Schnirelmannin lause

Ida Still

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Kevät 2021

Tiivistelmä: Ida Still, *Schnirelmannin lause* (engl. *Schnirelmann's theorem*), matematiikan pro gradu -tutkielma, 47 sivua, Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, kevät 2021.

Tämän tutkielman tarkoituksena on esittää todistus neuvostoliittolaisen matemaatikon Lev Schnirelmannin 1930-luvun alussa osoittamalle tulokselle, jonka mukaan on olemassa sellainen luku S, että jokainen ykköstä suurempi luonnollinen luku voidaan esittää alkulukujen summana, jossa summattavia on korkeintaan S kappaletta. Schnirelmannin lause on merkittävä additiivisen lukuteorian tulos, sillä sen avulla päästiin lähemmäksi yhtä lukuteorian ratkaisematonta ongelmaa, Goldbachin konjektuuria.

Työn alussa osoitetaan alkulukujen tiheyteen liittyvät Mertensin lauseet, joita tarvitaan Schnirelmannin lauseen todistamiseen. Mertensin lauseista ensimmäinen kertoo, miten lukua x pienempien alkulukujen käänteislukujen $1/p$ summa käyttäytyy, kun x kasvaa rajatta. Mertensin toinen lause puolestaan kertoo saman lukujen $(1 - 1/p)$ tulolle.

Schnirelmannin lauseeseen liittyvät olennaisesti seulamenetelmät, joilla voidaan arvioida kokoa positiivisista kokonaisluvuista koostuvalle, tietyt ehdot täyttävälle seulotulle joukolle. Yleinen ongelma, johon seuloja hyödynnetään, on muotoa: Jos $\mathcal{A}$ on äärellinen joukko positiivisia kokonaislukuja ja $\mathcal{P}$ äärellinen joukko alkulukuja, niin kuinka paljon on sellaisia joukon $\mathcal{A}$ alkioita, jotka eivät ole jaollisia millään $p \in \mathcal{P}$? Seulamenetelmien yleisen idean lisäksi työssä tutustutaan tarkemmin norjalaisen matemaatikon Viggo Brunin kehittämään seulaan, jota hyödyntämällä saadaan osoitettua muutama Schnirelmannin lauseen todistamiseen tarvittava aputulos. Nämä tulokset liittyvät siihen, kuinka monella eri tavalla luonnollinen luku voidaan esittää kahden alkuluvun summana.

Työn tärkeimpiä käsitteitä on Schnirelmannin tiheys, jolla voidaan mitata luonnollisten lukujen osajoukon kokoa. Työssä käydään läpi Schnirelmannin tiheyden ominaisuuksia ja osoitetaan tulos, jonka avulla voidaan arvioida Schnirelmannin tiheyttä joukkojen summalle. Lisäksi osoitetaan, että jokainen epänegatiivisista kokonaisluvuista koostuva joukko $\mathcal{A}$, joka sisältää nollan ja jonka Schnirelmannin tiheys on positiivinen, on jonkin kertaluvun kanta epänegatiivisten kokonaislukujen joukolle. Tällä tarkoitetaan sitä, että on olemassa luonnollinen luku h siten, että jokainen epänegatiivinen kokonaisluku voidaan esittää sellaisena joukon $\mathcal{A}$ alkioiden summana, jossa summattavia on h kappaletta. Tätä tulosta hyödyntäen esitetään lopuksi todistus Schnirelmannin lauseelle.

Sisällys

Johdanto

Additiivisen lukuteorian tyypillinen ongelma on tutkia, voidaanko jokainen riittävän suuri kokonaisluku esittää jonkin tietyn epänegatiivisista kokonaisluvuista koostuvan joukon alkioiden summana. Eräs merkittävä additiivisen lukuteorian tulos on esimerkiksi Lagrangen neljän neliön lause, jonka mukaan jokainen luonnollinen luku voidaan esittää neljän neliön summana. Tämän työn tarkoituksena on todistaa eräs samankaltainen additiivisen lukuteorian tulos, *Schnirelmannin lause*, jonka mukaan on olemassa sellainen luku S, että jokainen ykköstä suurempi luonnollinen luku voidaan esittää alkulukujen summana, jossa summattavia on korkeintaan S kappaletta.

Schnirelmannin lause on nimetty neuvostoliittolaisen matemaatikon Lev Schnirelmannin (1905-1938) mukaan, sillä hän osoitti kyseisen tuloksen 1930-luvun alussa. Tämä oli merkittävä askel kohti yhtä lukuteorian ratkaisematonta ongelmaa, Goldbachin konjenktuuria:

Jokainen parillinen kokonaisluku > 2 voidaan esittää kahden alkuluvun summana.

Schnirelmannin lauseeseen liittyy läheisesti myös toisen neuvostoliittolaisen matemaatikon, I. M. Vinogradovin, muutamaa vuotta myöhemmin osoittama tulos, jonka mukaan jokainen riittävän suuri pariton kokonaisluku voidaan esittää kolmen alkuluvun summana. [**2, 9**]

Pienintä lukua S, jolle Schnirelmannin lauseen ominaisuus on pystytty osoittamaan, kutsutaan *Schnirelmannin vakioksi*. Vuosien saatossa monet matemaatikot ovat saaneet Schnirelmannin vakioksi yhä pienempiä lukuja. Esimerkiksi, vuonna 1982 Hans Riesel ja R. C. Vaughan saivat Schnirelmannin vakioksi 19, ja edelleen vuonna 1995 ranskalainen matemaatikko Olivier Ramaré sai sen pienennettyä lukuun 7. Ramaré myös osoitti, että jokainen parillinen kokonaisluku voidaan esittää korkeintaan kuuden alkuluvun summana. Vuonna 2012 Terence Tao puolestaan onnistui näyttämään, että jokainen pariton kokonaisluku voidaan esittää korkeintaan viiden alkuluvun summana. Näin ollen Schnirelmannin vakio pieneni edelleen lukuun 6. [**10**]

Additiivisen lukuteorian ongelmiin liittyvät vahvasti erilaiset seulamenetelmät. Myös Schnirelmannin lauseen todistamiseen tarvitaan erästä seulamenetelmää, *Brunin seulaa*, joka on nimetty sen kehittäjän, norjalaisen matemaatikon Viggo Brunin (1885–1978) mukaan. *Seulaksi* kutsutaan lukuteoriassa menetelmää, jolla voidaan arvioida kokoa positiivisista kokonaisluvuista koostuvalle seulotulle joukolle, joka toteuttaa tietyt ehdot. Seulamenetelmien avulla on onnistuttu osoittamaan monia tuloksia, joilla on päästy lähemmäksi lukuteorian ratkaisemattomia ongelmia, kuten Goldbachin konjektuuria sekä otaksumaa siitä, että alkulukupareja on äärettömän monta:

On olemassa äärettömän monta alkulukua p siten, että myös $p + 2$ on alkuluku.

Seulamenetelmillä on saatu osoitettua esimerkiksi, että:

Jokainen riittävän suuri parillinen kokonaisluku voidaan esittää kahden sellaisen luvun summana, joilla on korkeintaan yhdeksän alkutekijää. (Brun, 1920)

Jokainen riittävän suuri parillinen kokonaisluku voidaan esittää joko kahden alkuluvun summana tai alkuluvun ja kahden alkuluvun tulon summana. (Chen, 1973)

On olemassa äärettömän monta lukuparia siten, että lukujen erotus on 2 ja molemmilla luvuilla on korkeintaan 9 alkutekijää. (Brun, 1920)

On olemassa äärettömän monta alkulukua p siten, että p+2 on joko alkuluku tai kahden alkuluvun tulo. (Chen, 1973) [**3, 9**]

Tämän työn ensimmäisessä luvussa käydään läpi työssä käytettäviä merkintöjä ja muistutellaan mieleen tarvittavia esitietoja. Toisessa luvussa puolestaan tutustutaan työn kannalta merkittäviin aputuloksiin, Mertensin lauseisiin. Kolmannessa luvussa käsitellään seulamenetelmiä, joihin tutustutaan ensin yleisesti: tarkastellaan, mitä seulamenetelmät ovat ja mihin niitä käytetään, sekä käydään läpi tarvittavia merkintöjä. Tämän jälkeen käsitellään tarkemmin Brunin seulaa, jonka avulla luvussa 4 osoitetaan muutama Schnirelmannin lauseen todistamiseen tarvittava aputulos. Nämä tulokset liittyvät siihen, kuinka monella eri tavalla luonnollinen luku voidaan esittää kahden alkuluvun summana. Viimeisessä luvussa tutustutaan Schnirelmannin tiheyden käsitteeseen ja esitetään todistus Schnirelmannin lauseelle.

Pääasiallisena lähteenä tässä työssä on käytetty Paul Pollackin teosta *Not Always Buried Deep: A Second Course in Elementary Number Theory* [**9**], johon luvut 3–5 pitkälti pohjautuvat. Seulamenetelmiin liittyen tärkeänä lähteenä on käytetty myös George Greavesin teosta *Sieves in Number Theory* [**3**]. Viimeisessä luvussa keskeisinä lähteinä Pollackin teoksen lisäksi on hyödynnetty Alina C. Cojocarun ja M. Ram Murtyn teosta *An Introduction to Sieve Methods and their Applications* [**2**] sekä A. Y. Khinchinin teosta *Three Pearls of Number Theory* [**5**]. Lisää additiivisen lukuteorian klassisista ongelmista löytyy muun muassa Melvyn B. Nathansonin teoksesta *Additive Number Theory. The Classical Bases* [**7**]. Seulamenetelmiä käsittelevistä teoksista mainittakoon lisäksi Heini Halberstamin ja Hans-Egon Richertin teos *Sieve Methods* [**4**].

LUKU 1

Esitietoja

Tähän lukuun on koottu työssä käytettäviä merkintöjä sekä tarvittavia määritelmiä ja aputuloksia. Luvun pääasiallisina lähteinä on käytetty Tom M. Apostolin teosta *Introduction to Analytic Number Theory* [**1**], Melvyn B. Nathansonin teosta *Elementary Methods in Number Theory* [**8**] ja Heli Tuomisen luentomonistetta *Lukuteorian alkeet* [**11**].

Merkintä	*Selitys*
$\mathbb{N}$	Luonnollisten lukujen joukko $\{1, 2, 3, \dots\}$
$\mathbb{N}_0$	Epänegatiivisten kokonaislukujen joukko $\{0, 1, 2, \dots\}$
$\mathbb{Z}$	Kokonaislukujen joukko $\{\dots, -2, -1, 0, 1, 2, \dots\}$
$A \cup B$	Joukkojen A ja B yhdiste, $A \cup B = \{x : x \in A \text{ tai } x \in B\}$
$A \cap B$	Joukkojen A ja B leikkaus, $A \cap B = \{x : x \in A \text{ ja } x \in B\}$
$a \mid b$	Luku b on jaollinen luvulla a
$a \nmid b$	Luku b ei ole jaollinen luvulla a
$\text{syt}(a, b)$	Lukujen a ja b suurin yhteinen tekijä
$\text{pyj}(a, b)$	Lukujen a ja b pienin yhteinen jaettava
$a \pmod b$	Luvun a jakojäännös, kun jaetaan luvulla b
$\#A$	Joukon A alkioiden lukumäärä
$\lfloor x \rfloor$	Suurin kokonaisluku, joka on pienempi tai yhtäsuuri kuin x
$\lceil x \rceil$	Pienin kokonaisluku, joka on suurempi tai yhtäsuuri kuin x
$\{x\}$	Luvun x desimaaliosa

1.1. Jaollisuudesta

Muistutellaan ensin mieleen muutamia jaollisuuteen liittyviä määritelmiä ja tuloksia, joita työssä tarvitaan.

MÄÄRITELMÄ 1.1. Olkoot $a, b \in \mathbb{Z}$. Luku b on *jaollinen* luvulla a, jos

$$b = ka \quad \text{jollain } k \in \mathbb{Z}.$$

Tällöin sanotaan, että a on luvun b *tekijä/jakaja* ja että a *jakaa* luvun b. Jos b on jaollinen luvulla a, niin merkitään $a \mid b$. Jos b ei ole jaollinen luvulla a, niin merkitään $a \nmid b$.

MÄÄRITELMÄ 1.2. Olkoot $a, b \in \mathbb{Z}$ ja ainakin toinen luvuista erisuuri kuin nolla. Lukujen a ja b *suurin yhteinen tekijä* $\text{syt}(a, b)$ on suurin kokonaisluku, joka jakaa molemmat luvut a ja b, toisin sanoen

$$\text{syt}(a, b) = \max\{d \in \mathbb{Z} : d \mid a \text{ ja } d \mid b\}.$$

MÄÄRITELMÄ 1.3. Olkoot $a, b \in \mathbb{Z}$ ja $a, b \neq 0$. Lukujen a ja b *pienin yhteinen jaettava* $\text{pyj}(a, b)$ on pienin positiivinen kokonaisluku, joka on jaollinen molemmilla luvuilla a ja b, toisin sanoen

$$\text{pyj}(a, b) = \min\{c \in \mathbb{N} : a \mid c \text{ ja } b \mid c\}.$$

MÄÄRITELMÄ 1.4. Kokonaisluvut a ja b ovat *keskenään jaottomat*, jos

$$\text{syt}(a, b) = 1.$$

LEMMA 1.5. (Bézoutin lemma) *Olkoot $a, b \in \mathbb{Z}$ ja $a \neq 0$. Tällöin on olemassa luvut $x, y \in \mathbb{Z}$ siten, että*

$$\text{syt}(a, b) = ax + by.$$

TODISTUS. Löytyy Tuomisen luentomonisteesta [**11**]. □

1.2. Alkuluvut ja alkutekijähajotelma

Määritellään seuraavaksi, mikä on alkuluku, ja tarkastellaan luonnollisten lukujen alkutekijähajotelmaa. Osoitetaan lisäksi, että alkulukuja on äärettömän monta.

MÄÄRITELMÄ 1.6. Luonnollinen luku $p \geq 2$ on *alkuluku*, jos sen ainoat positiiviset tekijät ovat luvut 1 ja p. Lukua 1 suurempaa luonnollista lukua, joka ei ole alkuluku, sanotaan *yhdistetyksi luvuksi*.

ESIMERKKI 1.7. Luvut 2, 3, 5 ja 7 ovat alkulukuja. Luvut 4 ja 6 ovat yhdistettyjä lukuja. Ainoa parillinen alkuluku on luku 2. Luku 1 ei ole alkuluku eikä yhdistetty luku.

LAUSE 1.8. (Eukleideen lemma) *Olkoon p alkuluku ja olkoot $a, b \in \mathbb{Z}$. Tällöin, jos $p \mid ab$, niin $p \mid a$ tai $p \mid b$.*

TODISTUS. Oletuksen mukaan $ab = kp$ jollain $k \in \mathbb{Z}$. Jos $p \mid a$, niin väite on selvä. Oletetaan siis, että $p \nmid a$. Koska p on alkuluku, niin nyt $\text{syt}(a, p) = 1$. Näin ollen Bézoutin lemman nojalla löytyy luvut $x, y \in \mathbb{Z}$ siten, että

$$1 = ax + py.$$

Kertomalla nyt yhtälön molemmat puolet luvulla b saadaan

$$b = abx + bpy = kpx + bpy = (kx + by)p,$$

missä $kx + by \in \mathbb{Z}$. Siis $p \mid b$. □

LAUSE 1.9. (Aritmetiikan peruslause) *Jokainen luonnollinen luku $n > 1$ voidaan esittää alkulukujen tulona. Tällaista esitystä kutsutaan luvun n alkutekijähajotelmaksi, ja se on tekijöiden järjestystä vaille yksikäsitteinen.*

TODISTUS. Löytyy Apostolin teoksesta [**1**] sivulta 17. □

ESIMERKKI 1.10. Luvun 780 alkutekijähajotelma on

$$780 = 2^2 \cdot 3 \cdot 5 \cdot 13.$$

LAUSE 1.11. *Alkulukuja on äärettömän monta.*

TODISTUS. Olkoon $p_1, \ldots, p_n$ äärellinen joukko alkulukuja. Näytetään, että löytyy sellainen alkuluku, joka ei kuulu tähän joukkoon. Tästä seuraa, että alkulukuja on äärettömän monta.

Tarkastellaan lukua

$$N = p_1 \cdots p_n + 1.$$

Koska $N > 1$, niin aritmetiikan peruslauseesta seuraa, että luku N on jaollinen jollain alkuluvulla p. Jos $p = p_i$ jollain $i = 1, \ldots, n$, niin tällöin p jakaisi luvun

$$N - p_1 \cdots p_n = 1,$$

mikä on mahdotonta. Näin ollen $p \neq p_i$ kaikilla $i = 1, \ldots, n$. □

Tässä työssä kirjaimella p viitataan yleisesti alkulukuihin. Merkintää $\mathcal{P}$ käytetään tilanteesta riippuen ilmaisemaan joko äärellistä joukkoa alkulukuja tai kaikkien alkulukujen joukkoa.

LAUSE 1.12. (Eulerin tulo) *Olkoon $\mathcal{P}$ alkulukujen joukko. Tällöin kaikilla $s > 1$,*

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right)^{-1}.$$

TODISTUS. Olkoon $s > 1$. Tällöin summa $\sum_{n=1}^{\infty} n^{-s}$ suppenee itseisesti, joten sen termit voidaan järjestellä uudelleen mielivaltaisesti siten, että summa pysyy muuttumattomana. Nyt

$$\begin{aligned}
\prod_{p \in \mathcal{P}} \left(1 - \frac{1}{p^s}\right)^{-1} &= \frac{1}{1 - \frac{1}{p_1^s}} \cdot \frac{1}{1 - \frac{1}{p_2^s}} \cdot \frac{1}{1 - \frac{1}{p_3^s}} \cdots \\
&= \left(\sum_{k=0}^{\infty} \left(\frac{1}{p_1^s}\right)^k\right) \left(\sum_{k=0}^{\infty} \left(\frac{1}{p_2^s}\right)^k\right) \left(\sum_{k=0}^{\infty} \left(\frac{1}{p_3^s}\right)^k\right) \cdots \\
&= \left(1 + \frac{1}{p_1^s} + \frac{1}{p_1^{2s}} + \cdots\right) \left(1 + \frac{1}{p_2^s} + \frac{1}{p_2^{2s}} + \cdots\right) \cdots \\
&= 1 + \sum_{1 \leq i} \frac{1}{p_i^s} + \sum_{1 \leq i \leq j} \frac{1}{p_i^s p_j^s} + \sum_{1 \leq i \leq j \leq k} \frac{1}{p_i^s p_j^s p_k^s} + \cdots \\
&= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \cdots \\
&= \sum_{n=1}^{\infty} \frac{1}{n^s},
\end{aligned}$$

missä toinen yhtäsuuruus saadaan esittämällä tulon jokainen termi geometrisena summana. Viimeisissä vaiheissa summan termejä järjestelemällä päästään haluttuun lopputulokseen, sillä jokainen mahdollinen alkulukujen tulo esiintyy summassa nimittäjänä täsmälleen kerran ja jokainen ykköstä suurempi luonnollinen luku voidaan esittää alkulukujen tulona (järjestystä vaille) täsmälleen yhdellä tavalla. □

1.3. Kongruenssista

Palautetaan seuraavaksi mieleen muutamia seikkoja kongruenssiin liittyen.

MÄÄRITELMÄ 1.13. Olkoon $n \in \mathbb{N}$ ja olkoot $a, b \in \mathbb{Z}$. Luku a on *kongruentti* luvun b kanssa modulo n,

$$a \equiv b \pmod{n},$$

jos $n \mid (a - b)$.

HUOMAUTUS 1.14.

(1) Kongruenssin määritelmästä seuraa, että

$$a \equiv 0 \pmod{n} \iff n \mid a.$$

(2) Merkinnällä $a \pmod{b}$ tarkoitetaan luvun a jakojäännöstä luvulla b jaettaessa. Esimerkiksi $5 \pmod{3} = 2$.

LAUSE 1.15. (Kiinalainen jäännöslause) *Jos $n_1, n_2, \ldots, n_r \in \mathbb{N}$ ovat pareittain keskenään jaottomia ja $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, niin kongruenssiyhtälöryhmällä*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

on yksikäsitteinen ratkaisu modulo $N = n_1 n_2 \cdots n_r$. Edelleen, $x \equiv y \pmod{N}$, jos ja vain jos $x \equiv y \pmod{n_i}$ kaikilla $1 \leq i \leq r$.

TODISTUS. Löytyy Apostolin teoksesta [**1**] sivuilta 117–118. □

1.4. Aritmeettinen ja multiplikatiivinen funktio

Tässä työssä tarvitaan olennaisesti muutamia aritmeettisia funktioita, joten tarkastellaan niitä seuraavaksi. Määritellään myös, mikä on multiplikatiivinen funktio, ja tutustutaan tarkemmin erääseen tällaiseen funktioon, *Möbiuksen funktioon*.

MÄÄRITELMÄ 1.16. *Aritmeettinen funktio* on reaaliarvoinen kuvaus, joka on määritelty luonnollisille luvuille.

Tässä työssä tarvitaan seuraavia aritmeettisia funktioita:

$\pi(x)$	lukua x pienempien tai yhtä suurten alkulukujen lukumäärä
$\omega(n)$	luvun n erillisten alkutekijöiden lukumäärä
$\tau(n)$	luvun n positiivisten tekijöiden lukumäärä.

ESIMERKKI 1.17.

(a) Lukua 12 pienemmät alkuluvut ovat luvut 2, 3, 5, 7 ja 11, joten $\pi(12) = 5$.

(b) Luvun 12 alkutekijähajotelmasta $12 = 2^2 \cdot 3$ nähdään, että $\omega(12) = 2$.

(c) Luvun 12 positiiviset tekijät ovat luvut 1, 2, 3, 4, 6 ja 12, joten $\tau(12) = 6$.

MÄÄRITELMÄ 1.18. Aritmeettinen funktio f on *multiplikatiivinen*, jos kaikilla keskenään jaottomilla luonnollisilla luvuilla m ja n pätee $f(mn) = f(m)f(n)$.

Esimerkki 1.19.

(a) Funktiot $f(n) = 1$ ja $g(n) = n^2$ ovat multiplikatiivisia, sillä
$$f(mn) = 1 = 1 \cdot 1 = f(m)f(n)$$
ja
$$g(mn) = (mn)^2 = m^2n^2 = g(m)g(n)$$
kaikilla $m, n \in \mathbb{N}$.

(b) Funktio $\tau(n)$ on multiplikatiivinen. Nimittäin, jos $m, n \in \mathbb{N}$ ovat keskenään jaottomat, niin tällöin luvun mn jakajat ovat muotoa $d = rs$, missä r jakaa luvun m ja s jakaa luvun n. Näin ollen
$$\tau(mn) = \sum_{d \mid mn} 1 = \sum_{r \mid m,\, s \mid n} 1 = \left(\sum_{r \mid m} 1\right)\left(\sum_{s \mid n} 1\right) = \tau(m)\tau(n).$$

Esimerkki 1.20. Osoitetaan, että kaikilla $n \in \mathbb{N}$ pätee
$$2^{\omega(n)} \leq \tau(n).$$

Ratkaisu. Olkoon $n \in \mathbb{N}$ ja
$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$
luvun n alkutekijähajotelma, missä $p_1, p_2, \ldots, p_r$ ovat luvun n erilliset alkutekijät ja $a_i \geq 1$ kaikilla $i = 1, 2, \ldots, r$. Nyt siis $\omega(n) = r$. Lisäksi, koska funktio $\tau(n)$ on multiplikatiivinen, niin
$$\begin{aligned}\tau(n) &= \tau(p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}) \\ &= \tau(p_1^{a_1})\tau(p_2^{a_2}) \cdots \tau(p_r^{a_r}) \\ &= (a_1 + 1)(a_2 + 1) \cdots (a_r + 1).\end{aligned}$$
Näin ollen saadaan
$$\tau(n) = (a_1 + 1)(a_2 + 1) \cdots (a_r + 1) \geq \underbrace{2 \cdot 2 \cdots 2}_{r \text{ kpl}} = 2^r = 2^{\omega(n)}.$$

□

Määritelmä 1.21. Olkoon $n \in \mathbb{N}$. *Möbiuksen funktio* $\mu(n)$ määritellään seuraavasti:
$$\mu(n) = \begin{cases} 1, & \text{jos } n = 1, \\ (-1)^r, & \text{jos } n = p_1 p_2 \cdots p_r, \text{ missä alkuluvut } p_i \text{ ovat erisuuria,} \\ 0, & \text{jos } p^2 \mid n \text{ jollakin alkuluvulla } p. \end{cases}$$

Kokonaisluvun sanotaan olevan *neliövapaa*, jos se ei ole jaollinen minkään alkuluvun neliöllä. Siis $\mu(n) \neq 0$, jos ja vain jos luku n on neliövapaa.

Esimerkki 1.22.

(a) Luvun $50 = 2 \cdot 5^2$ alkutekijähajotelmasta nähdään, että luku on jaollinen alkuluvun neliöllä. Siispä $\mu(50) = 0$.

(b) Luku $14 = 2 \cdot 7$ on neliövapaa, joten $\mu(14) = (-1)^2 = 1$.

Möbiuksen funktiolla on seuraavat ominaisuudet:

LAUSE 1.23. *Möbiuksen funktio $\mu(n)$ on multiplikatiivinen, ja*

$$\sum_{d \mid n} \mu(d) = \begin{cases} 1, & \text{jos } n = 1, \\ 0, & \text{jos } n > 1. \end{cases}$$

TODISTUS. Osoitetaan ensin, että Möbiuksen funktio on multiplikatiivinen. Olkoot $m, n \in \mathbb{N}$ keskenään jaottomat. Jos $m = 1$, niin

$$\mu(mn) = \mu(1 \cdot n) = \mu(n) = 1 \cdot \mu(n) = \mu(1)\mu(n) = \mu(m)\mu(n).$$

Vastaavasti, jos $n = 1$. Jos ainakin toinen luvuista m ja n on jaollinen jonkin alkuluvun neliöllä, niin tällöin myös tulo mn on jaollinen kyseisen alkuluvun neliöllä. Näin ollen Möbiuksen funktion määritelmän mukaan

$$\mu(mn) = 0 = \mu(m)\mu(n).$$

Jos taas molemmat luvuista m ja n ovat neliövapaita siten, että luvulla m on r kappaletta alkutekijöitä ja luvulla n on s kappaletta alkutekijöitä, niin myös tulo mn on neliövapaa ja sillä on $r + s$ kappaletta alkutekijöitä. Näin ollen

$$\mu(mn) = (-1)^{r+s} = (-1)^r(-1)^s = \mu(m)\mu(n).$$

Siispä funktio $\mu(n)$ on multiplikatiivinen.

Osoitetaan sitten jälkimmäinen väite. Jos $n = 1$, niin väite on selvä, sillä tällöin

$$\sum_{d \mid n} \mu(d) = \mu(1) = 1.$$

Jos $n > 1$, niin olkoon

$$n = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

luvun n alkutekijähajotelma, ja asetetaan

$$N = p_1 p_2 \cdots p_r.$$

Jos d jakaa luvun n ja $\mu(d) \neq 0$, niin d on neliövapaa ja siten se jakaa myös luvun N. Koska luku N on erillisten alkulukujen tulo, jossa kerrottavia on r kappaletta, niin löytyy täsmälleen $\binom{r}{i}$ kappaletta sellaisia luvun N jakajia d, joille $\omega(d) = i$. Näiden huomioiden ja binomikaavan

$$(1 + x)^m = \sum_{k=0}^{m} \binom{m}{k} x^k$$

avulla saadaan

$$\begin{aligned}\sum_{d\,|\,n}\mu(d) &= \sum_{d\,|\,N}\mu(d)\\ &= \sum_{i=0}^{r}\sum_{\substack{d\,|\,N\\ \omega(d)=i}}\mu(d)\\ &= \sum_{i=0}^{r}\sum_{\substack{d\,|\,N\\ \omega(d)=i}}(-1)^i\\ &= \sum_{i=0}^{r}\binom{r}{i}(-1)^i\\ &= (1-1)^r\\ &= 0.\end{aligned}$$

□

1.5. Iso O -notaatio

Käydään seuraavaksi läpi työn kannalta oleellinen merkintä, ”iso O -notaatio”. Määritellään myös, mitä tarkoittaa, että funktiot ovat samaa kertaluokkaa tai asymptoottiset.

MÄÄRITELMÄ 1.24. Olkoon D positiivisten reaalilukujen rajoittamaton osajoukko. Olkoot lisäksi f ja g reaaliarvoisia funktioita joukolta D siten, että $g(x) > 0$ kaikilla riittävän suurilla x. Merkitään

$$f(x) = O(g(x)), \quad \text{kun } x \to \infty,$$

tai

$$f(x) \ll g(x), \quad \text{kun } x \to \infty,$$

jos on olemassa $M > 0$ ja $x_0 \in \mathbb{R}$ siten, että

$$|f(x)| \leq Mg(x) \quad \text{kaikilla } x \geq x_0.$$

Lukua M kutsutaan notaation *implisiittiseksi vakioksi*. Merkinnällä $f \gg g$ tarkoitetaan samaa kuin $g \ll f$. Jos sekä $f \ll g$ että $f \gg g$, niin merkitään

$$f \asymp g$$

ja sanotaan, että funktiot ovat *samaa kertaluokkaa* (engl. *same order of magnitude*). Edelleen, merkinnällä $O(g)$ tarkoitetaan mitä tahansa funktiota f, jolle $f = O(g)$. Lisäksi sanotaan, että funktiot f ja g ovat *asymptoottiset*, merkitään

$$f \sim g,$$

jos

$$\lim_{\substack{x\to\infty\\ x\in D}} \frac{f(x)}{g(x)} = 1.$$

HUOMAUTUS 1.25.

(a) Usein tarkasteltaessa funktion käyttäytymistä, kun muuttuja x kasvaa rajatta, jätetään tämä mainitsematta ja kirjoitetaan vain lyhyesti

$$f = O(g).$$

Iso O -notaatiota voidaan käyttää myös kuvaamaan funktion käyttäytymistä lähellä jotain reaalilukua a. Merkitään

$$f(x) = O(g(x)), \quad \text{kun } x \to a,$$

jos on olemassa positiiviset reaaliluvut λ ja M siten, että

$$|f(x)| \leq Mg(x)$$

kaikilla x, joille $|x - a| < \lambda$.

(b) Jos funktiot f ja g ovat asymptoottiset, niin tällöin ne ovat samaa kertaluokkaa ja edelleen $f \ll g$.

ESIMERKKI 1.26.

(a) Koska kaikilla $x \geq 1$,

$$\begin{aligned} |3x^2 - 2x + 1| &\leq |3x^2| + |2x| + |1| \\ &\leq 3x^2 + 2x^2 + x^2 \\ &= 6x^2, \end{aligned}$$

niin $3x^2 - 2x + 1 = O(x^2)$.

(b) Koska

$$\lim_{x \to \infty} \frac{x+1}{x} = 1,$$

niin $x + 1 \sim x$.

(c) Osoitetaan, että

$$O(f_1(x)) + O(f_2(x)) = O(\max\{f_1(x), f_2(x)\}), \quad \text{kun } x \to \infty.$$

RATKAISU. Merkinnällä $O(f_1(x))$ tarkoitetaan mitä tahansa funktiota g_1, jolle on olemassa $M_1 > 0$ ja $x_1 \in \mathbb{R}$ siten, että

$$|g_1(x)| \leq M_1 f_1(x) \quad \text{kaikilla } x \geq x_1.$$

Vastaavasti merkinnällä $O(f_2(x))$ tarkoitetaan mitä tahansa funktiota g_2, jolle on olemassa $M_2 > 0$ ja $x_2 \in \mathbb{R}$ siten, että

$$|g_2(x)| \leq M_2 f_2(x) \quad \text{kaikilla } x \geq x_2.$$

Nyt siis kaikilla $x \geq \max\{x_1, x_2\}$,

$$\begin{aligned} |g_1(x) + g_2(x)| &\leq M_1 f_1(x) + M_2 f_2(x) \\ &\leq (M_1 + M_2) \max\{f_1(x), f_2(x)\}, \end{aligned}$$

eli

$$O(f_1(x)) + O(f_2(x)) = O(\max\{f_1(x), f_2(x)\}).$$

□

(d) Kohdan (c) perusteella esimerkiksi,

$$O(x^2) + O(x) = O(x^2)$$

ja

$$O\left(\frac{1}{x}\right) + O\left(\frac{1}{\log x}\right) = O\left(\frac{1}{\log x}\right).$$

1.6. Chebyshevin estimaatti

Tarkastellaan luvun lopuksi *Chebyshevin estimaattina* tunnettuja epäyhtälöitä, jotka todisti 1850-luvulla venäläinen matemaatikko P. L. Chebyshev. Käydään tätä varten ensin läpi muutama tulos, joiden avulla Chebyshevin estimaatti saadaan johdettua.

Määritellään kaikille luonnollisille luvuille n ja alkuluvuille p funktio $v_p(n)$ suurimpana sellaisena kokonaislukuna r, jolla p^r jakaa luvun n, ts.

$$v_p(n) := \max\{r \geq 0 : p^r \mid n\}.$$

Tällöin siis $v_p(n) \geq 1$, jos ja vain jos p jakaa luvun n. Lisäksi luvun n alkutekijähajotelma voidaan kirjoittaa lyhyesti muodossa

$$n = \prod_{p \mid n} p^{v_p(n)}.$$

Toisaalta, koska $v_p(n) = 0$ kaikilla alkuluvuilla p, jotka eivät jaa lukua n, niin voidaan kirjoittaa myös

$$n = \prod_{p} p^{v_p(n)},$$

missä tulo otetaan kaikkien alkulukujen yli. Selvästi kaikilla luonnollisilla luvuilla m ja n pätee

$$v_p(mn) = v_p(m) + v_p(n),$$

eli funktio $v_p(n)$ on täydellisesti additiivinen. Esimerkiksi, koska $n! = 1 \cdot 2 \cdot 3 \cdots n$, niin

$$v_p(n!) = \sum_{m=1}^{n} v_p(m). \tag{1.1}$$

Osoitetaan, että funktiolle $v_p(n)$ pätee seuraava tulos:

LEMMA 1.27. *Kaikilla $n \in \mathbb{N}$ ja alkuluvuilla p pätee*

$$v_p(n!) = \sum_{r=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^r} \right\rfloor.$$

TODISTUS. Olkoon $m \in \mathbb{N}$, $1 \leq m \leq n$ ja $r \in \mathbb{N}_0$. Jos p^r jakaa luvun m, niin $p^r \leq m \leq n$ ja $r \leq \log n / \log p$. Koska r on kokonaisluku, niin $r \leq \lfloor \log n / \log p \rfloor$ ja

$$v_p(m) = \sum_{\substack{r=1 \\ p^r \mid m}}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} 1. \tag{1.2}$$

Sellaisia lukua n pienempiä tai yhtäsuuria luonnollisia lukuja, jotka ovat jaollisia luvulla p^r, on täsmälleen $\lfloor n/p^r \rfloor$ kappaletta. Tämän sekä huomioiden (1.1) ja (1.2) nojalla saadaan

$$\begin{aligned} v_p(n!) &= \sum_{m=1}^{n} v_p(m) = \sum_{m=1}^{n} \sum_{\substack{r=1 \\ p^r \mid m}}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} 1 \\ &= \sum_{r=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \sum_{\substack{m=1 \\ p^r \mid m}}^{n} 1 = \sum_{r=1}^{\left\lfloor \frac{\log n}{\log p} \right\rfloor} \left\lfloor \frac{n}{p^r} \right\rfloor. \end{aligned}$$

□

LEMMA 1.28. *Kaikilla $n \in \mathbb{N}$ ja $t \in \mathbb{R}$ pätee*

$$\lfloor nt \rfloor - n\lfloor t \rfloor \in \{0, 1, \ldots, n-1\}.$$

TODISTUS. Olkoon $n \in \mathbb{N}$ ja $t \in \mathbb{R}$. Tällöin $\lfloor nt \rfloor - n\lfloor t \rfloor \in \mathbb{Z}$. Lisäksi, koska kaikilla $x \in \mathbb{R}$ ja $k \in \mathbb{Z}$ pätee, että

$$\lfloor x + k \rfloor = \lfloor x \rfloor + k, \qquad \lfloor x \rfloor \leq x \qquad \text{ja} \qquad x - \lfloor x \rfloor < 1,$$

niin nyt

$$\begin{aligned} \lfloor nt \rfloor - n\lfloor t \rfloor &= \lfloor n\lfloor t \rfloor + n\{t\} \rfloor - n\lfloor t \rfloor \\ &= n\lfloor t \rfloor + \lfloor n\{t\} \rfloor - n\lfloor t \rfloor = \lfloor n\{t\} \rfloor \geq 0 \end{aligned}$$

ja

$$\lfloor nt \rfloor - n\lfloor t \rfloor \leq nt - n\lfloor t \rfloor = n(t - \lfloor t \rfloor) < n.$$

Näin ollen väite pätee. □

LEMMA 1.29. *Kaikilla $n \in \mathbb{N}$,*

$$\binom{2n}{n} \geq \frac{2^{2n}}{2n}.$$

TODISTUS. Löytyy Nathansonin teoksesta [**8**] sivulta 269. □

Hyödynnetään nyt näitä aputuloksia Chebyshevin estimaatin todistamiseen.

LAUSE 1.30. (Chebyshev) *On olemassa positiiviset vakiot c_1 ja c_2 sekä reaaliluku x_0 siten, että*

$$c_1 \frac{x}{\log x} \leq \pi(x) \leq c_2 \frac{x}{\log x} \quad \textit{kaikilla } x \geq x_0.$$

TODISTUS. Tässä työssä tarvitaan epäyhtälöistä ensimmäistä, joten käydään läpi sen todistuksen ideaa. Koko todistus löytyy Nathansonin teoksesta [**8**] sivuilta 271–273. Vaihtoehtoinen todistus lauseelle löytyy muun muassa Pollackin teoksesta [**9**].

Väitteen osoittamiseen tarvitaan apufunktioita

$$\theta(x) := \sum_{p \leq x} \log p \qquad \text{ja} \qquad \psi(x) := \sum_{p^k \leq x} \log p,$$

joista jälkimmäisessä summataan siis kaikkien sellaisten parien (p, k) yli, joissa p on alkuluku, k luonnollinen luku ja $p^k \leq x$. Esimerkiksi,

$$\theta(10) = \log 2 + \log 3 + \log 5 + \log 7$$

ja

$$\psi(10) = 3\log 2 + 2\log 3 + \log 5 + \log 7.$$

Selvästi pätee, että

$$\theta(x) \leq \psi(x).$$

Lisäksi $p^k \leq x$, jos ja vain jos $k \leq \lfloor \log x / \log p \rfloor$, joten

$$\begin{aligned}\psi(x) &= \sum_{\substack{p^k \leq x \\ k \geq 1}} \log p = \sum_{p \leq x} \left(\sum_{\substack{p^k \leq x \\ k \geq 1}} 1 \right) \log p = \sum_{p \leq x} \left\lfloor \frac{\log x}{\log p} \right\rfloor \log p \\ &\leq \sum_{p \leq x} \log x = \pi(x) \log x.\end{aligned}$$

Lähdetään nyt etsimään alarajaa funktiolle $\psi(x)$. Olkoon $n \in \mathbb{N}$ ja $N = \binom{2n}{n}$. Kirjoitetaan luku N muodossa

$$N = \binom{2n}{n} = \frac{(2n)!}{(n!)^2} = \frac{\prod_{p \leq 2n} p^{v_p((2n)!)}}{\left(\prod_{p \leq 2n} p^{v_p(n!)} \right)^2} = \prod_{p \leq 2n} p^{v_p((2n)!) - 2v_p(n!)},$$

missä Lemman 1.27 nojalla

$$v_p((2n)!) - 2v_p(n!) = \sum_{k=1}^{\left\lfloor \frac{\log 2n}{\log p} \right\rfloor} \left(\left\lfloor \frac{2n}{p^k} \right\rfloor - 2 \left\lfloor \frac{n}{p^k} \right\rfloor \right).$$

Lemmasta 1.28 seuraa, että $\lfloor 2t \rfloor - 2\lfloor t \rfloor \in \{0, 1\}$ kaikilla reaaliluvuilla t, joten

$$0 \leq v_p((2n)!) - 2v_p(n!) \leq \left\lfloor \frac{\log 2n}{\log p} \right\rfloor.$$

Lemman 1.29 nojalla puolestaan

$$\frac{2^{2n}}{2n} \leq N = \prod_{p \leq 2n} p^{v_p((2n)!) - 2v_p(n!)} \leq \prod_{p \leq 2n} p^{\left\lfloor \frac{\log 2n}{\log p} \right\rfloor},$$

joten ottamalla luonnollinen logaritmi puolittain saadaan

$$2n \log 2 - \log 2n \leq \sum_{p \leq 2n} \left\lfloor \frac{\log 2n}{\log p} \right\rfloor \log p = \psi(2n).$$

Olkoon nyt $x \geq 2$ ja $n = \lfloor x/2 \rfloor$. Tällöin

$$2n \leq x < 2n + 2$$

ja

$$\begin{aligned}\psi(x) &\geq \psi(2n) \geq 2n \log 2 - \log 2n \\ &> (x - 2) \log 2 - \log x = x \log 2 - \log x - 2 \log 2.\end{aligned}$$

Löydettiin siis alaraja funktiolle $\psi(x)$, ja siitä seuraa, että

$$\liminf_{x\to\infty} \frac{\psi(x)}{x} \geq \log 2. \tag{1.3}$$

Olkoon nyt $0 < \lambda < 1$. Tällöin

$$\begin{aligned}
\theta(x) &\geq \sum_{x^{1-\lambda} < p \leq x} \log p \\
&\geq \sum_{x^{1-\lambda} < p \leq x} (1-\lambda)\log x \\
&= (\pi(x) - \pi(x^{1-\lambda}))(1-\lambda)\log x \\
&\geq (1-\lambda)\,\pi(x)\log x - x^{1-\lambda}\log x,
\end{aligned}$$

joten

$$\frac{\theta(x)}{x} \geq \frac{(1-\lambda)\,\pi(x)\log x}{x} - \frac{\log x}{x^{\lambda}}.$$

Näin ollen

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} \geq (1-\lambda)\liminf_{x\to\infty} \frac{\pi(x)\log x}{x}.$$

Koska tämä pätee kaikilla $0 < \lambda < 1$, niin

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} \geq \liminf_{x\to\infty} \frac{\pi(x)\log x}{x}. \tag{1.4}$$

Toisaalta taas alussa tehdystä huomiosta

$$\theta(x) \leq \psi(x) \leq \pi(x)\log x$$

seuraa, että

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} \leq \liminf_{x\to\infty} \frac{\psi(x)}{x} \leq \liminf_{x\to\infty} \frac{\pi(x)\log x}{x}. \tag{1.5}$$

Nyt kohtien (1.3), (1.4) ja (1.5) nojalla,

$$\liminf_{x\to\infty} \frac{\theta(x)}{x} = \liminf_{x\to\infty} \frac{\psi(x)}{x} = \liminf_{x\to\infty} \frac{\pi(x)\log x}{x} \geq \log 2,$$

mikä osoittaa Chebyshevin epäyhtälöistä ensimmäisen.

□

Työssä tarvitaan myös Cauchy-Schwarzin epäyhtälöä summille, joten palautetaan se vielä mieleen.

LAUSE 1.31. (Cauchy-Schwarzin epäyhtälö) *Kaikille reaaliluvuille* $x_1, \ldots, x_n$ *ja* $y_1, \ldots, y_n$ *pätee*

$$\left(\sum_{i=1}^{n} x_i y_i\right)^2 \leq \left(\sum_{i=1}^{n} x_i^2\right)\left(\sum_{i=1}^{n} y_i^2\right).$$

TODISTUS. Huomataan, että

$$\begin{aligned}\sum_{i=1}^{n}\sum_{j=1}^{n}(x_iy_j - x_jy_i)^2 &= \sum_{i=1}^{n}\sum_{j=1}^{n}(x_i^2y_j^2 - 2x_iy_ix_jy_j + x_j^2y_i^2)\\ &= \sum_{i=1}^{n}x_i^2\sum_{j=1}^{n}y_j^2 + \sum_{j=1}^{n}x_j^2\sum_{i=1}^{n}y_i^2 - 2\sum_{i=1}^{n}x_iy_i\sum_{j=1}^{n}x_jy_j\\ &= 2\left(\sum_{i=1}^{n}x_i^2\right)\left(\sum_{i=1}^{n}y_i^2\right) - 2\left(\sum_{i=1}^{n}x_iy_i\right)^2.\end{aligned}$$

Koska $(x_iy_j - x_jy_i)^2 \geq 0$ kaikilla i ja j, niin yhtälön vasen puoli on suurempaa tai yhtä suurta kuin nolla. Tästä seuraa, että

$$\left(\sum_{i=1}^{n}x_iy_i\right)^2 \leq \left(\sum_{i=1}^{n}x_i^2\right)\left(\sum_{i=1}^{n}y_i^2\right).$$

□

LUKU 2

Mertensin lauseet

Tässä luvussa tarkastellaan kahta työn kannalta merkittävää aputulosta, *Mertensin lauseita*, jotka ovat puolalaisen matemaatikon Franz Mertensin vuonna 1874 osoittamia alkulukujen tiheyteen liittyviä tuloksia. Mertensin lauseita tarvitaan luvussa 4, kun osoitetaan muutama Schnirelmannin lauseen todistamiseen tarvittava aputulos. Lähteinä tässä luvussa on käytetty Melvyn B. Nathansonin teosta *Elementary Methods in Number Theory* [**8**] ja Paul Pollackin teosta *Not Always Buried Deep: A Second Course in Elementary Number Theory* [**9**].

Seuraava tulos, jota tarvitaan Mertensin ensimmäisen lauseen todistamiseen, on osittaisintegroinnin vastine summille.

LAUSE 2.1. (Osittaissummaus) *Olkoon $f(n)$ aritmeettinen funktio ja*

$$F(x) = \sum_{n \leq x} f(n).$$

Olkoon lisäksi g jatkuvasti derivoituva funktio välillä $[1, x]$, missä $x \geq 2$. Tällöin

$$\sum_{n \leq x} f(n)g(n) = F(x)g(x) - \int_1^x F(t)g'(t)\,dt.$$

TODISTUS. Koska $f(n) = F(n) - F(n-1)$ ja $F(1) = f(1)$, niin nyt

$$\begin{aligned}
\sum_{n \leq x} f(n)g(n) &= f(1)g(1) + \sum_{2 \leq n \leq x} f(n)g(n) \\
&= f(1)g(1) + \sum_{2 \leq n \leq x} (F(n) - F(n-1))g(n) \\
&= f(1)g(1) + \sum_{2 \leq n \leq x} F(n)g(n) - \sum_{2 \leq n \leq x} F(n-1)g(n) \\
&= \sum_{n \leq x} F(n)g(n) - \sum_{n \leq x-1} F(n)g(n+1) \\
&= F(\lfloor x \rfloor)g(\lfloor x \rfloor) + \sum_{n \leq x-1} F(n)(g(n) - g(n+1)) \\
&= F(x)g(\lfloor x \rfloor) + \sum_{n \leq x-1} F(n)(g(n) - g(n+1)).
\end{aligned}$$

Koska funktio g on jatkuvasti derivoituva välillä $[1, x]$, niin analyysin peruslauseen nojalla

$$g(n+1) - g(n) = \int_n^{n+1} g'(t)\,dt.$$

Lisäksi, koska $F(t) = F(n)$ kaikilla $n \leq t < n+1$, niin

$$F(n)(g(n+1) - g(n)) = \int_n^{n+1} F(t)g'(t)\,dt.$$

Näin ollen

$$\begin{aligned}\sum_{n \leq x} f(n)g(n) &= F(x)g(\lfloor x \rfloor) - \sum_{n \leq x-1} \int_n^{n+1} F(t)g'(t)\,dt \\ &= F(x)g(\lfloor x \rfloor) - \int_1^{\lfloor x \rfloor} F(t)g'(t)\,dt.\end{aligned}$$

Edelleen, koska

$$\int_{\lfloor x \rfloor}^{x} F(t)g'(t)\,dt = F(x)\int_{\lfloor x \rfloor}^{x} g'(t)\,dt = F(x)(g(x) - g(\lfloor x \rfloor)),$$

niin

$$\sum_{n \leq x} f(n)g(n) = F(x)g(x) - \int_1^x F(t)g'(t)\,dt.$$

□

Todistetaan nyt osittaissummausta hyödyntäen Mertensin lauseista ensimmäinen, joka kertoo, miten summa

$$\sum_{p \leq x} \frac{1}{p}$$

käyttäytyy, kun $x \to \infty$.

LAUSE 2.2. (Mertensin ensimmäinen lause) *On olemassa vakio B_1 siten, että*

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + B_1 + O\left(\frac{1}{\log x}\right), \quad \textit{kun } x \to \infty.$$

TODISTUS. Kirjoitetaan

$$\sum_{p \leq x} \frac{1}{p} = \sum_{p \leq x} \frac{\log p}{p}\frac{1}{\log p} = \sum_{2 \leq n \leq x} f(n)g(n),$$

missä

$$f(n) = \begin{cases} \frac{\log p}{p}, & \text{jos } n = p, \\ 0, & \text{muuten,} \end{cases}$$

ja

$$g(t) = \frac{1}{\log t}, \quad t > 1.$$

Olkoon

$$F(t) = \sum_{n \leq t} f(n) = \sum_{p \leq t} \frac{\log p}{p}.$$

Tällöin $F(t) = 0$ kaikilla $t < 2$. Lisäksi pätee, että

$$F(t) = \log t + r(t), \quad \text{missä } r(t) = O(1).$$

Perustelu tälle löytyy esimerkiksi Nathansonin teoksesta [**8**, s. 276–277]. Nyt integraali

$$\int_2^\infty \frac{r(t)}{t(\log t)^2}\,dt$$

suppenee itseisesti, ja

$$\int_x^\infty \frac{r(t)}{t(\log t)^2}\,dt = O\left(\frac{1}{\log x}\right).$$

Osittaissummauskaavalla saadaan

$$\begin{aligned}
\sum_{p\le x}\frac{1}{p} &= \sum_{2\le n\le x} f(n)g(n)\\
&= F(x)g(x) - \int_2^x F(t)g'(t)\,dt\\
&= \frac{\log x + r(x)}{\log x} + \int_2^x \frac{\log t + r(t)}{t(\log t)^2}\,dt\\
&= 1 + O\left(\frac{1}{\log x}\right) + \int_2^x \frac{1}{t\log t}\,dt + \int_2^x \frac{r(t)}{t(\log t)^2}\,dt\\
&= 1 + O\left(\frac{1}{\log x}\right) + \log\log x - \log\log 2\\
&\qquad + \int_2^\infty \frac{r(t)}{t(\log t)^2}\,dt - \int_x^\infty \frac{r(t)}{t(\log t)^2}\,dt\\
&= \log\log x + B_1 + O\left(\frac{1}{\log x}\right),
\end{aligned}$$

missä

$$B_1 = 1 - \log\log 2 + \int_2^\infty \frac{r(t)}{t(\log t)^2}\,dt.$$

□

Mertensin ensimmäisen lauseen mukaan siis

$$\sum_{p\le x}\frac{1}{p} \sim \log\log x.$$

Lisäksi Mertensin ensimmäisestä lauseesta seuraa, että kaikilla $y \ge x$ pätee

$$\begin{aligned}
\sum_{x<p\le y}\frac{1}{p} &= \sum_{p\le y}\frac{1}{p} - \sum_{p\le x}\frac{1}{p}\\
&= \log\log y + B_1 + O\left(\frac{1}{\log y}\right) - \left(\log\log x + B_1 + O\left(\frac{1}{\log x}\right)\right)\\
&= \log\frac{\log y}{\log x} + O\left(\frac{1}{\log x}\right), \quad \text{kun } x\to\infty.
\end{aligned} \tag{2.1}$$

Osoitetaan nyt tätä huomiota hyödyntäen seuraava aputulos, jota tullaan tarvitsemaan luvussa 4.

LEMMA 2.3. *Kun $x \to \infty$, niin kaikilla $y \geq x$,*

$$\prod_{x<p\leq y}\left(1-\frac{2}{p}\right)=\frac{(\log x)^2}{(\log y)^2}\left(1+O\left(\frac{1}{\log x}\right)\right).$$

TODISTUS. Oletetaan, että $x \geq 4$, jolloin $2/p \leq 1/2$ kaikilla $p \geq x$. Luonnollisen logaritmin Taylorin sarjasta saadaan, että kaikilla $|t| < 1$ pätee

$$\log(1+t)=t-\frac{t^2}{2}+\frac{t^3}{3}-\frac{t^4}{4}+\cdots=t+O(t^2), \quad \text{kun } t\to 0,$$

joten nyt

$$\log\left(1-\frac{2}{p}\right)=-\frac{2}{p}+O\left(\left(-\frac{2}{p}\right)^2\right)=-\frac{2}{p}+O\left(\frac{1}{p^2}\right).$$

Tämän ja huomion (2.1) nojalla saadaan

$$\begin{aligned}\sum_{x<p\leq y}\log\left(1-\frac{2}{p}\right)&=-2\sum_{x<p\leq y}\frac{1}{p}+O\left(\sum_{x<p\leq y}\frac{1}{p^2}\right)\\&=-2\left(\log\frac{\log y}{\log x}+O\left(\frac{1}{\log x}\right)\right)+O\left(\frac{1}{x}\right)\\&=\log\frac{(\log x)^2}{(\log y)^2}+O\left(\frac{1}{\log x}\right), \quad \text{kun } x\to\infty.\end{aligned}$$

Nyt siis

$$\begin{aligned}\prod_{x<p\leq y}\left(1-\frac{2}{p}\right)&=\exp\left(\sum_{x<p\leq y}\log\left(1-\frac{2}{p}\right)\right)\\&=\exp\left(\log\frac{(\log x)^2}{(\log y)^2}+O\left(\frac{1}{\log x}\right)\right)=\frac{(\log x)^2}{(\log y)^2}\left(1+O\left(\frac{1}{\log x}\right)\right),\end{aligned}$$

missä jälkimmäisin yhtäsuuruus seuraa siitä, että $\exp(t) = 1 + O(t)$ millä tahansa rajoitetulla välillä ja tässä $O(1/\log x)$ on rajoitettu, kun $x \geq 2$. □

Tarkastellaan sitten toista Mertensin lauseista. Se kertoo, miten tulo

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)$$

käyttäytyy, kun $x \to \infty$.

LAUSE 2.4. (Mertensin toinen lause) *On olemassa vakio C siten, että*

$$\prod_{p\leq x}\left(1-\frac{1}{p}\right)\sim\frac{e^{-C}}{\log x}, \quad \textit{kun } x\to\infty.$$

TODISTUS. Välillä $-1 < x \leq 1$ luonnolliselle logaritmille pätee

$$\log(1+x)=\sum_{n=1}^{\infty}\frac{(-1)^{n+1}}{n}x^n=x-\frac{x^2}{2}+\frac{x^3}{3}-\frac{x^4}{4}+\cdots,$$

joten

$$\log\left(1-\frac{1}{p}\right) = -\sum_{k=1}^{\infty}\frac{1}{kp^k}.$$

Nyt siis

$$\begin{aligned}\log\prod_{p\le x}\left(1-\frac{1}{p}\right) &= \sum_{p\le x}\log\left(1-\frac{1}{p}\right)\\ &= -\sum_{p\le x}\sum_{k=1}^{\infty}\frac{1}{kp^k}\\ &= -\sum_{p\le x}\frac{1}{p} - \sum_{p\le x}\sum_{k=2}^{\infty}\frac{1}{kp^k}.\end{aligned}$$

Koska geometrisen summan avulla saadaan

$$\sum_{k=2}^{\infty}\frac{1}{kp^k} \le \frac{1}{2}\sum_{k=2}^{\infty}\frac{1}{p^k} = \frac{1}{2p(p-1)} \le \frac{1}{p^2},$$

niin summa $\sum_p \sum_{k=2}^{\infty}(kp^k)^{-1}$ suppenee itseisesti, sanotaan lukuun B_2. Lisäksi

$$B_2 - \sum_{p\le x}\sum_{k=2}^{\infty}\frac{1}{kp^k} = \sum_{p>x}\sum_{k=2}^{\infty}\frac{1}{kp^k} \le \sum_{p>x}\frac{1}{p^2} \ll \frac{1}{x}$$

eli

$$\sum_{p\le x}\sum_{k=2}^{\infty}\frac{1}{kp^k} = B_2 - O\left(\frac{1}{x}\right).$$

Näin ollen Mertensin ensimmäisen lauseen nojalla saadaan

$$\begin{aligned}\log\prod_{p\le x}\left(1-\frac{1}{p}\right) &= -\log\log x - B_1 + O\left(\frac{1}{\log x}\right) - B_2 + O\left(\frac{1}{x}\right)\\ &= -\log\log x - B_1 - B_2 + O\left(\frac{1}{\log x}\right).\end{aligned}$$

Ottamalla nyt eksponentti molemmin puolin saadaan

$$\prod_{p\le x}\left(1-\frac{1}{p}\right) = \frac{\exp(-(B_1+B_2))}{\log x}\exp\left(O\left(\frac{1}{\log x}\right)\right)$$

joten väite seuraa, kun $C = B_1 + B_2$. □

LUKU 3

Seulamenetelmistä

Tässä luvussa tutustutaan seulamenetelmiin, joiden avulla on saatu osoitettua monia merkittäviä lukuteorian tuloksia. Ensin käsitellään seulamenetelmiä yleisesti ja käydään läpi tarvittavia merkintöjä. Tämän jälkeen tutustutaan tarkemmin erääseen seulamenetelmään, *Brunin seulaan*, jonka avulla Schnirelmannin lause saadaan todistettua. Luvun keskeisimpinä lähteinä on käytetty George Greavesin teosta *Sieves in Number Theory* [**3**] ja Paul Pollackin teosta *Not Always Buried Deep: A Second Course in Elementary Number Theory* [**9**].

3.1. Yleistä seulamenetelmistä

Seulamenetelmistä vanhin, ja ehkä tunnetuin, on antiikin kreikkalaisen matemaatikon Eratostheneen kehittämä menetelmä, jonka avulla voidaan helposti selvittää kaikki lukua x pienemmät alkuluvut. Tätä yksinkertaista menetelmää kutsutaan *Eratostheneen seulaksi*, ja se perustuu huomioon, jonka mukaan jokainen yhdistetty luku $n \leq x$ on jaollinen jollain alkuluvulla $p \leq \sqrt{x}$. Lukua x pienempien alkulukujen selvittämiseksi riittää siis vain tietää lukua $\sqrt{x}$ pienemmät alkuluvut. Ideana Eratostheneen seulassa on kirjoittaa ensin lista kaikista kokonaisluvuista väliltä $[2, x]$, ja tämän jälkeen käydä yksitellen läpi alkuluvut $p \leq \sqrt{x}$ ja yliviivata listalta kaikki luvun p monikerrat. Tällä tavalla jäljelle jää täsmälleen lukua x pienemmät alkuluvut. Esimerkiksi, jos $x = 30$, niin lukua $\sqrt{30}$ pienemmät alkuluvut, joilla seulotaan, ovat 2, 3 ja 5:

	2	3	4̸	5	6̸	7	8̸	9̸	10̸
11	12̸	13	14̸	15̸	16̸	17	18̸	19	20̸
21̸	22̸	23	24̸	25̸	26̸	27̸	28̸	29	30̸

Seulonnasta jäävät jäljelle luvut 2, 3, 5, 7, 11, 13, 17, 19, 23 ja 29. Nämä ovat lukua 30 pienemmät alkuluvut. [**3**]

Eratostheneen seulasta analyyttisemmän muotoilun esitti 1800-luvun alussa ranskalainen matemaatikko A. M. Legendre. Tällä *Legendren seulaksi* kutsutulla menetelmällä saadaan tietoa siitä, *kuinka paljon* lukua x pienempiä alkulukuja on. Edelleen kehittyneempiä ja lukuteoriassa merkittäviä seulamenetelmiä ovat muun muassa *Brunin seula* ja *Selbergin seula*. [**3**]

Seulamenetelmien avulla voidaan siis arvioida seulotun joukon kokoa eli sitä, kuinka paljon alkioita on jäljellä sen jälkeen, kun seulonta on tehty. Yleinen lukuteorian ongelma, johon seulamenetelmiä hyödynnetään, on muotoa: Jos $\mathcal{A}$ on äärellinen jono positiivisia kokonaislukuja ja $\mathcal{P}$ äärellinen joukko alkulukuja, niin kuinka paljon on sellaisia jonon $\mathcal{A}$ alkioita, jotka eivät ole jaollisia millään $p \in \mathcal{P}$? Tarkoituksena on siis arvioida lukua

$$S(\mathcal{A}, \mathcal{P}) := \#\{a \in \mathcal{A} : \mathrm{syt}(a, P) = 1\},$$

missä

$$P := \prod_{p \in \mathcal{P}} p.$$

Tässä seulontajoukon $\mathcal{A}$ vaaditaan olevan joukon sijasta jono, jotta seulontajoukoiksi käyvät myös sellaiset luonnollisten lukujen kokoelmat, joissa sama alkio esiintyy useampaan kertaan. Tällaisia kutsutaan *multijoukoiksi* (engl. *multiset*).

Usein äärellinen joukko alkulukuja, jolla seulotaan, saadaan katkaisemalla kaikkien alkulukujen ääretön joukko jostain kohtaa z. Tutkitaan siis, kuinka paljon on sellaisia jonon $\mathcal{A}$ alkioita, jotka eivät ole jaollisia millään $p \in \mathcal{P}$, $p \leq z$, missä $\mathcal{P}$ on kaikkien alkulukujen joukko. Tällöin merkitään

$$S(\mathcal{A}, \mathcal{P}, z) := \#\{a \in \mathcal{A} : \mathrm{syt}(a, P(z)) = 1\},$$

missä

$$P(z) := \prod_{\substack{p \in \mathcal{P} \\ p \leq z}} p.$$

Luvun $S(\mathcal{A}, \mathcal{P})$ arvioimiseksi täytyy olettaa, että jonolla $\mathcal{A}$ on jokin pituus X ja että tapahtumat ”luku on jaollinen alkuluvulla p” ovat kutakuinkin itsenäisiä ja niillä jokaisella on todennäköisyys $\alpha(p)$. Tällöin on luonnollista odottaa, että

$$S(\mathcal{A}, \mathcal{P}) \approx X \prod_{p \in \mathcal{P}} (1 - \alpha(p))$$

eli

$$S(\mathcal{A}, \mathcal{P}) = X \prod_{p \in \mathcal{P}} (1 - \alpha(p)) + E(X),$$

missä virhetermi E saadaan sitä pienemmäksi, mitä tehokkaampaa seulaa käytetään.

Tehdään edellinen vielä täsmällisemmin. Merkitään kirjaimella X siis seulontajoukon $\mathcal{A}$ kokoa, ja käytetään merkintää A_d ilmaisemaan jonon $\mathcal{A}$ niiden alkioiden lukumäärää, jotka ovat jaollisia luvulla d, eli

$$A_d := \#\{a \in \mathcal{A} : d \mid a\}.$$

Oletetaan lisäksi, että on olemassa multiplikatiivinen funktio α, joka saa arvoja väliltä $[0, 1]$ ja jolle kaikilla $d \mid P(z)$ pätee

$$A_d = X\alpha(d) + r(d), \tag{3.1}$$

missä virhetermi $r(d)$ on pieni. Käytännössä seulamenetelmiä hyödynnettäessä ensin *valitaan* X ja α, ja sen jälkeen *määritellään* virhetermi $r(d)$ siten, että (3.1) pätee.

Esimerkki 3.1. Olkoon $\mathcal{A} = \{n \in \mathbb{N} : n \leq x\}$ ja $\mathcal{P}$ alkulukujen joukko. Tällöin

$$S(\mathcal{A}, \mathcal{P}, z) = \pi(x, z),$$

missä $\pi(x, z)$ laskee niiden lukua x pienempien tai yhtäsuurten luonnollisten lukujen lukumäärän, jotka eivät ole jaollisia millään alkuluvulla $p \leq z$. Kaikilla d pätee

$$A_d = \left\lfloor \frac{x}{d} \right\rfloor,$$

joten, jos valitaan $X = x$ ja $\alpha(d) = 1/d$, niin

$$r(d) = -\left\{ \frac{x}{d} \right\},$$

sillä tällöin (3.1) pätee. Erityisesti $|r(d)| \leq 1$ kaikilla d.

3.2. Brunin seula

Seulamenetelmien juuret ulottuvat siis pitkälle antiikin aikaan, mutta modernin seulateorian parissa merkittävää työtä 1900-luvun alkupuolella teki norjalainen matemaatikko Viggo Brun (1885-1978). Tuohon aikaan Brunin aikaansaannokset jäivät vähemmälle huomiolle, mutta myöhemmin niiden merkitys ymmärrettiin. Brunin kehittämää seulaa hyödyntämällä saadaan todistettua Schnirelmannin lause. Tutustutaan siis seuraavaksi Brunin seulaan. Kaikki tässä luvussa esitetyt todistukset pohjautuvat Pollackin teokseen [**9**, s. 176–177 ja 182–185].

Brunin seulalla on kaksi eri muotoa, joista toisella saadaan arvioitua lukua $S(\mathcal{A}, \mathcal{P})$ ylhäältä ja toisella alhaalta. Schnirelmannin lauseen todistamiseen hyödynnetään näistä ylärajaa. Tätä ylärajaa varten tarvitaan seuraavaksi käsiteltävää tulosta vuorottelevista summista.

Olkoon $a_1, \ldots, a_n$ jono reaalilukuja, jossa on $n \in \mathbb{N}_0$ kappaletta alkioita. Määritellään kaikilla $k \in \mathbb{N}_0$ funktio $\delta_k(a_1 \ldots, a_n)$ summana kaikista sellaisista lukujen a_i tuloista, joissa on k kappaletta kerrottavia. Tällaisia tuloja on siis $\binom{n}{k}$ kappaletta. Määritellään lisäksi, että $\delta_0 = 1$ ja $\delta_k = 0$ kaikilla $k > n$. Esimerkiksi, jos $n = 2$, niin

$$\delta_0(a_1, a_2) = 1, \quad \delta_1(a_1, a_2) = a_1 + a_2, \quad \delta_2(a_1, a_2) = a_1 a_2$$

ja $\delta_k(a_1, a_2) = 0$ kaikilla $k > 2$. Kyseiselle funktiolle pätee seuraava tulos:

LEMMA 3.2. *Olkoot* $0 \leq a_1, \ldots, a_n \leq 1$*, missä* $n \in \mathbb{N}_0$*. Tällöin erotus*

$$\sum_{k=0}^{m} (-1)^k \, \delta_k(a_1, \ldots, a_n) - \prod_{j=1}^{n} (1 - a_j) \tag{3.2}$$

on joko epänegatiivinen tai epäpositiivinen riippuen siitä, onko luku m *parillinen vai pariton.*

TODISTUS. Osoitetaan väite induktiolla. Jos $n = 0$, niin tulo

$$T := \prod_{j=1}^{n} (1 - a_j)$$

on tyhjä. Tulkitaan tyhjä tulo ykköseksi. Lisäksi

$$\sum_{k=0}^{m} (-1)^k \, \delta_k = 1 - 0 + 0 - \cdots \pm 0 = 1.$$

Tällöin siis erotus (3.2) on nolla kaikilla m, joten väite pätee. Tehdään sitten induktio-oletus eli oletetaan, että väite pätee kaikilla m jokaiselle sellaiselle lukujonolle, jossa on n kappaletta alkioita ja kaikki alkiot ovat reaalilukuja väliltä [0,1]. Tutkitaan mielivaltaista reaalilukujonoa $0 \leq a_1, \ldots, a_{n+1} \leq 1$, jossa on siis $n + 1$ kappaletta alkioita, ja osoitetaan, että väite pätee myös tälle lukujonolle kaikilla m. Osoitetaan

siis, että

$$\begin{aligned}(3.3)\qquad &\left(\sum_{k=0}^{m}(-1)^k\,\delta_k(a_1,\ldots,a_{n+1})-\prod_{j=1}^{n+1}(1-a_j)\right)\\ &\qquad-\left(\sum_{k=0}^{m}(-1)^k\,\delta_k(a_1,\ldots,a_n)-\prod_{j=1}^{n}(1-a_j)\right)\end{aligned}$$

on joko epänegatiivinen tai epäpositiivinen riippuen siitä, onko luku m parillinen vai pariton. Jos $m=0$, niin erotus (3.3) sievenee muotoon

$$\prod_{j=1}^{n}(1-a_j)-\prod_{j=1}^{n+1}(1-a_j)=Ta_{n+1},$$

joka on epänegatiivinen. Jos taas $m>0$, niin erotus (3.3) voidaan kirjoittaa muodossa

$$\begin{aligned}&\sum_{k=1}^{m}(-1)^k(\delta_k(a_1,\ldots,a_{n+1})-\delta_k(a_1,\ldots,a_n))+Ta_{n+1}\\ &\qquad=\sum_{k=1}^{m}(-1)^k\,a_{n+1}\,\delta_{k-1}(a_1,\ldots,a_n)+Ta_{n+1}\\ &\qquad=a_{n+1}\left(T-\sum_{k=0}^{m-1}(-1)^k\,\delta_k(a_1,\ldots,a_n)\right).\end{aligned}$$

Induktio-oletuksen nojalla tämä on epänegatiivinen, kun m on parillinen, ja epäpositiivinen, kun m on pariton. Näin ollen induktioperiaatteen nojalla väite on osoitettu. □

Eräs edellisen lemman tärkeä erikoistapaus saadaan, kun $n\in\mathbb{N}$ ja

$$a_1=a_2=\cdots=a_n=1.$$

Tällöin

$$\prod_{j=1}^{n}(1-a_j)=(1-1)^n=0$$

ja

$$\delta_k(a_1,\ldots,a_n)=\delta_k(1,\ldots,1)=\binom{n}{k},$$

joten Lemmasta 3.2 seuraa, että summa

$$\sum_{k=0}^{m}(-1)^k\binom{n}{k}$$

on epänegatiivinen, jos luku m on parillinen, ja epäpositiivinen, jos m on pariton.

Todistetaan nyt edellistä lemmaa ja sen erikoistapausta hyödyntäen Brunin seulan yläraja. Palautetaan tätä varten mieleen joukon osituksen määritelmä.

MÄÄRITELMÄ 3.3. Olkoon I epätyhjä indeksijoukko ja olkoot $B_i, i \in I$, joukon A epätyhjiä osajoukkoja. Joukot B_i muodostavat joukon A *osituksen*, jos

$$\bigcup_{i \in I} B_i = A$$

ja

$$B_i \cap B_j = \emptyset \quad \text{aina, kun } i \neq j.$$

LAUSE 3.4. (Brunin seula, yläraja) *Olkoon $\mathcal{P}$ äärellinen joukko alkulukuja ja*

$$\mathcal{P} = \bigcup_{j=1}^{r} \mathcal{P}_j$$

sen ositus. Asetetaan $P_j := \prod_{p \in \mathcal{P}_j} p$, ja oletetaan, että $\alpha(p) < 1$ kaikilla $p \in \mathcal{P}$. Tällöin valitsemalla epänegatiiviset parilliset kokonaisluvut $m_1, \ldots, m_r$ miten tahansa, pätee

$$S(\mathcal{A}, \mathcal{P}) \leq X \prod_{p \in \mathcal{P}} (1 - \alpha(p)) \exp\left(\sum_{j=1}^{r} \left(\sum\nolimits^{(j)} \Big/ \prod\nolimits^{(j)} \right) \right) + O\Bigg(\sum_{\substack{d_1, \ldots, d_r \\ d_j \mid P_j,\, \omega(d_j) \leq m_j}} |r(d_1 \cdots d_r)| \Bigg), \tag{3.4}$$

missä kaikilla $1 \leq j \leq r$,

$$\prod\nolimits^{(j)} := \prod_{p \in \mathcal{P}_j} (1 - \alpha(p)) \qquad \textit{ja} \qquad \sum\nolimits^{(j)} := \sum_{\substack{d_j \mid P_j \\ \omega(d_j) = m_j + 1}} \alpha(d_j),$$

ja implisiittinen vakio ei riipu lauseen parametreista.

TODISTUS. Lauseen todistamiseen tarvitaan *seulontafunktiota*

$$s(n) := \begin{cases} 1, & \text{jos } \operatorname{syt}(n, P) = 1, \\ 0, & \text{muuten.} \end{cases}$$

Seulontafunktio $s(n)$ saa siis arvon 1, jos luvulla n ei ole yhtään alkutekijää $p \in \mathcal{P}$. Jos taas luku n on jaollinen jollain alkuluvulla $p \in \mathcal{P}$, niin seulontafunktio saa arvon 0. Näin ollen

$$S(\mathcal{A}, \mathcal{P}) = \sum_{a \in \mathcal{A}} s(a). \tag{3.5}$$

Möbiuksen funktion ominaisuudesta (Lause 1.23) seuraa, että seulontafunktio $s(n)$ voidaan esittää myös muodossa

$$s(n) = \sum_{d \mid \operatorname{syt}(n, P)} \mu(d) = \sum_{d \mid n,\, d \mid P} \mu(d). \tag{3.6}$$

Jälkimmäinen yhtäsuuruus pätee, sillä luvun $\operatorname{syt}(n, P)$ jakavat täsmälleen lukujen n ja P yhteiset tekijät. Tämä esitys on tärkeä myöhemmän todistuksen kannalta. Myös seuraavaa aputulosta tarvitaan:

LEMMA 3.5. *Olkoon $n \in \mathbb{N}$. Tällöin erotus*

$$\sum_{\substack{d \mid n,\, d \mid P \\ \omega(d) \leq m}} \mu(d) - \sum_{d \mid n,\, d \mid P} \mu(d)$$

on joko epänegatiivinen tai epäpositiivinen riippuen siitä, onko luku $m \geq 0$ parillinen vai pariton.

TODISTUS. Väitteen todistamiseen voidaan hyödyntää Lemman 3.2 erikoistapausta. Jos oletetaan, että luvulla n on täsmälleen l kappaletta alkutekijöitä $p \in \mathcal{P}$, niin saadaan

$$\sum_{\substack{d \mid n,\, d \mid P \\ \omega(d) \leq m}} \mu(d) = \sum_{k=0}^{m} (-1)^k \binom{l}{k} \begin{cases} = 1, & \text{jos } l = 0 \text{ eli } \operatorname{syt}(n, P) = 1, \\ \geq 0, & \text{jos } l \geq 1 \text{ ja } m \text{ parillinen}, \\ \leq 0, & \text{jos } l \geq 1 \text{ ja } m \text{ pariton}, \end{cases}$$

ja

$$\sum_{d \mid n,\, d \mid P} \mu(d) = s(n) = \begin{cases} 1, & \text{jos } l = 0, \\ 0, & \text{jos } l \geq 1. \end{cases}$$

Tämä osoittaa väitteen. □

Oletetaan sitten, että $\mathcal{P} = \bigcup_{j=1}^{r} \mathcal{P}_j$ on joukon $\mathcal{P}$ ositus, ja asetetaan

$$P_j := \prod_{p \in \mathcal{P}_j} p.$$

Nyt huomiosta (3.6), Möbiuksen funktion multiplikatiivisuudesta ja edellisen lemman todistuksesta seuraa, että valitsemalla epänegatiiviset parilliset kokonaisluvut $m_1, \ldots, m_r$ miten tahansa, pätee

$$\begin{aligned} s(n) = \sum_{d \mid n,\, d \mid P} \mu(d) &= \prod_{j=1}^{r} \sum_{d_j \mid n,\, d_j \mid P_j} \mu(d_j) \\ &\leq \prod_{j=1}^{r} \sum_{\substack{d_j \mid n,\, d_j \mid P_j \\ \omega(d_j) \leq m_j}} \mu(d_j) = \sum_{\substack{d_1, \ldots, d_r \\ d_j \mid n,\, d_j \mid P_j \\ \omega(d_j) \leq m_j}} \mu(d_1) \cdots \mu(d_r). \end{aligned}$$

Yhdistämällä tämän huomioon (3.5) ja muistamalla luvun alussa läpikäydyt seulamenetelmiin liittyvät merkinnät saadaan yläraja

$$\begin{aligned} S(\mathcal{A},\mathcal{P}) &\le \sum_{a\in\mathcal{A}} \sum_{\substack{d_1,\dots,d_r\\ d_j\mid a,\, d_j\mid P_j\\ \omega(d_j)\le m_j}} \mu(d_1)\cdots\mu(d_r) \\ &\le \sum_{\substack{d_1,\dots,d_r\\ d_j\mid P_j,\,\omega(d_j)\le m_j}} \mu(d_1)\cdots\mu(d_r)\, A_{d_1\cdots d_r} \\ &= X \sum_{\substack{d_1,\dots,d_r\\ d_j\mid P_j,\,\omega(d_j)\le m_j}} \mu(d_1)\cdots\mu(d_r)\,\alpha(d_1)\cdots\alpha(d_r) \\ &\qquad + \sum_{\substack{d_1,\dots,d_r\\ d_j\mid P_j,\,\omega(d_j)\le m_j}} \mu(d_1)\cdots\mu(d_r)\, r(d_1\cdots d_r). \end{aligned}$$

Näin ollen lukua $S(\mathcal{A},\mathcal{P})$ rajoittaa ylhäältä

$$X\prod_{j=1}^{r} \sum_{\substack{d_j\mid P_j\\ \omega(d_j)\le m_j}} \mu(d_j)\,\alpha(d_j) + \sum_{\substack{d_1,\dots,d_r\\ d_j\mid P_j,\,\omega(d_j)\le m_j}} \mu(d_1)\cdots\mu(d_r)\, r(d_1\cdots d_r). \tag{3.7}$$

Muokataan tätä vielä hieman, jotta yläraja saadaan samaan muotoon kuin Brunin seulassa. Lemmasta 3.2 seuraa, että kaikilla $1\le j\le r$,

$$\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\le m_j}} \mu(d_j)\,\alpha(d_j) - \prod_{p\in\mathcal{P}_j}(1-\alpha(p)) \ge 0.$$

Koska $\alpha(p)\le 1$ kaikilla $p\in\mathcal{P}_j$, niin

$$\prod_{p\in\mathcal{P}_j}(1-\alpha(p)) \ge 0.$$

Näin ollen myös

$$\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\le m_j}} \mu(d_j)\,\alpha(d_j) \ge 0 \quad \text{kaikilla } 1\le j\le r.$$

Lisäksi kaikilla $1\le j\le r$ pätee

$$\sum_{\substack{d_j\mid P_j\\ \omega(d_j)\le m_j}} \mu(d_j)\,\alpha(d_j) - \prod_{p\in\mathcal{P}_j}(1-\alpha(p)) \le \sum_{\substack{d_j\mid P_j\\ \omega(d_j)=m_j+1}} \alpha(d_j),$$

joten

$$0 \le \sum_{\substack{d_j\mid P_j\\ \omega(d_j)\le m_j}} \mu(d_j)\,\alpha(d_j) \le \prod_{p\in\mathcal{P}_j}(1-\alpha(p)) + \sum_{\substack{d_j\mid P_j\\ \omega(d_j)=m_j+1}} \alpha(d_j).$$

Jos siis asetetaan

$$\prod^{(j)} := \prod_{p \in \mathcal{P}_j} (1 - \alpha(p)) \qquad \text{ja} \qquad \sum^{(j)} := \sum_{\substack{d_j \mid P_j \\ \omega(d_j) = m_j + 1}} \alpha(d_j),$$

niin saadaan

$$X \prod_{j=1}^{r} \sum_{\substack{d_j \mid P_j \\ \omega(d_j) \le m_j}} \mu(d_j)\, \alpha(d_j) \le X \prod_{j=1}^{r} \left(\prod^{(j)} + \sum^{(j)} \right)$$

$$= X \prod_{p \in \mathcal{P}} (1 - \alpha(p)) \prod_{j=1}^{r} \left(1 + \sum^{(j)} \Big/ \prod^{(j)} \right).$$

Edellä jakaminen on järkevää, kun oletetaan, että $\alpha(p) < 1$ kaikilla $p \in \mathcal{P}$. Kun nyt muistetaan, että $1 + x \le \exp(x)$ kaikilla x, niin saadaan päätermi Brunin seulassa esiintyvään muotoon. Lisäksi, koska $|\mu(d)| \le 1$ kaikilla d, niin ylärajan (3.7) virhetermiä voidaan arvioida triviaalisti, ja yläraja saadaan muotoon

$$S(\mathcal{A}, \mathcal{P}) \le X \prod_{p \in \mathcal{P}} (1 - \alpha(p)) \exp \left(\sum_{j=1}^{r} \left(\sum^{(j)} \Big/ \prod^{(j)} \right) \right)$$

$$+ O\Bigg(\sum_{\substack{d_1, \ldots, d_r \\ d_j \mid P_j,\ \omega(d_j) \le m_j}} |r(d_1 \cdots d_r)| \Bigg).$$

□

LUKU 4

Luonnollisten lukujen esittäminen kahden alkuluvun summana

Tässä luvussa osoitetaan Brunin seulaa hyödyntäen kolme Schnirelmannin lauseen todistamiseen tarvittavaa aputulosta. Kaikki luvussa esitetyt todistukset pohjautuvat Paul Pollackin teokseen *Not Always Buried Deep: A Second Course in Elementary Number Theory* [**9**, s. 185–190 ja 200].

Käytetään merkintää $R(N)$ ilmaisemaan, kuinka monella eri tavalla järjestys huomioon ottaen luonnollinen luku N voidaan esittää kahden alkuluvun summana, toisin sanoen

$$R(N) := \sum_{p_1+p_2=N} 1.$$

Esimerkiksi $R(9) = 2$, sillä $9 = 2+7 = 7+2$. Osoitetaan seuraavaksi kolme tarvittavaa tulosta luvulle $R(N)$. Näistä ensimmäinen antaa luvulle $R(N)$ ylärajan.

LEMMA 4.1. *Kaikille luonnollisille luvuille $N \geq 2$ pätee*

$$R(N) \ll \frac{N}{(\log N)^2} \prod_{p \mid N} \left(1 + \frac{1}{p}\right).$$

TODISTUS. Olkoon $N \geq 2$ luonnollinen luku. Jos N on pariton, niin väite on selvä, sillä tällöin $R(N) \leq 2$. Nimittäin, jotta kahden luonnollisen luvun summa on pariton, on toisen luvuista oltava parillinen. Koska ainoa parillinen alkuluku on 2, niin kahden alkuluvun summana voidaan esittää ainoastaan ne parittomat N, jotka ovat muotoa $N = p + 2$, missä p on alkuluku.

Osoitetaan siis, että väite pätee myös kaikille parillisille N. Olkoon $\mathcal{P}$ alkulukujen joukko ja $\mathcal{A} := \{n(N-n) : n \in \mathbb{N},\ 1 \leq n \leq N\}$ multijoukko eli joukko, jossa sama alkio voi esiintyä useampaan kertaan. Tällöin millä tahansa $z > 0$ pätee

$$R(N) \leq 2z + S(\mathcal{A}, \mathcal{P}, z). \tag{4.1}$$

Nimittäin, jos $N = n + (N-n)$ on luvun N esitys kahden alkuluvun summana, niin tällöin joko vähintään toinen luvuista n ja $N-n$ kuuluu välille $[2, z]$ tai kummallakaan luvuista n ja $N-n$ ei ole yhtään alkutekijää $\leq z$. Ensimmäisessä tapauksessa mahdollisia lukuja n on korkeintaan $2z$ kappaletta, ja jälkimmäisessä tapauksessa mahdolliset luvut n (joille välttämättä $2 \leq n \leq N-2$) laskee $S(\mathcal{A}, \mathcal{P}, z)$.

Lähdetään siis seuraavaksi arvioimaan lukua $S(\mathcal{A}, \mathcal{P}, z)$. Tähän tarvitaan Brunin seulaa, joten valitaan ensin seulontaparametrit. Koska $\mathcal{A}$ on multijoukko, niin sen alkioiden lukumäärä on N. Olkoon siis $X = N$ ja $\alpha(d) = \nu(d)/d$, missä

$$\nu(d) := \#\{n \,(\mathrm{mod}\, d) : n(N-n) \equiv 0 \ (\mathrm{mod}\, d)\}.$$

Koska $0 \leq \nu(d) \leq d$ kaikilla d, niin funktio α saa vain arvoja väliltä $[0, 1]$. Lisäksi funktio ν on multiplikatiivinen, joten myös α on multiplikatiivinen kuten halutaan.

Perustellaan tämä lyhyesti. Merkitään $f(n) = n(N-n)$. Olkoot d_1 ja d_2 keskenään jaottomat sekä n_1 ja n_2 sellaiset, että

$$f(n_1) \equiv 0 \pmod{d_1} \qquad \text{ja} \qquad f(n_2) \equiv 0 \pmod{d_2}. \tag{4.2}$$

Tällöin kiinalaisen jäännöslauseen (Lause 1.15) mukaan on olemassa yksikäsitteinen luku n $(0 \leq n < d_1 d_2)$ siten, että

$$n \equiv n_1 \pmod{d_1} \qquad \text{ja} \qquad n \equiv n_2 \pmod{d_2}.$$

Lisäksi kaikille kokonaislukukertoimisille polynomeille $p(x)$ pätee, että jos

$$a \equiv b \pmod{c},$$

niin

$$p(a) \equiv p(b) \pmod{c}$$

(ks. [**1**, s. 107]). Siispä tälle kyseiselle n pätee

$$f(n) \equiv f(n_1) \equiv 0 \pmod{d_1}$$

ja

$$f(n) \equiv f(n_2) \equiv 0 \pmod{d_2},$$

joten kiinalaisen jäännöslauseen mukaan

$$f(n) \equiv 0 \pmod{d_1 d_2}. \tag{4.3}$$

Näin ollen jokaista yhtälöiden (4.2) ratkaisuparia (n_1, n_2) vastaa yksikäsitteinen ratkaisu yhtälölle (4.3). Tästä seuraa, että $\nu(d_1 d_2) = \nu(d_1)\nu(d_2)$, eli funktio ν on multiplikatiivinen.

Perustellaan sitten, että valituilla X ja α pätee

$$A_d = X\alpha(d) + r(d), \quad \text{missä} \ \ |r(d)| \leq \nu(d) \ \ \text{kaikilla} \ \ d \,|\, P(z).$$

Tässä A_d ilmaisee siis joukon $\mathcal{A}$ niiden alkioiden lukumäärän, jotka ovat jaollisia luvulla d. Koska $\mathcal{A}$ on multijoukko, täytyy siis tutkia, kuinka monta sellaista luonnollista lukua $1 \leq n \leq N$ on, joilla $n(N-n) \equiv 0 \pmod{d}$. Koska d:n peräkkäisen luonnollisen luvun joukossa on aina täsmälleen $\nu(d)$ kappaletta ratkaisuja kongruenssille $n(N-n) \equiv 0 \pmod{d}$, niin

$$A_d \approx \frac{N}{d} \cdot \nu(d) = X\alpha(d).$$

Virheen arvioimiseksi ajatellaan luonnollisten lukujen jakautuvan keskenään erillisiin paloihin siten, että jokainen pala sisältää täsmälleen d peräkkäistä luonnollista lukua. Tällöin lukua N pienempien tai yhtäsuurten luonnollisten lukujen joukkoon sisältyy $\lfloor N/d \rfloor$ ensimmäistä tällaista palaa. Toisaalta luvut $1 \leq n \leq N$ sisältyvät itse $\lceil N/d \rceil$ ensimmäiseen palaan. Näin ollen

$$\left\lfloor \frac{N}{d} \right\rfloor \nu(d) \leq A_d \leq \left\lceil \frac{N}{d} \right\rceil \nu(d),$$

ja siten virhetermille $r(d)$ pätee

$$|r(d)| = \left| A_d - \frac{N}{d} \cdot \nu(d) \right| \leq \nu(d).$$

Näytetään vielä, että kaikilla alkuluvuilla $p \leq N$,

$$\alpha(p) = \begin{cases} 1/p, & \text{jos } p \mid N, \\ 2/p, & \text{jos } p \nmid N. \end{cases} \tag{4.4}$$

Ensinnäkin huomataan, että ainakin luvut 0 ja $N \,(\mathrm{mod}\, p)$ kuuluvat joukkoon

$$\{n \,(\mathrm{mod}\, p) : n(N-n) \equiv 0 \ (\mathrm{mod}\ p)\}.$$

Eukleideen lemmasta (Lause 1.8) seuraa, että alkuluku $p \leq N$ jakaa luvun $n(N-n)$, jos ja vain jos $p \mid n$ tai $p \mid (N-n)$. Jos $p \mid n$, niin $n \,(\mathrm{mod}\, p) = 0$. Jos taas $p \mid (N-n)$, niin tällöin

$$N - n = kp \quad \text{eli} \quad n = N - kp$$

jollakin $k \in \mathbb{N}_0$. Jos nyt $p \mid N$, niin tällöin myös $p \mid n$ eli $n \,(\mathrm{mod}\, p) = 0$. Jos taas $p \nmid N$, niin

$$N = lp + q$$

joillakin yksikäsitteisillä $l, q \in \mathbb{N},\ 0 < q < p$. Siis

$$n = lp + q - kp = (l-k)p + q,$$

joten $n \,(\mathrm{mod}\, p) = q \neq 0$. Näin ollen, jos $p \mid N$, niin $\nu(p) = \#\{0\} = 1$, ja jos $p \nmid N$, niin $\nu(p) = \#\{0, q\} = 2$. Siispä kohta (4.4) seuraa. Lisäksi huomataan, että $\alpha(p) < 1$ kaikilla alkuluvuilla p, sillä N on parillinen.

Ajatellaan nyt, että $X = N$ menee kohti ääretöntä, kun $u > 1$ on lukittu. Tavoitteena on ensin näyttää, että kun u on valittu tarpeeksi suureksi, niin

$$S(\mathcal{A}, \mathcal{P}, z) \ll X \prod_{p \leq z} (1 - \alpha(p)), \quad \text{missä } \ z := X^{1/u}. \tag{4.5}$$

Jotta tähän voidaan hyödyntää Brunin seulaa, tarvitaan joukon $\mathcal{P} \cap [2, z]$ ositus. Otetaan käyttöön merkintä

$$\eta = \log \log X,$$

ja valitaan parametrit

$$K := 1,57 \quad \text{ja} \quad K_1 := 1,571.$$

Tässä olennaista on vain se, että $1 < K < K_1$, mutta käytetään samoja parametreja kuin Pollackin todistuksessa [**9**, s. 186].

Suurilla X pätee $\eta < z = X^{1/u}$, joten jos valitaan pienin sellainen kokonaisluku R, jolle

$$z^{1/K^R} < \eta,$$

niin tällöin $R \geq 1$. Lisäksi $R \to \infty$, kun $X \to \infty$. Määritellään sitten

$$z_j = \begin{cases} z^{1/K^j}, & \text{kun } 0 \leq j \leq R-1, \\ \eta, & \text{kun } j = R, \\ 1, & \text{kun } j = R+1, \end{cases}$$

ja ositetaan joukko $\mathcal{P} \cap [2, z]$ osajoukkoihin

$$\mathcal{P}_j := \{p \in \mathcal{P} : z_j < p \leq z_{j-1}\}, \quad 1 \leq j \leq R+1.$$

Määritellään lisäksi vastaavat epänegatiiviset parilliset kokonaisluvut $m_1, \ldots, m_{R+1}$ asettamalla

$$m_j = 2j \quad \text{kaikilla } \ j = 1, \ldots, R$$

ja valitsemalla luvuksi m_{R+1} pienin sellainen parillinen kokonaisluku, joka on vähintään yhtä suuri kuin joukon $\mathcal{P}_{R+1}$ alkioiden lukumäärä.

Nyt Brunin seula (Lause 3.4) antaa ylärajan luvulle $S(\mathcal{A}, \mathcal{P}, z)$. Yritetään siis tätä ylärajaa hyödyntämällä päästä arvioon (4.5). Lähdetään ensin arvioimaan Brunin seulan päätermiä. Käytetään tässä merkintöjä

$$\sum^{(j)} \quad \text{ja} \quad \prod^{(j)}$$

ilmaisemaan samaa kuin Brunin seulassa. Muistetaan lisäksi, miten sivulla 28 määriteltiin luvut P_j. Edellä luku m_{R+1} valittiin siten, että sellaisia luvun P_{R+1} jakajia d_{R+1}, joille $\omega(d_{R+1}) = m_{R+1} + 1$, ei ole olemassa. Näin ollen

$$\sum^{(R+1)} = \sum_{\substack{d_{R+1} \mid P_{R+1} \\ \omega(d_{R+1}) = m_{R+1}+1}} \alpha(d_{R+1}) = 0, \tag{4.6}$$

eli termi $\sum^{(j)} / \prod^{(j)}$ katoaa, kun $j = R + 1$. Brunin seulan (3.4) päätermin arvioimiseksi riittää siis arvioida suhdetta $\sum^{(j)} / \prod^{(j)}$, kun $j = 1, 2 \ldots, R$. Arvioidaan ensin nimittäjää.

Huomataan, että kaikilla $j = 1, 2, \ldots, R - 1$ pätee

$$\frac{(\log z_j)^2}{(\log z_{j-1})^2} = \frac{\left(\log z^{1/K^j}\right)^2}{\left(\log z^{1/K^{j-1}}\right)^2} = \frac{1}{K^2}.$$

Lisäksi, koska $z^{1/K^R} < \eta$, niin

$$\frac{(\log z_R)^2}{(\log z_{R-1})^2} = \frac{(\log \eta)^2}{\left(\log z^{1/K^{R-1}}\right)^2} > \frac{\left(\log z^{1/K^R}\right)^2}{\left(\log z^{1/K^{R-1}}\right)^2} = \frac{1}{K^2}.$$

Siispä kaikilla $j = 1, 2, \ldots, R$,

$$\frac{(\log z_j)^2}{(\log z_{j-1})^2} \geq \frac{1}{K^2}. \tag{4.7}$$

Lisäksi, koska kaikki luvuista $z_1, \ldots, z_R$ ovat suurempia tai yhtäsuuria kuin η, niin ne lähestyvät ääretöntä, kun $X \to \infty$. Näin ollen huomion (4.4) sekä Lemman 2.3 nojalla suurilla X ja kaikilla $j = 1, 2, \ldots, R$ pätee

$$\begin{aligned} \prod^{(j)} &= \prod_{p \in \mathcal{P}_j} (1 - \alpha(p)) = \prod_{z_j < p \leq z_{j-1}} (1 - \alpha(p)) \\ &\geq \prod_{z_j < p \leq z_{j-1}} \left(1 - \frac{2}{p}\right) = \frac{(\log z_j)^2}{(\log z_{j-1})^2} \left(1 + O\left(\frac{1}{\log z_j}\right)\right) \\ &\geq \frac{1}{K^2} \left(1 + O\left(\frac{1}{\log \eta}\right)\right) \geq \frac{1}{K_1^2}. \end{aligned} \tag{4.8}$$

Arvioidaan sitten osoittajaa. Huomiosta (4.7) seuraa, että kaikilla $j = 1, 2, \ldots, R$,

$$\frac{\log z_{j-1}}{\log z_j} \leq K.$$

Tämän ja huomion (2.1) nojalla saadaan, että riittävän suurilla X,

$$\sum_{z_j < p \le z_{j-1}} \frac{2}{p} = 2\log\frac{\log z_{j-1}}{\log z_j} + O\left(\frac{1}{\log z_j}\right) \le 2\log K + O\left(\frac{1}{\log \eta}\right) \le 2\log K_1.$$

Lisäksi huomataan, että kun tulo

$$\left(\sum_{p\in\mathcal{P}_j} \alpha(p)\right)^{m_j+1} = \left(\sum_{p\in\mathcal{P}_j} \alpha(p)\right)\cdots\left(\sum_{p\in\mathcal{P}_j} \alpha(p)\right)$$

kerrotaan auki, niin saadussa summassa jokainen termi $\alpha(d_j)$, missä $d_j \mid P_j$ ja $\omega(d_j) = m_j + 1$, esiintyy täsmälleen $(m_j+1)!$ kertaa. Näin ollen kaikilla $1 \le j \le R$,

$$\begin{aligned}\sum\nolimits^{(j)} &= \sum_{\substack{d_j \mid P_j \\ \omega(d_j) = m_j+1}} \alpha(d_j) \le \frac{1}{(m_j+1)!}\left(\sum_{p\in\mathcal{P}_j}\alpha(p)\right)^{m_j+1} \\ &\le \frac{1}{(m_j+1)!}\left(\sum_{p\in\mathcal{P}_j}\frac{2}{p}\right)^{m_j+1} \le \frac{(2\log K_1)^{m_j+1}}{(m_j+1)!}.\end{aligned} \tag{4.9}$$

Näin saatiin arvioitua sekä osoittajaa että nimittäjää. Yhdistämällä nyt kohdat (4.8) ja (4.9) keskenään sekä muistamalla huomion (4.6) ja eksponenttifunktion Taylorin sarjakehitelmän saadaan, että suurilla X pätee

$$\begin{aligned}\sum_{j=1}^{R+1}\left(\sum\nolimits^{(j)} \Big/ \prod\nolimits^{(j)}\right) &\le K_1^2 \sum_{j=1}^{R} \frac{(2\log K_1)^{2j+1}}{(2j+1)!} \\ &\le K_1^2 \sum_{n=0}^{\infty} \frac{(2\log K_1)^n}{n!} = K_1^2 \exp(2\log K_1).\end{aligned}$$

Huomataan siis, että $X\prod_{p\le z}(1-\alpha(p))$ vakiolla kerrottuna rajoittaa ylhäältä Brunin seulan päätermiä. Lisäksi Mertensin ensimmäisestä lauseesta (Lause 2.2) seuraa, että

$$\sum_{p\le x}\frac{1}{p} \asymp \log\log x.$$

Tämän ja huomion

$$\log(1+x) \sim x, \quad \text{kun } x \to 0,$$

nojalla millä tahansa kiinteällä $u > 1$ pätee

$$\begin{aligned}\prod_{2<p\le X^{1/u}}\left(1-\frac{2}{p}\right) &= \exp\left(\sum_{2<p\le X^{1/u}} \log\left(1-\frac{2}{p}\right)\right) \\ &\asymp \exp\left(\sum_{2<p\le X^{1/u}} -\frac{2}{p}\right) \asymp \exp(-2\log\log X^{1/u}) = \frac{u^2}{(\log X)^2}.\end{aligned}$$

Nyt tästä ja huomiosta (4.4) seuraa, että

$$X \prod_{p \le X^{1/u}} (1 - \alpha(p)) \ge \frac{1}{2} X \prod_{2 < p \le X^{1/u}} \left(1 - \frac{2}{p}\right) \asymp \frac{X}{(\log X)^2}, \quad \text{kun } X \to \infty.$$

Näin ollen arvion

$$S(\mathcal{A}, \mathcal{P}, z) \ll X \prod_{p \le z} (1 - \alpha(p))$$

saamiseksi täytyy enää vain varmistaa, että Brunin seulan virhetermissä esiintyvä summa

$$\sum_{\substack{d_1, \dots, d_{R+1} \\ d_j | P_j,\ \omega(d_j) \le m_j}} |r(d_1 \cdots d_{R+1})| \tag{4.10}$$

on pienempää kertaluokkaa kuin $X/(\log X)^2$. Näytetään, että valitsemalla sopivasti luku u saadaan, että summalle (4.10) pätee $\ll X^\lambda$ jollakin vakiolla $\lambda < 1$.

Huomataan, että kaikilla d_j $(1 \le j \le R+1)$, joilla $d_j \mid P_j$ ja $\omega(d_j) \le m_j$ pätee $d_j \le z_{j-1}^{m_j}$. Lisäksi siitä, millä tavalla luku m_{R+1} valittiin, seuraa, että $m_{R+1} \le \eta$, joten

$$d_{R+1} \le z_R^{m_{R+1}} = \eta^{m_{R+1}} \le \eta^\eta.$$

Näin ollen kaikille summassa (4.10) esiintyville virheen $r(\cdot)$ argumenteille $d_1 \cdots d_{R+1}$ pätee

$$d_1 \cdots d_{R+1} \le \left(\prod_{j=1}^{R} z_{j-1}^{m_j} \right) \eta^\eta.$$

Edelleen, koska

$$\begin{aligned} \left(\prod_{j=1}^{R} z_{j-1}^{m_j} \right) &= z_0^{m_1} z_1^{m_2} \cdots z_{R-1}^{m_R} \\ &= z^{m_1} \left(z^{1/K}\right)^{m_2} \cdots \left(z^{1/K^{R-1}}\right)^{m_R} \\ &= z^{\sum_{j=1}^{R} m_j / K^{j-1}} \\ &= X^{\frac{1}{u}\left(\sum_{j=1}^{R} m_j / K^{j-1}\right)} \end{aligned}$$

ja

$$\begin{aligned} \eta^\eta &= (\log\log X)^{\log\log X} \\ &= \left(e^{\log\log\log X}\right)^{\log\log X} \\ &= \left(\left(X^{1/\log X}\right)^{\log\log\log X}\right)^{\log\log X} \\ &= X^{\log\log X \log\log\log X / \log X} \end{aligned}$$

niin

$$d_1 \cdots d_{R+1} \le X^{\frac{1}{u}\left(\sum_{j=1}^{R} m_j / K^{j-1}\right)} X^{\log\log X \log\log\log X / \log X}.$$

Lisäksi aritmeettis-geometrisen sarjan ominaisuuksien avulla saadaan

$$\sum_{j=1}^{R} \frac{m_j}{K^{j-1}} \le \sum_{j=1}^{\infty} \frac{2j}{K^{j-1}} = \frac{2K^2}{(K-1)^2} = 15,173\ldots.$$

Valitaan nyt luvuksi u jotain tätä suurempaa, sanotaan $u = 16$. Voidaan osoittaa, että jos $\epsilon > 0$, niin

$$X^{\log\log X \log\log\log X/\log X} \leq X^{\epsilon}$$

kaikilla riittävän suurilla X. Näin ollen riittävän suurilla X kaikille tuloille $d_1 \cdots d_{R+1}$ pätee

$$d_1 \cdots d_{R+1} \leq X^{15,2/16}.$$

Lisäksi funktion ν multiplikatiivisuudesta, huomiosta, että $\nu(p) \leq 2$ kaikilla alkuluvuilla $p \leq N$, ja Esimerkistä 1.20 seuraa, että kaikilla d, jotka jakavat luvun $P(z)$, pätee

$$|r(d)| \leq \nu(d) = \prod_{p \,|\, d} \nu(p) \leq 2^{\omega(d)} \leq \tau(d).$$

Koska joukot $\mathcal{P}_j$ ovat pareittain erillisiä alkuluvuista koostuvia joukkoja ja luonnollisen luvun alkutekijähajotelma on tekijöiden järjestystä vaille yksikäsitteinen, niin jokainen luonnollinen luku voidaan esittää muodossa $d_1 \cdots d_{R+1}$ korkeintaan yhdellä tavalla. Näin ollen summaa (4.10) rajoittaa ylhäältä

$$\sum_{n \leq X^{15,2/16}} \tau(n) = \sum_{n \leq X^{15,2/16}} \sum_{c \,|\, n} 1 \leq X^{15,2/16} \sum_{c \leq X^{15,2/16}} \frac{1}{c} \ll X^{15,2/16} \log X,$$

missä jälkimmäisin vaihe seuraa siitä, että summa

$$\sum_{n \leq x} \frac{1}{n}$$

on asymptoottinen funktion $\log x$ kanssa (ks. [**1**, s. 55]). Lisäksi, koska $\log X \ll X^{\epsilon}$ kaikilla $\epsilon > 0$, niin saatiin arvioitua virhetermiä kuten haluttiin.

Nyt siis Brunin seulan ja edellä tehtyjen arvioiden nojalla on saatu näytettyä, että kaikilla suurilla X pätee

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, X^{1/16}) &\ll X \prod_{p \leq X^{\frac{1}{16}}} (1 - \alpha(p)) \\ &= X \prod_{\substack{p \leq X^{\frac{1}{16}} \\ p \nmid N}} \left(1 - \frac{2}{p}\right) \prod_{\substack{p \leq X^{\frac{1}{16}} \\ p \,|\, N}} \left(1 - \frac{1}{p}\right), \end{aligned}$$

missä yhtäsuuruus seuraa huomiosta (4.4). Edelleen huomion

$$\left(1 - \frac{2}{p}\right) \leq \left(1 - \frac{1}{p}\right)^2$$

ja Mertensin toisen lauseen (Lause 2.4) avulla saadaan

$$\begin{aligned} S(\mathcal{A},\mathcal{P},X^{1/16}) &\ll X \prod_{\substack{p\le X^{\frac{1}{16}}\\ p\nmid N}}\left(1-\frac{1}{p}\right)^2 \prod_{\substack{p\le X^{\frac{1}{16}}\\ p\mid N}}\left(1-\frac{1}{p}\right) \\ &= X \prod_{p\le X^{\frac{1}{16}}}\left(1-\frac{1}{p}\right)^2 \prod_{\substack{p\le X^{\frac{1}{16}}\\ p\mid N}}\left(1-\frac{1}{p}\right)^{-1} \\ &\ll \frac{X}{(\log X)^2}\prod_{p\mid N}\left(1-\frac{1}{p}\right)^{-1}. \end{aligned}$$

Hyödyntämällä nyt Eulerin tuloa (Lause 1.12) huomataan, että

$$\begin{aligned} \prod_{p\mid N}\left(1-\frac{1}{p}\right)^{-1} \Big/ \prod_{p\mid N}\left(1+\frac{1}{p}\right) &= \prod_{p\mid N}\left(1-\frac{1}{p^2}\right)^{-1} \\ &\le \prod_{p\in\mathcal{P}}\left(1-\frac{1}{p^2}\right)^{-1} = \sum_{n=1}^{\infty}\frac{1}{n^2} < \infty, \end{aligned}$$

sillä ylärajaksi saatu sarja on yliharmoninen ja siten suppenee. Näin ollen suurilla X pätee

$$S(\mathcal{A},\mathcal{P},X^{1/16}) \ll \frac{X}{(\log X)^2}\prod_{p\mid N}\left(1+\frac{1}{p}\right).$$

Kun nyt yhdistetään tämä alussa tehtyyn huomioon (4.1), saadaan, että kaikilla suurilla positiivilla parillisilla luvuilla N pätee

$$\begin{aligned} R(N) &\le S(\mathcal{A},\mathcal{P},X^{1/16}) + 2X^{1/16} \\ &\ll \frac{X}{(\log X)^2}\prod_{p\mid N}\left(1+\frac{1}{p}\right) = \frac{N}{(\log N)^2}\prod_{p\mid N}\left(1+\frac{1}{p}\right). \end{aligned}$$

Saatiin siis osoitettua lemman väite riittävän suurille N. Rajoitetuille N väite on triviaali. □

Seuraava tulos antaa alarajan summalle $\sum R(N)$.

LEMMA 4.2. *Kun $x\to\infty$, niin*

$$\sum_{N\le x} R(N) \gg \frac{x^2}{(\log x)^2}.$$

TODISTUS. Hyödynnetään väitteen todistamiseen Chebyshevin estimaattia (Lause 1.30), jonka mukaan siis pätee

$$\pi(x) \gg \frac{x}{\log x}, \quad \text{kun } x\to\infty.$$

Tämän avulla saadaan

$$\sum_{N\le x} R(N) = \sum_{N\le x}\sum_{p_1+p_2=N} 1 = \sum_{p_1+p_2\le x} 1 \ge \left(\sum_{p\le x/2} 1\right)^2$$
$$= (\pi(x/2))^2 \gg \left(\frac{x/2}{\log x/2}\right)^2 \gg \frac{x^2}{(\log x)^2}.$$

□

Osoitetaan lopuksi vielä kolmas tulos lukuun $R(N)$ liittyen. Se antaa ylärajan summalle $\sum R(N)^2$.

LEMMA 4.3. *Kun $x \to \infty$, niin*

$$\sum_{N\le x} R(N)^2 \ll \frac{x^3}{(\log x)^4}.$$

TODISTUS. Tehdään aluksi eräs todistuksessa tarvittava huomio. Olkoon $N \in \mathbb{N}$ ja

$$N = p_1^{a_1} p_2^{a_2} \cdots p_r^{a_r}$$

luvun N alkutekijähajotelma. Olkoon lisäksi N' luvun N erillisten alkutekijöiden tulo eli

$$N' = p_1 p_2 \cdots p_r.$$

Tällöin

$$\prod_{p\,|\,N}\left(1+\frac{1}{p}\right) = \left(1+\frac{1}{p_1}\right)\left(1+\frac{1}{p_2}\right)\cdots\left(1+\frac{1}{p_r}\right) = \sum_{d\,|\,N'}\frac{1}{d} \le \sum_{d\,|\,N}\frac{1}{d}.$$

Hyödyntämällä nyt tätä huomiota sekä Lemman 4.1 antamaa ylärajaa luvulle $R(N)$ saadaan

$$\sum_{N\le x} R(N)^2 \ll \sum_{2\le N\le x}\left(\frac{N}{(\log N)^2}\prod_{p\,|\,N}\left(1+\frac{1}{p}\right)\right)^2$$
$$\ll \frac{x^2}{(\log x)^4}\sum_{2\le N\le x}\left(\prod_{p\,|\,N}\left(1+\frac{1}{p}\right)\right)^2$$
$$\ll \frac{x^2}{(\log x)^4}\sum_{2\le N\le x}\left(\sum_{d\,|\,N}\frac{1}{d}\right)^2.$$

Täytyy siis näyttää vielä, että

$$\sum_{2\le N\le x}\left(\sum_{d\,|\,N}\frac{1}{d}\right)^2 \ll x.$$

Tätä varten huomataan, että kaikille luonnollisille luvuille d_1 ja d_2 pätee

$$\mathrm{pyj}(d_1,d_2) \ge \max\{d_1,d_2\} \ge (d_1 d_2)^{1/2}.$$

Nyt

$$\sum_{N\le x}\left(\sum_{d\,|\,N}\frac{1}{d}\right)^2 = \sum_{N\le x}\sum_{d_1|\,N}\sum_{d_2\,|\,N}\frac{1}{d_1d_2} = \sum_{d_1,\,d_2\le x}\frac{1}{d_1d_2}\sum_{\substack{N\le x\\ d_1|\,N,\,d_2\,|\,N}} 1$$

$$\le \sum_{d_1,\,d_2\le x}\frac{1}{d_1d_2}\frac{x}{\operatorname{pyj}(d_1,d_2)} \le x\sum_{d_1,\,d_2\le x}\frac{1}{(d_1d_2)^{\frac{3}{2}}} \le x\left(\sum_{d=1}^{\infty} d^{-\frac{3}{2}}\right)^2 \ll x.$$

Tässä ylärajaan saatu sarja on yliharmoninen ja siten suppenee. Näin saatiin siis haluttu väite todistettua. □

LUKU 5

Schnirelmannin lause

Tässä luvussa tutustutaan Schnirelmannin lauseeseen. Aluksi tarkastellaan Schnirelmannin tiheyden käsitettä ja käydään läpi tarvittavia aputuloksia, minkä jälkeen esitetään todistus Schnirelmannin lauseelle. Luvun pääasiallisina lähteinä on käytetty Alina C. Cojocarun ja M. Ram Murtyn teosta *An Introduction to Sieve Methods and their Applications* [**2**], A. Y. Khinchinin teosta *Three Pearls of Number Theory* [**5**] ja Paul Pollackin teosta *Not Always Buried deep: A Second Course in Elementary Number Theory* [**9**].

5.1. Schnirelmannin tiheys

Tutustutaan ensin tärkeään määritelmään, *Schnirelmannin tiheyteen*, joka on kätevä tapa mitata luonnollisten lukujen osajoukon kokoa.

MÄÄRITELMÄ 5.1. Joukon $\mathcal{A} \subset \mathbb{N}_0$ *Schnirelmannin tiheys* $\sigma(\mathcal{A})$ on

$$\sigma(\mathcal{A}) := \inf_{n \in \mathbb{N}} \frac{A(n)}{n},$$

missä $A(n) = \#\{a \in \mathcal{A} : 1 \leq a \leq n\}$.

Yllä merkinnällä $A(n)$ tarkoitetaan siis joukon $\mathcal{A}$ niiden alkioiden lukumäärää, jotka eivät ylitä lukua n (nollaa ei lasketa mukaan). Koska $0 \leq A(n) \leq n$, niin Schnirelmannin tiheydelle pätee $0 \leq \sigma(\mathcal{A}) \leq 1$. Toisin kuin luonnollisen tiheyden,

$$d(\mathcal{A}) := \lim_{n \to \infty} \frac{A(n)}{n},$$

tapauksessa, Schnirelmannin tiheyteen vaikuttaa merkittävästi se, sisältääkö tarkasteltava joukko pieniä lukuja vai ei. Esimerkiksi, jos $1 \notin \mathcal{A}$, niin $A(1) = 0$ ja siten $\sigma(\mathcal{A}) = 0$. Jos joukko $\mathcal{A}$ sisältää kaikki luonnolliset luvut, niin $A(n) = n$ kaikilla $n \in \mathbb{N}$ ja siten $\sigma(\mathcal{A}) = 1$. Jos taas $n \notin \mathcal{A}$ jollain $n \in \mathbb{N}$, niin tällöin $A(n) \leq n - 1$ ja

$$\sigma(\mathcal{A}) \leq \frac{A(n)}{n} \leq \frac{n-1}{n} = 1 - \frac{1}{n} < 1.$$

Näin ollen joukon $\mathcal{A}$ Schnirelmannin tiheys on 1, jos ja vain jos $\mathcal{A}$ sisältää kaikki luonnolliset luvut.

ESIMERKKI 5.2. Esimerkkejä Schnirelmannin tiheydestä:

(a) Kaikille joukoille $\mathcal{A}$, jotka ovat muotoa $\mathcal{A} = \{1 + r(n-1) : n \in \mathbb{N}\}, r \in \mathbb{N}$, pätee $\sigma(\mathcal{A}) = 1/r$.

(b) Kaikille joukoille $\mathcal{B}$, jotka ovat muotoa $\mathcal{B} = \{bq^{n-1} : n \in \mathbb{N}\}, b, q \in \mathbb{N}$, pätee $\sigma(\mathcal{B}) = 0$.

(c) Jos $\sigma(\mathcal{C}) = 0$ ja $1 \in \mathcal{C}$, niin kaikilla $\epsilon > 0$ on olemassa luku m siten, että $C(m)/m < \epsilon$.

Muistutellaan seuraavaksi mieleen *summajoukon* määritelmä, joka on keskeinen Schnirelmannin lauseen käsittelyssä.

MÄÄRITELMÄ 5.3. Joukkojen $\mathcal{A}, \mathcal{B} \subset \mathbb{N}_0$ summa $\mathcal{A} + \mathcal{B}$ on joukko

$$\mathcal{A} + \mathcal{B} = \{a + b : a \in \mathcal{A},\, b \in \mathcal{B}\}.$$

Lisäksi, jos $h \in \mathbb{N}$, niin asetetaan

$$h\mathcal{A} = \overbrace{\mathcal{A} + \cdots + \mathcal{A}}^{h \text{ kpl}}.$$

Joukon $\mathcal{A}$ sanotaan olevan *kertaluvun h kanta* joukolle $\mathbb{N}_0$, jos joukko $h\mathcal{A}$ sisältää kaikki epänegatiiviset kokonaisluvut, toisin sanoen jos jokainen epänegatiivinen kokonaisluku voidaan esittää sellaisena joukon $\mathcal{A}$ alkioiden summana, jossa summattavia on h kappaletta. Schnirelmann huomasi, että joukko, jonka Schnirelmannin tiheys on positiivinen, on jonkin kertaluvun kanta joukolle $\mathbb{N}_0$. Jotta tämä voidaan osoittaa, tarkastellaan ensin hieman lisää Schnirelmannin tiheyden ominaisuuksia.

Seuraava tulos antaa työkalun, jonka avulla voidaan arvioida summajoukon Schnirelmannin tiheyttä. Lemman todistus mukailee Khinchinin [**5**, s. 22–23] teoksessaan esittämää todistusta.

LEMMA 5.4. *Olkoot $\mathcal{A}, \mathcal{B} \subset \mathbb{N}_0$ sellaisia, että $0 \in \mathcal{A}$ ja $0 \in \mathcal{B}$. Tällöin*

$$\sigma(\mathcal{A} + \mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\,\sigma(\mathcal{B}).$$

TODISTUS. Olkoon $n \in \mathbb{N}$. Kuten Schnirelmannin tiheyden määritelmässä, käytetään merkintää $A(n)$ ilmaisemaan joukon $\mathcal{A}$ niiden nollasta eroavien alkioiden lukumäärän, jotka ovat pienempiä tai yhtäsuuria kuin n, siis

$$A(n) = \#\{a \in \mathcal{A} : 1 \leq a \leq n\}.$$

Käytetään merkintöjä $B(n)$ ja $(A + B)(n)$ ilmaisemaan vastaavia lukuja joukoille $\mathcal{B}$ ja $\mathcal{A} + \mathcal{B}$.

Joukossa $\mathcal{A} \cap [1, n]$ on $A(n)$ kappaletta alkioita. Olkoon

$$0 < a_1 < a_2 < \cdots < a_{A(n)} \leq n$$

näiden alkioiden luettelo. Koska $0 \in \mathcal{B}$, niin kyseiset alkiot sisältyvät myös joukkoon $\mathcal{A} + \mathcal{B}$. Olkoot nyt a_k ja a_{k+1} kaksi peräkkäistä alkiota joukosta $\mathcal{A} \cap [1, n]$. Näiden välissä on $a_{k+1} - a_k - 1 = l$ kappaletta luonnollisia lukuja, jotka eivät kuulu joukkoon $\mathcal{A}$. Nämä ovat luvut

$$a_k + 1,\, a_k + 2, \ldots,\, a_k + l = a_{k+1} - 1.$$

Osa näistä luvuista kuuluu joukkoon $\mathcal{A} + \mathcal{B}$, erityisesti ne, jotka ovat muotoa $a_k + r$, missä $r \in \mathcal{B}$. Kyseistä muotoa olevia lukuja on yhtä paljon kuin joukossa $\mathcal{B} \cap [1, l]$ on alkioita, siis $B(l)$ kappaletta. Näin ollen joukon $\mathcal{A}$ kahden peräkkäisen alkion välissä on vähintään $B(l)$ kappaletta luonnollisia lukuja, jotka sisältyvät joukkoon $\mathcal{A} + \mathcal{B}$. Tästä seuraa, että

$$(A + B)(n) \geq A(n) + \Sigma B(l),$$

missä summataan yli kaikkien joukon $\mathcal{A}$ peräkkäisten alkioiden välien. Schnirelmannin tiheyden määritelmän mukaan $B(l) \geq \sigma(\mathcal{B})l$, joten

$$(A+B)(n) \geq A(n) + \sigma(\mathcal{B})\Sigma\, l.$$

Tässä $\Sigma\, l$ kertoo niiden lukua n pienempien tai yhtäsuurten luonnollisten lukujen lukumäärän, jotka eivät kuulu joukkoon $\mathcal{A}$. Siis $\Sigma\, l = n - A(n)$. Näin ollen saadaan

$$(A+B)(n) \geq A(n) + \sigma(\mathcal{B})\big(n - A(n)\big) = A(n)\big(1 - \sigma(\mathcal{B})\big) + \sigma(\mathcal{B})n.$$

Jälleen Schnirelmannin tiheyden määritelmän mukaan $A(n) \geq \sigma(\mathcal{A})n$, joten

$$(A+B)(n) \geq \sigma(\mathcal{A})n\big(1 - \sigma(\mathcal{B})\big) + \sigma(\mathcal{B})n.$$

Tästä seuraa, että

$$\frac{(A+B)(n)}{n} \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\,\sigma(\mathcal{B}).$$

Koska n oli mielivaltainen luonnollinen luku, niin pätee

$$\sigma(\mathcal{A}+\mathcal{B}) \geq \sigma(\mathcal{A}) + \sigma(\mathcal{B}) - \sigma(\mathcal{A})\,\sigma(\mathcal{B}).$$

□

Esimerkki 5.5. Olkoon $r \geq 1$ ja olkoot $\mathcal{A}_1, \ldots, \mathcal{A}_r \subset \mathbb{N}_0$ sellaisia, että $0 \in \mathcal{A}_i$ kaikilla $i = 1, \ldots, r$. Osoitetaan induktiolla, että

$$\sigma(\mathcal{A}_1 + \cdots + \mathcal{A}_r) \geq 1 - \prod_{i=1}^{r}(1 - \sigma(\mathcal{A}_i)).$$

Ratkaisu. Kun $r = 1$, niin väite on selvä. Lisäksi edellisen lemman nojalla pätee

$$\sigma(\mathcal{A}_1 + \mathcal{A}_2) \geq \sigma(\mathcal{A}_1) + \sigma(\mathcal{A}_2) - \sigma(\mathcal{A}_1)\,\sigma(\mathcal{A}_2),$$

mikä voidaan kirjoittaa myös muodossa

$$\sigma(\mathcal{A}_1 + \mathcal{A}_2) \geq 1 - (1 - \sigma(\mathcal{A}_1))(1 - \sigma(\mathcal{A}_2)).$$

Siispä väite pätee myös, kun $r = 2$. Tehdään sitten induktio-oletus eli oletetaan, että väite pätee, kun $r = k$. Merkitään $\mathcal{B} = \mathcal{A}_1 + \cdots + \mathcal{A}_k$, jolloin induktio-oletuksen mukaan

$$\sigma(\mathcal{B}) = \sigma(\mathcal{A}_1 + \cdots + \mathcal{A}_k) \geq 1 - \prod_{i=1}^{k}(1 - \sigma(\mathcal{A}_i)).$$

Nyt

$$\begin{aligned}
\sigma(\mathcal{A}_1 + \cdots + \mathcal{A}_{k+1}) &= \sigma(\mathcal{B} + \mathcal{A}_{k+1}) \\
&\geq 1 - (1 - \sigma(\mathcal{B}))(1 - \sigma(\mathcal{A}_{k+1})) \\
&\geq 1 - \left[\prod_{i=1}^{k}(1 - \sigma(\mathcal{A}_i))\right](1 - \sigma(\mathcal{A}_{k+1})) \\
&= 1 - \prod_{i=1}^{k+1}(1 - \sigma(\mathcal{A}_i)),
\end{aligned}$$

eli väite pätee myös, kun $r = k + 1$. Näin ollen induktioperiaatteen nojalla väite on todistettu. □

HUOMAUTUS 5.6. Vuonna 1942 matemaatikko Henry Mann esitti julkaisussaan [**6**] summan tiheydelle vielä tarkemman arvion, jonka mukaan

$$\sigma(\mathcal{A}+\mathcal{B}) \geq \min\{1, \sigma(\mathcal{A})+\sigma(\mathcal{B})\}.$$

Tällä tuloksella voisi ohittaa seuraavaksi esiteltävän lemman käytön.

5.2. Schnirelmannin lause

Ennen Schnirelmannin lauseen todistusta käydään läpi vielä pari tarvittavaa aputulosta. Seuraavan lemman todistus mukailee Pollackin [**9**, s. 197] teoksessaan esittämää todistusta. Jälkimmäiselle tulokselle esitetty todistus puolestaan pohjautuu Cojocarun ja Murtyn teokseen [**2**, s. 102].

LEMMA 5.7. *Olkoot $\mathcal{A}, \mathcal{B} \subset \mathbb{N}_0$ sellaisia, että $0 \in \mathcal{A}$, $0 \in \mathcal{B}$ ja $\sigma(\mathcal{A})+\sigma(\mathcal{B}) \geq 1$. Tällöin $\mathcal{A}+\mathcal{B} = \mathbb{N}_0$. Erityisesti, jos $\sigma(\mathcal{A}) \geq \frac{1}{2}$, niin $2\mathcal{A} = \mathbb{N}_0$.*

TODISTUS. Koska $\mathcal{A}, \mathcal{B} \subset \mathbb{N}_0$, niin myös $\mathcal{A}+\mathcal{B} \subset \mathbb{N}_0$. Näytetään, että jokainen einegatiivinen kokonaisluku kuuluu summajoukkoon $\mathcal{A}+\mathcal{B}$. Olkoon siis $n \in \mathbb{N}_0$. Olkoon lisäksi

$$0 = a_0 < a_1 < a_2 < \cdots$$

joukon $\mathcal{A}$ alkioiden luettelo ja

$$0 = b_0 < b_1 < b_2 < \cdots$$

joukon $\mathcal{B}$ alkioiden luettelo. Tarkastellaan seuraavaa listaa, jossa kaikki luvut ovat kokonaislukuja väliltä $[0, n]$:

$$0 = a_0,\ a_1, \ldots,\ a_{A(n)},\ n = n-b_0,\ n-b_1, \ldots,\ n-b_{B(n)}.$$

Tässä listassa on yhteensä $(A(n)+1)+(B(n)+1)$ kappaletta lukuja. Nyt Schnirelmannin tiheyden määritelmän ja oletuksen nojalla pätee

$$(A(n)+1)+(B(n)+1) \geq \sigma(\mathcal{A})n + \sigma(\mathcal{B})n + 2 \geq n+2 > n+1.$$

Kuitenkin, välillä $[0, n]$ on ainoastaan $n+1$ kokonaislukua. Näin ollen täytyy olla $a_i = n - b_j$ joillakin i ja j, missä $0 \leq i \leq A(n)$ ja $0 \leq j \leq B(n)$. Mutta tällöin $n = a_i + b_j \in \mathcal{A}+\mathcal{B}$. Siispä $\mathbb{N}_0 \subset \mathcal{A}+\mathcal{B}$, ja näin ollen $\mathcal{A}+\mathcal{B} = \mathbb{N}_0$. □

LAUSE 5.8. *Olkoon $\mathcal{A} \subset \mathbb{N}_0$ sellainen, että $0 \in \mathcal{A}$ ja $\sigma(\mathcal{A}) > 0$. Tällöin $m\mathcal{A} = \mathbb{N}_0$ jollakin $m \in \mathbb{N}$, eli joukko $\mathcal{A}$ on kertaluvun m kanta joukolle $\mathbb{N}_0$.*

TODISTUS. Esimerkissä 5.5 osoitettiin, että kaikilla $k \in \mathbb{N}$ pätee

$$\sigma(k\mathcal{A}) \geq 1 - (1-\sigma(\mathcal{A}))^k.$$

Koska $\sigma(\mathcal{A}) > 0$, niin $1-\sigma(\mathcal{A}) < 1$. Voidaan siis valita riittävän suuri k siten, että

$$(1-\sigma(\mathcal{A}))^k \leq \frac{1}{2}.$$

Tällöin

$$\sigma(k\mathcal{A}) \geq \frac{1}{2},$$

joten edellisen lemman nojalla $2k\mathcal{A} = \mathbb{N}_0$. Näin ollen väite pätee, kun $m = 2k$. □

Nyt ollaan viimein valmiita todistamaan Schnirelmannin lause. Tässä esitetty todistus pohjautuu Pollackin teokseen [**9**, s. 199–201].

LAUSE 5.9. (Schnirelmannin lause) *On olemassa luku S siten, että jokainen luonnollinen luku $n > 1$ voidaan esittää alkulukujen summana, jossa summattavia on korkeintaan S kappaletta.*

TODISTUS. Tehdään aluksi huomio, johon palataan todistuksessa myöhemmin: mikäli joukolla $\mathcal{A} \subset \mathbb{N}_0$ on positiivinen alatiheys eli

$$\liminf_{x\to\infty} \frac{A(x)}{x} > 0, \tag{5.1}$$

niin tällöin joukon $\mathcal{B} = \mathcal{A} \cup \{0, 1\}$ Schnirelmannin tiheys on positiivinen. Nimittäin, koska ominaisuudesta (5.1) seuraa, että on olemassa $\sigma_0 > 0$ ja $N_0 \in \mathbb{N}$ siten, että

$$\frac{A(N)}{N} \geq \sigma_0 \quad \text{kaikilla } N \geq N_0,$$

niin joukon $\mathcal{B}$ Schnirelmannin tiheydelle pätee

$$\sigma(\mathcal{B}) \geq \min\left\{\sigma_0, \frac{1}{N_0}\right\} > 0.$$

Koska lisäksi $0 \in \mathcal{B}$, niin Lauseen 5.8 nojalla joukko $\mathcal{B}$ on kertaluvun m kanta joukolle $\mathbb{N}_0$, jollakin $m \in \mathbb{N}$. Tätä huomiota tarvitaan myöhemmin todistuksessa.

Käytetään taas merkintää $R(N)$ ilmaisemaan, kuinka monella eri tavalla luonnollinen luku N voidaan esittää kahden alkuluvun summana, ja asetetaan

$$\mathcal{A} := \{N \in \mathbb{N} : R(N) > 0\}.$$

Nyt luvussa 4 perusteltujen tulosten avulla saadaan joukolle $\mathcal{A}$ osoitettua seuraava ominaisuus:

LAUSE 5.10. *Joukolla $\mathcal{A}$ on positiivinen alatiheys.*

TODISTUS. Kirjoitetaan $R(N) = R(N) \cdot 1$, jolloin Cauchy-Schwarzin epäyhtälön (Lause 1.31) sekä Lemmojen 4.2 ja 4.3 avulla saadaan

$$\begin{aligned}\frac{x^4}{(\log x)^4} \ll \left(\sum_{N\leq x} R(N)\right)^2 &= \left(\sum_{\substack{N\leq x\\ R(N)>0}} R(N)\cdot 1\right)^2 \\ &\leq \sum_{\substack{N\leq x\\ R(N)>0}} R(N)^2 \sum_{\substack{N\leq x\\ R(N)>0}} 1 \ll \frac{x^3}{(\log x)^4} A(x).\end{aligned}$$

Näin ollen $x \ll A(x)$, kun $x \to \infty$, eli toisin sanoen joukolla $\mathcal{A}$ on positiivinen alatiheys. □

Asetetaan nyt $\mathcal{B} := \mathcal{A} \cup \{0, 1\}$. Tällöin, kuten alussa huomattiin, joukko $\mathcal{B}$ on joukon $\mathbb{N}_0$ kertaluvun m kanta jollakin $m \in \mathbb{N}$. Näin ollen kaikilla luonnollisilla luvuilla $n \geq 2$ voidaan kirjoittaa

$$n - 2 = p_1 + p_2 + \cdots + p_{2k} + \overbrace{1 + 1 + \cdots + 1}^{l \text{ kpl}},$$

missä luvut p_i ovat alkulukuja, k ja l ovat ei-negatiivisia kokonaislukuja ja $k+l \leq m$. Siis

$$n = p_1 + \cdots + p_{2k} + (l+2).$$

Koska $l+2 \geq 2$, niin luku $l+2$ voidaan kirjoittaa summana kakkosista ja kolmosista, missä summattavia on korkeintaan

$$\frac{l+2}{2} = \frac{l}{2} + 1 \leq \frac{m}{2} + 1$$

kappaletta. Näin ollen jokainen luonnollinen luku $n \geq 2$ voidaan kirjoittaa alkulukujen summana, jossa summattavia on korkeintaan

$$2k + \frac{m}{2} + 1 \leq 2m + \frac{m}{2} + 1 = \frac{5m}{2} + 1$$

kappaletta. Valitaan siis $S = 5m/2 + 1$, ja Schnirelmannin lause seuraa. □

Kirjallisuutta

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

[2] Alina Carmen Cojocaru ja M. Ram Murty: *An Introduction to Sieve Methods and their Applications.* Cambridge University Press, 2006.

[3] George Greaves: *Sieves in Number Theory.* Springer-Verlag, Berlin, Heidelberg, New York, 2001.

[4] Heini Halberstam ja Hans-Egon Richert: *Sieve Methods.* London Mathematical Society Monographs, No 4, Academic Press, London, New York, 1974.

[5] A. Y. Khinchin: *Three Pearls of Number Theory.* Graylock Press, Rochester, N.Y., 1956.

[6] Henry B. Mann: A Proof of the Fundamental Theorem on the Density of Sums of Set of Positive Integers. *Annals of Mathematics*, 43 (1942), 523–527. doi:10.2307/1968807

[7] Melvyn B. Nathanson: *Additive Number Theory. The Classical Bases.* Springer-Verlag, New York, 1996.

[8] Melvyn B. Nathanson: *Elementary Methods in Number Theory.* Graduate Texts in Mathematics, Springer-Verlag, New York, Berlin, Heidelberg, 2000.

[9] Paul Pollack: *Not Always Buried Deep: A Second Course in Elementary Number Theory.* American Mathematical Society, 2009.

[10] Ian Stewart: *The Great Mathematical Problems.* Profile Books, 2013.

[11] Heli Tuominen: *Lukuteorian alkeet.* Luentomoniste, Jyväskylän yliopisto, 2009. https://www.jyu.fi/science/fi/maths/opiskelu/yleista-opiskelusta/luentomonisteita/mat0913 (haettu 21.4.2021)