
Todistus. Katso [20, s. 303-305]. □

Funktionaaliyhtälöstä saadaan laskettua nollakohtia ζ-funktiolle, ja tämän takia kyseisiä nollakohtia kutsutaan *triviaaleiksi nollakohdiksi*. Riemannin ζ-funktiolla on triviaaleja nollakohtia jokaisessa pisteessä $z = -2k$, missä $k \in \mathbb{N}$. Kuvassa 4.2 nähtiin funktion viisi ensimmäistä triviaalia nollakohtaa.

Funktiolla ζ on triviaalien nollakohtien lisäksi *ei-triviaaleiksi* kutsuttuja nollakohtia. Bernhard Riemann julkaisi vuonna 1859 ainoan lukuteoreettisen teoksensa [3]. Tämä teos mullisti silloisen lukuteorian, koska näihin sivuihin mahtui myöhemmin milleniumongelmaksi kutsuttu matematiikan hypoteesi. Kyseisessä teoksessa Riemann muotoili kaksi tulosta koskien analyyttisesti jatketun ζ-funktion nollakohtia. Riemann väitti teoksessaan, että funktiolla on äärettömän monta ei-triviaalia nollakohtaa, jotka sijaitsevat kaikki yhdensuuntaisvyössä $0 < \mathrm{Re}(z) < 1$. Toinen väite oli, että kaikki nämä ei-triviaalit nollakohdat löytyvät suoralta $\mathrm{Re}(z) = \frac{1}{2}$. Ensimmäisen väitteen todisti J. Hadamard vuonna 1893. Toinen hypoteeseistä jäi ilman todistusta. David Hilbert lisäsi Riemannin muotoileman hypoteesin ratkaisemattomien matemaattisten ongelmien listaansa vuonna 1900 [5]. Riemannin hypoteesi on todistamatta tätä tutkielmaa kirjoittaessani maaliskuussa 2020.

Muotoillaan seuraavaksi Riemannin kuuluisa hypoteesi ja tutkitaan, miten matemaatikot ovat yrittäneet sitä lähestyä vuosien varrella.

Hypoteesi 4.20. *(Riemannin hypoteesi) Kaikki Riemannin* ζ*-funktion ei-triviaalit nollakohdat sijaitsevat kriittiseksi suoraksi kutsutussa joukossa* $\mathrm{Re}(z) = \frac{1}{2}$.



Kuva 4.3: Funktion ζ triviaalit ja ei-triviaalit nollakohdat kompleksitasossa. Punainen piste on ζ-funktion napa kohdassa $z = 1$.

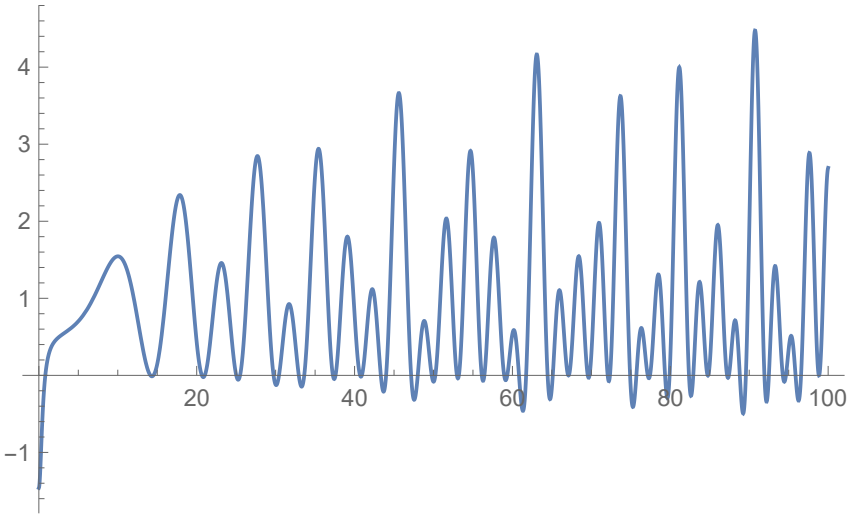
Kuvan 4.3 avulla käydään seuraavaksi läpi, mitä tarkoittavat kriittinen nauha ja kriittinen suora. Kriittisellä nauhalla tarkoitetaan edellä mainittua yhdensuuntaisvyötä $0 < \mathrm{Re}(z) < 1$ ja kriittinen suora $\mathrm{Re}(z) = \frac{1}{2}$ on kuvassa 4.3 merkitty katkoviivalla. Riemannin hypoteesi mukaan loput ζ-funktion nollakohdat löytyvät tältä suoralta.

Riemann esitteli kaavan, jonka avulla hän pyrki osoittamaan ζ-funktion nollakohtien lukumäärää $N(T)$ suljetussa suorakaiteessa $\{0 \leq \mathrm{Re}(z) \leq 1, 0 \leq \mathrm{Im}(z) \leq T\}$. Riemann muotoili lauseen, muttei saanut sitä todistettua. Todistuksen sai tehtyä von Mangoldt vuonna 1905 [20]. G. H. Hardy todisti vuonna 1915, että ei-triviaaleja nollakohtia on ääretön määrä kriittisellä suoralla [3]. Arvioita nollakohtien määrästä ja yksinkertaisuudesta tehtiin useita, kunnes vuonna 1903 J. P. Gram laski ensimmäiset 15 ζ-funktion nollakohtaa [24]. Levinson pystyi vuonna 1947 osoittamaan, että ainakin $\frac{1}{3}$ ei-triviaaleista nollakohdista sijaitsee kriittisellä suoralla. Tätä tulosta on pystytty parantamaan oletukseen, että ainakin 40 prosentia ei-triviaaleista nollakohdista sijaitsee kyseisellä suoralla [9].

Tästä eteenpäin tietokoneiden kehittyessä nollakohtia on pystytty laskemaan jo miljoonien edestä. Asiasta enemmän kiinnostuneet voivat tutustua Andrew Odlyzkon tekemiin löydöksiin nollakohtien alalla, sillä hän on omilla nettisivuillaan [22] listannut ζ-funktion nollakohtia monilla erilaisilla tavoilla.

Kuvasta 4.3 nähdään, että ei-triviaalit nollakohdat sijoittuvat kriittiselle suoralle symmetrisesti reaaliakseliin nähden. Käyttäytyminen johtuu ζ-funktion konjugaattiominaisuudesta: $\zeta(\overline{z}) = \overline{\zeta(z)}$.

Riemannin hypoteesin todistuksessa pitäisi pystyä osoittamaan, että kaikki loput nollakohdat sijoittuvat tähän kriittiseen linjaan tai pitäisi pystyä näyttämään, että löytyy yksikin nollakohta tämän kriittisen linjan ulkopuolelta. Tähän ajatukseen ovat matemaatikot tarttuneet myös eliminointinäkökulman kautta. Matemaatikot ovat yrittäneet osoittaa, että kriittisen suoran ympärillä ζ-funktiolla olisi "nollakohta vapaa alue" joukossa $\left\{\frac{1}{2} < \mathrm{Re}(z) < 1\right\}$. Tämän tuloksen todistaminen osoittaisi sen, ettei hypoteesin ulkopuolisia nollakohtia olisi tällä välillä.



Kuva 4.4: Funktion ζ imaginaariosan $\mathrm{Im}(z) = it$ kertoimen t vaihtelu välillä [1,100].

Suomalaisilla matemaatikoilla on ollut paikkansa Riemannin hypoteesiä ratkoessa. Tunnetuin suomalainen tällä matematiikan alalla on ollut Ernst Lindelöf, koska hänen hypoteesinsa jälkeen ovat muutkin matemaatikot yrittäneet lähestyä ongelmaa aivan uudesta näkökulmasta. Lindelöf vei hypoteesin tutkimuksen suunnan kohti ζ-funktion momentteja, mikä on nykyään arvostettu tutkimuksenhaara Riemannin hypoteesia lähestyessä. Lindelöf muotoili vuonna 1908 *Lindelöfin hypoteesiksi* kutsutun tuloksensa.

Lause 4.21. $\zeta\left(\frac{1}{2} + it\right) = \mathrm{O}(t^{\varepsilon})$, *jokaiselle* $\varepsilon \in \mathbb{R}_+$.

Lindelöfin hypoteesi on huomattavasti heikompi Riemannin hypoteesiin verrattuna, koska Riemannin hypoteesistä seuraa Lindelöfin hypoteesi, mutta toisin päin päättely ei päde. Funktion ζ momenteista, Lindelöfin hypoteesista ja muista tärkeistä Lindelöfin tuloksista ζ-funktiolla saralla voi lukea lisää lähteestä [16].

Riemannin hypoteesi on keskeisin avoin ongelma matematiikassa. Hän, joka hypoteesin saa näytettyä todeksi tai kumottua sen, pääsee historiankirjoituksiin Riemannin, Eulerin ja muiden kuuluisien matemaatikkojen rinnalle.

Kirjallisuutta

[1] Sergei Abramovich, Yakov Yu. Nikitin: *On the probability of co-primality of two natural numbers chosen at random (Who was the first to pose and solve this problem?)*, arXiv.org, math, arXiv:1608.05435v2, 11.4.2017

[2] Tom M. Apostol: *A proof that Euler missed: evaluating $\zeta(2)$ the easy way*, Math. Intelligencer, 5(3):59-60, 1983.

[3] Tom M. Apostol: *Introduction to Analytic Number Theory*, Springer-Verlag, New York, Inc., 1976.

[4] Tom M. Apostol: *Mathematical Analysis*, Addison-Wesley Publishing Company, 1974.

[5] Carl B. Boyer: *A History of Mathematics*, Princeton University Press, 1985.

[6] W. A. Coppel: *Number Theory: an introduction to mathematics, second edition*, Springer, 2009.

[7] L. Debnath: *A Brief History of the Most Remarkable Numbers π, g and δ in Mathematical Sciences with Applications.*, International Journal of Applied and Computational Mathematics, Vol. 1, No. 4, pp. 607-638, 2015.

[8] Emilio Elizalde: *Ten Physical Applications of Spectral Zeta Functions, second edition*, Springer-Verlag, 2012.

[9] Benjamin Fine, Gerhard Rosenberger: *Number Theory; An Introduction via the Distribution of Primes*, Birkhäuser Boston, 2007.

[10] E. Hairer, G. Wanner: *Analysis by Its History*, Springer-Verlag, New York, Inc., 1996.

[11] Markku Halmetoja: *Baselin ongelma*, Solmu Matematiikkalehti, No. 1, pp. 15-18, 2019.

[12] G. H. Hardy, E. M. Wright: *An Introduction to the Theory of Numbers, sixth edition*, Oxford University Press Inc., New York, 2008.

[13] Question 281 answered by Mr. Heath: *The Ladies Diary*, J. Wilde, 1747. Luettavissa Google-kirjoissa, s. 23.

[14] Lars Holst: *A Proof of Euler's Infinite Product for the Sine*, The American Mathematical Monthly, Vol.119, No. 6, pp. 518-521, 2012.

[15] G. J. O. Jameson: *The Prime Number Theorem*, Cambridge University Press, New York, 2003.

[16] Henry Joutsijoki: *Riemannin ζ-funktio ja sen sovelluksia, lisensiaatintutkimus*, Tampereen yliopisto, 2010.

[17] Lassi Kurittu: *Lukuteoria 2, luentomoniste*, Jyväskylän yliopisto, 2014.

[18] Question 281 by Mr. J. May Jr: *The Ladies Diary*, J. Wilde, 1747. Luettavissa Google-kirjoissa, s. 34.

[19] Melvyn B. Nathanson: *Elementary Methods in Number Theory*, Springer-Verlag New York, 2000.

[20] Rolf Nevanlinna, V. Paatero: *Funktioteoria, toinen painos*, Kustannusosakeyhtiö Otavan laakapaino, Keuruu, 1971.

[21] Ivan Niven, Herbert S. Zuckerman: *An Introduction to the Theory of Numbers, second edition*, John Wiley & Sons, Inc., 1966.

[22] Andrew Odlyzko: *Tables of zeros of the Riemann zeta function,* `http://www.dtc.umn.edu/~odlyzko/zeta_tables/index.html`

[23] Bruce P. Palka: *An Introduction to Complex Function Theory*, Springer-Verlag New York Inc., 1991.

[24] Paulo Ribenboim: *The Little Book of Big Primes*, New York: Springer cop, 1991.

[25] W.D. Wallis: *A Beginner's Guide to Discrete Mathematics, second edition*, Springer Science+Business Media, 2012

[26] Elias Wegert: *Visual Complex Functions; An Introduction with Phase Portraits*, Springer Basel, 2012