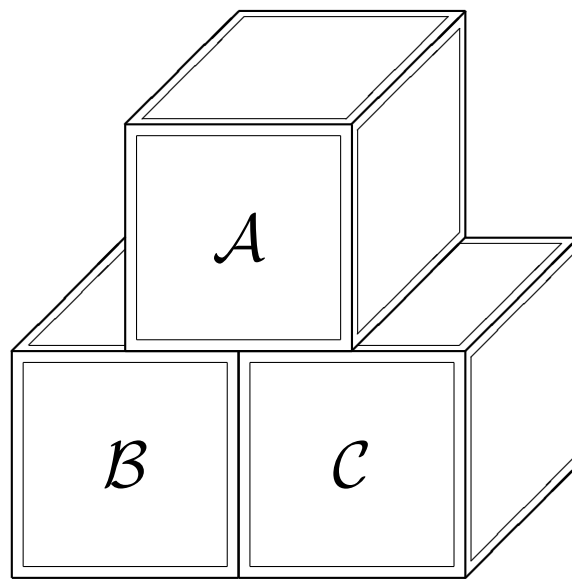


# Abc-konjektuuri



Pro gradu -tutkielma  
Marko Lamminsalo  
180897  
Itä-Suomen yliopisto  
5. maaliskuuta 2014

# Sisältö

<b>1</b>	<b>Johdanto</b>	<b>1</b>
1.1	Merkinnöistä . . . . .	5
<b>2</b>	<b>Peruskäsitteitä</b>	<b>6</b>
2.1	Jaollisuudesta ja kongruensseista . . . . .	6
2.2	Binomilauseen sovelluksia . . . . .	11
2.3	Hiloista . . . . .	14
2.4	Ryhmistä ja niiden välisistä kuvauksista . . . . .	18
2.5	Polynomeista . . . . .	24
2.6	Elliptisistä käyristä . . . . .	26
2.7	Analyysin perustuloksia . . . . .	30
2.8	Alkulukuihin liittyviä tuloksia . . . . .	35
<b>3</b>	<b>Abc-konjektuuri ja siihen liittyviä tuloksia</b>	<b>42</b>
3.1	Abc-kolmikot ja radikaali . . . . .	42
3.2	Abc-konjektuuri . . . . .	45
3.3	Abc-konjektuuriin liittyviä tuloksia . . . . .	51
3.4	$L$ -arvojen joukosta ja sen kasautumispisteistä . . . . .	53
3.5	Abc-konjektuurin efektiivisestä muodosta . . . . .	58
3.6	Abc-osumien lukumäärästä . . . . .	59
3.7	Logaritmisten abc-osumien lukumäärästä . . . . .	67
3.8	Szpiroin konjektuureista . . . . .	72
3.9	Fermat'n suuri lause . . . . .	77
<b>4</b>	<b>Abc-konjektuurin seurauksia</b>	<b>80</b>
4.1	Abc-kolmikiin liittyviä tuloksia . . . . .	80
4.2	Aritmeettisista lukujonoista . . . . .	82
4.3	Luvuista, joilla on samat alkutekijät . . . . .	83
4.4	Catalanin ja Pillain konjektuurit . . . . .	84
4.5	Hallin konjektuuri . . . . .	86
4.6	Fermat-Catalanin konjektuuri . . . . .	88
4.7	Shorey-Tijdemanin konjektuuri . . . . .	89
4.8	Erdős-Stewartin konjektuuri . . . . .	90
4.9	Erdős-Woodsin konjektuuri arvolla $k = 3$ . . . . .	91
4.10	Richardin konjektuuri . . . . .	92
4.11	Brocard-Ramanujan yhtälö $n! + 1 = m^2$ . . . . .	93
4.12	Simmonsin yhtälö $n! = m(m^2 - 1)$ . . . . .	94
4.13	Gandhin yhtälö $x^n + y^n = n!z^n$ . . . . .	95
4.14	Voimakkaista luvuista . . . . .	97
4.15	Wieferichin alkuluvuista . . . . .	100
4.16	Edgarin ja Shorey-Tijdemanin probleema . . . . .	102
4.17	Goormaghtighin ja Batemanin ongelma . . . . .	103
4.18	Croftin ongelma . . . . .	104
4.19	Muita seurauksia . . . . .	105

<b>5</b>	<b>Abc-konjektuurin yleistyksiä</b>	<b>107</b>
5.1	Abc-konjektuurin kongruenssiversio . . . . .	107
5.2	$n$ -konjektuuri . . . . .	112
5.3	Stothers-Masonin lause . . . . .	116
5.4	Yleistys meromorffifunktioille . . . . .	119
<b>6</b>	<b>Yhteenveto</b>	<b>123</b>
	<b>Viitteet</b>	<b>124</b>
<b>A</b>	<b>50 laadultaan parasta <math>abc</math>-kolmikkoa</b>	<b>129</b>
<b>B</b>	<b>50 laadultaan parasta <math>abc</math>-Szpiro-kolmikkoa</b>	<b>131</b>
<b>C</b>	<b>Abc-osumien lukumäärä</b>	<b>133</b>
<b>D</b>	<b>31 ensimmäistä <math>abc</math>-osumaa</b>	<b>134</b>
<b>E</b>	<b>31 ensimmäistä logaritmista <math>abc</math>-osumaa</b>	<b>135</b>
<b>F</b>	<b>Java-koodi logaritmisten <math>abc</math>-osumien etsimiseen</b>	<b>136</b>

## Taulukot

1	Maplella laskettuja luvun $7^{2^n} - 1$ kanonisia esityksiä. . . . .	46
2	Viisi suurimman $L$ -arvon antavaa $abc$ -kolmikkoa. . . . .	50
3	Kolmikot $(a, b, c) \in \mathbb{N}^3$ , joille $a + b = c$ , $\text{syt}(a, b, c) = 1$ ja $a \leq b < c < 10$ . . .	59
4	Logaritmistien ja tavallisten $abc$ -osumien lukumääräfunktioiden arvoja. . . . .	68

## Kuvat

1	Konveksin joukon $V$ sisään jäävä osa eräästä avaruuden $\mathbb{R}^2$ hilasta. . . . .	17
2	Elliptinen käyrä ja kaksi singulaarista käyrää. . . . .	27
3	$abc$ -osumien lukumääräfunktio $N(X)$ ja alarajafunktio $\exp((\log X)^{\frac{1}{2}})$ . . . . .	66
4	$abc$ -osumien lukumääräfunktio $N(X)$ ja sitä rajoittavia funktioita. . . . .	66
5	Logaritmistien $abc$ -osumien lukumääräfunktio $N_{\log}(X)$ ja sitä rajoittavia funktioita. . . . .	71
6	Eri konjektuurien välisiä implikaatioita. . . . .	79

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos ejusdem nominis fas est dividere: cujus rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

– Pierre Fermat <sup>1</sup>

---

<sup>1</sup>Fermat'n alkuperäinen huomautus Diophantoksen Aritmetican marginaalissa [70]

# 1 Johdanto

Lukuteorialle tyypillisiä ovat ongelmat, jotka ovat helposti esittävässä mutta vaikeasti ratkaistavissa. Ongelmista kaikkein kuuluisin lienee edellisellä sivullakin esitetty 1600-luvulta [16, s. 2] peräisin oleva Fermat'n suuri lause, joka modernimmin voidaan ilmaista seuraavasti: yhtälöllä

$$x^n + y^n = z^n \tag{1.1}$$

ei ole ratkaisua nollassa eroavilla kokonaisluvuilla  $x, y, z$  ja  $n \geq 3$ . Fermat ei kuitenkaan esittänyt väittämälleen todistusta, koska se "ei mahtunut kirjan marginaaliin". Helpon näköinen ratkaisematon ongelma innosti monia nimekkäitäkin matemaatikkoita (mm. Euler, Dirichlet ja Cauchy) sekä uuden lukuteorian kehitystä [16], kunnes viimein vuonna 1995 väitteelle lopullisen, varsin epätriviaalin, todistuksen esitti Andrew Wiles [70]. Eräs Fermat'n suuren lauseen todistamiseksi tarkoitettu propositio on tämän tutkielman aiheena oleva *Abc*-konjektuuri [4, s. 442].

Joseph Oesterlén ja David Masserin vuonna 1985 formuloiman *Abc*-konjektuurin suuria innoittajia ovat mm. Szpiron vuonna 1983 elliptisille käyrille esittämä heikko konjektuuri [49, s. 167] sekä Stothersin (1981) ja Masonin (1983) todistama polynomilause [37, s. 165–170]. Molemmissa väittämissä oleellisena asiana on yhteys alkioiden yhteenlaskun ja kertolaskun välillä. Szpiron heikon konjektuurin mukaan on olemassa reaaliluvut  $\alpha > 0$  ja  $\beta > 0$  siten, että jokaiselle puolivakaalle rationaaliselle elliptiselle käyrälle  $E$  pätee epäyhtälö

$$|\Delta| \leq \alpha N_E^\beta, \tag{1.2}$$

missä  $\Delta$  on käyrän  $E$  minimaalidiskriminantti ja  $N_E = \text{rad}(\Delta)$  johtaja. Tarkastelussa ovat siis kahden muuttujan polynomifunktion  $f$ ,  $f(x, y) = 0$ , muodostamat ei-singulaariset eli itseään leikkaamattomat ja sileät käyrät. Varsinainen yhteys yhteenlaskun ja kertolaskun kanssa käy selkeämmin ilmi ns. Freyn käyriä käsittelevästä Lemmasta 2.6.13 sekä alaluvusta 3.8. Stothers-Masonin lauseessa puolestaan tarkastellaan kolmea keskenään jaotonta kompleksikertoimista polynomia  $f, g$  ja  $h$ , joista ainakin yksi on vakiosta poikkeava ja jotka toteuttavat yhtälön  $f + g = h$ . Polynomien asteille on tällöin voimassa epäyhtälö

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq n_0(fgh) - 1, \tag{1.3}$$

missä  $n_0(fgh)$  ilmoittaa tulopolynomien  $fgh$  eri nollakohtien lukumäärän. Lausetta tarkastellaan lähemmin alaluvussa 5.3. Varsinainen kokonaislukuja koskeva *Abc*-konjektuuri ei siis ole irrallinen väittäjä vaan tiiviisti yhteydessä Diophantoksen yhtälöihin, elliptisiin käyriin sekä polynomeihin.

*Abc*-konjektuurilla on tarkastelutyylistä riippuen useita formulaatioita, joista seuraavassa esitetään viisi. Alkuperäinen formulaatio on seuraavan muotoinen [37, s. 171]: Jokaista lukua  $\varepsilon > 0$  kohti on olemassa luku  $C(\varepsilon) > 0$  siten, että kaikilla nollassa eroavilla suhteellisilla alkuluvuilla  $a, b$  ja  $c$ , joilla pätee  $a + b = c$ , on voimassa epäyhtälö

$$\max\{|a|, |b|, |c|\} \leq C(\varepsilon) \text{rad}(abc)^{1+\varepsilon}, \tag{1.4}$$

missä  $\text{rad}(abc)$  on tulon  $abc$  alkutekijöiden tulo. Tavallisesti määritellään konjektuurin oletukset toteuttavat luvut  $a, b, c$  siten, että  $0 < a < b < c$ , jolloin puhutaan *abc-summasta* tai *abc-kolmikosta*  $(a, b, c)$ . Näin ollen epäyhtälö (1.4) sievenee muotoon

$$c \leq C(\varepsilon) \text{rad}(abc)^{1+\varepsilon}. \quad (1.5)$$

Ekvivalentisti *Abc*-konjektuuri voidaan esittää myös seuraavasti: Jokaista lukua  $\varepsilon > 0$  kohti on olemassa korkeintaan äärellinen määrä *abc*-kolmikoita  $(a, b, c)$  siten, että on voimassa epäyhtälö

$$c > \text{rad}(abc)^{1+\varepsilon}. \quad (1.6)$$

Kolmas ekvivalentti tapa esittää *Abc*-konjektuuri perustuu ns. *L-arvoon*, joka määritellään *abc*-kolmikoiden  $(a, b, c)$  avulla asettamalla  $c = \text{rad}(abc)^{L(a,b,c)}$ , toisin sanoen

$$L(a, b, c) = \frac{\log c}{\log \text{rad}(abc)}. \quad (1.7)$$

Tällöin konjektuuri saa muodon: Jokaista  $\varepsilon > 0$  kohden on olemassa luku  $C(\varepsilon) > 0$  sitten, että kaikilla *abc*-kolmikoilla  $(a, b, c)$  on voimassa epäyhtälö

$$L(a, b, c) \leq 1 + \varepsilon + \frac{\log(C(\varepsilon))}{\log \text{rad}(abc)}. \quad (1.8)$$

Sama voidaan esittää myös seuraavasti: Jokaista reaalilukua  $\varepsilon > 0$  kohden on olemassa korkeintaan äärellisen monta *abc*-kolmikkoa  $(a, b, c) \in \mathbb{N}^3$ , joiden *L*-arvolle pätee

$$L(a, b, c) > 1 + \varepsilon. \quad (1.9)$$

*L*-arvoihin liittyvä tarkastelu voidaan viedä vielä pidemmälle ja osoittaa, että *Abc*-konjektuuri on voimassa jos ja vain jos

$$\limsup\{L(a, b, c) : (a, b, c) \in \mathbb{N}^3, \text{synt}(a, b) = 1, a + b = c\} = 1, \quad (1.10)$$

toisin sanoen *L*-arvojen joukon kasaantumispisteiden supremum on 1 [8]. Siirtämällä *Abc*-konjektuurin tarkastelu *L*-arvoihin saadaan väitteelle erilainen näkökulma ja käyttöön kasaantumispisteisiin liittyviä menetelmiä, joita ei kokonaisluvuille voida soveltaa.

Vaikkei *Abc*-konjektuuri olekaan voimassa ilman lukua  $\varepsilon > 0$ , saadaan *Abc*-konjektuurin oletukset toteuttavista *abc*-kolmikoista lisää tietoa tarkastelemalla tilannetta  $\varepsilon = 0$ . Tällaisia epäyhtälön

$$\text{rad}(abc) < c \quad (1.11)$$

toteuttavia *abc*-kolmikoita kutsutaan *abc-osumiksi* [14]. Ehdon (1.11) toteuttavia *abc*-kolmikoita on ääretön määrä. Mikäli merkitään *abc*-osumien lukumäärää funktiolla  $N$ ,

$$N(X) = |\{abc\text{-osuma } (a,b,c) \in \mathbb{N}^3 \mid c \leq X\}|, \quad (1.12)$$

voidaan osoittaa *abc*-osumien lukumäärällä olevan seuraavanlainen alaraja [14]: Jokaista  $\varepsilon > 0$  kohti on olemassa  $X_0 > 0$  siten, että kaikilla  $X \geq X_0$  on voimassa epäyhtälö

$$N(X) \geq \exp((\log X)^{\frac{1}{2}-\varepsilon}). \quad (1.13)$$

Epäyhtälöä (1.11) tiukemman ehdon

$$\text{rad}(abc) < \frac{c}{\log c} \quad (1.14)$$

toteuttavia  $abc$ -kolmikoita kutsutaan *logaritmisiksi abc-osumiksi*. Myös logaritmisia  $abc$ -osumia voidaan osoittaa olevan ääretön määrä ja niille vastaavasti on voimassa epäyhtälön (1.13) mukainen alaraja. Logaritmisiin  $abc$ -osumiin liittyvät tulokset ovat aiemmin kirjallisuudessa julkaisematonta tietoa ja niitä tarkastellaan lähemmin alaluvussa 3.7.

$Abc$ -konjektuurilla on valtavasti seurauksia, joista kohtalainen lista löytyy Abderrahmane Nitaj'n kotisivuilta [48]. Sovelluksia on moniin kuuluisiinkin tuloksiin (mm. Catalanin, Szpiroin ja Mordellin konjektuurit, Rothin lause) mutta erityisesti sovelluksia löytyy seuraavilta aloilta [8]:

- a) Diophantoksen yhtälöt ja epäyhtälöt
- b) Elliptiset käyrät
- c) Polynomit

Vaikkei  $Abc$ -konjektuurin avulla pystytä todistamaan itse Fermat'n suurta lausetta vaan pelkästään sen asymptoottinen versio, konjektuuri on silti voimakas Diophantoksen yhtälöitä yhdistävä tekijä. Vuonna 1970 Yuri Matiyasevich osoitti, ettei mielivaltaiselle Diophantoksen yhtälölle ole olemassa yleistä ratkaisumenetelmää [23]. Käytännössä tämä tarkoittaa siis suurta työmäärää, sillä jokainen yhtälö on ratkaistava erikseen.  $Abc$ -konjektuurin avulla pystytään kuitenkin osoittamaan monen Diophantoksen yhtälön tapauksessa vain äärellisen ratkaisujoukon olemassaolo.

$Abc$ -konjektuurilla on myös monia yleistyksiä [48]. Luonnollisen muuttujien määrään liittyvän yleistyksen, ns.  $n$ -konjektuurin [6], lisäksi  $Abc$ -konjektuuri voidaan esittää kongruenssimuodossa [17] tai helpohkosti modifioida yleisille lukukunnille sopivaksi [59, s. 260–261]. Baker ja Granville ovat esittäneet myös ehdotuksia alkuperäisen konjektuurin tarkentamiseksi [2]. Oman lisänsä tuo Stothers-Masonin “polynomien  $Abc$ -konjektuuri“, jota Hu ja Yang [30] ovat kehitelleet edelleen ei-Arkhimedisille meromorfisille funktiokunnille. Tietyillä oletuksilla kunnan suhteen kokonaisille funktioille  $a$ ,  $b$  ja  $c$ , joista ainakin yksi on vakioista eroava, joilla ei ole yhteisiä nollakohtia ja joilla  $a + b = c$ , voidaan osoittaa epäyhtälö

$$\max\{T(r, a), T(r, b), T(r, c)\} \leq \overline{N}\left(r, \frac{1}{abc}\right) - \log r + \mathcal{O}(1), \quad (1.15)$$

missä  $T$  ja  $\overline{N}$  ovat Nevanlinnan arvojenjakautumisteoriaan liittyviä funktioita. Tällöin Stothers-Masonin lause on itse asiassa seuraus yleisemmästä tapauksesta. Hu ja Yang ovat esittäneet myös luonnollisen funktioiden lukumäärään liittyvän yleistyksen tulokselleen [30, s. 287–288].

Yleisesti uskotaan  $Abc$ -konjektuurin olevan totta arvolla  $\varepsilon = 1$ , vaikkei sen todenperäisyydestä olekaan vielä varmaa tietoa [24]. Tässä ns. heikon  $Abc$ -konjektuurin tapauksessa vakioksi  $C(\varepsilon)$  uskotaan riittävän  $C(\varepsilon) = 1$  [4, s. 403]. Hyvin monipuolisena ja käyttökelpoisena



tuloksena todistuksen voisi olettaa olevan varsin epätriviaali, mutta on kuitenkin muistettava, että  $Abc$ -konjektuurin funktiokunta-analogi on suhteellisen helposti todistettavissa [4, s. 401]. Uusimman ratkaisuehdotuksen on esittänyt Shinichi Mochizuki 500-sivuisella neljän artikkelin sarjalla vuoden 2012 syyskuussa [3], [72]. Nähtäväksi jää onko Mochizukin todistus aukoton, ja jos on, niin onko olemassa alkeellisempaa todistusta.

Tässä tutkielmassa tarkastellaan  $Abc$ -konjektuuria lukuteorian kannalta. Tarkoituksena on tuoda esille taustalla olevaa teoriaa sekä valaista  $Abc$ -konjektuurin väitettä ja sen yhteyksiä muihin teorioihin. Fermat'n suurta lausetta tarkastellaan esimerkinomaisesti sen yksinkertaisuuden sekä historiallisen tärkeyden takia. Tutkielma jakautuu kuuteen lukuun. Tässä luvussa esitetään teorian aikaraami sekä yleisiä asioita teoriasta. Luvussa 2 käydään läpi tärkeimmät jatkossa tarvittavat aputulokset. Luku 3 on tutkielman pääluke ja siinä tarkastellaan  $Abc$ -konjektuuria ja siihen liittyviä tuloksia. Luvussa 4 osoitetaan monia  $Abc$ -konjektuurin lukuteoreettisia seurauksia pääpainona erilaiset historialliset Diophantoksen yhtälöt. Luvussa 5 esitellään muutamia  $Abc$ -konjektuurin yleistyksiä ja luvussa 6 esitetään yhteenvedo tutkielman aiheista. Lisäksi liitteissä on esitetty konjektuuriin liittyviä numeerisia taulukoita. Tässä tutkielmassa ei käsitellä logaritmiin  $abc$ -osumiin liittyvää algoritmia lukuunottamatta muita numeeristen tulosten löytämiseen käytettyjä algoritmeja.

Tutkielmassa käytetty  $Abc$ -konjektuuriin liittyvä kirjallisuus on melko hajanaista. Yleisten suuntaviivojen saamiseksi on käytetty Joseph Oesterlén artikkelia [49], Abderrahmane Nitaj'n teoksia [46], [47] [48], Kalle Saaren tutkielmaa [56] sekä artikkeleita [8], [36] ja [24].  $Abc$ -kolmikoihin liittyviä tuloksia löytyy parhaiten lähteistä [22], [14]. Luvun 2 alalukujen yhteydessä on mainittu teokset, joihin teoria perustuu, ja lukujen 3,4 ja 5 alalukujen yhteydessä on mainittu mahdollisimman tarkkaan esityksessä käytetyt alkuperäiset lähteet.

## 1.1 Merkinnoistä

Tässä tutkielmassa käytetään seuraavia merkintöjä:

$$\mathbb{N} = \{1, 2, 3, \dots\}$$

$$\mathbb{N}_{\geq k} = \{k, k+1, k+2, \dots\}, \text{ missä } k \in \mathbb{N}$$

$$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$$

$$\mathbb{Z}_{\geq 0} = \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \dots\}$$

$$\mathbb{Q} = \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\}$$

$$[a, b] = \{x \in \mathbb{R} : a \leq x \leq b\}, \text{ missä } a, b \in \mathbb{R}$$

$$[a, b) = \{x \in \mathbb{R} : a \leq x < b\}, \text{ missä } a, b \in \mathbb{R}$$

$$(a, b) = \{x \in \mathbb{R} : a < x < b\}, \text{ missä } a, b \in \mathbb{R}$$

$$\mathbb{R}_{>0} = \mathbb{R} \cap (0, \infty)$$

$\log x$  luvun  $x$  luonnollinen ( $e$ -kantainen) logaritmi

$$\log^n x = (\log x)^n$$

$\exp(x) = e^x$  eli eksponenttifunktio  $e$  arvolla  $x$

$|G|$  joukon  $G$  alkioden lukumäärä

*Diophantoksen yhtälöllä tai epäyhtälöllä* tarkoitetaan yhtälöä tai epäyhtälöä, jolle etsitään vain kokonaislukuratkaisuja [1, s. 5]. *Efektiiivisesti laskettavissa olevalla* (engl. effectively computable) tarkoitetaan taas sitä, että teoriassa ratkaisu voidaan selvittää (tietokone)algoritmin avulla [51].

## 2 Peruskäsitteitä

$Abc$ -konjektuurin sekä siihen liittyvien tulosten ymmärtämiseksi täytyy tuntea taustalla olevaa teoriaa, jota tässä luvussa pyritään tiivistetysti eri aihepiireihin jaoteltuna esittämään. Tiivistettynäkin luku on laaja, sillä tärkeimmät tutkielmassa käytettävät aputulokset on esitetty todistuksineen. Yksityiskohdista johtuen taustateoriaan perehtynyt lukija voikin siirtyä suoraan lukuun 3.

Tässä luvussa käsitellään monia asioita, joilla ei näennäisestä ole toistensa kanssa paljoakaan tekemistä.  $Abc$ -konjektuuri kuitenkin yhdistää yksittäiset teoriat: jaollisuustarkastelu liittyy oleellisesti  $abc$ -kolmikoihin, analyysin tulosten avulla päästään tarkastelemaan  $Abc$ -konjektuuria kasaantumispisteiden kautta ja polynomitulokset liittyvät  $Abc$ -konjektuurin polynomiversioon. Binomilauseen sovellukset toimivat yleisinä aputuloksina. Suurin osa alaluvun teoriasta keskittyy riittävän apukoneiston rakentamiseen  $abc$ -osumien alarajafunktion todistusta varten: siihen liittyy hilat, ryhmät ja niiden väliset kuvaukset sekä alkulukuihin liittyvät tulokset.

Alalukujen tarkastelu on räätälöity  $Abc$ -konjektuurin tarpeisiin. Kattavamman käsityksen yksittäisistä aihepiireistä saa alaluvuissa mainittuihin lähteisiin perehtymällä.

### 2.1 Jaollisuudesta ja kongruensseista

Lukuteoriassa tutkitaan yleisesti lukuja ja niiden ominaisuuksia. Tässä tutkielmassa kuitenkin rajoitutaan pääosin kokonaislukuihin, joihin liittyvää teoriaa on ilman todistuksia esitetty seuraavassa lähteisiin [38] ja [54] perustuen. Jatkossa tunnettuina pidetään mm. kokonaislukujen algebrallisia perusominaisuuksia sekä yksikäsitteistä jakoyhtälöä. Esimerkkien avulla on pyritty havainnollistamaan myöhemmin tarvittavia aputuloksia.

Aloitetaan tarkastelu jaollisuudesta sekä suurimmasta yhteisestä tekijästä.

**Määritelmä 2.1.1.** Luku  $a \in \mathbb{Z}$  on luvun  $b \in \mathbb{Z}$  tekijä, jos  $b = ak$  jollakin  $k \in \mathbb{Z}$ . Tällöin merkitään  $a \mid b$  ja sanotaan, että luku  $b$  on *jaollinen* luvulla  $a$ .

**Huomautus 2.1.2.** (i) Kaikilla  $a \in \mathbb{Z}$  pätee  $a \mid 0$ , sillä  $0 = a \cdot 0$ .

(ii) Jos  $b \neq 0$  ja  $a \mid b$ , niin  $|a| \leq |b|$ . Kaikilla  $k \in \mathbb{Z} \setminus \{0\}$  nimittäin  $|b| = |ak| = |a||k| \geq |a|$ .

(iii) Jos  $a \mid b$ , niin  $a^n \mid b^n$  kun  $n \in \mathbb{N}$ . Sillä jos  $b = ak$ , niin  $b^n = a^n k^n$  jollakin  $k \in \mathbb{Z}$ .

(iv) Jos  $a \mid b$  ja  $a \mid c$ , niin  $a \mid (b \pm c)$  sillä  $b \pm c = a(k_b \pm k_c)$  joillakin  $k_b, k_c \in \mathbb{Z}$ .

Havainnollistetaan jaollisuutta seuraavalla esimerkillä.

**Esimerkki 2.1.3.** Osoitetaan induktiolla, että  $8 \mid 9^n - 1$  kaikilla  $n \in \mathbb{N}$ .

1°) Väite pätee arvolla  $n = 1$ , sillä  $9^1 - 1 = 8$ .

2°) Oletetaan, että väite pätee arvolla  $n = k \geq 1$ . Tällöin arvolla  $n = k + 1$  saadaan

$$9^{k+1} - 1 = 9^k 9 - 9 + 8 = 9(9^k - 1) - 8 = 9 \cdot 8j - 8 = 8(9j - 1),$$

sillä induktio-oletuksen nojalla  $9^k - 1 = 8j$  jollekin  $j \in \mathbb{N}$ . Kohtien 1°) ja 2°) sekä induktioperiaatteen nojalla väite pätee kaikilla  $n \in \mathbb{N}$ .

**Määritelmä 2.1.4.** Lukujen  $a_1, \dots, a_n \in \mathbb{Z}$ , joista ainakin yksi on nollasta eroava, suurin yhteinen tekijä  $\text{sy}(a_1, \dots, a_n)$  on luku

$$\text{sy}(a_1, \dots, a_n) = \max \{k \in \mathbb{N} : k \mid a_i \text{ kaikilla } i = 1, \dots, n\}.$$

**Lause 2.1.5.** Olkoot  $a_1, \dots, a_n \in \mathbb{Z}$  siten, että  $a_{i_0} \neq 0$  jollekin  $i_0 \in \{1, \dots, n\}$ . Tällöin

$$\text{syt}(a_1, \dots, a_n) = \min(\mathbb{N} \cap \{x_1 a_1 + \dots + x_n a_n : x_i \in \mathbb{Z}\}).$$

**Esimerkki 2.1.6.** (i) Jos  $n \in \mathbb{N}$ , niin  $\text{syt}(n, n+1) = 1$ . Väite seuraa lineaarikombinaatiosta

$$1 = n + 1 - n = 1 \cdot (n + 1) + (-1) \cdot n$$

ja Lauseesta 2.1.5.

(ii) Jos  $a, b \in \mathbb{N}$  siten, että  $\text{syt}(a, b) = 1$ , niin  $\text{syt}(a + b, a - b) \leq 2$ . Oletuksen  $\text{syt}(a, b) = 1$  nojalla nimittäin on olemassa vakiot  $x_1, x_2 \in \mathbb{Z}$  siten, että  $x_1 a + x_2 b = 1$ . Tällöin

$$(x_1 + x_2)(a + b) + (x_1 - x_2)(a - b) = 2x_1 a + 2x_2 b = 2,$$

jolloin väite seuraa Lauseesta 2.1.5.

Edellisen esimerkin tuloksia pidetään jatkossa tunnettuina ilman erillistä mainintaa. Seuraava tulos on oleellinen myöhemmin esiintyvien  $abc$ -kolmikoiden suurimman yhteisen tekijän määrittämisen kannalta.

**Lemma 2.1.7.** Jos  $a, b \in \mathbb{N}$  ja  $c \in \mathbb{Z}$ , niin  $\text{syt}(a + cb, b) = \text{syt}(a, b)$ .

Jaollisuustarkastelu johtaa lopulta huomioon kahdenlaisista luvuista.

**Määritelmä 2.1.8.** Luku  $a > 1$  on *alkuluku*, mikäli sillä on vain triviaalit tekijät  $\pm 1$  ja  $\pm a$ , muulloin luku  $a$  on *yhdistetty*.

**Määritelmä 2.1.9.** Olkoon  $\text{syt}(a_1, \dots, a_n) = 1$ . Tällöin sanotaan, että luvut  $a_1, \dots, a_n$  ovat *suhteellisia alkulukuja* (*keskenään jaottomia*).

Tarkasteltavien lukujen ei siis tarvitse olla alkulukuja ollakseen keskenään jaottomia. Luvuista voidaan myös tehdä suhteellisia alkulukuja ja osoittaa joitain suurimpaan yhteiseen tekijään liittyviä tuloksia.

**Lemma 2.1.10.** Olkoot  $a_1, \dots, a_n \in \mathbb{Z}$  siten, että  $a_{i_0} \neq 0$  jollekin  $i_0 \in \{1, \dots, n\}$  ja olkoon  $d = \text{syt}(a_1, \dots, a_n)$ . Tällöin

$$\text{syt}\left(\frac{a_1}{d}, \dots, \frac{a_n}{d}\right) = 1.$$

**Lemma 2.1.11.** Olkoot  $a, b, c \in \mathbb{N}$ .

- (i) Jos  $a \mid c$  ja  $b \mid c$  siten, että  $\text{syt}(a, b) = 1$ , niin  $ab \mid c$ .
- (ii) Jos  $\text{syt}(a, c) = \text{syt}(b, c) = 1$ , niin  $\text{syt}(ab, c) = 1$ .
- (iii) Jos  $\text{syt}(a, b) = 1$ , niin  $\text{syt}(a^k, b^m) = 1$  kaikilla  $k, m \in \mathbb{N}$ .

**Lemma 2.1.12** (Eukleides). Jos  $a \mid bc$  ja  $\text{syt}(a, b) = 1$ , niin  $a \mid c$ .

Eukleiden lemma johtaa seuraavaan tulokseen ja lopulta Aritmetiikan peruslauseeseen.

**Lemma 2.1.13.** *Luku  $p \in \mathbb{N} \setminus \{1\}$  on alkuluku, jos ja vain jos kaikilla  $a, b \in \mathbb{N}$  on voimassa implikaatio*

$$p \mid ab \implies p \mid a \text{ tai } p \mid b.$$

**Lause 2.1.14** (Aritmetiikan peruslause). *Jokainen luonnollinen luku  $n \geq 2$  voidaan esittää järjestyttä vaille yksikäsitteisellä tavalla tulona*

$$n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}, \quad (2.1)$$

missä  $p_i$ :t ovat eri alkulukuja ja  $a_i \in \mathbb{N}$ .

Tuloa (2.1) kutsutaan luvun  $n$  *kanoniseksi esitykseksi* tai *alkutekijäesitykseksi* ja lukuja  $p_i$  luvun  $n$  *alkutekijöiksi*.

**Huomautus 2.1.15.** Aritmetiikan peruslause voidaan yleistää myös negatiivisia kokonaislukuja koskeväksi yhtälön (2.1) oikeaa puolta modifioimalla. Kokonaisluku  $n \in \mathbb{Z} \setminus \{0, \pm 1\}$  voidaan tällöin esittää kanonisessa muodossa

$$n = (-1)^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},$$

missä  $p_i$ :t ovat eri alkulukuja,  $a_0 \in \{0, 1\}$  ja  $a_1, \dots, a_n \in \mathbb{N}$ .

**Määritelmä 2.1.16.** Lukujen  $a_1, \dots, a_n \in \mathbb{N}$  *pienin yhteinen monikerta*  $\text{pym}(a_1, \dots, a_n)$  on luku  $d \in \mathbb{N}$ , jolle on voimassa seuraavat ehdot:

- (i)  $a_i \mid d$  kaikilla  $i = 1, \dots, n$ ;
- (ii) Jos  $c \in \mathbb{N}$  ja  $a_i \mid c$  kaikilla  $i = 1, \dots, n$ , niin  $d \mid c$ .

Jaollisuutta voidaan merkitä myös käyttämällä kongruenssia, jonka Gauss toi lukuteoriaan julkaisussaan *Disquisitiones Arithmeticae* vuonna 1801.

**Määritelmä 2.1.17.** Olkoon  $m \in \mathbb{N}$  ja olkoot  $a, b \in \mathbb{Z}$ . Mikäli  $m \mid (a - b)$ , luku  $a$  on *kongruentti luvun  $b$  kanssa modulo  $m$*  ja sitä merkitään

$$a \equiv b \pmod{m}.$$

Jos  $m \nmid (a - b)$ , merkitään  $a \not\equiv b \pmod{m}$ .

**Lemma 2.1.18.** *Olkoot  $a, b, c, d \in \mathbb{Z}$  ja olkoon  $m \in \mathbb{N}$ .*

- (i) *Jos  $a \equiv b \pmod{m}$  ja  $c \equiv d \pmod{m}$ , niin  $a + c \equiv b + d \pmod{m}$ .*
- (ii) *Jos  $a \equiv b \pmod{m}$  ja  $c \equiv d \pmod{m}$ , niin  $ac \equiv bd \pmod{m}$ .*

**Lemma 2.1.19.** *Olkoot  $a, b, c, d \in \mathbb{Z}$  ja olkoon  $m \in \mathbb{N}$ . Tällöin*

- (i)  $a \equiv a \pmod{m}$  (*refleksiivisyys*)
- (ii) *Jos  $a \equiv b \pmod{m}$ , niin  $b \equiv a \pmod{m}$ . (symmetrisyys)*
- (iii) *Jos  $a \equiv b \pmod{m}$  ja  $b \equiv c \pmod{m}$ , niin  $a \equiv c \pmod{m}$  (transitiivisuus)*

Kongruenssia voidaan soveltaa jaollisuuden tarkastelussa seuraavien esimerkkien tapaan.

**Esimerkki 2.1.20.** Osoitetaan induktiolla, että kaikilla  $n \in \mathbb{N}$  pätee  $2^n \mid (3^{2^n} - 1)$ .

1°) Tapauksessa  $n = 1$  saadaan  $3^2 - 1 = 8 = 2 \cdot 4$ .

2°) Oletetaan, että väite pätee arvolla  $n = k \geq 1$ . Tällöin arvolla  $n = k + 1$

$$3^{2^{k+1}} - 1 = 3^{2^{k2}} - 1 = (3^{2^k})^2 - 1^2 = (3^{2^k} - 1)(3^{2^k} + 1),$$

jolloin induktiooletuksen ja tiedon  $3^{2^k} \equiv 1^{2^k} \equiv 1 \pmod{2}$  nojalla  $2^{k+1} \mid (3^{2^{k+1}} - 1)$ . Näin ollen kohtien 1°) ja 2°) sekä induktioperiaatteen nojalla väite pätee kaikilla  $n \in \mathbb{N}$ .

**Huomautus 2.1.21.** Esimerkin 2.1.20 päättelyä imitoimalla voidaan itse asiassa osoittaa, että  $2^{n+2} \mid (3^{2^n} - 1)$  kaikilla  $n \in \mathbb{N}$ .

**Esimerkki 2.1.22.** Osoitetaan induktiolla, että  $2^{n+3}5^2 \mid 7^{2^n} - 1$  kaikilla  $n \in \mathbb{N} \setminus \{1\}$ .

1°) Tapauksessa  $n = 2$  saadaan  $7^{2^2} - 1 = 2400 = 2^5 \cdot 3 \cdot 5^2$ .

2°) Oletetaan, että väite pätee arvolla  $n = k \geq 2$ . Tällöin arvolla  $n = k + 1$

$$7^{2^{k+1}} - 1 = 7^{2^k2} - 1 = (7^{2^k})^2 - 1^2 = (7^{2^k} - 1)(7^{2^k} + 1),$$

jolloin induktiooletuksesta ja kongruensseista

$$7^{2^k} \equiv 1^{2^k} \equiv 1 \equiv -1 \pmod{2}$$

$$7^{2^k} = 7^{2 \cdot 2^{k-1}} = 49^{2^{k-1}} \equiv (-1)^{2^{k-1}} \equiv 1 \pmod{25}$$

seuraa kongruenssin transitiivisuuden nojalla  $2^{(k+1)+3}5^2 \mid 7^{2^{k+1}} - 1$ . Näin ollen induktioväite pätee kohtien 1°) ja 2°) sekä induktioperiaatteen nojalla.

Kongruenssien sieventäminen ei täysin mukaile tavallisen yhtälön aritmetiikkaa.

**Lause 2.1.23** (Tulon supistusääntö). *Olkoot  $a, b, c \in \mathbb{Z}$  ja olkoon  $m \in \mathbb{N}$  siten, että  $ac \equiv bc \pmod{m}$ . Tällöin*

$$a \equiv b \left( \pmod{\frac{m}{\text{syt}(m, c)}} \right).$$

**Lause 2.1.24.** *Olkoot  $a, b \in \mathbb{Z}$  ja  $k, m_i \in \mathbb{N}$  kaikilla  $i = 1, \dots, k$ . Jos  $a \equiv b \pmod{m_i}$  kaikilla  $i = 1, \dots, k$  ja  $\text{syt}(m_i, m_j) = 1$  kaikilla  $i \neq j$ , niin tällöin*

$$a \equiv b \pmod{m_1 m_2 \cdots m_k}.$$

Lineaarisen kongruenssin ratkaisujen olemassaololle voidaan osoittaa seuraava tulos.

**Lause 2.1.25.** *Olkoot  $a, b \in \mathbb{Z}$  ja olkoon  $m \in \mathbb{N}$  siten, että  $\text{syt}(a, m) = d$ . Tällöin jos*

(i)  $d \nmid b$ , *niin kongruenssilla  $ax \equiv b \pmod{m}$  ei ole ratkaisua.*

(ii)  $d \mid b$ , *niin kongruenssilla  $ax \equiv b \pmod{m}$  on täsmälleen  $d$  ei-kongruenttia ratkaisua modulo  $m$ .*

Tarkastellaan vielä lopuksi eksponentiaalisia kongruensseja. Fermat esitti ensimmäisenä alkoiden kertalukuihin liittyvän tuloksensa, jonka Euler myöhemmin yleisti käyttämällä lukuteorian kannalta oleelliseksi havaittua funktiota  $\phi$ .

**Lause 2.1.26** (Fermat'n pieni lause). *Olkoon  $p$  alkuluku ja olkoon  $a \in \mathbb{Z}$  siten, että  $p \nmid a$ . Tällöin*

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

**Määritelmä 2.1.27.** *Eulerin funktioksi* kutsutaan kuvausta  $\phi : \mathbb{N} \rightarrow \mathbb{N}$ , jonka arvo  $\phi(n)$  ilmoittaa niiden lukujen  $a \in \{1, \dots, n\}$  lukumäärän, joille  $\text{sy}(a, n) = 1$ .

**Huomautus 2.1.28.** Koska  $\text{sy}(n, n) > 1$  ja  $\text{sy}(1, n) = \text{sy}(n-1, n) = 1$ , kaikilla  $n \in \mathbb{N}_{\geq 3}$  pätee

$$2 \leq \phi(n) \leq n-1.$$

Seuraavat tulokset helpottavat Eulerin funktion arvon määrittämistä.

**Lemma 2.1.29.** *Olkoon  $p$  alkuluku ja  $k \in \mathbb{N}$ . Tällöin  $\phi(p^k) = p^k - p^{k-1}$ .*

**Lause 2.1.30.** *Olkoot  $m, n \in \mathbb{N}$  suhteellisia alkulukuja. Tällöin  $\phi(mn) = \phi(m)\phi(n)$ .*

**Huomautus 2.1.31.** Funktion  $\phi$  arvo on parillinen kaikilla  $n \in \mathbb{N}_{\geq 3}$ . Aritmetiikan peruslausetta (Lause 2.1.14), Lausetta 2.1.30 ja Lemmaa 2.1.29 soveltamalla nimittäin nähdään, että mikäli luvulla  $n$  on pariton alkutekijä, niin myös  $\phi(n)$  on parillinen, sillä kahden parittoman luvun erotus on parillinen. Jos luvulla  $n$  on pelkästään alkutekijä 2, niin  $\phi(n)$  on vastaavasti myös parillinen, sillä kahden parillisen luvun erotus on parillinen.

**Lause 2.1.32** (Eulerin lause). *Olkoon  $n \in \mathbb{N}$  ja  $a \in \mathbb{Z}$  siten, että  $\text{sy}(a, n) = 1$ . Tällöin*

$$a^{\phi(n)} \equiv 1 \pmod{n}.$$

**Määritelmä 2.1.33.** *Luvun  $a$  kertaluvuksi modulo  $m$  sanotaan lukua*

$$\text{ord}_m a = \min\{k \in \mathbb{N} : a^k \equiv 1 \pmod{m}\}.$$

**Lemma 2.1.34.** *Olkoon  $m \in \mathbb{N}$  ja  $a \in \mathbb{Z}$  siten, että  $\text{sy}(a, m) = 1$ . Tällöin luvulle  $x \in \mathbb{N}$  pätee  $a^x \equiv 1 \pmod{m}$  jos ja vain jos  $\text{ord}_m a \mid x$ .*

**Seuraus 2.1.35.** *Olkoon  $m \in \mathbb{N}$  ja  $a \in \mathbb{Z}$  siten, että  $\text{sy}(a, m) = 1$ . Tällöin  $\text{ord}_m a \mid \phi(m)$ .*

## 2.2 Binomilauseen sovelluksia

Eräs kombinatoriikan käyttökelpoisimmista tuloksista on binomilause, jonka avulla voidaan helposti laskea binomien ei-negatiiviset potenssit. Tarkastellaan seuraavaksi binomilauseen avulla saatavia jatkoon kannalta tarpeellisia tuloksia kirjojen [54, s. 8–15] ja [55, s. 5–24] sekä kirjoittajan oman pohdinnan perusteella.

Aloitetaan kertomasta, jonka avulla voidaan määritellä binomikerroin.

**Määritelmä 2.2.1.** Olkoon  $n \in \mathbb{N}$ . Lukua  $n! = 1 \cdot 2 \cdot 3 \cdots n$  kutsutaan *luvun  $n$  kertomaksi*. Lisäksi asetetaan  $0! = 1$ .

**Määritelmä 2.2.2.** Olkoot  $n, k \in \mathbb{Z}_{\geq 0}$  siten, että  $k \leq n$ . Tällöin lukua

$$\binom{n}{k} = \frac{n!}{k!(n-k)!}$$

kutsutaan *binomikertoimeksi*.

**Huomautus 2.2.3.** Binomikerroin voidaan tulkita siten, että se kertoo kuinka monta erilaista  $k$  alkioista osajoukkoa voidaan ottaa  $n$  alkioisesta joukosta, kun alkioiden ottojärjestyksellä ei ole merkitystä [55, s. 6]. Näin ollen kaikki binomikerrointen arvot ovat positiivisia kokonaislukuja.

Seuraava aputuloks osoittaa binomikerrointen arvoilla olevan tiettyä symmetriaa.

**Lemma 2.2.4.** Olkoot  $n, k \in \mathbb{Z}_{\geq 0}$  siten, että  $k \leq n$ . Tällöin

$$\binom{n}{n-k} = \binom{n}{k} \quad \text{sekä} \quad \binom{2n+1}{n} = \binom{2n+1}{n+1}.$$

*Todistus.* Binomikertoimen määritelmästä saadaan suoraan yhtäsuuruudet

$$\begin{aligned} \binom{n}{k} &= \frac{n!}{k!(n-k)!} = \frac{n!}{(n-k)!(n-(n-k))!} = \binom{n}{n-k} \\ \binom{2n+1}{n} &= \frac{(2n+1)!}{n!(2n+1-n)!} = \frac{(2n+1)!}{(n+1)!(2n+1-(n+1))!} = \binom{2n+1}{n+1} \end{aligned}$$

joista väite seuraa. □

**Huomautus 2.2.5.** Luvuilla  $n, k \in \mathbb{N}$ ,  $k \leq n$ , on voimassa myös yhtälö

$$\binom{n}{k} + \binom{n}{k-1} = \binom{n+1}{k},$$

jonka avulla voidaan konstruoida binomikerrointen arvoja kuvaava ns. *Pascalin kolmio*.

Binomikertoimilla ja summien potensseilla on seuraavanlainen yhteys:

**Lause 2.2.6** (Binomilause). Olkoot  $x, y \in \mathbb{R}$  ja  $n \in \mathbb{N}$ . Tällöin

$$(x+y)^n = \sum_{k=0}^n \binom{n}{k} x^k y^{n-k}.$$



**Huomautus 2.2.7.** Huomautuksen 2.2.3 ja binomilauseen avulla voidaan osoittaa, että jokaisella  $n$ -alkioisella joukolla,  $n \in \mathbb{N}$ , on  $2^n$  erilaista osajoukkoa. Summaamalla nimittäin yli kaikkien erilaisten  $k$ :n alkion osajoukkojen saadaan binomilauseetta hyödyntämällä

$$\sum_{k=0}^n \binom{n}{k} = (1+1)^n = 2^n.$$

Binomilauseen avulla saadaan eräs yläraja binomikerrointen arvoille.

**Esimerkki 2.2.8.** Olkoon  $m \in \mathbb{N}$ . Tarkastellaan binomikerrointa

$$M = \binom{2m+1}{m} = \frac{(2m+1)!}{m!(2m+1-m)!} = \frac{(2m+1)2m(2m-1)\cdots(m+2)}{m!},$$

joka Huomautuksen 2.2.3 nojalla on positiivinen kokonaisluku. Lemman 2.2.4 ja binomilauseen nojalla saadaan näin ollen ylöspäin arvioimalla

$$M = \frac{1}{2} \left[ \binom{2m+1}{m} + \binom{2m+1}{m+1} \right] < \frac{1}{2} \left[ \sum_{k=0}^{2m+1} \binom{2m+1}{k} \right] = \frac{1}{2} (1+1)^{2m+1} = 4^m.$$

Binomilauseen avulla binomikertoimien neliöiden summa voidaan yksinkertaisemmin esittää yhden binomikertoimen avulla.

**Lemma 2.2.9.** *Olkoon  $n \in \mathbb{N}$ . Tällöin*

$$\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}.$$

*Todistus.* Soveltamalla binomilauseetta yhtälöön  $(1+x)^{2n} = (1+x)^n(1+x)^n$  saadaan

$$\sum_{k=0}^{2n} \binom{2n}{k} x^{2n-k} = \left( \sum_{k=0}^n \binom{n}{k} x^{n-k} \right) \left( \sum_{k=0}^n \binom{n}{k} x^{n-k} \right).$$

Kun nyt tarkastellaan termin  $x^n$  kertoimia saadaan vasemmalta puolelta arvoksi suoraan  $\binom{2n}{n}$  ja oikealta puolelta suorittamalla kertolasku ja Lemmaa 2.2.4 soveltamalla

$$\binom{n}{0}\binom{n}{n} + \binom{n}{1}\binom{n}{n-1} + \cdots + \binom{n}{n}\binom{n}{0} = \binom{n}{0}^2 + \binom{n}{1}^2 + \cdots + \binom{n}{n}^2 = \sum_{k=0}^n \binom{n}{k}^2,$$

mistä väite yhtäsuuruuden nojalla seuraa. □

Osoitetaan lopuksi kaksi myöhemmin tarvittavaa jaollisuuteen liittyvää tulosta, joista ensimmäinen on yksinkertaisempi esittää ilman binomilauseetta.

**Lemma 2.2.10.** *Olkoot  $a, b, n \in \mathbb{N}$  siten, että  $a < b$  ja  $n$  on parillinen. Tällöin*

$$(b+a)^n - (b-a)^n = 4ab \left( (b+a)^{n-2} + (b+a)^{n-4}(b-a)^2 + \cdots + (b-a)^{n-2} \right).$$

*Todistus.* Merkitään  $x = b + a$  ja  $y = b - a$  sekä  $n = 2m$  jollekin  $m \in \mathbb{N}$ . Tällöin

$$\begin{aligned} x^n - y^n &= (x - y) (x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1}) \\ &= (x - y) \left( \sum_{k=0}^{n-1} x^{n-1-k} y^k \right), \end{aligned}$$

mikä nähdään kertomalla auki yhtälön oikea puoli. Koska  $n = 2m$ , saadaan edelleen

$$\begin{aligned} \sum_{k=0}^{n-1} x^{n-1-k} y^k &= (x + y) \left( \sum_{j=0}^{m-1} x^{2m-2-2j} y^{2j} \right) \\ &= (x + y) (x^{n-2} + x^{n-4}y^2 + \cdots + x^2y^{n-4} + y^{n-2}), \end{aligned}$$

mikä jälleen nähdään kertomalla auki yhtälön oikea puoli. Väite seuraa yhdistämällä edellä olevat yhtälöt.  $\square$

**Lemma 2.2.11.** *Olkoon  $n \in \mathbb{N}$ . Määritellään luvut  $x_n$  ja  $y_n$  yhtälöllä*

$$x_n + y_n \sqrt{2} = (3 + 2\sqrt{2})^n. \quad (2.2)$$

(i) *Tällöin luvut toteuttavat myös yhtälön  $x_n - y_n \sqrt{2} = (3 - 2\sqrt{2})^n$ .*

(ii) *Jos  $n = 2^m$ , niin  $2^{m+1} \mid y_n$  kaikilla  $m \in \mathbb{N}$ .*

*Todistus.* (i) Binomilauseetta soveltamalla saadaan

$$\begin{aligned} (3 + 2\sqrt{2})^n &= \sum_{k=0}^n \binom{n}{k} 3^k (2\sqrt{2})^{n-k} \\ (3 - 2\sqrt{2})^n &= \sum_{k=0}^n \binom{n}{k} 3^k (-2\sqrt{2})^{n-k} \end{aligned}$$

Verrataan yhtälöiden oikeita puolia. Kun  $n - k$  on parillinen, summan termi on molemmissa yhtälöissä sama kokonaisluku. Vastaavasti, kun  $n - k$  on pariton, saadaan kokonaislukukertoiminen  $\sqrt{2}$ -termi, jonka etumerkki ylemmässä summassa on positiivinen ja alemmassa negatiivinen. Soveltamalla päättelyä summien jokaiseen termiin saadaan väite.

(ii) Osoitetaan kohta todistuksen [56, s. 4] ajatusta mukaillen. Kirjoittamalla  $n = 2^m$ , missä  $m \in \mathbb{N}$ , ja soveltamalla yhtälöä (2.2) saadaan

$$x_{2^{m+1}} + y_{2^{m+1}} \sqrt{2} = (3 + 2\sqrt{2})^{2^{m+1}} = (x_{2^m} + y_{2^m} \sqrt{2})^2 = x_{2^m}^2 + 2y_{2^m}^2 + 2x_{2^m}y_{2^m} \sqrt{2}.$$

Yhtälöstä nähdään, että  $y_{2^{m+1}} = 2x_{2^m}y_{2^m}$ . Osoitetaan väite induktiolla käyttäen hyväksi tätä tulosta.

1°) Tapauksessa  $m = 1$  saadaan  $n = 2$ , jolloin  $x_n + y_n \sqrt{2} = 17 + 12\sqrt{2}$ . Näin ollen väite pätee arvolla  $m = 1$ , sillä  $4 \mid 12$  eli  $2^{m+1} \mid y_n$ .

2°) Oletetaan, että väite pätee arvolla  $m = k \geq 1$ . Tällöin arvolla  $m = k + 1$  saadaan yllä olevan tuloksen ja induktio-oletuksen nojalla

$$y_{2^{k+1}} = 2x_{2^k}y_{2^k} = 2x_{2^k}2^{k+1}j = 2^{k+2}x_{2^k}j,$$

missä  $j \in \mathbb{N}$ . Siis  $2^{k+2} \mid y_{2^{k+1}}$ , ja väite pätee myös arvolla  $k + 1$ . Kohtien 1°) ja 2°) sekä induktioperiaatteen nojalla väite pätee kaikilla  $m \in \mathbb{N}$ .  $\square$

## 2.3 Hiloista

Hiloihin liittyvä teoria (engl. Geometry of Numbers) perustuu Minkowskin huomioon, jonka mukaan jotkin lukuteoreettiset tulokset voivat olla hyvin intuitiivisesti selviä, kun niitä tarkastellaan  $n$ -ulotteisessa Euklidisessa avaruudessa [9, s. 1]. Seuraavassa esitetään Minkowskin konveksin kappaleen lauseen ymmärtämiseksi tarvittavaa teoriaa rajoittuen tarkastelussa avaruuteen  $\mathbb{R}^n$ . Erään näkökulman hilojen soveltamisesta lukuteoriassa saa nopeasti kirjasta [32, s. 206–215], syvällisemmin aihetta on käsitelty kirjassa [9], johon tämä alaluku havainnollistavia esimerkkejä lukuunottamatta pääosin perustuu.

Aloitetaan määrittelemällä täysiasteinen hila.

**Määritelmä 2.3.1.** Olkoon joukko  $E = \{e_1, \dots, e_n\}$  avaruuden  $\mathbb{R}^n$  jokin kanta. Tällöin joukkoa

$$\Lambda = \left\{ \sum_{j=1}^n u_j e_j \in \mathbb{R}^n : u_j \in \mathbb{Z} \right\}$$

kutsutaan avaruuden  $\mathbb{R}^n$   $E$ -kantaiseksi hilaksi.

**Huomautus 2.3.2.** Avaruuden  $\mathbb{R}^n$  kanta  $E$  määrittää yksikäsitteisen hilan, mutta hila ei määritä yksikäsitteistä kantaa. Hilan kantojen välillä on kuitenkin yhteys: mikäli  $E$  ja  $E'$ ,  $E \neq E'$ , ovat hilan  $\Lambda$  kantoja, pätee niille yhtälö

$$\det(E) = \pm \det(E'). \quad (2.3)$$

**Esimerkki 2.3.3.** Tarkastellaan avaruutta  $\mathbb{R}^2$  ja hilaa  $\Lambda = \mathbb{Z} \times \mathbb{Z}$ . Kannat  $E$  ja  $E'$ ,

$$E = \left\{ \begin{pmatrix} 1 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ 1 \end{pmatrix} \right\} \quad \text{ja} \quad E' = \left\{ \begin{pmatrix} -1 \\ 0 \end{pmatrix}, \begin{pmatrix} 1 \\ 1 \end{pmatrix} \right\},$$

määrittävät nyt selvästi saman hilan  $\Lambda$ . Kantojen vektoreista muodostetuille matriiseille pätee

$$\det(E) = \begin{vmatrix} 1 & 0 \\ 0 & 1 \end{vmatrix} = 1 = - \begin{vmatrix} -1 & 1 \\ 0 & 1 \end{vmatrix} = -\det(E').$$

Vaihtamalla vektorien järjestystä matriiseja muodostettaessa saadaan determinanteista vastalukuja, mikä ei kuitenkaan vaikuta lopputulokseen; yhtälö (2.3) on joka tapauksessa voimassa.

Yllä olevan nojalla jokaiseen hilaan voidaan liittää yksikäsitteinen luku, determinantti.

**Määritelmä 2.3.4.** Olkoon  $\Lambda \subset \mathbb{R}^n$  hila, jonka muodostaa jokin avaruuden  $\mathbb{R}^n$  kanta  $E = \{e_1, \dots, e_n\}$ . Hilan  $\Lambda$  *determinantti* on luku

$$\det(\Lambda) = |\det(E)| = |\det(e_1, \dots, e_n)|.$$

**Huomautus 2.3.5.** Determinantille pätee aina  $\det(\Lambda) > 0$ , sillä määritelmän mukaan kannan  $E$  muodostavat vektorit  $e_1, \dots, e_n$  ovat lineaarisesti riippumattomia.

Esitetään seuraavaksi yleistetty versio Minkowskin konveksin kappaleen lauseesta, jonka avulla voidaan muodostaa yhteys joukon konveksisuuden, symmetrisyyden ja tilavuuden sekä hilapisteiden lukumäärän välille. Sitä ennen tarvitaan kuitenkin vielä seuraava määritelmä.

**Määritelmä 2.3.6.** Olkoon  $V$  avaruuden  $\mathbb{R}^n$  epätyhjä osajoukko. Joukko  $V$  on

- (i) *konvekksi*, mikäli kaikilla  $x, y \in V$  pätee  $\lambda x + (1 - \lambda)y \in V$ , missä  $0 \leq \lambda \leq 1$ .
- (ii) *origon suhteen symmetrinen*, mikäli kaikilla  $x \in V$  pätee  $-x \in V$ .

**Lause 2.3.7** (Minkowskin konveksin kappaleen lause). *Olkoon  $\Lambda \subset \mathbb{R}^n$  hila, jota määrittää jokin avaruuden  $\mathbb{R}^n$  kanta  $E$ , ja olkoon  $V \subset \mathbb{R}^n$  konvekksi ja origon suhteen symmetrinen epätyhjä joukko. Jos joukon  $V$  tilavuudelle  $\text{vol}(V)$  on voimassa epäyhtälö*

$$\text{vol}(V) > m2^n \det(\Lambda) \quad (2.4)$$

*jollakin  $m \in \mathbb{N}$ , niin joukko  $V$  sisältää ainakin  $m$  erilaista nollasta eroavaa hilapisteparia  $\pm v_i \in \Lambda$ ,  $i = 1, \dots, m$ .*

**Huomautus 2.3.8.** Lauseessa 2.3.7 tilavuudella  $\text{vol}(V)$  tarkoitetaan joukon  $V$  Lebesguemittaa. Usein tarkasteltavat joukot ovat kuitenkin niin “yksinkertaisia”, että tarkempaa mitallisuustarkastelua ei tarvitse suorittaa vaan tilavuus saadaan selville helpommilla keinoilla.

Jatkoa varten valitaan Lauseessa 2.3.7 käytetty joukko  $V$  siten, että sen tilavuus tunnetaan. Tämä onnistuu (skalaarimonikertaa vaille) yksikäsitteisesti seuraavan lemmän avulla [14, s. 1866–1867].

**Lemma 2.3.9.** *Olkoon  $n \in \mathbb{N}$ . Määritellään joukko  $V \subset \mathbb{R}^n$  siten, että*

$$V = \left\{ x \in \mathbb{R}^n \mid \sum_{\substack{i=1 \\ x_i > 0}}^n x_i \leq 1 \text{ ja } \sum_{\substack{i=1 \\ x_i < 0}}^n |x_i| \leq 1 \right\}.$$

*Tällöin*

$$\text{vol}(V) = \frac{(2n)!}{n!^3}.$$

*Todistus.* Olkoon  $p \in \mathbb{Z}_{\geq 0}$  siten, että  $0 \leq p \leq n$ . Määritellään lukua  $p$  vastaava joukko

$$K_p = \left\{ x = (x_1, \dots, x_n) \in \mathbb{R}^n \mid x_i \geq 0 \text{ kaikilla } i \leq p \text{ ja } x_i \leq 0 \text{ kaikilla } i > p \right\},$$

missä  $p$  on viimeinen indeksi, jolla luku  $x_i$  on ei-negatiivinen.

Lasketaan tilavuus kappaleen  $V$  sille osalle, joka kuuluu joukkoon  $K_p$ . Määritellään ensin  $m$ -ulotteinen hyperpyramidi

$$Y_m = \left\{ x = (x_1, \dots, x_m) \in \mathbb{R}^m \mid x_1, \dots, x_m \geq 0 \text{ ja } \sum_{i=1}^m x_i \leq 1 \right\},$$

jonka tilavuus on  $\frac{1}{m!}$ . Samaistamalla avaruus  $\mathbb{R}^n$  avaruuden  $\mathbb{R}^p \times \mathbb{R}^{n-p}$  kanssa saadaan

$$K_p \cap V = Y_p \times (-Y_{n-p}).$$

Näin ollen

$$\text{vol}_n(K_p \cap V) = \text{vol}_p(Y_p) \cdot \text{vol}_{n-p}(Y_{n-p}) = \frac{1}{p!} \cdot \frac{1}{(n-p)!}.$$

Olkoon sitten  $I \subset \{1, 2, \dots, n\}$ . Määritellään

$$K_I := \{x = (x_1, \dots, x_n) \in \mathbb{R}^n \mid x_i \geq 0 \text{ kaikille } i \in I \text{ ja } x_i \leq 0 \text{ kaikille } i \notin I\}.$$

Koska  $n$  alkioisella joukolla on  $2^n$  osajoukkoa (Huomautus 2.2.7), kappaleen  $V$  tilavuus saadaan summaamalla yli kaikkien  $2^n$  mahdollisen joukon  $I$ , joilla  $K_I$  sisältää joukon  $V$  pisteitä. Tässä on huomattava, että  $K_p = K_{\{1, 2, \dots, p\}}$ . Jos  $I$  sisältää  $p$  alkioita, niin symmetrian nojalla

$$\text{vol}_n(K_I \cap V) = \frac{1}{p!(n-p)!}.$$

Edelleen, jos  $I$  sisältää  $p$  alkioita, joukolle  $I$  on  $\binom{n}{p}$  mahdollisuutta. Summaamalla yli kaikkien mahdollisten joukkojen  $I$  saadaan

$$\text{vol}(V) = \sum_{p=0}^n \binom{n}{p} \frac{1}{p!(n-p)!} = \sum_{p=0}^n \binom{n}{p} \frac{1}{p!(n-p)!} \cdot \frac{n!}{n!} = \frac{1}{n!} \sum_{p=0}^n \binom{n}{p}^2$$

Lemman 2.2.9 nojalla  $\sum_{k=0}^n \binom{n}{k}^2 = \binom{2n}{n}$ , joten saadaan

$$\text{vol}(V) = \frac{1}{n!} \binom{2n}{n} = \frac{1}{n!} \cdot \frac{(2n)!}{n!(2n-n)!} = \frac{(2n)!}{n!^3}.$$

□

**Huomautus 2.3.10.** Skalaarilla  $\alpha \in \mathbb{R}_{>0}$  skaalatessa joukko  $V$  saa muodon

$$V = \left\{ x \in \mathbb{R}^n \mid \sum_{\substack{i=1 \\ x_i > 0}}^n x_i \leq \alpha \text{ ja } \sum_{\substack{i=1 \\ x_i < 0}}^n |x_i| \leq \alpha \right\}.$$

Tällöin

$$\text{vol}(V) = \frac{(2n)! \alpha^n}{n!^3}.$$

Havainnollistetaan Lemman 2.3.9 tulosta esimerkillä.

**Esimerkki 2.3.11.** Tarkastellaan avaruuden  $\mathbb{R}^2$  hilaa  $\Lambda$ ,

$$\Lambda = \left\{ \begin{pmatrix} a_1 \log 3 \\ a_2 \log 5 \end{pmatrix} \in \mathbb{R}^2 : a_1, a_2 \in \mathbb{Z} \right\},$$

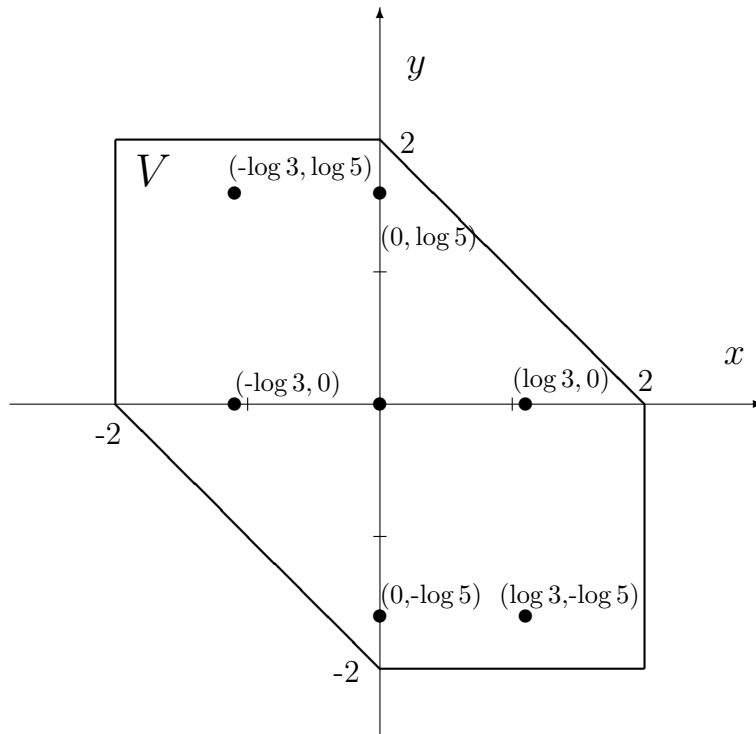
jonka (eräs) kanta on  $E$ ,

$$E = \left\{ \begin{pmatrix} \log 3 \\ 0 \end{pmatrix}, \begin{pmatrix} 0 \\ \log 5 \end{pmatrix} \right\}.$$

Näin ollen  $\det(\Lambda) = \log 3 \log 5 \approx 1,768$ . Valitaan Lemman 2.3.9 mukainen joukko  $V \subset \mathbb{R}^2$  ja skaalataan luvulla 2, jolloin Huomautuksen 2.3.10 mukaisesti  $\text{vol}(V) = \frac{(2 \cdot 2)! 2^2}{2!^3} = 12$ . Lauseen 2.3.7 epäyhtälö (2.4) saa nyt muodon

$$12 > m 4 \log 3 \log 5.$$

Epäyhtälö toteutuu arvolla  $m = 1$  muttei enää arvolla  $m = 2$ . Joukko  $V$  sisältää siis ainakin yhden nollasta eroavan hilapisteparin  $\pm v \in \Lambda$ . Itse asiassa joukko  $V$  sisältää kolme tällaista paria (kuva 1). Lause 2.3.7 antaa siis kovin “varovaisen” arvion tilanteesta.



Kuva 1: Konveksin joukon  $V$  sisään jäävä osa eräästä avaruuden  $\mathbb{R}^2$  hilasta.

**Esimerkki 2.3.12.** Esimerkki 2.3.11 voidaan helposti yleistää avaruuteen  $\mathbb{R}^n$ . Merkitään luvuilla  $p_1, \dots, p_n$   $n$ :ää ensimmäistä paritonta alkulukua. Tällöin joukko  $\Lambda_n \subset \mathbb{R}^n$ ,

$$\Lambda_n = \{(a_1 \log p_1, \dots, a_n \log p_n) \in \mathbb{R}^n : a_1, \dots, a_n \in \mathbb{Z}\}$$

muodostaa avaruuden  $\mathbb{R}^n$  hilan, jonka determinantti on

$$\det(\Lambda_n) = \log p_1 \log p_2 \cdots \log p_n = \prod_{i=1}^n \log p_i.$$

Määritellään lopuksi vielä alihila ja siihen liittyvä indeksi.

**Määritelmä 2.3.13.** Hila  $\Lambda \subset \mathbb{R}^n$  on hilan  $\Delta \subset \mathbb{R}^n$  *alihila*, jos kaikilla  $x \in \Lambda$  pätee  $x \in \Delta$ . Hiloihin  $\Lambda$  ja  $\Delta$  liittyvää lukua  $D$ ,

$$D = \frac{\det(\Lambda)}{\det(\Delta)},$$

kutsutaan *hilan  $\Lambda$  indeksiksi hilassa  $\Delta$* .

## 2.4 Ryhmistä ja niiden välisistä kuvauksista

Tarkastellaan seuraavaksi ryhmiä ja niiden ominaisuuksia. Alaluvun päätarkoituksena on selkiyttää alla olevan *abc*-osumien alarajafunktiota koskevan Lauseen 3.6.9 todistuksen ryhmäteoriaan nojaavaa osaa, joten tarkastelu keskittyy multiplikatiivisten kokonaislukujen ryhmään sekä homomorfismeihin. Yleisemmän käsityksen ryhmäteoriasta ja algebrasta saa lähteinä käytetyistä kirjoista [19, s. 11–144] ja [32, s. 1–117], joiden tuloksia ja määritelmiä on pyritty havainnollistamaan jatkon kannalta oleellisin esimerkein.

Aloitetaan aiheen käsittely laskutoimituksen ja ryhmän määrittelyllä.

**Määritelmä 2.4.1.** Joukossa  $G$  määritelty laskutoimitus  $\circ$  on funktio  $G \times G \rightarrow G$ . Merkitään näin saatavaa joukon  $G$  alkioita  $\circ(a, b) = a \circ b$ , missä  $(a, b) \in G \times G$ .

**Määritelmä 2.4.2.** Paria  $(G, \circ)$  kutsutaan *ryhmäksi*, jos laskutoimitus  $\circ$  on suljettu joukossa  $G$  ja seuraavat kolme kohtaa ovat voimassa:

- (i) kaikilla  $a, b, c \in G$  pätee  $(a \circ b) \circ c = a \circ (b \circ c)$  (liitännäisyys)
- (ii) on olemassa  $e \in G$  siten, että kaikilla  $x \in G$   $e \circ x = x \circ e = x$  (neutraalialkio)
- (iii) jokaista  $a \in G$  kohti on olemassa  $a' \in G$  siten, että  $a \circ a' = a' \circ a = e$  (käänteisalkio).

Paria  $(G, \circ)$  kutsutaan *Abelin ryhmäksi*, mikäli lisäksi on voimassa

- (iv) kaikilla  $a, b \in G$  pätee  $a \circ b = b \circ a$  (vaihdannaisuus).

**Esimerkki 2.4.3.** (i) Olkoot  $p_1, \dots, p_n$   $n$  ensimmäistä paritonta alkulukua ja olkoon  $\mathcal{Q}_n$ ,

$$\mathcal{Q}_n = \{p_1^{a_1} \cdots p_n^{a_n} \mid a_1, \dots, a_n \in \mathbb{Z}\}.$$

Pari  $(\mathcal{Q}_n, *)$ , missä  $*$  on tavallinen kertolasku, on Abelin ryhmä.

(ii) Olkoon  $\Lambda \subset \mathbb{R}^n$  hila. Tällöin  $\Lambda$  muodostaa ryhmän tavallisen yhteenlaskun suhteen.

**Määritelmä 2.4.4.** Olkoon  $n \in \mathbb{N}$ . Joukkoa  $\mathbb{Z}_n = \{0, 1, 2, \dots, n-1\}$  kutsutaan nimellä *kokonaisluvut modulo  $n$* , ja siinä määritellään modulaariset laskutoimitukset  $+_n$  ja  $*_n$  kaikilla  $a, b \in \mathbb{Z}$  asettamalla

$$a +_n b = (a + b) \pmod{n} \quad \text{ja} \quad a *_n b = (ab) \pmod{n}.$$

**Huomautus 2.4.5.** Yllä olevassa määritelmässä sekä jatkossa samaistetaan yksinkertaisuuden vuoksi kongruenssiluokat  $[k]$  ja luvut  $k$  kaikilla  $k = 0, 1, \dots, n-1$ .

**Määritelmä 2.4.6.** Olkoon  $n \in \mathbb{N}$ . Joukkoa  $\mathbb{Z}_n^* = \{x \in \mathbb{Z}_n : \text{syt}(x, n) = 1\}$  kutsutaan nimellä *multiplikatiiviset kokonaisluvut modulo  $n$*  ja siitä muodostetusta ryhmästä (engl. multiplicative group of integers modulo  $n$ ) käytetään merkintää  $(\mathbb{Z}_n^*, *_n)$ ,  $(\mathbb{Z}/n\mathbb{Z})^*$ ,  $(\mathbb{Z}/n\mathbb{Z})^\times$  tai  $U_n$  (group of units).

**Huomautus 2.4.7.** Pari  $(\mathbb{Z}_n^*, *_n)$  on Abelin ryhmä kaikilla  $n \in \mathbb{N}$  [32, s. 98].

**Esimerkki 2.4.8.** Arvoilla  $n = 2, 3, 4, 8$  ja  $16$  saadaan joukot

$$\mathbb{Z}_2^* = \{1\}, \quad \mathbb{Z}_3^* = \{1, 2\}, \quad \mathbb{Z}_4^* = \{1, 3\}, \quad \mathbb{Z}_8^* = \{1, 3, 5, 7\}, \quad \mathbb{Z}_{16}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}.$$

Tarkastellaan seuraavaksi ryhmän alkion potensseja sekä ryhmän virittämistä.

**Määritelmä 2.4.9.** Olkoon  $(G, \circ)$  ryhmä ja  $n \in \mathbb{N}$ . Alkion  $g \in G$   $n$ :näs potenssi määritellään induktiivisesti asettamalla

$$\begin{cases} g^0 = e \\ g^n = g \circ g^{n-1} \\ g^{-n} = (g^{-1})^n = g^{-1} \circ g^{-n+1} \end{cases}$$

missä  $e$  on ryhmän  $G$  neutraalialkio ja  $g^{-1}$  alkion  $g$  käänteisalkio.

**Määritelmä 2.4.10.** Olkoon  $(G, \circ)$  ryhmä ja  $H \subseteq G$  sekä  $g \in G$ . Jos pari  $(H, \circ)$  on ryhmä, niin sitä kutsutaan ryhmän  $G$  aliryhmäksi. Jos edelleen

$$H = \{g^n : n \in \mathbb{Z}\},$$

niin tällöin aliryhmää  $H$  kutsutaan alkion  $g$  virittämäksi ryhmän  $G$  sykliseksi aliryhmäksi ja käytetään merkintää  $H = \langle g \rangle$ .

**Huomautus 2.4.11.** Jos on olemassa koko ryhmän  $G$  virittävä alkio  $g \in G$ , toisin sanoen  $\langle g \rangle = G$ , niin tällöin alkioita  $g$  kutsutaan ryhmän  $G$  virittäjäksi ja ryhmää  $G$  sykliseksi.

**Esimerkki 2.4.12.** Ryhmät  $(\mathbb{Z}_2^*, *_2)$  ja  $(\mathbb{Z}_4^*, *_4)$  ovat syklisiä, sillä  $\langle 1 \rangle = \mathbb{Z}_2^*$  ja  $\langle 3 \rangle = \mathbb{Z}_4^*$ .

Kaikki ryhmät  $(\mathbb{Z}_n^*, *_n)$  eivät kuitenkaan ole syklisiä [32, s. 106].

**Lause 2.4.13.** Olkoon  $m \in \mathbb{N}$ . Ryhmä  $(\mathbb{Z}_{2^m}^*, *_2^m)$  on syklinen jos ja vain jos  $m = 1$  tai  $m = 2$ .

*Todistus.* Esimerkin 2.4.12 nojalla riittää osoittaa että  $(\mathbb{Z}_{2^m}^*, *_2^m)$  ei ole syklinen, kun  $m \geq 3$ . Osoitetaan tämä induktiolla luvun  $m$  suhteen näyttämällä, että ryhmässä  $(\mathbb{Z}_{2^m}^*, *_2^m)$  ei ole kertalukua  $\phi(2^m) = 2^{m-1}$  olevaa alkioita vaan

$$a^{2^{m-2}} \equiv 1 \pmod{2^m} \tag{2.5}$$

kaikilla parittomilla luvuilla  $a \in \mathbb{Z}$ .

1°) Koska  $a = 2b + 1$  jollekin  $b \in \mathbb{Z}$ , saadaan arvolla  $m = 3$

$$a^2 = 4b(b+1) + 1 \equiv 1 \pmod{8},$$

sillä toinen luvuista  $b$  ja  $b+1$  on parillinen. Kongruenssi (2.5) on siis voimassa arvolla  $m = 3$ .

2°) Oletetaan, että väite pätee arvolla  $m = k \geq 1$ . Tällöin kaikilla parittomilla luvuilla  $a \in \mathbb{Z}$  on voimassa yhtälö

$$a^{2^{k-2}} = 1 + h2^k$$

jollakin  $h \in \mathbb{Z}$ . Korottamalla yhtälö puolittain toiseen potenssiin saadaan

$$a^{2^{(k+1)-2}} = (1 + h2^k)^2 = 1 + h2^{k+1} + h^2 2^{2k} = 1 + 2^{k+1}(h + h^2 2^{k-1}) \equiv 1 \pmod{2^{k+1}},$$

joten väite on voimassa myös arvolla  $m = k+1$ . Kohtien 1°) ja 2°) sekä induktioperiaatteen nojalla väite pätee kaikilla  $m \geq 3$ .  $\square$



Seuraava tulos perustuu kirjaan [32, s. 107–108].

**Lemma 2.4.14.** *Olkoon  $m \in \mathbb{N}_{\geq 3}$ . Tällöin  $\mathbb{Z}_{2^m}^* = \{\pm 3^i : 0 \leq i < 2^{m-2}\}$ .*

*Todistus.* Olkoon  $k$  alkion 3 kertaluku joukossa  $\mathbb{Z}_{2^m}^*$ . Eulerin lauseen nojalla  $k$  jakaa luvun  $\phi(2^m) = 2^{m-1}$ , ts.  $k = 2^j$  jollekin  $j \leq m - 1$ . Lauseen 2.4.13 nojalla joukossa  $\mathbb{Z}_{2^m}^*$  ei ole kertalukua  $2^{m-1}$  olevaa alkioita, joten  $j \leq m - 2$ . Huomautusta 2.1.21 arvolla  $n = m - 3$  soveltamalla saadaan

$$2^{m-3} \mid 3^{2^{m-3}} - 1,$$

toisin sanoen  $3^{2^{m-3}} \not\equiv 1 \pmod{2^m}$ , jolloin  $j > m - 3$ . Siispä  $j = 2^{m-2}$ . Näin ollen alkiolla 3 on  $2^{m-2}$  toisistaan eroavaa potenssia  $3^i$  ( $0 \leq i < 2^{m-2}$ ) joukossa  $\mathbb{Z}_{2^m}^*$ . Potenssit  $3^i$  antavat kaikki joukon  $\mathbb{Z}_{2^m}^*$  lukujen 1 tai 3 kanssa kongruentit alkioit modulo 8, kun taas potenssit  $-3^i$  antavat joukon  $\mathbb{Z}_{2^m}^*$  lukujen  $-1$  ja  $-3$  kanssa kongruentit alkioit modulo 8. Näin ollen kaikilla joukon  $\mathbb{Z}_{2^m}^*$  alkiolla on esitysmuoto  $\pm 3^i$  jollekin  $i = 0, 1, \dots, 2^{m-2} - 1$ .  $\square$

**Huomautus 2.4.15.** Vastaavanlaisella päättelyllä voidaan osoittaa, että kaikilla  $m \in \mathbb{N}_{\geq 3}$  pätee  $\mathbb{Z}_{2^m}^* = \{\pm 5^i : 0 \leq i < 2^{m-2}\}$  [32, s. 107–108]. Tällöin potenssit  $5^i$  antavat kaikki joukon  $\mathbb{Z}_{2^m}^*$  luvun 1 kanssa kongruentit alkioit modulo 4 ja potenssit  $-5^i$  antavat joukon  $\mathbb{Z}_{2^m}^*$  luvun  $-1$  kanssa kongruentit alkioit modulo 4.

Koska  $3 \equiv -1 \pmod{4}$ , Lemman 2.4.14 ja Huomautuksen 2.4.15 nojalla saadaan:

**Lause 2.4.16.** *Olkoon  $m \in \mathbb{N}_{\geq 3}$ . Tällöin  $\mathbb{Z}_{2^m}^* = \{3^i 5^j : 0 \leq i, j < 2^{m-2}\}$ .*

Havainnollistetaan tilannetta esimerkillä.

**Esimerkki 2.4.17.** Tarkastellaan ryhmää  $(\mathbb{Z}_{2^4}^*, *_2^4)$ , jolloin  $\mathbb{Z}_{2^4}^* = \{1, 3, 5, 7, 9, 11, 13, 15\}$ . Luvut saadaan edellisen lauseen nojalla tulon  $3^i 5^j$  moduloista seuraavasti:

$$\begin{aligned} 3^4 * 5^0 &= 81 \equiv 1 \pmod{16} \\ 3^1 * 5^0 &\equiv 3 \pmod{16} \\ 3^0 * 5^1 &\equiv 5 \pmod{16} \\ 3^1 * 5^3 &= 375 \equiv 7 \pmod{16} \\ 3^2 * 5^0 &\equiv 9 \pmod{16} \\ 3^3 * 5^0 &= 27 \equiv 11 \pmod{16} \\ 3^0 * 5^3 &= 125 \equiv 13 \pmod{16} \\ 3^1 * 5^1 &\equiv 15 \pmod{16} \end{aligned}$$

Siirrytään sitten tarkastelemaan kahden ryhmän välisiä kuvauksia.

**Määritelmä 2.4.18.** Olkoot  $(G, \circ)$  ja  $(G', \bullet)$  ryhmiä. Funktiota  $f : G \rightarrow G'$  kutsutaan *homomorfismiksi* tai *ryhmähomomorfismiksi*, mikäli kaikilla  $a, b \in G$  pätee

$$f(a \circ b) = f(a) \bullet f(b).$$

Seuraavasta tuloksesta nähdään, että homomorfismi säilyttää joitain ryhmän rakenteellisia ominaisuuksia [19, s. 128–129]

**Lause 2.4.19.** Olkoon  $f : G \rightarrow G'$  homomorfismi.

- (i) Jos  $e$  on ryhmän  $G$  neutraalialkio, niin  $f(e) = e'$  on ryhmän  $G'$  neutraalialkio.
- (ii) Jos  $a \in G$ , niin  $f(a^{-1}) = f(a)^{-1}$ .
- (iii) Jos  $H$  on ryhmän  $G$  aliryhmä, niin  $f(H)$  on ryhmän  $G'$  aliryhmä.
- (iv) Jos  $K'$  on ryhmän  $G'$  aliryhmä, niin  $f^{-1}(K')$  on ryhmän  $G$  aliryhmä.

**Esimerkki 2.4.20.** (i) Olkoon  $n \in \mathbb{N}$ . Tällöin funktio  $f : \mathbb{Z} \rightarrow \mathbb{Z}_n$ , joka kuvaa luvun sen jakojäännökselle modulo  $n$ , on homomorfismi [19, s. 127–128].

(ii) Esimerkissä 2.4.3 mainitulta  $n$ :stä ensimmäisestä parittomasta alkuluvusta muodostetulta ryhmältä  $(\mathcal{Q}_n, *)$  voidaan muodostaa homomorfismi ryhmälle  $(\mathbb{R}^n, +)$  asettamalla  $\varphi_n : \mathcal{Q}_n \rightarrow \mathbb{R}^n$ ,

$$\varphi_n(p_1^{a_1} \cdots p_n^{a_n}) = (a_1 \log p_1, \dots, a_n \log p_n).$$

Näin muodostettu homomorfismi  $\varphi_n$  on *injektiivinen*.

(iii) Olkoot  $n, m \in \mathbb{N}_{\geq 2}$ . Kuvaus  $g$  ryhmältä  $(\mathcal{Q}_n, *)$  ryhmälle  $(\mathbb{Z}_{2^m}, *_m)$  on homomorfismi, kun tulkitaan  $q \in \mathcal{Q}_n$  osamääränä  $q = \frac{b}{c}$ ,  $\text{syt}(b, c) = 1$ , ja asetetaan

$$g(q) = b *_m c = (bc) \pmod{2^m}.$$

Lauseen 2.4.16 nojalla näin muodostettu homomorfismi  $g$  on *surjektiivinen*.

**Määritelmä 2.4.21.** Jos kahden ryhmän  $G$  ja  $G'$  välinen funktio  $h : G \rightarrow G'$  on homomorfismi ja bijektio, sitä sanotaan *isomorfismiksi*. Mikäli tällainen isomorfismi on olemassa, ryhmiä  $G$  ja  $G'$  sanotaan *isomorfisiksi*.

Jokaisen homomorfismin kautta saadaan neutraalialkiolle kuvautuva ydin.

**Määritelmä 2.4.22.** Olkoon  $f : G \rightarrow G'$  homomorfismi ryhmältä  $(G, \circ)$  ryhmälle  $(G', \bullet)$  ja olkoon  $e'$  ryhmän  $G'$  neutraalialkio. Joukkoa

$$\ker f = f^{-1}(\{e'\}) = \{x \in G : f(x) = e'\}$$

kutsutaan homomorfismin  $f$  *ytimeksi* (engl. *kernel*).

Aliryhmiin liittyvillä sivuluokilla on yhteys homomorfismeihin.

**Määritelmä 2.4.23.** Olkoon  $(G, \circ)$  ryhmä,  $(H, \circ)$  sen aliryhmä ja  $g \in G$ . Joukkoa

$$H \circ g = \{h \circ g : h \in H\}$$

sanotaan *alkion  $g$  määräämäksi oikeanpuoleiseksi sivuluokaksi* (tai jäännösluokaksi) modulo  $H$  (engl. *right coset*). Vastaavasti, joukkoa

$$g \circ H = \{g \circ h : h \in H\}$$

sanotaan *alkion  $g$  määräämäksi vasemmanpuoleiseksi sivuluokaksi modulo  $H$*  (engl. *left coset*). Ryhmän  $(G, \circ)$  ollessa vaihdannainen (Abelin ryhmä) puhutaan vain *alkion  $g$  määräämästä sivuluokasta modulo  $H$* .

**Huomautus 2.4.24.** Sivuluokat voidaan määritellä myös kongruenssirelaation avulla:

$$a \equiv b \pmod{H}, \text{ jos ja vain jos } a \circ b^{-1} \in H.$$

Näin myös nimitykset “jäännösluokka” ja “modulo  $H$ ” ovat perusteltuja. Tässä ekvivalenssiluokat ovat edellä määritellyt sivuluokat.

**Esimerkki 2.4.25.** Tarkastellaan ryhmää  $(\mathbb{Z}_{23}, *_23)$  ja sen triviaalia aliryhmää  $(\{1\}, *_23)$ . Löydetään neljä sivuluokkaa:

$$\begin{aligned} \{1\} &= \{1\} \\ 3 *_23 \{1\} &= \{3\} \\ 5 *_23 \{1\} &= \{5\} \\ 7 *_23 \{1\} &= \{7\} \end{aligned}$$

Koska  $(\mathbb{Z}_{23}, *_23)$  on Abelin ryhmä, vasemman- ja oikeanpuoleiset sivuluokat ovat samat. Lisäksi koska sivuluokkien yhdisteenä saadaan  $\mathbb{Z}_{23}^*$ , yllä on esitetty kaikki mahdolliset *sivuluokat modulo*  $\{1\}$ .

**Määritelmä 2.4.26.** Olkoon  $(G, \circ)$  ryhmä ja ryhmä  $(N, \circ)$  sen aliryhmä. Ryhmä  $(N, \circ)$  on *normaali aliryhmä*, mikäli kaikilla  $g \in G$  pätee

$$N \circ g = g \circ N.$$

**Huomautus 2.4.27.** Kaikki Abelin ryhmät ovat normaaleja [19, s. 132]. Lisäksi joukko-homomorfismin  $f : G \rightarrow G'$  muodostama aliryhmä  $\ker f \subseteq G$  on normaali.

**Määritelmä 2.4.28.** Olkoon  $(G, \circ)$  ryhmä ja  $(N, \circ)$  sen normaali aliryhmä. Sivuluokkaryhmää  $G/N$  kutsutaan tällöin *aliryhmän*  $(N, \circ)$  *määräämäksi ryhmän*  $(G, \circ)$  *tekijäryhmäksi* (engl. *factor group* tai *quotient group*).

**Esimerkki 2.4.29.** Esimerkin 2.4.25 tapauksessa muodostettiin aliryhmän  $(\{1\}, *_23)$  määräämä ryhmän  $(\mathbb{Z}_{23}^*, *_23)$  tekijäryhmä

$$(\mathbb{Z}_{23}^*/\{1\}, *_23) = \{\{1\}, \{3\}, \{5\}, \{7\}\}.$$

Homomorfismeista voidaan muodostaa tekijäryhmiä seuraavasti [19, s. 137].

**Lause 2.4.30.** Olkoon  $f : G \rightarrow G'$  homomorfismi ytimenään  $\ker f = H$ . Ryhmän  $H$  sivuluokat muodostavat tekijäryhmän  $G/H$ , missä

$$(aH)(bH) = (ab)H$$

kaikilla  $a, b \in G$ . Lisäksi kuvaus  $\mu : G/H \rightarrow f(G)$  on isomorfismi.

**Esimerkki 2.4.31.** Tarkastellaan vielä Esimerkin 2.4.20 kohdassa (iii) ryhmältä  $(\mathcal{Q}_n, *)$  ryhmälle  $(\mathbb{Z}_{2^m}, *_2m)$  muodostettua homomorfismia  $g$ . Homomorfismin ytimeksi saadaan

$$\ker g = \left\{ \frac{b}{c} \in \mathcal{Q}_n \mid bc \equiv 1 \pmod{2^m}, \text{syt}(b, c) = 1 \right\},$$

toisin sanoen kaikki sellaiset alkioit, jotka ovat suhteellisia alkulukuja ja toistensa käänteisalkioita modulo  $2^m$ . Tarkastelemalla tilannetta sivuluokkien kannalta ja Huomautusta 2.4.24 soveltamalla voidaan homomorfismin ytimelle käyttää merkintää

$$\ker g = \mathcal{Q}_{n,m} = \left\{ \frac{b}{c} \in \mathcal{Q}_n \mid b \equiv c \pmod{2^m}, \text{syt}(b, c) = 1 \right\}.$$

Lisäksi koska  $g(\mathcal{Q}_n) = \mathbb{Z}_{2^m}$  Lauseen 2.4.16 nojalla, Lauseen 2.4.30 mukaan on siten olemassa isomorfismi

$$\mu : (\mathcal{Q}_n / \mathcal{Q}_{n,m}, *) \rightarrow (\mathbb{Z}_{2^m}, *_{2^m}).$$

Tarkastellaan lopuksi ryhmän alkioiden lukumäärään liittyviä tuloksia.

**Määritelmä 2.4.32.** Olkoon  $(G, \circ)$  ryhmä. Ryhmän *kertaluvulla*  $|G|$  tarkoitetaan ryhmän  $(G, \circ)$  alkioiden lukumäärää.

**Esimerkki 2.4.33.** Ryhmän  $(\mathbb{Z}_n^*, *_n)$  kertaluku saadaan suoraan Eulerin funktion arvona. Tapauksessa  $n = 2^m$  saadaan siten

$$|\mathbb{Z}_{2^m}^*| = \phi(2^m) = 2^m - 2^{m-1} = 2^{m-1}.$$

Esimerkin 2.4.31 nojalla ryhmien  $(\mathcal{Q}_n / \mathcal{Q}_{n,m}, *)$  ja  $(\mathbb{Z}_{2^m}, *_{2^m})$  välillä on olemassa bijektio, joten näin ollen

$$|\mathcal{Q}_n / \mathcal{Q}_{n,m}| = |\mathbb{Z}_{2^m}^*| = 2^{m-1}.$$

**Lause 2.4.34** (Lagrange). *Olkoon  $G$  äärellinen ryhmä ja  $H$  sen aliryhmä. Tällöin ryhmän  $H$  kertaluku jakaa ryhmän  $G$  kertaluvun.*

**Määritelmä 2.4.35.** Olkoon  $G$  ryhmä ja  $H$  sen aliryhmä. Ryhmän  $H$  vasemmanpuoleisten sivuluokkien lukumäärää ryhmässä  $G$  kutsutaan *ryhmän  $H$  indeksiksi ryhmässä  $G$*  ja merkitään  $(G : H)$ .

**Huomautus 2.4.36.** Tarkasteltava ryhmä  $G$  voi olla äärellinen tai ääretön. Jos  $G$  on äärellinen, niin silloin myös  $(G : H)$  on äärellinen ja Lagrangen lauseen (Lause 2.4.34) nojalla

$$(G : H) = \frac{|G|}{|H|}.$$

Jos taas  $G$  on ääretön, niin  $(G : H)$  joko on äärellinen tai päädytään vertailemaan kardinaaliteetteja.

**Huomautus 2.4.37.** Jos  $H$  on ryhmän  $G$  normaali aliryhmä, niin tällöin  $|G/H| = (G : H)$ .

**Esimerkki 2.4.38.** Tarkastellaan indeksiä vielä hilojen tapauksessa. Olkoon  $\Lambda \subset \mathbb{R}^n$  hilan  $\Delta \subset \mathbb{R}^n$  alihila. Määritelmän 2.3.13 nojalla hiloille pätee

$$(\Delta : \Lambda) = \frac{\det(\Lambda)}{\det(\Delta)}.$$

Jos  $\Lambda$  muodostaa ryhmän  $\Delta$  normaalin aliryhmän, niin tällöin Huomautuksen 2.4.37 nojalla

$$|\Delta / \Lambda| = \frac{\det(\Lambda)}{\det(\Delta)}.$$

## 2.5 Polynomeista

*Abc*-konjektuurin polynomivastineen ymmärtämiseksi palautetaan mieleen muutamia polynomeihin liittyviä tuloksia. Seuraavassa esityksessä on nähtävissä jo polynomien ja kokonaislukujen välistä yhteyttä, mitä *Abc*-konjektuurikin havainnollistaa.

Aloitetaan polynomien algebrallisesta määritelmästä [19, s. 199].

**Määritelmä 2.5.1.** Olkoon  $R$  rengas. Ääretöntä summaa  $f$ ,

$$f(x) = \sum_{i=0}^{\infty} a_i x^i = a_0 + a_1 x + \cdots + a_n x^n + \cdots, \quad (2.6)$$

missä  $a_i \in R$  ja  $a_i \neq 0$  vain äärellisellä määrällä indeksejä  $i$ , kutsutaan *polynomiksi*  $f$ , jonka kertoimet kuuluvat renkaaseen  $R$ . Lukuja  $a_i$  kutsutaan polynomin  $f$  kertoimiksi. Suurinta lukua  $i$ , jolla  $a_i \neq 0$ , kutsutaan *polynomin  $f$  asteeksi*  $\deg f$ .

**Huomautus 2.5.2.** Mikäli  $a_i = 0$  kaikilla  $i > n$ , summalle (2.6) käytetään yksinkertaisempaa esitystä

$$f(x) = \sum_{i=0}^n a_i x^i = a_0 + a_1 x + \cdots + a_n x^n.$$

Yleisesti yhden muuttujan  $x$  polynomien renkaasta käytetään merkintää  $R[x]$ ,

$$R[x] = \{a_0 + a_1 x + a_2 x^2 \cdots + a_n x^n \mid n \geq 0, a_i \in R \text{ kaikilla } i = 0, \dots, n\}.$$

Tyypillisesti tarkastelu rajoittuu renkaaseen  $\mathbb{C}[x]$  tai  $\mathbb{Z}[x]$ .

**Lemma 2.5.3.** *Olko  $f, g \in \mathbb{C}[x]$  nollasta eroavia polynomeja. Tällöin niiden asteille on voimassa*

$$\begin{aligned} \deg(f + g) &\leq \max\{\deg f, \deg g\}, \\ \deg(fg) &= \deg f + \deg g. \end{aligned}$$

Polynomien tarkastelussa keskitytään usein nollakohtiin [37, s. 111].

**Määritelmä 2.5.4.** Olkoon  $f \in \mathbb{C}[x]$  polynomi. Lukua  $\alpha \in \mathbb{C}$  kutsutaan polynomin  $f$  juureksi, mikäli  $f(\alpha) = 0$ .

Juurten avulla polynomi voidaan esittää tekijämuodossa [37, s. 165]. Pidetään tässä tunnettuna Algebran peruslausetta, jonka mukaan  $n$ -asteisen polynomin  $f \in \mathbb{C}[x]$  juurten lukumäärä on monikerrat mukaanlukien sama kuin polynomin aste.

**Lause 2.5.5.** *Olkoon  $f \in \mathbb{C}[x]$  nollasta poikkeava polynomi. Tällöin  $f$  voidaan esittää muodossa*

$$f(x) = c \prod_{j=1}^r (x - \alpha_j)^{m_j} = c(x - \alpha_1)^{m_1} \cdots (x - \alpha_r)^{m_r},$$

missä  $c \in \mathbb{C} \setminus \{0\}$  ja  $\alpha_j$  ovat toisistaan eroavia polynomin  $f$  juuria moninkertoinaan  $m_j$  kaikilla  $j = 1, \dots, r$ . Erityisesti, jos  $f(\alpha) = 0$ , niin  $f$  voidaan esittää muodossa

$$f(x) = (x - \alpha)^{m(\alpha)} g(x),$$

missä  $g(\alpha) \neq 0$  ja  $m(\alpha)$  on juuren  $\alpha$  moninkerta.

**Huomautus 2.5.6.** Jos  $m(\alpha) = 1$ , puhutaan polynomin  $f$  yksinkertaisesta juuresta. Jos taas  $m(\alpha) \geq 2$ , on kyseessä polynomin  $f$  moninkertainen juuri.

Lause 2.5.5 perustuu jakoyhtälön soveltamiseen renkaassa  $\mathbb{C}[x]$ . Jos nimittäin polynomeille  $f, g \in \mathbb{C}[x]$  pätee  $f \mid g$ , niin tällöin on olemassa vakiosta eroava  $h \in \mathbb{C}[x]$  siten, että

$$g = fh.$$

Koska ensimmäisen asteen polynomit ovat jaottomia renkaassa  $\mathbb{C}[x]$ , voidaan Lauseen 2.5.5 antamaa faktorointia hyödyntää seuraavassa määritelmässä [37, s. 119].

**Määritelmä 2.5.7.** Olkoot  $f, g \in \mathbb{C}[x]$  nollasta poikkeavia polynomeja. Polynomien  $f$  ja  $g$  suurimmalla yhteisellä tekijällä  $\text{sy}(f, g)$  tarkoitetaan polynomia  $h$ , jolle pätee  $h \mid f$  ja  $h \mid g$ .

**Huomautus 2.5.8.** Jos on olemassa  $h_1 \in \mathbb{C}[x]$  siten, että Määritelmän 2.5.7 funktioille  $f$  ja  $g$  pätee  $h_1 \mid f$  ja  $h_1 \mid g$ , niin tällöin  $h_1 \mid \text{sy}(f, g) = h$ .

Tarkastellaan lopuksi vielä syklotomista teoriaa pohjautuen kirjaan [65, s. 82–91].

**Määritelmä 2.5.9.** Lukua  $\zeta \in \mathbb{C}$  kutsutaan  $n$ :neksi ykkösen juureksi (engl.  $n$ -th root of unity), mikäli luvulle  $n \in \mathbb{N}$  pätee  $\zeta^n = 1$ . Mikäli  $n$  on pienin sellainen luku, jolle  $\zeta^n = 1$ , lukua  $\zeta \in \mathbb{C}$  kutsutaan *primitiiviseksi  $n$ :neksi ykkösen juureksi*

**Huomautus 2.5.10.** Kaikkien  $n$ :nsien ykkösen juurten joukko  $\mu_n$  koostuu pisteistä

$$\mu_n = \left\{ e^{\frac{2\pi ij}{n}} = \cos \frac{2\pi j}{n} + i \sin \frac{2\pi j}{n} : j = 0, 1, \dots, n-1 \right\}.$$

Primitiivisten  $n$ :nsien ykkösen juurten tapauksessa lisätään vielä oletus  $\text{sy}(j, n) = 1$ . Koska pisteet jakavat kompleksitason yksikköympyrän  $n$ :ään yhtä suureen osaan, kutsutaan ykkösen juurten teoriaa ympyrän jakamista tarkoittavaksi *syklotomiseksi* teoriaksi.

Primitiivisten ykkösen juurten avulla määritellään syklotomiset polynomit.

**Määritelmä 2.5.11.** Olkoon  $n \in \mathbb{N}$ . Tällöin  $n$ :s *syklotominen polynomi*  $\Phi_n \in \mathbb{C}[x]$  määritellään induktiivisesti asettamalla  $\Phi_1(x) = x - 1$  ja arvoilla  $n \geq 2$

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{d \mid n} \Phi_d(x)},$$

missä  $d$  käy läpi kaikki luvun  $n$  tekijät pois lukien luvun  $d = n$ .

Voidaan osoittaa, että polynomin  $\Phi_n$  kertoimet ovat kokonaislukuja kaikilla  $n \in \mathbb{N}$ . Mikäli jätetään pois primitiivisyysehto, Huomatukseen 2.5.10 perustuen voidaan osoittaa seuraava myöhemmin tarvittava tulos:

**Lemma 2.5.12.** *Olkoon  $n \in \mathbb{N}$  pariton. Tällöin polynomi*

$$x^n - 1 = \prod_{\zeta \in \{\mu_0, \dots, \mu_n\}} (x - \zeta)$$

*voidaan esittää muodossa*

$$x^n - 1 = (x - 1) \prod_{j=1}^{\frac{n-1}{2}} \left( x^2 - 2 \cos \left( \frac{2\pi j}{n} \right) x + 1 \right).$$

## 2.6 Elliptisistä käyristä

Elliptisiin käyriin liittyvä teoria on hyvin laaja. Tässä alaluvussa käydään läpi vain jatkossa esitettävän Szpiron konjektuurin kannalta oleellisia tuloksia, mistä johtuen kerroinkuntana toimii rationaaliluvut  $\mathbb{Q}$ . Syvällisemmän käsityksen aiheesta saa kirjasta [59], johon alaluku pohjautuu.

**Määritelmä 2.6.1.** Olkoot  $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$ . Weierstrassin yhtälön

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \quad (2.7)$$

avulla määriteltyä käyrää  $E$  kutsutaan *elliptiseksi käyräksi*.

**Määritelmä 2.6.2.** Elliptisen käyrän *diskriminantti* on luku

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,$$

missä luvut  $b_2, b_4, b_6$  ja  $b_8$  saadaan yhtälöistä

$$\begin{aligned} b_2 &= a_1^2 + 4a_2 \\ b_4 &= a_1a_3 + 2a_4 \\ b_6 &= a_3^2 + 4a_6 \\ b_8 &= a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2. \end{aligned}$$

**Huomautus 2.6.3.** Käyttämällä lisäksi merkintöjä

$$c_4 = b_2^2 - 24b_4 \quad \text{ja} \quad c_6 = -b_2^3 + 36b_2b_4 - 216b_6,$$

voidaan kuvata elliptisen käyrän geometrista luonnetta. Nimittäin

- (i)  $\Delta \neq 0$ , jos ja vain jos käyrällä ei ole singulaarisia pisteitä, ts. ei ole sellaisia pisteitä  $(x_0, y_0) \in \mathbb{R}^2$ , jotka toteuttavat elliptisestä käyrästä muodostetulla funktiolla  $f$ ,  $f(x, y) = 0$ , ehdon

$$\frac{\partial f(x_0, y_0)}{\partial x} = \frac{\partial f(x_0, y_0)}{\partial y} = 0.$$

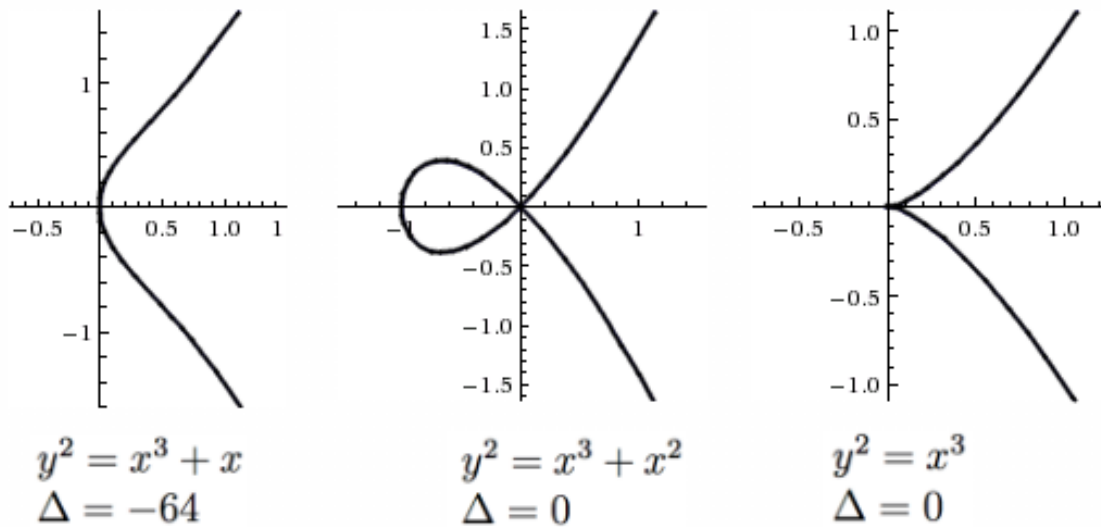
- (ii)  $\Delta = 0$  ja  $c_4 \neq 0$ , jos ja vain jos käyrällä on singulaarinen piste, jossa käyrälle voidaan piirtää kaksi toisistaan eroavaa tangenttia (engl. node).
- (iii)  $\Delta = c_4 = 0$ , jos ja vain jos käyrällä on singulaarinen piste, jossa käyrälle voidaan piirtää vain yksi tangentti (engl. cusp).

Tapauksissa (ii) ja (iii) käyrällä on vain yksi singulaarinen piste. Intuitiivisesti singulaarisella pisteellä tarkoitetaan pistettä, jossa käyrällä on solmukohta tai jossa käyrä ei ole sileä, ks. Kuva 2. Vain ehdon (i) toteuttavista ei-singulaarisista yhtälön (2.7) avulla määritellyistä käyristä käytetään nimitystä elliptinen käyrä.

**Huomautus 2.6.4.** Mikäli kerroinkunnan karakteristika on erisuuri kuin 2 tai 3, kuten joukon  $\mathbb{Q}$  tapauksessa, yhtälön (2.7) avulla määritetty elliptinen käyrä voidaan muuttujanvaihtojen avulla esittää muodossa

$$E : y^2 = x^3 + Ax + B,$$

johon monissa sovelluksissa implisiittisesti viitataan. Tällöin  $\Delta = -16(4A^3 + 27B^2)$ .



Kuva 2: Elliptinen käyrä ja kaksi singulaarista käyrää.

Elliptisiin käyriin liittyvillä luvuilla on seuraavanlainen yhteys.

**Lemma 2.6.5.** *Edellä olevilla merkinnöillä pätee*

(i)  $4b_8 = b_2b_6 - b_4^2$

(ii)  $1728 \cdot \Delta = c_4^3 - c_6^2$ .

*Todistus.* Suoralla laskulla saadaan

$$\begin{aligned} b_2b_6 - b_4^2 &= a_1^2a_3^2 + 4a_1^2a_6 + 4a_2a_3^2 + 16a_2a_6 - (a_1^2a_3^2 + 4a_1a_3a_4 + 4a_4^2) \\ &= 4a_1^2a_6 - 4a_1a_3a_4 + 16a_2a_6 + 4a_2a_3^2 - 4a_4^2 = 4b_8. \end{aligned}$$

sekä

$$\begin{aligned} c_4^3 - c_6^2 &= (b_2^6 - 72b_2^4b_4 + 1728b_2^2b_4^2 - 13824b_4^3) \\ &\quad - (b_2^6 - 72b_2^4b_4 + 432b_2^3b_6 + 1296b_2^2b_4^2 - 15552b_2b_4b_6 + 46656b_6^2) \\ &= 432b_2^2b_4^2 - 432b_2^3b_6 - 13824b_4^3 + 15552b_2b_4b_6 - 46656b_6^2 \\ &= 432(-b_2^2(b_2b_6 - b_4^2)) - 1728(8b_4^3) + 1728(9b_2b_4b_6) - 1728(27b_6^2), \end{aligned}$$

mistä väite seuraa edellisen yhtäsuuruusketjun nojalla. □

Havainnollistetaan tilannetta esimerkillä.

**Esimerkki 2.6.6.** Olkoot  $a, b, c \in \mathbb{Z}$ ,  $abc \neq 0$ . Muodostetaan elliptinen käyrä  $E$  yhtälöllä

$$E : y^2 = x(x - a)(x + b) = x^3 + (b - a)x^2 - abx.$$

Tällöin edellisillä merkinnöillä

$$b_2 = 4(b - a), \quad b_4 = -2ab, \quad b_6 = 0, \quad b_8 = -(ab)^2,$$



jolloin diskriminantiksi saadaan

$$\begin{aligned}\Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 = 16(a^2 - 2ab + b^2)a^2 b^2 + 64a^3 b^3 \\ &= 16(a^4 b^2 - 2a^3 b^3 + a^2 b^4 + 4a^3 b^3) = 16(a^4 b^2 + 2a^3 b^3 + a^2 b^4) \\ &= 16(ab(a+b))^2\end{aligned}$$

ja edelleen

$$\begin{aligned}c_4 &= b_2^2 - 24b_4 = 16(a^2 - 2ab + b^2) + 16(3ab) \\ &= 16(a^2 + ab + b^2), \\ c_6 &= -b_2^3 + 36b_2 b_4 - 216b_6 = -64(b-a)(a^2 - 2ab + b^2) - 288(b-a)(ab) \\ &= -32(b-a)(2a^2 - 4ab + 2b^2 + 9ab) = -32(b-a)(2a^2 + 5ab + 2b^2) \\ &= -32(b-a)(a+2b)(2a+b).\end{aligned}$$

**Määritelmä 2.6.7.** Elliptisen käyrän  $E$  yhtälöä (2.7) kutsutaan *minimaalimalliksi*, mikäli  $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$  ja  $|\Delta|$  on minimaalinen. Tällöin diskriminanttia  $\Delta$  kutsutaan käyrän  $E$  *minimaalidiskriminantiksi* ja siitä voidaan käyttää selkiyttävää merkintää  $\Delta_{min}$ .

Minimaalimallin tapauksessa siis  $c_4, c_6, \Delta \in \mathbb{Z}$ . Jokaisella elliptisellä käyrällä on minimaalimalli [59, s. 186]. Minimaalimallin muodostamista helpottaa seuraava tulos [46, s. 7]:

**Lemma 2.6.8.** *Olkoot  $a, b, c \in \mathbb{Z} \setminus \{0\}$  siten, että ne toteuttavat ehdot*

$$a + b + c = 0, \quad a \equiv -1 \pmod{4}, \quad 16 \mid b.$$

*Tällöin niiden avulla voidaan muodostaa minimaalimalli  $E_{abc}$  asettamalla*

$$E_{abc} : y^2 + xy = x^3 + \frac{b-a-1}{4}x^2 - \frac{ab}{16}x.$$

**Huomautus 2.6.9.** Lemman 2.6.8 tapauksessa  $b_2 = b-a$ ,  $b_4 = -\frac{ab}{8}$ ,  $b_6 = 0$  ja  $b_8 = -(\frac{ab}{16})^2$ , jolloin

$$\begin{aligned}\Delta &= -b_2^2 b_8 - 8b_4^3 - 27b_6^2 + 9b_2 b_4 b_6 = (b-a)^2 \left(\frac{ab}{16}\right)^2 + \left(\frac{a^3 b^3}{64}\right) \\ &= \left(\frac{ab}{16}\right)^2 (b^2 - 2ab + a^2 + 4ab) = \left(\frac{ab}{16}\right)^2 (b+a)^2 = \left(\frac{ab(b+a)}{16}\right)^2 = \left(\frac{abc}{16}\right)^2\end{aligned}$$

ja

$$c_4 = b_2^2 - 24b_4 = (b-a)^2 + 3ab = b^2 + ab + a^2 = (b+a)^2 - ab = c^2 - ab.$$

**Määritelmä 2.6.10.** Olkoon  $p \in \mathbb{N}$  alkuluku ja olkoon  $E$  yhtälön (2.7) määräämä elliptinen käyrä. Mikäli kertoimista  $a_1, a_2, a_3, a_4, a_6$  otetaan jakojäännös modulo  $p$ , saadaan käyrä

$$\tilde{E} : y^2 + \tilde{a}_1 xy + \tilde{a}_3 y = x^3 + \tilde{a}_2 x^2 + \tilde{a}_4 x + \tilde{a}_6$$

jota kutsutaan *reduktioksi* mod  $p$ .

Reduktion avulla voidaan luokitella elliptisiä käyriä. Olkoon  $E$  elliptinen käyrä ja  $\tilde{E}$  sen minimaalimallista muodostettu reduktio modulo  $p$ . Merkitään  $\tilde{\Delta}$  ja  $\tilde{c}_4$  käyrään  $\tilde{E}$  liittyviä lukuja. Reduktion  $\tilde{E}$  sanotaan olevan

- (i) *hyvä* (vakaa), mikäli  $\tilde{\Delta} \neq 0$ .
- (ii) *multiplikatiivinen* (puolivakaa), mikäli  $\tilde{\Delta} = 0$  ja  $\tilde{c}_4 \neq 0$ .
- (iii) *additiivinen* (epävakaa), mikäli  $\tilde{\Delta} = \tilde{c}_4 = 0$ .

Elliptistä käyrää sanotaan *puolivakaaksi*, mikäli sen kaikki reduktiot modulo  $p$  ovat joko hyviä tai multiplikatiivisia. Itse asiassa voidaan osoittaa [59, s. 196], että elliptinen käyrä  $E$  on puolivakaa, jos ja vain jos sen minimaalimallista lasketuille luvuille  $\Delta$  ja  $c_4$  pätee joko  $p \nmid \Delta$  tai  $p \mid \Delta$  ja  $p \nmid c_4$ .

Esitetään vielä lopuksi yksi elliptisiin käyriin liittyvä luku, johtaja (engl. conductor).

**Määritelmä 2.6.11.** Olkoon  $p$  alkuluku ja olkoon  $E$  elliptinen käyrä, jonka minimaalidiskriminantti on  $\Delta$  ja  $\tilde{E}$  reduktio modulo  $p$ . Käyrän  $E$  *johtaja* on luku

$$N_E = \prod_{p \mid \Delta} p^{m_p},$$

missä

$$m_p = \begin{cases} 1, & \text{jos käyrä } \tilde{E} \text{ on multiplikatiivinen} \\ 2, & \text{jos käyrä } \tilde{E} \text{ on additiivinen ja } p \neq 2, 3 \\ 2 + \varepsilon_p, & \text{jos käyrä } \tilde{E} \text{ on additiivinen ja } p = 2, 3 \text{ sekä } 0 \leq \varepsilon_p \leq 3. \end{cases}$$

**Huomautus 2.6.12.** Määritelmässä 2.6.11 olevaa modulolukuun  $p$  liittyvää lukua  $\varepsilon_p$  ei tässä yhteydessä määritellä tarkemmin mutta voidaan kuitenkin todeta sen liittyvän arvioihin  $m_3 \leq 3$  ja  $m_2 \leq 5$  [59, s. 256]. Jatkossa tarkastellaan pelkästään puolivakaita elliptisiä käyriä, jolloin käyrän johtajan määritelmä sievenee muotoon

$$N_E = \prod_{p \mid \Delta} p = \text{rad}(\Delta),$$

missä olevaa radikaalifunktiota  $\text{rad}$  tarkastellaan myöhemmin alaluvussa 3.1.

Seuraavan aputuloksen avulla näytetään vielä alaluvun lopuksi elliptisten käyrien sekä Diofantoksen yhtälöiden välinen yhteys.

**Lemma 2.6.13.** *Olkoot  $a, b, c \in \mathbb{Z} \setminus \{0\}$  siten, että  $a + b = c$  ja  $\text{syt}(a, b, c) = 1$ , ja olkoon  $E$  elliptinen käyrä, joka määritellään yhtälöllä*

$$E : y^2 = x(x + a)(x - b).$$

- (i) *Käyrän  $E$  minimaalidiskriminantti  $\Delta$  on joko*

$$|\Delta| = 2^4 |abc|^2 \quad \text{tai} \quad |\Delta| = 2^{-8} |abc|^2.$$

- (ii) *Käyrällä  $E$  on multiplikatiivinen reduktio modulo  $p$  kaikilla parittomilla alkuluvuilla  $p$ , jotka jakavat tulon  $abc$ .*

**Huomautus 2.6.14.** Lemman 2.6.13 elliptistä käyrää kutsutaan löytäjensä mukaan *Frey'n käyriksi* ja siihen liittyviä suureita on laskettu Esimerkissä 2.6.6.

## 2.7 Analyysin perustuloksia

Matematiikan osa-aluetta, jossa reaali- ja kompleksianalyysin ideoita ja menetelmiä käytetään kokonaislukuja koskevilla ongelmilla, kutsutaan *analyttiseksi lukuteoriaksi* [1, s. 7]. Tämän alaluvun tarkoituksena on palauttaa mieleen joitakin analyysin perustuloksia sekä tarkastella muutamia jatkossa sovellettavia yksinkertaisia tuloksia.

Aloitetaan raja-arvon määritelmästä [66, s. 34].

**Määritelmä 2.7.1.** Olkoon  $x_0 \in \mathbb{R}$  ja  $r > 0$ . Funktiolla  $f : (x_0 - r, x_0 + r) \setminus \{x_0\} \rightarrow \mathbb{R}$  on pisteessä  $x_0$  *raja-arvo*  $L \in \mathbb{R}$ , jota merkitään

$$\lim_{x \rightarrow x_0} f(x) = L,$$

jos jokaista lukua  $\varepsilon > 0$  vastaa luku  $\delta > 0$  siten, että

$$0 < |x - x_0| < \delta \implies |f(x) - L| < \varepsilon.$$

Erityisesti jatkossa tarvitaan raja-arvoa äärettömydessä [66, s. 43].

**Määritelmä 2.7.2.** Olkoon  $\alpha \in \mathbb{R}$ . Funktio  $f : (\alpha, \infty) \rightarrow \mathbb{R}$  *kasvaa rajatta* kun  $x \rightarrow +\infty$ , mitä merkitään

$$\lim_{x \rightarrow \infty} f(x) = +\infty,$$

jos jokaista lukua  $M > 0$  vastaa luku  $x_M > 0$  siten, että

$$x > x_M \implies f(x) > M.$$

Pidetään tunnettuna yleisimmät raja-arvoon liittyvät laskusäännöt. Epämääräisissä raja-arvotilanteissa  $\frac{0}{0}$  tai  $\frac{\pm\infty}{\pm\infty}$  tarvitaan kuitenkin seuraavaa L'Hospitalin lausetta [66, s. 88–89]:

**Lause 2.7.3** (L'Hospital). *Olkoot  $f$  ja  $g$  avoimella välillä  $(a, b) \subset \mathbb{R}$  derivoituvia funktioita siten, että funktiolla  $g'$  ei ole nollakohtia välillä  $(a, b)$ . Oletetaan lisäksi, että joko*

$$\lim_{x \rightarrow b^-} f(x) = \lim_{x \rightarrow b^-} g(x) = 0 \quad \text{tai} \quad \lim_{x \rightarrow b^-} f(x) = \pm\infty \quad \text{ja} \quad \lim_{x \rightarrow b^-} g(x) = \pm\infty,$$

*ja että on olemassa luku  $L \in \mathbb{R} \cup \{\pm\infty\}$  siten, että*

$$\lim_{x \rightarrow b^-} \frac{f'(x)}{g'(x)} = L.$$

*Tällöin*

$$\lim_{x \rightarrow b^-} \frac{f(x)}{g(x)} = L.$$

**Huomautus 2.7.4.** L'Hospitalin lause on voimassa myös raja-arvoilla  $x \rightarrow a+$ ,  $x \rightarrow \pm\infty$  ja  $x \rightarrow c$  jollekin  $c \in (a, b)$ , mikäli lauseen oletukset vain muuten ovat voimassa [66, s. 91]. Tarvittaessa L'Hospitalin lausetta voidaan myös soveltaa useamman kerran edellyttäen että vaaditut oletukset pysyvät voimassa.

Havainnollistetaan L'Hospitalin lausetta esimerkillä.

**Esimerkki 2.7.5.** (i) Olkoon  $n \in \mathbb{N}$ . Osoitetaan, että  $\frac{x}{\log^n x} \rightarrow \infty$ , kun  $x \rightarrow \infty$ . Merkinällä  $\log^n x$  tarkoitetaan tässä potenssia  $(\log x)^n$ . L'Hospitalin lausetta toistuvasti  $n$  kertaa soveltamalla saadaan

$$\lim_{x \rightarrow \infty} \frac{x}{\log^n x} = \lim_{x \rightarrow \infty} \frac{1}{n(\log^{n-1} x) \frac{1}{x}} = \lim_{x \rightarrow \infty} \frac{x}{n \log^{n-1} x} = \dots = \lim_{x \rightarrow \infty} \frac{x}{n!} = \infty.$$

Tulos voidaan tulkita myös siten, että funktio  $x$  kasvaa funktiota  $\log^n x$  nopeammin kaikilla  $n \in \mathbb{N}$ . Vertailtaessa vielä keskenään funktioita  $\log^n x$  nähdään jo sieventämällä, että

$$\lim_{x \rightarrow \infty} \frac{\frac{x}{\log^m x}}{\frac{x}{\log^n x}} = \lim_{x \rightarrow \infty} \log^{n-m} x = \infty$$

kaikilla  $m \in \mathbb{N}$ ,  $m < n$ .

(ii) Funktio  $\frac{x}{\log^3 x}$  kasvaa funktiota  $\log \log x$  nopeammin, kun  $x \rightarrow \infty$ . Tämä nähdään neljä kertaa L'Hospitalin lausetta soveltamalla:

$$\begin{aligned} \lim_{x \rightarrow \infty} \frac{\frac{x}{\log^3 x}}{\log \log x} &= \lim_{x \rightarrow \infty} \frac{x}{\log^3 x \log \log x} = \lim_{x \rightarrow \infty} \frac{x}{3 \log^2 x \log \log x + \log^2 x} \\ &= \lim_{x \rightarrow \infty} \frac{x}{6 \log x \log \log x + 3 \log x + 2 \log x} \\ &= \lim_{x \rightarrow \infty} \frac{x}{6 \log \log x + 6 + 5} = \lim_{x \rightarrow \infty} \frac{x \log x}{6} = \infty. \end{aligned}$$

Polynomien arvoja on helppo laskea, joten niiden avulla voidaan approksimoida monimutkaisempia funktiota tietyin ehdoin esimerkiksi seuraavasti [66, s. 98–99].

**Määritelmä 2.7.6.** Olkoon  $x_0 \in \mathbb{R}$  ja olkoon funktio  $f$   $n$  kertaa derivoituva jossakin pisteen  $x_0$  ympäristössä  $(x_0 - r, x_0 + r)$ ,  $r > 0$ . Tällöin polynomia  $T_n(x; x_0)$ ,

$$T_n(x; x_0) = \sum_{k=0}^n \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k,$$

missä  $n \in \mathbb{N}$ , sanotaan *funktion  $f$  astetta  $n$  olevaksi Taylorin polynomiksi pisteessä  $x_0$* .

Antamalla  $n \rightarrow \infty$  saadaan päättymätön Taylorin sarja [66, s. 265].

**Määritelmä 2.7.7.** Olkoon funktio  $f$  äärettömästi derivoituva avoimella välillä  $I \subset \mathbb{R}$  ja olkoon  $x_0 \in I$ . Sarjaa

$$\sum_{k=0}^{\infty} \frac{f^{(k)}(x_0)}{k!} (x - x_0)^k,$$

sanotaan *funktion  $f$  Taylorin sarjaksi pisteessä  $x_0$* .

Taylorin sarja on yksikäsitteinen; jos funktiolla  $f$  on potenssisarja jollakin avoimella välillä  $I \subset \mathbb{R}$ , niin kyseinen sarja on tällöin funktion  $f$  Taylorin sarja [66, s. 265]. Seuraavan esimerkin avulla nähdään kuinka yleisten suppenevien sarjojen konstruointiin voidaan käyttää aiemmin määritettyä Taylorin sarjaa.

**Esimerkki 2.7.8.** (a) Määritetään Taylorin sarja funktiolle  $f(t) = \log(1+t)$  pisteessä  $t_0 = 0$ . Välillä  $(-1, 1)$  funktio  $f$  on äärettömästi derivoituva, joten Määritelmän 2.7.7 mukaan saadaan

$$\log(1+t) = t - \frac{t^2}{2} + \frac{t^3}{3} - \frac{t^4}{4} + \dots = \sum_{k=1}^{\infty} (-1)^{k-1} \frac{t^k}{k}, \quad \text{kun } -1 < t < 1.$$

Sarjan suppeneminen nähdään suoraan geometrisen sarjan suppenemisen perusteella.

(b) Määritetään (a)-kohdan avulla suppeneva sarja funktiolle  $g$ ,  $g(x) = \log(1 - \frac{1}{\log x})$ . Sijoittamalla  $t = -\frac{1}{\log x}$  yllä olevaan lausekkeeseen saadaan

$$\log\left(1 - \frac{1}{\log x}\right) = -\frac{1}{\log x} - \frac{1}{2 \log^2 x} - \frac{1}{3 \log^3 x} - \dots = -\sum_{k=1}^{\infty} \frac{1}{k(\log x)^k}.$$

Tässä tapauksessa suppenemisväliksi saadaan  $-1 < -\frac{1}{\log x} < 1$ , toisin sanoen  $|\log x| > 1$ .

Asymptoottista tarkastelua varten otetaan käyttöön seuraava merkintä [1, s. 53].

**Merkintä 2.7.9.** Olkoon  $a \in \mathbb{R}$ . Jos on olemassa vakio  $C > 0$  siten, että funktioille  $f$  ja  $g > 0$  pätee epäyhtälö

$$|f(x)| \leq Cg(x) \tag{2.8}$$

kaikilla  $x \geq a$ , niin tällöin merkitään

$$f = \mathcal{O}(g) \quad \text{tai} \quad f(x) = \mathcal{O}(g(x)).$$

**Huomautus 2.7.10.** Epäyhtälön (2.8) nojalla jos  $f = \mathcal{O}(g)$ , niin myös  $-f = \mathcal{O}(g)$ . Näin ollen siis  $\mathcal{O}(g) = -\mathcal{O}(g)$ , joten jatkossa voidaan rajoittua positiiviseen merkintään  $\mathcal{O}(g)$ .

Kerätään merkintään liittyvät tulokset omaksi lemmakseen.

**Lemma 2.7.11.** *Olkoon  $\alpha \in \mathbb{R}$ , ja olkoot  $f, f_1, f_2, g, g_1, g_2 : (a, \infty) \rightarrow \mathbb{R}$  funktioita siten, että  $g, g_1, g_2 > 0$  ja*

$$\lim_{x \rightarrow \infty} g(x) = \lim_{x \rightarrow \infty} g_1(x) = \lim_{x \rightarrow \infty} g_2(x) = \infty.$$

- (i) *Kaikilla  $k \in \mathbb{R}$  pätee  $k = \mathcal{O}(g)$ .*
- (ii) *Kaikilla  $k \in \mathbb{R} \setminus \{0\}$  pätee  $\mathcal{O}(kg) = \mathcal{O}(g)$ .*
- (iii) *Jos  $f = \mathcal{O}(g)$ , niin  $kf = \mathcal{O}(g)$  kaikilla  $k \in \mathbb{R}$ .*
- (iv) *Jos  $f > 0$ , niin  $f \cdot \mathcal{O}(g) = \mathcal{O}(fg)$ .*
- (v) *Jos  $f_1 = \mathcal{O}(g_1)$  ja  $f_2 = \mathcal{O}(g_2)$ , niin  $f_1 f_2 = \mathcal{O}(g_1 g_2)$ .*
- (vi) *Jos  $f > 0$ , niin  $f + \mathcal{O}(g) = \mathcal{O}(f + g)$ .*
- (vii) *Jos  $f_1 = \mathcal{O}(g_1)$  ja  $f_2 = \mathcal{O}(g_2)$ , niin  $f_1 + f_2 = \mathcal{O}(|g_1| + |g_2|)$  sekä  $f_1 + f_2 = \mathcal{O}(\max\{|g_1|, |g_2|\})$ . Erityisesti, jos  $g_1 = g_2$ , niin  $f_1 + f_2 = \mathcal{O}(g_1)$ .*

**Huomautus 2.7.12.** Lemman tulokset perustuvat oleellisesti epäyhtälön (2.8) ja itseisarvon arviointiin sekä äärettömän raja-arvon määritelmään (Määritelmä 2.7.2). Erityisesti L'Hospitalin lausetta hyödyntämällä rajatta kasvavien funktioiden  $f$  ja  $g$  tapauksessa saadaan, että

$$\lim_{x \rightarrow \infty} \frac{g(x)}{|f(x)|} = \infty \quad \implies \quad f(x) = \mathcal{O}(g(x)).$$

**Huomautus 2.7.13.** Lemmassa 2.7.11 tarkastellaan tyypillistä tapausta, jossa  $\mathcal{O}$ -merkinnän sisällä oleva funktio kasvaa rajatta. Merkintää voidaan luonnollisesti soveltaa myös rajoitettujen funktioiden tapauksessa, jolloin käytetään merkintää  $\mathcal{O}(1)$ . Tällöin ainakin osa Lemman 2.7.11 tuloksista on voimassa.

Lisäksi seuraavaa aputulosta tarvitaan [43, s. 215], [56, s. 25–26].

**Lemma 2.7.14.** *Olkoon  $n \in \mathbb{N}$ . Tällöin*

$$\left(\frac{n}{e}\right)^n < n!.$$

*Todistus.* Väite on selvästi voimassa arvolla  $n = 1$ . Koska logaritmi on aidosti kasvava ja Riemann-integroituva jokaisella välillä  $[1, b]$ ,  $b > 1$ , saadaan kaikilla  $n \geq 2$  arvio

$$\int_{n-1}^n \log x \, dx \leq \int_{n-1}^n \log n \, dx = \log n.$$

Ottamalla nyt logaritmi kertomasta ja käyttämällä yllä olevaa tietoa saadaan

$$\begin{aligned} \log n! &= \sum_{k=2}^n \log k \geq \sum_{k=2}^n \int_{k-1}^k \log x \, dx \\ &= \int_1^n \log x \, dx = \int_1^n x \log x - x \\ &= n \log n - n - (1 \cdot \log 1 - 1) \\ &= n \log n - n + 1 \\ &> n \log n - n, \end{aligned}$$

mistä väite seuraa. □

Yllä olevaa ajatusta jatkamalla saadaan seuraava approksimaatio.

**Lause 2.7.15** (Stirlingin kaava). *Olkoon  $n \in \mathbb{N}$ . Tällöin suurilla muuttujan  $n$  arvoilla*

$$\log n! = n \log n - n + \mathcal{O}(\log n).$$

**Huomautus 2.7.16.** Lauseen 2.7.15 tulosta voidaan perustella Lemman 2.7.14 todistuksessa puolisuunnikassäännön avulla saatavalla arviolla

$$\log n! \approx \int_1^n \log x \, dx = n \log n - n + 1.$$

Lemman 2.7.11 nojalla nimittäin  $1 = \mathcal{O}(\log n)$ . Lauseen analyttisempi todistus löytyy lähteistä [1, s. 68] tai [43, s. 208].

Sovelletaan Stirlingin kaavaa seuraavassa myöhemmin tarvittavassa aputuloksessa.

**Lemma 2.7.17.** *Olkoon  $n \in \mathbb{N}$ . Tällöin suurilla muuttujan  $n$  arvoilla pätee*

$$\log \left( \frac{(2n)!}{(n!)^3 2^n} \right) = n \log \left( \frac{2e}{n} \right) + \mathcal{O}(\log n).$$

*Todistus.* Lausetta 2.7.15 sekä logaritmin laskusääntöjä soveltamalla saadaan

$$\begin{aligned} \log \left( \frac{(2n)!}{(n!)^3 2^n} \right) &= \log(2n)! - 3 \log n! - n \log 2 \\ &= 2n \log(2n) - 2n + \mathcal{O}(\log 2n) - 3n \log n + 3n - n \log 2 - 3\mathcal{O}(\log n) \\ &= (2n - n) \log 2 + (2n - 3n) \log n + n + \mathcal{O}(\log n) \\ &= n \log 2 - n \log n + n \log e + \mathcal{O}(\log n) \\ &= n \log \left( \frac{2e}{n} \right) + \mathcal{O}(\log n). \end{aligned}$$

□

## 2.8 Alkulukuihin liittyviä tuloksia

Klassinen ongelma lukuteoriassa on alkulukujen jakautuminen. Vaikka tiedetäänkin alkulukuja olevan äärettömästi, niiden lukumäärää pystytään approksimoimaan vain asympotootisesti funktiolla  $\frac{x}{\log x}$ . Tässä alaluvussa tarkastellaan alkulukuihin liittyviä erilaisia arvioita keskittyen kuitenkin  $abc$ -osumien alarajafunktiota koskevan Lauseen 3.6.9 todistuksessa tarvittavien aputuloksien käsittelyyn.

Lähdetään liikkeelle arviosta, joka on hyvin oleellinen sovellettaessa  $Abc$ -konjektuuria erilaisiin Diophantoksen yhtälöihin ja epäyhtälöihin [43, s. 269-270].

**Lemma 2.8.1.** *Kaikilla  $n \in \mathbb{N}$  ja alkuluvuilla  $p$  pätee*

$$\prod_{p \leq n} p < 4^n.$$

*Todistus.* Osoitetaan väite induktiolla.

1°) Tapauksissa  $n = 1$  ja  $n = 2$  saadaan  $1 < 4^1$  ja  $2 < 4^2$ , joten väite on voimassa.

2°) Oletetaan, että väite pätee arvolla  $n = k \geq 2$ . Jos  $k$  on pariton, niin arvolla  $n = k + 1$

$$\prod_{p \leq k+1} p = \prod_{p \leq k} p < 4^k < 4^{k+1}$$

induktio-oletuksen nojalla.

Jos taas  $k$  on parillinen, niin  $n = k + 1 = 2m + 1$  jollekin  $m \in \mathbb{N}$ . Tällöin

$$\prod_{p \leq k+1} p = \prod_{p \leq m+1} p \prod_{m+2 \leq p \leq 2m+1} p.$$

Tarkastellaan sitten binomikerrointa  $M$ ,

$$M = \binom{2m+1}{m} = \frac{(2m+1)2m(2m-1) \cdots (m+2)}{m!}.$$

Esimerkin 2.2.8 nojalla  $M$  on kokonaisluku ja sille pätee arvio

$$M < 4^m.$$

Olkoon sitten  $p$  alkuluku väliltä  $m + 2 \leq p \leq 2m + 1$ . Tällöin  $p$  jakaa tulon

$$(2m+1)2m(2m-1) \cdots (m+2)$$

mutta ei kertomaa  $m!$ , sillä  $m < p$ . Täten  $p \mid M$  ja siten myös  $(\prod_{m+2 \leq p \leq 2m+1} p) \mid M$ . Näin ollen pätee

$$\prod_{m+2 \leq p \leq 2m+1} p \leq M < 4^m. \quad (2.9)$$

Nyt induktio-oletuksen nojalla väite pätee arvolla  $m + 1 < k$ , toisin sanoen

$$\prod_{p \leq m+1} p < 4^{m+1}, \quad (2.10)$$

jolloin epäyhtälöistä (2.9) ja (2.10) seuraa

$$\prod_{p \leq k+1} p = \prod_{p \leq m+1} p \prod_{m+2 \leq p \leq 2m+1} p < 4^{m+1} 4^m = 4^{k+1}.$$

Väite seuraa kohdista 1°) ja 2°) sekä induktioperiaatteesta.  $\square$



**Huomautus 2.8.2.** Lemmalla 2.8.1 on läheinen yhteys ns. Chebyshevin funktioon  $\vartheta$ ,

$$\vartheta(x) = \sum_{p \leq x} \log p = \log \prod_{p \leq x} p.$$

Lemma 2.8.1 voidaankin esittää ekvivalenttisesti muodossa: kaikilla reaaliluvuilla  $x \geq 1$

$$\vartheta(x) < x \log 4.$$

Funktion  $\vartheta$  avulla Chebyshev tarkasteli alkulukujen lukumääräfunktion  $\pi$  kasvunopeutta [43, s. 267–268].

**Määritelmä 2.8.3.** Funktiota  $\pi : \mathbb{R}_{>0} \rightarrow \mathbb{Z}_{\geq 0}$ ,

$$\pi(x) = \text{lukumäärä alkuluvuille, jotka ovat } \leq x,$$

kutsutaan *alkulukujen lukumääräfunktiksi*.

Alkulukujen lukumääräfunktion asymptoottista kasvunopeutta kuvaavan lauseen alkulukutaulukoiden perusteella totesivat itsenäisesti Gauss (1792) ja Legendre (1798) mutteivat pystyneet sitä todistamaan [1, s. 8–9]. Varsinaisen todistuksen tulokselle esittivät Hadamard ja de la Vallee-Poussin vasta vuonna 1896.

**Lause 2.8.4** (Alkulukulause). *Olkoon  $\pi$  alkulukujen lukumääräfunktio. Tällöin*

$$\lim_{x \rightarrow \infty} \frac{\pi(x)}{\frac{x}{\log x}} = 1.$$

**Huomautus 2.8.5.** Alkulukulauseen mukaan funktio  $\pi$  käyttäytyy asymptoottisesti samalla tavalla kuin funktio  $\frac{x}{\log x}$ , mikä ei kuitenkaan tarkoita niiden erotusten olevan lähellä nollaa. Funktio  $\pi$  virhetermeineen [31, s. 65] voidaan esittää muodossa

$$\pi(x) = x \left( \frac{1}{\log x} + \frac{1}{\log^2 x} + \cdots + \frac{(k-1)!}{\log^k x} + \mathcal{O}\left(\frac{1}{\log^{k+1} x}\right) \right).$$

Arvolla  $k = 3$  saadaan

$$\pi(x) = x \left( \frac{1}{\log x} + \frac{1}{\log^2 x} + \frac{2}{\log^3 x} + \mathcal{O}\left(\frac{1}{\log^4 x}\right) \right), \quad (2.11)$$

mikä on tarvittava tarkkuus alla olevan parittomien alkulukujen logaritmisia summia koskevan Lemman 2.8.8 todistuksessa.

Lemman 2.8.8 todistuksessa tarvitaan myös seuraavaa Abelin summakaavaa [1, s.77].

**Lause 2.8.6** (Abel). *Olkoon  $n \in \mathbb{N}$  ja olkoon funktio  $A : \mathbb{R} \rightarrow \mathbb{R}$  määritelty funktion  $a : \mathbb{N} \rightarrow \mathbb{R}$  avulla siten, että*

$$A(x) = \sum_{n \leq x} a(n),$$

missä  $A(x) = 0$ , jos  $x < 1$ . Oletetaan, että funktiolla  $f$  on jatkuva derivaatta välillä  $[y, x]$ , missä  $0 < y < x$ . Tällöin

$$\sum_{y < n \leq x} a(n)f(n) = A(x)f(x) - A(y)f(y) - \int_y^x A(t)f'(t)dt.$$

Avataan Lemmassa 2.8.8 tarvittavaa Abelin lauseen sovellusta esimerkin avulla.

**Esimerkki 2.8.7.** Olkoon  $n \in \mathbb{N}$  ja olkoot  $p_1, \dots, p_n$   $n$  ensimmäistä paritonta alkulukua. Määritellään funktio  $a : \mathbb{N} \rightarrow \mathbb{R}$  siten, että

$$a(n) = \begin{cases} 1, & \text{jos } n \text{ on alkuluku} \\ 0 & \text{muulloin.} \end{cases}$$

Tällöin

$$\pi(x) = \sum_{p \leq x} 1 = \sum_{1 < n \leq x} a(n),$$

joten Lausetta 2.8.6 arvolla  $y = 2$  sovellettaessa saadaan

$$\sum_{i=1}^n f(p_i) = f(x)\pi(x) - f(2) - \int_2^x f'(t)\pi(t)dt.$$

Asettamalla edelleen  $f(x) = \log x$  ja  $f(x) = \log \log x$  saadaan vastaavasti

$$\sum_{i=1}^n \log p_i = \pi(x) \log x - \log 2 - \int_2^x \frac{\pi(t)}{t} dt \quad (2.12)$$

$$\sum_{i=1}^n \log \log p_i = \pi(x) \log \log x - \log \log 2 - \int_2^x \frac{\pi(t)}{t \log t} dt. \quad (2.13)$$

Osoitetaan seuraavaksi alaluvun päätulos [14, s. 1867–1869].

**Lemma 2.8.8.** *Olkoon  $x \in \mathbb{R}_{>0}$ . Merkitään lukua  $x$  pienempien tai yhtäsuurten parittomien alkulukujen lukumäärää luvulla  $n = \pi(x) - 1$  ja olkoot  $p_1, \dots, p_n$   $n$  ensimmäistä paritonta alkulukua. Tällöin*

$$\begin{aligned} \sum_{i=1}^n \log p_i &= n \log \left( \frac{x}{e} \right) - \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right), \\ \sum_{i=1}^n \log \log p_i &= n \log \left( \frac{x}{n} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right). \end{aligned}$$

*Todistus.* Todistuksen ajatus perustuu Abelin kaavan soveltamiseen Esimerkin 2.8.7 mukaisesti. Tarkastellaan aluksi Lemman ensimmäistä väitettä ja yhtälöä (2.12). Arviota (2.11) soveltamalla saadaan

$$\pi(x) \log x - \log 2 = x \left( 1 + \frac{1}{\log x} + \frac{2}{\log^2 x} + \mathcal{O} \left( \frac{1}{\log^3 x} \right) \right) \quad (2.14)$$

ja

$$\int_2^x \frac{\pi(t)}{t} dt = \int_2^x \left( \frac{1}{\log t} + \frac{1}{\log^2 t} + \mathcal{O} \left( \frac{1}{\log^3 t} \right) \right) dt, \quad (2.15)$$

kun käytetään arviota  $\log 2 = \mathcal{O} \left( \frac{x}{\log^3 x} \right)$  ja  $\frac{2x}{\log^3 x} + \mathcal{O} \left( \frac{x}{\log^4 x} \right) = \mathcal{O} \left( \frac{x}{\log^3 x} \right)$  (Lemma 2.7.11).

Osittaisintegroinnin mukaan kaikilla  $m \in \mathbb{N}$ ,  $a, b \in \mathbb{R}$ ,  $a, b > 1$  pätee

$$\int_a^b \frac{1}{\log^m t} dt = \int_a^b \frac{t}{\log^m t} + m \int_a^b \frac{1}{\log^{m+1} t} dt. \quad (2.16)$$

Yhtälön (2.16) nojalla saadaan yhtälöstä (2.15) siten edelleen

$$\begin{aligned} \int_2^x \frac{\pi(t)}{t} dt &= \int_2^x \frac{1}{\log t} dt + \int_2^x \frac{1}{\log^2 t} dt + \int_2^x \mathcal{O}\left(\frac{1}{\log^3 t}\right) dt \\ &= \int_2^x \frac{t}{\log t} + \int_2^x \frac{1}{\log^2 t} dt + \int_2^x \frac{t}{\log^2 t} + 2 \int_2^x \frac{1}{\log^3 t} dt + \mathcal{O}\left(\frac{x}{\log^3 x}\right) \\ &= \int_2^x \frac{t}{\log t} + \int_2^x \frac{t}{\log^2 t} + \int_2^x \frac{1}{\log^3 t} dt + \int_2^x \frac{t}{\log^2 t} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) \\ &= \frac{x}{\log x} + \frac{2x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right), \end{aligned}$$

sillä kaikille vakioille  $c \in \mathbb{R}$  pätee  $c = \mathcal{O}\left(\frac{x}{\log^3 x}\right)$  Lemman 2.7.11 mukaan. Sijoittamalla nyt yllä oleva sekä yhtälö (2.14) alkuperäiseen yhtälöön (2.12) saadaan

$$\sum_{i=1}^n \log p_i = x + \mathcal{O}\left(\frac{x}{\log^3 x}\right). \quad (2.17)$$

Alussa asetettiin  $n = \pi(x) - 1$ . Kirjoittamalla (2.11) uudelleen käyttämällä geometrista sarjaa saadaan

$$\begin{aligned} n &= \frac{x}{\log x} \left(1 + \frac{1}{\log x} + \frac{2}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right)\right) - 1 \\ &= \frac{x}{\log x} \left(\sum_{i=0}^{\infty} \left(\frac{1}{\log x}\right)^i + \frac{1}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right)\right) \\ &= \frac{x}{\log x} \left(\frac{1}{1 - \frac{1}{\log x}} + \frac{1}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right)\right) \\ &= x \left(\frac{1}{\log x - 1} + \frac{1}{\log^3 x} + \mathcal{O}\left(\frac{1}{\log^4 x}\right)\right), \end{aligned}$$

missä  $-1 = \mathcal{O}\left(\frac{x}{\log^4 x}\right)$ . Kertomalla saatu yhtälö puolittain luvulla  $\log x - 1$  saadaan edelleen

$$\begin{aligned} n(\log x - 1) &= x \left(1 + \frac{\log x}{\log^3 x} - \frac{1}{\log^3 x} + (\log x - 1)\mathcal{O}\left(\frac{1}{\log^4 x}\right)\right) \\ &= x + \frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right), \end{aligned} \quad (2.18)$$

josta edelleen termejä siirtämällä sekä huomiota

$$\log x - 1 = \log x - \log e = \log\left(\frac{x}{e}\right)$$

soveltamalla saadaan lopulta

$$x = n \log \left( \frac{x}{e} \right) - \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right). \quad (2.19)$$

Lemman ensimmäinen väite seuraa yhdistämällä yhtälöt (2.17) ja (2.19).

Tarkastellaan sitten Lemman toista väitettä ja yhtälöä (2.13). Aiemmin asetetun noljalla  $\pi(x) = n + 1$ , jolloin huomioita  $\log \log x = \mathcal{O}(\log \log x)$  ja  $\log \log 2 = \mathcal{O}(\log \log x)$  soveltamalla saadaan

$$\pi(x) \log \log x - \log \log 2 = n \log \log x + \mathcal{O}(\log \log x). \quad (2.20)$$

Vastaavasti yhtälöä (2.11) käyttämällä sekä yhtälön (2.16) mukaan osittaisintegroimalla saadaan

$$\begin{aligned} \int_2^x \frac{\pi(t)}{t \log t} dt &= \int_2^x \frac{1}{t \log t} \cdot t \left( \frac{1}{\log t} + \frac{1}{\log^2 t} + \frac{2}{\log^3 t} + \mathcal{O} \left( \frac{1}{\log^4 t} \right) \right) dt \\ &= \int_2^x \left( \frac{1}{\log^2 t} + \mathcal{O} \left( \frac{1}{\log^3 t} \right) \right) dt \\ &= \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right). \end{aligned} \quad (2.21)$$

Sijoittamalla tulokset (2.20) ja (2.21) alkuperäiseen yhtälöön (2.13) saadaan

$$\sum_{i=1}^n \log \log p_i = n \log \log x - \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right), \quad (2.22)$$

sillä  $\log \log x = \mathcal{O} \left( \frac{x}{\log^3 x} \right)$ .

Toisaalta, koska  $\log x - 1 = \log x \left( 1 - \frac{1}{\log x} \right)$ , saadaan

$$\begin{aligned} n \log(\log x - 1) &= n \left( \log \log x + \log \left( 1 - \frac{1}{\log x} \right) \right) \\ &= n \left( \log \log x - \left[ \frac{1}{\log x} + \mathcal{O} \left( \frac{1}{\log^2 x} \right) \right] \right) \\ &= n \log \log x - (\pi(x) - 1) \left[ \frac{1}{\log x} + \mathcal{O} \left( \frac{1}{\log^2 x} \right) \right] \\ &= n \log \log x - \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \end{aligned}$$

missä toinen yhtäsuuruus seuraa Taylorin sarjakehitelmästä (Esimerkki 2.7.8) ja neljäs arviosta (2.11) sekä huomiosta  $\frac{1}{\log x} = \mathcal{O} \left( \frac{x}{\log^3 x} \right)$ . Näin ollen yhtälö (2.22) voidaan kirjoittaa muodossa

$$\sum_{i=1}^n \log \log p_i = n \log(\log x - 1) + \mathcal{O} \left( \frac{x}{\log^3 x} \right),$$

josta lopulta saadaan

$$\begin{aligned}
\sum_{i=1}^n \log \log p_i &= n \log \left( \frac{n(\log x - 1)}{n} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \\
&= n \log \left( \frac{x(1 + \mathcal{O}(\frac{1}{\log^2 x}))}{n} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \\
&= n \left( \log \left( \frac{x}{n} \right) + \log \left[ 1 + \mathcal{O} \left( \frac{1}{\log^2 x} \right) \right] \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \\
&= n \log \left( \frac{x}{n} \right) + \mathcal{O} \left( \frac{x}{\log x} \right) \cdot \mathcal{O} \left( \frac{1}{\log^2 x} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \\
&= n \log \left( \frac{x}{n} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right),
\end{aligned}$$

missä toinen yhtäsuuruus seuraa yhtälöstä (2.18) ja neljäs yhtälöstä (2.11) saatavasta arviosta  $\pi(x) - 1 = \mathcal{O}(\frac{x}{\log x})$  sekä arviosta  $\log \left( 1 + \mathcal{O}(\frac{1}{\log^2 x}) \right) = \mathcal{O}(\frac{1}{\log^2 x})$ , sillä  $\log 1 = 0$ . Lemman toinen väite seuraa.  $\square$

**Huomautus 2.8.9.** Lemma 2.8.8 antaa tarkasteltaville parittomien alkulukujen tuloista otetuille logaritmisille summille oleellisesti asympotoottisen arvion, mikä käy ilmi todistuksessa käytetyistä  $\mathcal{O}$ -merkinnöistä. Merkintään  $\mathcal{O}$  liittyviä tuloksia on esitetty tarkemmin Lemmassa 2.7.11.

Sovelletaan näin saatua tulosta vielä kolmeen myöhemmin tarvittavaan aputulokseen. Lemmoissa esiintyvä funktio  $B$  määritellään myöhemmin Lauseen 3.6.9 todistuksessa.

**Lemma 2.8.10.** *Olkoon  $x \in \mathbb{R}_{>0}$ . Merkitään lukua  $x$  pienempien tai yhtäsuurten parittomien alkulukujen lukumäärää luvulla  $n = \pi(x) - 1$  ja olkoot  $p_1, \dots, p_n$   $n$  ensimmäistä paritonta alkulukua sekä  $B : \mathbb{R}_{>0} \rightarrow \mathbb{R}_{>0}$  kasvava funktio. Tällöin*

$$\log \left( \frac{(2n)!}{(n!)^3 2^n} B(x)^n \right) - \sum_{i=1}^n \log \log p_i \geq n \log \left( \frac{2eB(x)}{x} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right)$$

*Todistus.* Lemmoja 2.7.17 ja 2.8.8 sekä logaritmin laskusääntöjä soveltamalla saadaan

$$\begin{aligned}
&\log \left( \frac{(2n)!}{(n!)^3 2^n} B(x)^n \right) - \sum_{i=1}^n \log \log p_i \\
&= n \log \left( \frac{2e}{n} \right) + \mathcal{O}(\log n) + n \log B(x) - n \log \left( \frac{x}{n} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \\
&= n \left( \log \left( \frac{2e}{n} \right) + \log B(x) + \log \left( \frac{n}{x} \right) \right) + \mathcal{O}(\log n) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \\
&\geq n \log \left( \frac{2eB(x)}{x} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right),
\end{aligned}$$

sillä  $\mathcal{O}(\log n) = \mathcal{O}(\frac{x}{\log x})$  alkulukulauseen nojalla (Lause 2.8.4) ja  $\mathcal{O}(\frac{x}{\log^3 x}) = \mathcal{O}(\frac{x}{\log x})$ .  $\square$

**Lemma 2.8.11.** *Olkoon  $m \in \mathbb{N}$  siten, että Lemman 2.8.10 merkinnöillä pätee*

$$2^m \geq \exp \left[ n \log \left( \frac{2eB(x)}{x} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right]. \quad (2.23)$$

*Tällöin*

$$\left( \frac{1}{2^m} \right)^\alpha \prod_{i=1}^n p_i \leq \exp \left( n \log \left( \frac{x}{e} \left( \frac{x}{2eB(x)} \right)^\alpha \right) - \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right).$$

*Todistus.* Lemmaa 2.8.8 sekä epäytälöä (2.23) soveltamalla saadaan

$$\begin{aligned} \left( \frac{1}{2^m} \right)^\alpha \prod_{i=1}^n p_i &= \exp \left( \log \left[ \left( \frac{1}{2^m} \right)^\alpha \prod_{i=1}^n p_i \right] \right) \\ &\leq \exp \left( \log \left[ \exp \left[ n \log \left( \frac{2eB(x)}{x} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right] \right]^{-\alpha} + \log \left[ \prod_{i=1}^n p_i \right] \right) \\ &= \exp \left( -\alpha n \log \left( \frac{2eB(x)}{x} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) + \sum_{i=1}^n \log p_i \right) \\ &= \exp \left( n \log \left( \frac{x}{2eB(x)} \right)^\alpha + \mathcal{O} \left( \frac{x}{\log^3 x} \right) + n \log \left( \frac{x}{e} \right) - \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right) \\ &= \exp \left( n \log \left( \frac{x}{e} \left( \frac{x}{2eB(x)} \right)^\alpha \right) - \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right). \end{aligned}$$

□

**Lemma 2.8.12.** *Oletetaan, että Lemman 2.8.11 oletusten lisäksi pätee*

$$\frac{2eB(x)}{x} = \left( \frac{x}{e} \right)^{\frac{1}{\alpha}}.$$

*Mikäli määritellään luku  $n$  alkulukufunktion  $\pi$  avulla siten, että  $n = \pi(x) - 1$ , saadaan*

$$2^m \geq \exp \left( \frac{x}{\alpha} \left[ 1 + \frac{1}{\log^2 x} + \mathcal{O} \left( \frac{1}{\log^3 x} \right) \right] \right).$$

*Todistus.* Koska  $\log \left( \frac{x}{e} \right) = \log x - 1$ , saadaan oletusten sekä arvion (2.11) nojalla

$$\begin{aligned} 2^m &\geq \exp \left[ n \log \left( \frac{2eB(x)}{x} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right] = \exp \left( \frac{n}{\alpha} \log \left( \frac{x}{e} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right) \\ &= \exp \left( \frac{x}{\alpha} \left[ \frac{1}{\log x} + \frac{1}{\log^2 x} + \frac{2}{\log^3 x} + \mathcal{O} \left( \frac{1}{\log^4 x} \right) \right] (\log x - 1) \right) \\ &= \exp \left( \frac{x}{\alpha} \left[ 1 + \frac{1}{\log^2 x} + \mathcal{O} \left( \frac{1}{\log^3 x} \right) \right] \right). \end{aligned}$$

□

### 3 Abc-konjektuuri ja siihen liittyviä tuloksia

*Abc*-konjektuuri voidaan esittää monessa muodossa käyttötarkoituksesta riippuen. Tässä luvussa tarkastellaan alkuperäistä *Abc*-konjektuuria, sen eri formulaatioita sekä tyypillisimpiä tapoja lähestyä konjektuuria. Lopuksi tarkastellaan *Abc*-konjektuurin yhteyttä sen innoittajina toimineisiin Szpiron konjektuureihin sekä Fermat'n suureen lauseeseen.

#### 3.1 Abc-kolmikot ja radikaali

*Abc*-konjektuurin esittämiseksi sekä merkintöjen yksinkertaistamiseksi määritellään aluksi *abc*-summa ja -kolmikko lähteitä [14] ja [46, s. 2] soveltaen.

**Määritelmä 3.1.1.** Luvut  $a, b, c \in \mathbb{Z} \setminus \{0\}$  muodostavat *abc*-summan, mikäli  $a + b = c$  ja  $\text{syt}(a, b) = 1$ . *Abc*-summan muodostavaa kolmikkoa  $(a, b, c) \in \mathbb{Z}^3$  kutsutaan *abc-kolmikoksi*.

**Huomautus 3.1.2.** (i) Jatkossa oletetaan yksinkertaisuuden vuoksi, että  $0 < a < b < c$  ellei muuta mainita. Kyseinen tilanne saadaan nimittäin aina aikaan *abc*-summan termejä siirtämällä ja valitsemalla tarvittaessa uudelleen luvut  $a, b$  ja  $c$ .

(ii) Oletuksesta  $\text{syt}(a, b) = 1$  seuraa  $\text{syt}(a, b, c) = 1$ . Soveltamalla Lemmaa 2.1.7 kaksi kertaa saadaan

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

Lauseen 2.1.5 nojalla siten  $\text{syt}(a, b) = \text{syt}(a, c) = \text{syt}(b, c) = 1$ , jolloin myös  $\text{syt}(a, b, c) = 1$ .

**Esimerkki 3.1.3.** Lukuteoriassa esiintyy paljon *abc*-kolmikoita [46, s. 2–3]:

(i) Pythagoraan kolmikot  $(x, y, z) \in \mathbb{N}^3$ , jotka ovat muotoa

$$\begin{aligned}x &= m^2 - n^2 \\y &= 2mn \\z &= m^2 + n^2,\end{aligned}$$

missä  $m, n \in \mathbb{N}$ ,  $m > n$ ,  $\text{syt}(m, n) = 1$ , ja toinen luvuista  $m$  ja  $n$  on pariton ja toinen parillinen [54, s. 394-395].

(ii) Fermat'n luvuista  $F_n = 2^{2^n} + 1$ ,  $n \in \mathbb{N}$ , muodostetut kolmikot  $(1, 2^{2^n}, F_n)$ .

(iii) Mersennen alkuluvuista  $M_p = 2^p - 1$ ,  $p$  alkuluku, muodostetut kolmikot  $(1, M_p, 2^p)$ .

Tulkitsemalla kongruenssiyhtälöitä yhtälöiksi saadaan *abc*-kolmikoita myös

(iv) Fermat'n pienestä lauseesta, jonka mukaan jokaiselle alkuluvulle  $p$  pätee  $a^{p-1} \equiv 1 \pmod{p}$  aina, kun  $a \in \mathbb{Z}$  ja  $\text{syt}(p, a) = 1$ .

(v) Fermat'n pienen lauseen yleistyksestä Eulerin lauseesta, jonka mukaan  $a^{\phi(n)} \equiv 1 \pmod{n}$ , missä  $n \in \mathbb{N}$ ,  $a \in \mathbb{Z}$  siten, että  $\text{syt}(a, n) = 1$ , ja  $\phi$  on Eulerin funktio.

- (vi) Wilsonin lauseesta, jonka mukaan jokainen alkuluku  $p$  toteuttaa kongruenssin  $(p-1)! \equiv -1 \pmod{p}$ .  $Abc$ -kolmikoita saadaan myös Wilsonin alkuluvuista  $p$ , jotka toteuttavat kongruenssin  $(p-1)! \equiv -1 \pmod{p^2}$ .
- (vii) Wieferichin alkuluvuista  $p$ , jotka toteuttavat kongruenssin  $2^{p-1} \equiv 1 \pmod{p^2}$ .
- (viii) Carmichaelin luvuista, toisin sanoen yhdistetyille luvuille  $n \in \mathbb{N}$ , joille on voimassa kongruenssi  $b^{n-1} \equiv 1 \pmod{n}$  kaikilla  $b \in \mathbb{N}$ , joille  $\text{sy}(n, b) = 1$ .

$Abc$ -konjektuurin kannalta oleellinen on myös radikaalin käsite [43, s. 172], [46, s. 3].

**Määritelmä 3.1.4.** Olkoon  $n \in \mathbb{Z} \setminus \{0\}$ . Luvun  $n$  *radikaali* määritellään alkutekijöiden tulona

$$\text{rad}(n) = \prod_{p|n} p,$$

missä  $p$  on alkuluku. Lisäksi asetetaan  $\text{rad}(1) = \text{rad}(-1) = 1$ .

**Huomautus 3.1.5.** Radikaalin määritelmästä nähdään suoraan, että  $\text{rad}(n) \mid n$ . Radikaalin voikin tulkita annetun luvun suurimmaksi neliövapaaksi tekijäksi [23]. Toisin sanoen,  $k^2 \nmid \text{rad}(n)$  kaikilla  $n \in \mathbb{Z} \setminus \{0\}$  ja  $k \in \mathbb{N} \setminus \{1\}$ .

Havainnollistetaan määritelmää seuraavalla esimerkillä.

**Esimerkki 3.1.6.** Olkoon  $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ . Tällöin luvulla  $n$  on yleistetty kanoninen esitys (Lause 2.1.14 ja Huomautus 2.1.15)

$$n = (-1)^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n},$$

missä luvut  $p_1, \dots, p_n$  ovat eri alkulukuja,  $a_0 \in \{0, 1\}$  ja  $a_1, \dots, a_n \in \mathbb{N}$ . Luvun  $n$  radikaali on siten

$$\text{rad}(n) = \text{rad}\left((-1)^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}\right) = p_1 p_2 \cdots p_n.$$

Seuraavaan aputulokseen on kerätty jatkon kannalta oleelliset radikaalin ominaisuudet.

**Lemma 3.1.7.** *Olkoot  $a, b, m, n \in \mathbb{N}$ . Tällöin*

- (i)  $\text{rad}(a) \leq a$ .
- (ii)  $\text{rad}(ab) \leq \text{rad}(a) \text{rad}(b)$ , missä pätee yhtäsuuruus jos vain jos  $\text{sy}(a, b) = 1$ .
- (iii)  $\text{rad}(a^m b^n) \leq \text{rad}(a) \text{rad}(b)$ .

*Todistus.* Oletetaan, että  $a, b, m, n \geq 2$ , sillä muuten väitteet pätevät triviaalisti. Luvuilla on Aritmetiikan peruslauseen (Lause 2.1.14) nojalla kanoniset esitykset  $a = p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}$  ja  $b = q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m}$ , missä  $p_i = q_j$  joillekin  $i$  ja  $j$ , mikäli  $\text{sy}(a, b) \neq 1$ . Näin ollen

$$\text{rad}(a) = \text{rad}(p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}) = p_1 p_2 \cdots p_n \leq p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n} = a$$

kaikilla  $a \in \mathbb{N} \setminus \{1\}$ , mistä väite (i) seuraa. Edelleen

$$\begin{aligned} \text{rad}(ab) &= \text{rad}(p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n} \cdot q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m}) \\ &\leq p_1 p_2 \cdots p_n \cdot q_1 q_2 \cdots q_m \\ &= \text{rad}(p_1^{t_1} p_2^{t_2} \cdots p_n^{t_n}) \text{rad}(q_1^{s_1} q_2^{s_2} \cdots q_m^{s_m}) = \text{rad}(a) \text{rad}(b), \end{aligned}$$

mikä osoittaa väitteen (ii). Väite (iii) seuraa väiteestä (ii) ja radikaalin määritelmästä.  $\square$



**Huomautus 3.1.8.** Kohdan (ii) nojalla radikaalifunktio on multiplikaatiivinen.

Osoitetaan vielä työhön [56, s. 9–10] perustuen, että  $abc$ -kolmikon lukujen tulon radikaali voi saada mielivaltaisen suuria arvoja.

**Merkintä 3.1.9.** Olkoot  $P, s \in \mathbb{N}$  siten, että  $P \geq 3$  ja  $0 < p_1 < p_2 < \dots < p_s \leq P$ , missä  $p_1, \dots, p_s$  ovat alkulukuja. Käytetään merkintää  $S_P$  joukolle

$$S_P = \{(-1)^{a_0} p_1^{a_1} p_2^{a_2} \cdots p_s^{a_s} : a_0 \in \{0, 1\} \text{ ja } a_1, \dots, a_s \in \mathbb{N} \cup \{0\}\}.$$

**Lemma 3.1.10.** *Olkoot  $x, y \in S_P$  siten, että  $\text{sy}(x, y) = 1$ ,  $|x| < |y|$  ja  $|y| \geq 3$ . Tällöin*

$$\text{rad}(x + y) \geq C \sqrt{\frac{\log |y|}{\log \log |y|}}$$

missä  $C > 0$  on vain luvusta  $P$  riippuva efektiivisesti laskettavissa oleva vakio.

*Todistus.* Koska luvun  $x + y$  radikaali on vähintään yhtä suuri kuin sen suurin alkutekijä, väite seuraa tuloksesta [58, Corollary 1.2, s. 41–45].  $\square$

Lemman suorana seurauksena saadaan

**Lemma 3.1.11.** *Olkoot  $x, y, z \in S$  siten, että  $\text{sy}(x, y) = 1$ ,  $|x| < |y|$ ,  $|y| \geq 3$  ja  $x + y = z$ . Tällöin luku  $\max(|x|, |y|, |z|)$  on rajoitettu kaikilla  $x, y, z$ .*

*Todistus.* Koska Lemman 3.1.10 oletukset sisältyvät väitteen oletuksiin, saadaan edellisen Lemman nojalla

$$\sqrt{\frac{\log |y|}{\log \log |y|}} \leq \frac{1}{C} \text{rad}(x + y) = \frac{1}{C} \text{rad}(z) \leq \frac{1}{C} p_1 p_2 \cdots p_s,$$

missä  $C$  on vain luvusta  $P$  riippuva vakio. Yllä olevan nojalla luku  $|y|$  on rajoitettu ja oletuksen mukaan  $|x|$  on rajoitettu, jolloin myös luku  $|z|$  on rajoitettu. Näin ollen myös maksimi luvuista  $|x|, |y|$  ja  $|z|$  on rajoitettu.  $\square$

**Huomautus 3.1.12.** Lemma 3.1.11 osoittaa itse asiassa, että joukko

$$\{(x, y, z) \in S_P^3 : \text{sy}(x, y) = 1, |x| < |y|, x + y = z\}$$

on äärellinen.

Saatua tulosta voidaan nyt soveltaa  $abc$ -kolmikon radikaaliin.

**Lause 3.1.13.** *Olkoon  $P \in \mathbb{N}_{\geq 3}$ . On vain äärellisesti  $abc$ -kolmikoita  $(a, b, c) \in \mathbb{Z}^3$ , joille  $\text{rad}(abc) \in S_P$ .*

*Todistus.* Jos  $\text{rad}(abc) \in S_P$ , niin tällöin lukujen  $a, b$  ja  $c$  alkutekijät kuuluvat joukkoon  $S_P$ . Valitsemalla tarvittaessa uudelleen luvut  $a, b$  ja  $c$  siten, että  $|a| < |b|$ , väite seuraa Lemmasta 3.1.11 ja Huomautuksesta 3.1.12.  $\square$

Koska avaruus  $\mathbb{N}^3$  on numeroituva, myös  $abc$ -kolmikoiden muodostama joukko on sen osajoukkona numeroituva. Näin ollen saadaan seuraava tulos.

**Lause 3.1.14.** *Olkoon jono  $(a_n, b_n, c_n)_{n \in \mathbb{N}}$  jokin  $abc$ -kolmikoiden järjestys. Tällöin*

$$\lim_{n \rightarrow \infty} \text{rad}(a_n b_n c_n) = \infty.$$

*Todistus.* Olkoon  $P \in \mathbb{N}_{\geq 3}$ . Nyt edellisen lauseen nojalla on olemassa luku  $n_0$  siten, että  $\text{rad}(a_n b_n c_n) > P$  aina kun  $n \geq n_0$ . Väite seuraa.  $\square$

## 3.2 Abc-konjektuuri

Oesterlé ja Masser esittivät *Abc*-konjektuurin vuonna 1985 yrityksenä ymmärtää paremmin Fermat'n suurta lausetta [47, s. 3–4], [49]. Heillä oli kuitenkin hieman erilainen näkemys konjektuurin formuloinnista: Masserin versio ammensi Stothers-Masonin lauseesta kun taas Oesterlé pohjasi näkemyksensä Szpiron elliptisiä käyriä koskeviin konjektuureihin [2].

Tässä alaluvussa tarkastellaan *Abc*-konjektuuria ja sen tyypillisimpiä esitysmuotoja soveltamalla edellisessä alaluvussa määriteltyä *abc*-kolmikon käsitettä. Aloitetaan tarkastelu esittämällä Masserin mukainen formulaatio *Abc*-konjektuurista [2], [46, s. 8–9].

**Konjektuuri 3.2.1** (*Abc*, versio I). *Jokaista reaalityyppistä lukua  $\varepsilon > 0$  kohden on olemassa luku  $C(\varepsilon) > 0$  siten, että kaikilla *abc*-kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  on voimassa epäyhtälö*

$$c \leq C(\varepsilon) \operatorname{rad}(abc)^{1+\varepsilon}. \quad (3.1)$$

Konjektuuri voidaan esittää yleisemmässä muodossa hieman oletuksia muuttamalla.

**Konjektuuri 3.2.2.** *Jokaista reaalityyppistä lukua  $\varepsilon > 0$  kohden on olemassa reaalityyppinen luku  $C(\varepsilon) > 0$  siten, että kaikilla *abc*-kolmikoilla  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$ , on voimassa epäyhtälö*

$$\max\{|a|, |b|, |c|\} \leq C(\varepsilon) \operatorname{rad}(abc)^{1+\varepsilon}.$$

**Huomautus 3.2.3.** Edellä esitetyt *Abc*-konjektuurit ovat ns. vahvassa muodossa, sillä lukua  $\varepsilon > 0$  ei ole kiinnitetty eikä lukua  $C(\varepsilon)$  siten ole tarkemmin määritetty. Heikosta muodosta puhutaan, mikäli oletetaan konjektuurin olevan totta vain jollekin kiinnitettylle luvulle  $\varepsilon > 0$ , esimerkiksi arvolle  $\varepsilon = 1$ . [4, s. 403]

Konjektuuri voidaan esittää myös hieman eri tavalla:

**Konjektuuri 3.2.4** (*Abc*, versio II). *Jokaista reaalityyppistä lukua  $\varepsilon > 0$  kohden on olemassa korkeintaan äärellisen monta *abc*-kolmikkaa  $(a, b, c) \in \mathbb{N}^3$ , joille pätee*

$$c > \operatorname{rad}(abc)^{1+\varepsilon}. \quad (3.2)$$

Osoitetaan, että konjektuurit ovat ekvivalentteja.

**Lause 3.2.5.** *Konjektuuri 3.2.1 on voimassa, jos ja vain jos Konjektuuri 3.2.4 on voimassa.*

*Todistus.* Oletetaan ensin, että Konjektuuri 3.2.1 on voimassa. Olkoon  $\varepsilon > 0$  mielivaltainen mutta kiinnitetty. Mikäli  $0 < C(\varepsilon) \leq 1$ , niin yksikään *abc*-kolmikko ei toteuta epäyhtälöä (3.2) ja väite on selvä. Jos  $C(\varepsilon) > 1$ , niin oletetaan vastoin väitettä, että on äärettömästi epäyhtälön (3.2) toteuttavia *abc*-kolmikoita  $(a, b, c)$ . Nämä kolmikot toteuttavat epäyhtälöketjun

$$\operatorname{rad}(abc)^{1+\varepsilon} < c < C(\varepsilon) \operatorname{rad}(abc)^{1+\varepsilon}$$

ja lisäksi kolmikoiden luku  $c$  voi saada mielivaltaisen suuria arvoja. Tästä johtuen Konjektuuria 3.2.1 arvolla  $\frac{\varepsilon}{2}$  sovellettaessa saadaan ristiriita oletuksen kanssa, sillä ei ole olemassa sellaista vakioa  $C(\frac{\varepsilon}{2})$ , että epäyhtälö

$$c \leq C\left(\frac{\varepsilon}{2}\right) \operatorname{rad}(abc)^{1+\frac{\varepsilon}{2}}$$

toteutuu kaikilla  $abc$ -kolmikoilla. Näin ollen epäyhtälön (3.2) toteuttavia  $abc$ -kolmikoita on korkeintaan äärellinen määrä.

Oletetaan sitten kääntäen, että Konjektuuri 3.2.4 on voimassa. Olkoon  $\varepsilon > 0$  mielivaltainen mutta kiinnitetty. Valitaan nyt

$$C(\varepsilon) = \max \left\{ 1, \sup \frac{c}{\text{rad}(abc)^{1+\varepsilon}} \right\},$$

missä supremum otetaan yli kaikkien epäyhtälön (3.2) toteuttavien  $abc$ -kolmikoiden. Näin ollen epäyhtälö (3.1) pätee kaikilla  $abc$ -kolmikoilla.  $\square$

Esitetään vielä yksi edellisten kanssa samantapainen  $Abc$ -konjektuurin muoto [46, s. 9].

**Konjektuuri 3.2.6.** *Jokaista reaalityttöä  $\varepsilon > 0$  kohden on olemassa luku  $C(\varepsilon) > 0$  siten, että kaikilla  $abc$ -kolmikoilla  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$ , on voimassa epäyhtälö*

$$\text{rad}(abc) \geq C(\varepsilon) (\max(|a|, |b|, |c|))^{1-\varepsilon}.$$

**Lause 3.2.7.** *Konjektuuri 3.2.2 ja Konjektuuri 3.2.6 ovat yhtäpitäviä.*

*Todistus.* Olkoot  $A, B \in \mathbb{R}_{>0}$ . Tällöin epäyhtälö

$$A \leq C(\varepsilon) B^{1+\varepsilon}$$

on ekvivalentti epäyhtälön

$$B \geq \left( \frac{A}{C(\varepsilon)} \right)^{\frac{1}{1+\varepsilon}} = \left( \frac{A}{C(\varepsilon)} \right)^{\frac{1+\varepsilon-\varepsilon'}{1+\varepsilon}} = C_1(\varepsilon') A^{1-\varepsilon'}$$

kanssa, kun valitaan  $\varepsilon' = \frac{\varepsilon}{1+\varepsilon}$  ja  $C_1(\varepsilon') = C(\frac{\varepsilon'}{1-\varepsilon'})^{\varepsilon'-1}$ . Väite seuraa.  $\square$

$Abc$ -konjektuurille voidaan esittää seuraava tulkinta:  $abc$ -kolmikosta muodostetun tulon  $abc$  kanonisessa esityksessä monet alkutekijät esiintyvät vain kerran ja jos jotkin alkutekijät esiintyvät useammin, niitä kompensoidaan joko suurilla alkutekijöillä tai monilla kerran esiintyvillä alkutekijöillä [36, s. 40]. Tulkintaa havainnollistaa seuraava taulukko, jossa tarkastellaan  $abc$ -kolmikoiden

$$a_n = 1, \quad b_n = 7^{2^n} - 1, \quad c_n = 7^{2^n}$$

kanonisia esityksiä arvoilla  $n = 2, 3, 4, 5, 6$  (Taulukko 1).

$n$	$a$	$b$	$c$
2	1	$2^5 \cdot 3 \cdot 5^2$	$7^4$
3	1	$2^6 \cdot 3 \cdot 5^2 \cdot 1201$	$7^8$
4	1	$2^7 \cdot 3 \cdot 5^2 \cdot 17 \cdot 1201 \cdot 169553$	$7^{16}$
5	1	$2^8 \cdot 3 \cdot 5^2 \cdot 17 \cdot 353 \cdot 1201 \cdot 169553 \cdot 47072139617$	$7^{32}$
6	1	$(7^{32} - 1)$ :n alkutekijät $\cdot 2 \cdot 7699649 \cdot 134818753 \cdot 531968664833$	$7^{64}$

Taulukko 1: Maplella laskettuja luvun  $7^{2^n} - 1$  kanonisia esityksiä.

Myös kirjan [53, s. 399–428] taulukot suhteellisten alkulukujen  $a^n \pm b^m$  kanonisista esityksistä tukevat edellä esitettyä tulkintaa.

Tarkastellaan sitten lähemmin  $Abc$ -konjektuuria. Seuraavasta lauseesta nähdään, että  $abc$ -kolmikidon muodostavien lukujen täytyy olla suhteellisia alkulukuja.

**Lause 3.2.8.** *Konjektuuri 3.2.4 ei ole voimassa, mikäli  $\text{sy}(a, b, c) > 1$ .*

*Todistus.* Valitaan  $\varepsilon = 1$  sekä luvut

$$a_n = 3^n, \quad b_n = 2 \cdot 3^n \quad \text{ja} \quad c_n = 3^{n+1}$$

kaikilla  $n \in \mathbb{N}$ . Tällöin selvästi  $a_n + b_n = c_n$ , ja edelleen

$$\text{rad}(a_n b_n c_n)^2 = (2 \cdot 3)^2 = 36 < 3^{n+1}$$

kaikilla  $n > 2$ . On siis äärettömän monta kolmikkoa  $(a_n, b_n, c_n)$ , joille  $c_n > \text{rad}(a_n b_n c_n)^{1+\varepsilon}$ , joten Konjektuuri 3.2.4 ei ole voimassa.  $\square$

$Abc$ -konjektuurissa luku  $C(\varepsilon) > 0$  on luvusta  $\varepsilon > 0$  riippuva mutta muuten sitä ei määritellä mitenkään tarkemmin. Eräs konjektuuriin liittyvä ongelma onkin kyseisten lukujen riippuvuussuhteen tarkempi määrittäminen. Artikkelissa [2] A. Baker ehdottaakin ongelman kiertämistä modifioimalla  $Abc$ -konjektuuria yhdenmukaisemmaksi logaritmistien muotojen kanssa seuraavasti.

**Konjektuuri 3.2.9** ( $Abc$ , Bakerin versio I). *Olkoon  $\varepsilon > 0$ . Tällöin on olemassa luvusta  $\varepsilon$  riippumaton vakio  $C > 0$  siten, että kaikille  $abc$ -kolmikoille  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$ , pätee epäyhtälö*

$$\max(|a|, |b|, |c|) \leq C (\varepsilon^{-\omega} \text{rad}(abc))^{1+\varepsilon},$$

missä  $\omega$  on tulon  $abc$  eri alkutekijöiden lukumäärä.

Hän ehdottaa myös seuraavaa muotoa.

**Konjektuuri 3.2.10** ( $Abc$ , Bakerin versio II). *Olkoon  $\varepsilon > 0$ . Tällöin on olemassa luvusta  $\varepsilon$  riippumattomat vakiot  $C > 0$  ja  $\kappa > 0$  siten, että kaikille  $abc$ -kolmikoille  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$ , pätee epäyhtälö*

$$\max(|a|, |b|, |c|) \leq C \varepsilon^{-\kappa \omega(ab)} \text{rad}(abc)^{1+\varepsilon},$$

missä  $\omega(ab)$  on tulon  $ab$  eri alkutekijöiden lukumäärä.

Mainitaan tässä yhteydessä vielä seuraava edellisten kanssa samankaltainen modifikaatio, joka on peräisin A. Granvillen kommentteista koskien A. Bakerin esityksiä [2].

**Konjektuuri 3.2.11** ( $Abc$ , Granville). *Olkoon  $\lambda > 0$  absoluuttinen vakio. Tällöin on olemassa vakio  $C > 0$  siten, että kaikille  $abc$ -kolmikoille  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$ , pätee epäyhtälö*

$$\max(|a|, |b|, |c|) \leq C \lambda^{\Omega(abc)} \text{rad}(abc),$$

missä  $\Omega(abc)$  on tulon  $abc$  alkutekijöiden lukumäärä.

Määrittelyongelmista huolimatta voidaan osoittaa, että luvun  $C(\varepsilon)$  suuruus riippuu jossain määrin käänteisesti luvun  $\varepsilon$  valinnasta. Tämän osoittamiseksi määritellään luku  $C(\varepsilon)$  tutkielman [56, s. 4] mukaisesti yhtälöllä

$$C(\varepsilon) = \sup \frac{c}{\text{rad}(abc)^{1+\varepsilon}},$$

missä supremum otetaan yli kaikkien  $abc$ -kolmikoiden. Näin luku  $C(\varepsilon)$  on yksikäsitteinen positiivinen reaaliluku tai ääretön kaikilla luvun  $\varepsilon > 0$  arvoilla. Itse asiassa, jos  $Abc$ -konjektuuri on totta, niin luku  $C(\varepsilon)$  on tällöin äärellinen (Huomautus 3.2.14). Seuraava tulos osoittaa luvun  $C(\varepsilon)$  kasvavan rajatta, kun luku  $\varepsilon$  lähenee nollaa [46, s. 10].

**Lause 3.2.12.** *Jos Konjektuuri 3.2.1 on voimassa, niin*

$$\lim_{\varepsilon \rightarrow 0} C(\varepsilon) = +\infty.$$

*Todistus.* Valitaan jokaista lukua  $n \in \mathbb{N}$  kohti kokonaisluvut  $x_n$  ja  $y_n$  siten, että

$$x_n + y_n\sqrt{2} = (3 + 2\sqrt{2})^n.$$

Lemman 2.2.11 nojalla luvut  $x_n$  ja  $y_n$  toteuttavat tällöin myös yhtälön  $x_n - y_n\sqrt{2} = (3 - 2\sqrt{2})^n$ , jolloin yhtälöt puolittain kertomalla saadaan

$$x_n^2 - 2y_n^2 = 1.$$

Valitaan nyt  $n = 2^m$ , jolloin Lemman 2.2.11 nojalla pätee  $2^{m+1} \mid y_n$  kaikilla  $m \in \mathbb{N}$ .

Oletetaan sitten, että Konjektuuri 3.2.1 on totta ja sovelletaan sitä  $abc$ -summaan

$$x_n^2 = 1 + 2y_n^2.$$

Ylöspäin arvioimalla saadaan

$$x_n^2 \leq C(\varepsilon) \text{rad}(2x_n y_n)^{1+\varepsilon} \leq C(\varepsilon) \left(\frac{x_n y_n}{2^m}\right)^{1+\varepsilon} \leq C(\varepsilon) \left(\frac{x_n^2}{2^m}\right)^{1+\varepsilon} = C(\varepsilon) \frac{x_n^{2(1+\varepsilon)}}{2^{m(1+\varepsilon)}},$$

josta edelleen

$$\frac{2^{m(1+\varepsilon)}}{x_n^{2\varepsilon}} \leq C(\varepsilon).$$

Antamalla nyt  $\varepsilon \rightarrow 0$  saadaan

$$\lim_{\varepsilon \rightarrow 0} C(\varepsilon) \geq 2^m,$$

mikä pätee kaikilla  $m \in \mathbb{N}$ . Väite seuraa.  $\square$

Tarkastellaan sitten konjektuurissa esiintyvää lukua  $\varepsilon > 0$ , joka on havaittavin ero  $Abc$ -konjektuurin kokonaisluku- ja polynomiversion (Stothers-Masonin lause) välillä. Osoitetaan W. Jastrzebowskin ja D. Spielmanin artikkelissa [36, s. 40–41] antamaa vastaesimerkkiä käyttämällä, että luvun  $\varepsilon$  olemassaolo on perusteltua.

**Lause 3.2.13.** *Konjektuuri 3.2.1 ei pidä paikkaansa, jos  $\varepsilon = 0$ .*

*Todistus.* Oletetaan vastoin väitettä, että on olemassa vakio  $K > 0$  siten, että kaikilla  $abc$ -kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  pätee epäyhtälö

$$c \leq K \operatorname{rad}(abc). \quad (3.3)$$

Asetetaan jokaisella  $n \in \mathbb{N}$   $abc$ -kolmikko  $(a, b, c)$  siten, että

$$a_n = 1, \quad b_n = 3^{2^n} - 1 \quad \text{ja} \quad c_n = 3^{2^n}.$$

Esimerkin 2.1.20 nojalla kaikilla  $n \in \mathbb{N}$  pätee  $2^n \mid (3^{2^n} - 1)$ , joten Lemmaa 3.1.7 soveltamalla saadaan tulon  $a_n b_n c_n$  radikaalille arvio

$$\begin{aligned} \operatorname{rad}(a_n b_n c_n) &= \operatorname{rad}(1 \cdot [3^{2^n} - 1] \cdot 3^{2^n}) = 3 \operatorname{rad}(3^{2^n} - 1) \\ &= 3 \operatorname{rad}\left(2^n \cdot \frac{3^{2^n} - 1}{2^n}\right) \leq 3 \cdot 2 \left(\frac{3^{2^n} - 1}{2^n}\right) = 6 \left(\frac{3^{2^n} - 1}{2^n}\right). \end{aligned}$$

Epäyhtälön (3.3) nojalla siten

$$3^{2^n} \leq 6K \left(\frac{3^{2^n} - 1}{2^n}\right),$$

josta saadaan edelleen

$$2^n \leq 6K \frac{3^{2^n} - 1}{3^{2^n}} = 6K \left(1 - \frac{1}{3^{2^n}}\right).$$

Antamalla muuttujan  $n$  kasvaa rajatta saadaan haettu ristiriita.  $\square$

**Huomautus 3.2.14.** Lauseen 3.2.13 mukaan ei siis ole olemassa sellaista vakioa  $K > 0$ , että kaikilla  $abc$ -kolmikoilla epäyhtälö (3.3) olisi voimassa. Esittämällä epäyhtälö (3.3) muodossa

$$\frac{1}{K} \leq \frac{\operatorname{rad}(abc)}{c}$$

saadaan tulkinta, jonka mukaan suhde  $\frac{\operatorname{rad}(abc)}{c}$  voidaan saada mielivaltaisen pieneksi. Tämä ei kuitenkaan enää onnistu, mikäli luku  $\frac{\operatorname{rad}(abc)}{c}$  korvataan luvulla  $\operatorname{rad}(abc)^{1+\varepsilon}$ , missä  $\varepsilon > 0$ . Konjektuurin 3.2.1 mukaan nimittäin on olemassa jokin luvusta  $\varepsilon$  riippuva alaraja (luku  $\frac{1}{C(\varepsilon)}$ ), jota pienemmäksi osamäärää

$$\frac{\operatorname{rad}(abc)^{1+\varepsilon}}{c}$$

ei saada, vaikka käydään läpi kaikki  $abc$ -kolmikot [23]. Erityisesti tämä tarkoittaa sitä, että luku  $C(\varepsilon)$  on äärellinen.

Esitetään vielä lopuksi Oesterlén lähestymistapa  $Abc$ -konjektuuriin [2], [46, s. 9]. Hän tarkasteli  $abc$ -kolmikon  $(a, b, c) \in \mathbb{N}^3$  laatua kuvaavaa  $L$ -arvoa, joka saadaan yhtälöstä

$$c = \operatorname{rad}(abc)^{L(a,b,c)}. \quad (3.4)$$

Yhtälöstä (3.4) saadaan  $L$ -arvolle seuraava määritelmä [8, s. 77].

**Määritelmä 3.2.15.**  $abc$ -kolmikon  $(a, b, c) \in \mathbb{N}^3$   $L$ -arvo määritellään lukuna

$$L = L(a, b, c) = \frac{\log c}{\log \text{rad}(abc)}.$$

**Huomautus 3.2.16.** Määritelmä 3.2.15 voidaan esittää yleisemmässä muodossa tarkastelemalla  $abc$ -kolmikoita  $(a, b, c) \in \mathbb{Z}$ ,  $abc \neq 0$ . Tällöin  $L$ -arvo määritellään lukuna

$$L = L(a, b, c) = \frac{\log \max(|a|, |b|, |c|)}{\log \text{rad}(abc)},$$

missä luku  $\log \max(|a|, |b|, |c|)$  on  $abc$ -kolmikon *korkeus* [20].

Tyypillisesti  $L$ -arvo on välillä  $[\frac{1}{3}, 1]$ .  $abc$ -konjektuurin kannalta mielenkiintoisia ovat kuitenkin  $L$ -arvot, jotka ovat suurempia kuin yksi, sillä suuri  $L$ -arvo kertoo  $abc$ -kolmikon suurimman luvun olevan huomattavan suuri suhteessa kolmikon radikaaliin. Suurten  $L$ -arvojen avulla saadaan arvioita  $abc$ -konjektuurissa esiintyvälle luvulle  $\varepsilon > 0$ .

$abc$ -kolmikon sanotaan olevan laadultaan *hyvä*, mikäli sen  $L$ -arvo on suurempi kuin 1,4 [47, s. 18]. Tällaisia kolmikoita tunnetaan tällä hetkellä 234 ja ne on esitetty laadun mukaan laskevassa järjestyksessä lähteessä [61]. Alla on taulukoitu kaikki tunnetut  $abc$ -kolmikot, joilla  $L > 1,55$  (Taulukko 2). Laajempi esitys hyvistä  $abc$ -kolmikoista löytyy liitteestä A.

No.	L(a,b,c)	$a$	$b$	$c$	löytövuosi
1	1,6299	2	$3^{10}109$	$23^5$	1987
2	1,6260	$11^2$	$3^25^67^3$	$2^{21}23$	1985
3	1,6235	$19 \cdot 1307$	$7 \cdot 29^231^8$	$2^83^{22}5^4$	1994
4	1,5808	283	$5^{11}13^2$	$2^83^817^3$	1993
5	1,5679	1	$2 \cdot 3^7$	$5^47$	1988

Taulukko 2: Viisi suurimman  $L$ -arvon antavaa  $abc$ -kolmikkoa.

Oesterlén esitti kysymyksen, onko  $L$ -arvojen joukko rajoitettu [6]. Tätä kysymystä tarkastellaan lähemmin alaluvussa 3.4. Konjektuurit 3.2.1 ja 3.2.4 voidaan kirjoittaa  $L$ -arvoa käyttämällä seuraavissa ekvivalenteissa muodoissa.

**Konjektuuri 3.2.17** (Abc, versio III). *Jokaista reaali lukua  $\varepsilon > 0$  kohden on olemassa luku  $C(\varepsilon) > 0$  siten, että että kaikilla  $abc$ -kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  on voimassa epäyhtälö*

$$L(a, b, c) \leq (1 + \varepsilon) + \frac{\log C(\varepsilon)}{\log \text{rad}(abc)}.$$

**Konjektuuri 3.2.18** (Abc, versio IV). *Jokaista reaali lukua  $\varepsilon > 0$  kohden on olemassa korkeintaan äärellisen monta  $abc$ -kolmikkoa  $(a, b, c) \in \mathbb{N}^3$ , joiden  $L$ -arvolle pätee*

$$L(a, b, c) > 1 + \varepsilon.$$

**Huomautus 3.2.19.** Konjektuurin 3.2.17 epäyhtälölle on voimassa radikaalista riippumaton yläraja

$$L(a, b, c) \leq 1 + \varepsilon + \frac{\log C(\varepsilon)}{\log 2},$$

sillä  $\text{rad}(abc) \geq 2$  kaikilla  $abc$ -kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  [44].

### 3.3 Abc-konjektuuriin liittyviä tuloksia

*Abc*-konjektuurin nojalla *abc*-kolmikon suurimmalla luvulla on kolmikon radikaalista riippuva polynomiaalinen yläraja. Tarkastellaan seuraavaksi *abc*-kolmikon suurimman luvun eksponentiaaliseen ylärajaan sekä lukujen  $C(\varepsilon)$  ja  $\varepsilon$  väliseen suhteeseen liittyviä tuloksia, joita on pystytty osoittamaan ilman oletuksia *Abc*-konjektuurin todenperäisyydestä.

Ensimmäisen eksponentiaaliseen ylärajaan liittyvän tuloksen osoittivat Stewart ja Tijdeman vuonna 1986 [64].

**Lause 3.3.1** (Stewart, Tijdeman). *Kaikilla abc-kolmikoilla pätee epäyhtälö*

$$c < \exp(D \operatorname{rad}(abc)^{15}),$$

missä  $D$  on efektiivisesti laskettavissa oleva vakio.

**Huomautus 3.3.2.** Tässä efektiivisesti laskettavissa (engl. effectively computable) olevalla tarkoitetaan sitä, että teoriassa ratkaisu voidaan selvittää (tietokone)algoritmin avulla [51]. Käytännössä ratkaisun selvittäminen tosin saattaa olla hyvinkin työlästä ja hidasta.

Stewart ja Yu paransivat tulosta logaritmin lineaarimuotojen  $p$ -adisten arvioiden avulla vuonna 1991 [62].

**Lause 3.3.3.** *On olemassa efektiivisesti laskettavissa oleva vakio  $K$  siten, että kaikille abc-kolmikoille on voimassa epäyhtälö*

$$c < \exp\left(\operatorname{rad}(abc)^{\frac{2}{3} + \frac{K}{\log \log \operatorname{rad}(abc)}}\right).$$

*Erityisesti jokaista lukua  $\varepsilon > 0$  kohti on olemassa efektiivisesti laskettavissa oleva vakio  $K(\varepsilon)$  siten, että kaikille abc-kolmikoille pätee*

$$c < \exp\left(K(\varepsilon) \operatorname{rad}(abc)^{\frac{2}{3} + \varepsilon}\right).$$

Vuonna 2001 Stewart ja Yu paransivat edelleen tulostaan [63].

**Lause 3.3.4.** *On olemassa efektiivisesti laskettavissa oleva vakio  $K$  siten, että kaikille abc-kolmikoille on voimassa epäyhtälö*

$$c < \exp\left(K \operatorname{rad}(abc)^{\frac{1}{3}} (\log \operatorname{rad}(abc))^3\right).$$

He osoittivat myös seuraavan Lauseen 3.3.4 heikomman version:

**Lause 3.3.5.** *Jokaista lukua  $\varepsilon > 0$  kohti on olemassa efektiivisesti laskettavissa oleva vakio  $K(\varepsilon)$  siten, että kaikille abc-kolmikoille pätee*

$$c < \exp\left(K(\varepsilon) \operatorname{rad}(abc)^{\frac{1}{3} + \varepsilon}\right).$$

**Huomautus 3.3.6.** Vaikka edellä olevat tulokset ovatkin *Abc*-konjektuurin väittämää heikompi antaen luvulle  $c$  vain eksponentiaalisen ylärajan, niissä esiintyvät vakiot ovat kuitenkin efektiivisesti laskettavissa riippuen pelkästään luvusta  $\varepsilon$ .



Stewart ja Tijdeman osoittivat vuonna 1986 myös seuraavan tuloksen, jonka mukaan  $Abc$ -konjektuurin väittäjä on "lähellä parasta mahdollista" [64].

**Lause 3.3.7.** *Jokaista  $\delta > 0$  kohti on olemassa äärettömästi  $abc$ -kolmikoita, joille pätee*

$$c > \text{rad}(abc) \exp \left( (4 - \delta) \frac{\sqrt{\log \text{rad}(abc)}}{\log \log \text{rad}(abc)} \right).$$

Lauseen 3.3.7 avulla Nitaj osoitti seuraavan tuloksen vuonna 1996 [47, s. 19–20].

**Lause 3.3.8.** *Kaikilla  $k > 0$  ja  $k_1 > 0$  on olemassa  $abc$ -kolmikko  $(a, b, c) \in \mathbb{N}^3$ , jolle*

$$c > k \text{rad}(abc) (\log \text{rad}(abc))^{k_1}.$$

*Todistus.* Olkoot  $k, k_1 > 0$  ja olkoon  $(a, b, c) \in \mathbb{N}^3$   $abc$ -summa siten, että  $0 < a < b < c$  ja luvut toteuttavat yhtälön

$$c \leq k \text{rad}(abc) (\log \text{rad}(abc))^{k_1}.$$

Olettamalla kolmikon  $(a, b, c)$  toteuttavan myös Lauseen 3.3.7 epäyhtälön saadaan

$$\text{rad}(abc) \exp \left( (4 - \delta) \frac{\sqrt{\log \text{rad}(abc)}}{\log \log \text{rad}(abc)} \right) < c \leq k \text{rad}(abc) (\log \text{rad}(abc))^{k_1}$$

jollekin  $\delta > 0$ . Tarkastellaan sitten reunimmaisista epäyhtälöistä. Jakamalla puolittain luvulla  $\text{rad}(abc)$  ja ottamalla puolittain logaritmi saadaan

$$(4 - \delta) \frac{\sqrt{\log \text{rad}(abc)}}{\log \log \text{rad}(abc)} < \log (k (\log \text{rad}(abc))^{k_1}),$$

josta edelleen

$$(4 - \delta) \sqrt{\log \text{rad}(abc)} < (\log k + k_1 \log \log \text{rad}(abc)) \log \log \text{rad}(abc).$$

Näin ollen luku  $\text{rad}(abc)$  on rajoitettu mikä johtaa ristiriitaan Lauseen 3.1.14 kanssa.  $\square$

Tuloksen avulla saadaan kielteinen vastaus kysymykseen, voidaanko  $Abc$ -konjektuurissa vakio  $C(\varepsilon)$  valita jonkinlaisena luvun  $\varepsilon > 0$  potenssin käänteislukuna [47, s. 20].

**Lause 3.3.9.** *Kaikilla  $k > 0$  on olemassa luku  $\varepsilon > 0$  ja  $abc$ -kolmikko  $(a, b, c) \in \mathbb{N}^3$  siten, että*

$$c > \frac{1}{\varepsilon^k} \text{rad}(abc)^{1+\varepsilon}.$$

*Todistus.* Olkoon  $k > 0$ . Oletetaan vastoin väitettä, että kaikilla  $\varepsilon > 0$  ja kaikilla  $abc$ -kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  pätee epäyhtälö

$$c \leq \frac{1}{\varepsilon^k} \text{rad}(abc)^{1+\varepsilon}.$$

Valitsemalla näin ollen  $\varepsilon = \frac{k}{\log \text{rad}(abc)}$  ja soveltamalla tietoa  $\text{rad}(abc)^{\frac{1}{\log \text{rad}(abc)}} = e$  epäyhtälö saa muodon

$$c \leq \left( \frac{e}{k} \right)^k \text{rad}(abc) (\log \text{rad}(abc))^k$$

ollen voimassa kaikilla  $abc$ -kolmikoilla. Tämä on ristiriita Lauseen 3.3.8 kanssa.  $\square$

### 3.4 $L$ -arvojen joukosta ja sen kasautumispisteistä

$abc$ -kolmikon  $(a, b, c) \in \mathbb{N}^3$   $L$ -arvo [8, s. 77] määriteltiin osamääränä

$$L = L(a, b, c) = \frac{\log c}{\log \operatorname{rad}(abc)}.$$

Käytetään kaikkien  $L$ -arvojen joukolle merkintää  $\mathcal{L}$ , toisin sanoen

$$\mathcal{L} = \{L(a, b, c) : (a, b, c) \in \mathbb{N}^3, \operatorname{syt}(a, b) = 1, a + b = c\}.$$

Tässä alaluvussa tarkastellaan lähemmin joukkoon  $\mathcal{L}$  liittyviä tuloksia. Luvun lopussa tarkastellaan joukon  $\mathcal{L}$  kasaantumispisteitä sekä esitetään kasaantumispisteiden supremumin avulla  $abc$ -kojektuurille ekvivalentti esitysmuoto.

Aloitetaan osoittamalla, että ainoastaan  $abc$ -kolmikolla  $(1, 1, 2)$   $L$ -arvo on rationaaliluku.

**Lemma 3.4.1.** *Olkoon  $(a, b, c) \in \mathbb{N}^3 \setminus \{1, 1, 2\}$  mielivaltainen  $abc$ -kolmikko. Tällöin*

$$L(a, b, c) \notin \mathbb{Q}.$$

*Todistus.* Oletetaan vastoin väitettä, että on olemassa ehdot toteuttava  $abc$ -kolmikko, jolle

$$L(a, b, c) = \frac{\log c}{\log \operatorname{rad}(abc)} = \frac{m}{n}, \quad (3.5)$$

missä  $m, n \in \mathbb{N}$ . Yhtälö (3.5) voidaan esittää ekvivalenttissa muodossa

$$c^n = \operatorname{rad}(abc)^m, \quad (3.6)$$

josta nähdään, että luvulla  $c$  ja tulolla  $abc$  täytyy olla samat alkutekijät. Huomautuksen 3.1.2 nojalla kuitenkin  $\operatorname{syt}(a, b) = \operatorname{syt}(b, c) = \operatorname{syt}(a, c) = 1$ , joten yhtälö (3.6) voi toteutua vain jos  $a = b = 1$ . Siis  $(a, b, c) = (1, 1, 2)$ , mikä on ristiriita.  $\square$

Osoitetaan sitten, että on korkeintaan äärellinen määrä tietyn  $L$ -arvon antavia  $abc$ -kolmikoita [44, s. 3]. Sitä varten tarvitsemme kuitenkin seuraavaa aputulosta [69, s. 51].

**Lemma 3.4.2.** *Jos luvut  $l_1, l_2, l_3, l'_1, l'_2, l'_3$  ovat nollasta eroavia algebrallisten lukujen logaritmeja ja*

$$\frac{l_1}{l'_1} = \frac{l_2}{l'_2} = \frac{l_3}{l'_3} \notin \mathbb{Q},$$

*niin luvut  $l_1, l_2, l_3$  ovat  $\mathbb{Q}$ -lineaarisesti riippuvia, ts. lineaarisesti riippuvia joukossa  $\mathbb{Q}$ .*

**Huomautus 3.4.3.** Lemmassa 3.4.2 myös luvut  $l'_1, l'_2, l'_3$  ovat  $\mathbb{Q}$ -lineaarisesti riippuvia, mikä nähdään vaihtamalla lukujen  $l_i$  ja  $l'_i$ ,  $i = 1, 2, 3$ , roolit.

**Lause 3.4.4.** *Olkoon  $\lambda \in \mathbb{R}_{>0}$ . Tällöin on olemassa korkeintaan äärellisen monta  $abc$ -kolmikkoa  $(a, b, c) \in \mathbb{N}^3$ , joiden  $L$ -arvolle pätee  $L(a, b, c) = \lambda$ .*

*Todistus.* Olkoot  $(a_i, b_i, c_i) \in \mathbb{N}^3 \setminus \{1, 1, 2\}$ ,  $i = 1, 2, 3$ , eri  $abc$ -kolmikoita, joilla on sama  $L$ -arvo  $\lambda$ . Merkitään kunkin kolmikon radikaalia  $r_i = \text{rad}(a_i b_i c_i)$  kaikilla  $i = 1, 2, 3$ . Tällöin Lemman 3.4.1 nojalla

$$\frac{\log c_1}{\log r_1} = \frac{\log c_2}{\log r_2} = \frac{\log c_3}{\log r_3} = \lambda \notin \mathbb{Q},$$

joten Lemman 3.4.2 ja Huomautuksen 3.4.3 mukaan luvut  $\log r_1$ ,  $\log r_2$  ja  $\log r_3$  ovat  $\mathbb{Q}$ -lineaarisesti riippuvia. Tällöin on olemassa luvut  $k_1, k_2, k_3 \in \mathbb{Z}$ , joille  $\text{sy}(k_1, k_2, k_3) = 1$ , siten, että

$$k_3 \log r_3 = k_1 \log r_1 + k_2 \log r_2,$$

joka edelleen voidaan esittää muodossa

$$r_3^{k_3} = r_1^{k_1} r_2^{k_2}.$$

Koska radikaali on aina neliövapaa, saadaan kaksi eri tapausta.

- Jos  $\text{sy}(r_1, r_2) = 1$ , niin tällöin  $k_1 = k_2 = k_3 = 1$  ja  $r_3 = r_1 r_2$ .
- Jos  $\text{sy}(r_1, r_2) \neq 1$ , niin tällöin joko  $k_3 = k_1 = 1$  ja  $k_2 = 0$ , jolloin  $r_3 = r_1$ , tai  $k_3 = k_2 = 1$  ja  $k_1 = 0$ , jolloin  $r_3 = r_2$

Tapauksista nähdään, että on korkeintaan kolme sellaista radikaalia  $\text{rad}(abc)$ , joita vastaavien  $abc$ -kolmikoiden  $L$ -arvo on  $\lambda$ . Lauseen 3.1.13 nojalla on vain äärellisen monta sellaista  $abc$ -kolmikkoa, joilla on sama radikaali. Väite seuraa.  $\square$

Määritellään sitten  $L$ -arvojen jonolle reaalityyppisten tapausten kasaantumispiste salliin myös tilanne, jossa kasaantumispiste on ääretön [66, s. 197].

**Määritelmä 3.4.5.** Piste  $\lambda \in \mathbb{R}_{>0} \cup \{\infty\}$  on joukon  $\mathcal{L}$  kasaantumispiste, jos on olemassa sellainen  $L$ -arvojen jono  $(L_n)_{n \in \mathbb{N}}$ , jolla  $L_n \neq \lambda$  kaikilla  $n \in \mathbb{N}$  ja

$$\lim_{n \rightarrow \infty} L_n = \lambda. \quad (3.7)$$

**Huomautus 3.4.6.** Jos jonolla  $(L_n)_{n \in \mathbb{N}}$  on raja-arvo (3.7), niin myös sen kaikilla osajonoilla on sama raja-arvo [66, s. 196].

Edellistä tulosta soveltamalla voidaan edelleen osoittaa seuraavat tulokset [56, s. 11–12].

**Lause 3.4.7.** Olkoon  $\lambda \in \mathbb{R}_{>0}$ . Luku  $\lambda$  on joukon  $\mathcal{L}$  kasaantumispiste, jos ja vain jos on olemassa eri  $abc$ -kolmikoista muodostuva jono  $((a_n, b_n, c_n))_{n \in \mathbb{N}}$ , jolle

$$\lim_{n \rightarrow \infty} L(a_n, b_n, c_n) = \lambda.$$

*Todistus.* Oletetaan ensin, että luku  $\lambda$  on joukon  $\mathcal{L}$  kasaantumispiste. Määritelmän 3.4.5 nojalla on siten olemassa  $L$ -arvojen jono  $(L_n)_{n \in \mathbb{N}}$ , jolle  $L_n \neq \lambda$  kaikilla  $n \in \mathbb{N}$  ja

$$\lim_{n \rightarrow \infty} L_n = \lambda.$$

Koska jokainen luku  $L_n$  on jonkin  $abc$ -kolmikon  $L$ -arvo, lauseen väite seuraa.

Oletetaan kääntäen, että on olemassa sellainen eri  $abc$ -kolmikoista muodostuva jono  $((a_n, b_n, c_n))_{n \in \mathbb{N}}$ , jolle pätee

$$\lim_{n \rightarrow \infty} L(a_n, b_n, c_n) = \lambda.$$

Lauseen 3.4.4 nojalla voidaan nyt muodostaa sellainen  $L$ -arvojen osajono  $(L(a_k, b_k, c_k))_{k \in \mathbb{N}}$ , jolle  $L(a_k, b_k, c_k) \neq \lambda$  kaikilla  $k \in \mathbb{N}$ . Huomautuksen 3.4.6 nojalla näin muodostetulla osajonolla on sama raja-arvo alkuperäisen jonon kanssa, joten se täyttää Määritelmän 3.4.5 oletukset. Piste  $\lambda$  on siis joukon  $\mathcal{L}$  kasaantumispiste.  $\square$

**Lause 3.4.8.** *Olkoon  $\alpha \in \mathbb{R}_{>0}$ . Jos on olemassa äärettömän monta eri  $abc$ -kolmikkoa, joille*

$$L(a, b, c) \geq \alpha,$$

*niin joukolla  $\mathcal{L}$  on kasaantumispiste, joka on vähintään  $\alpha$ .*

*Todistus.* Oletuksen toteuttavien  $abc$ -kolmikoiden joukosta voidaan muodostaa  $L$ -arvojen jono, joka suppenee kohti jotain pistettä  $\lambda \in [\alpha, \infty[$ . Lauseen 3.4.4 nojalla voidaan nyt muodostaa sellainen  $L$ -arvojen osajono  $(L(a_k, b_k, c_k))_{k \in \mathbb{N}}$ , jolle  $L(a_k, b_k, c_k) \neq \lambda$  kaikilla  $k \in \mathbb{N}$ . Huomautuksen 3.4.6 nojalla edelleen osajonon raja-arvo on sama kuin alkuperäisen jonon, jolloin väite seuraa Lauseesta 3.4.7.  $\square$

**Huomautus 3.4.9.** Koska kaikkien  $abc$ -kolmikoiden  $(a, b, c) \in \mathbb{N}^3$   $L$ -arvo on suurempi kuin nolla, Lauseen 3.4.8 nojalla joukolla  $\mathcal{L}$  on ainakin yksi kasaantumispiste. Joukon  $\mathcal{L}$  kasaantumispisteiden joukko on siis epätyhjä.

Pienimmälle kasaantumispisteelle saadaan itse asiassa seuraava helppo arvio [8, s. 95].

**Lause 3.4.10.** *Joukon  $\mathcal{L}$  jokainen kasaantumispiste on vähintään  $\frac{1}{3}$ .*

*Todistus.* Koska jokaisen  $abc$ -kolmikoiden  $(a, b, c) \in \mathbb{N}^3$  radikaalille pätee epäyhtälö

$$\text{rad}(abc) \leq abc < c^3,$$

saadaan  $L$ -arvolle alaraja

$$L(a, b, c) = \frac{\log c}{\log \text{rad}(abc)} > \frac{\log c}{\log c^3} = \frac{1}{3}.$$

Väite seuraa Lauseesta 3.4.8.  $\square$

Otetaan käyttöön seuraava merkintä [7, s. 66].

**Merkintä 3.4.11.** Käytetään joukon  $\mathcal{L}$  kasaantumispisteille merkintää  $\mathcal{L}'$ .

**Huomautus 3.4.12.** Lauseen 3.4.10 tulos voidaan tulkita siten, että  $\mathcal{L}' \subset [\frac{1}{3}, \infty[$ .

Tarkastellaan seuraavaksi joukkoon  $\mathcal{L}'$  liittyviä tuloksia. Vuonna 2000 J. Browkin [8, s. 95] osoitti, että

$$\left[ \frac{1}{3}, \frac{1}{2} \right] \subset \mathcal{L}'.$$

Tulos oli yksinkertaistus J. Browkinin, M. Filasetan, G. Greavesin ja A. Schinzelin vuonna 1997 julkaisemasta teoreemasta [7], jossa oleellisesti samoilla menetelmillä osoitettiin

$$\left[ \frac{1}{3}, \frac{15}{16} \right] \subset \mathcal{L}'.$$

G. Greaves ja A. Nitaj pystyivät vielä parantamaan tulosta vuonna 1999 [26].

**Lause 3.4.13** (Greaves, Nitaj).

$$\left[ \frac{1}{3}, \frac{36}{37} \right] \subset \mathcal{L}'.$$

Vuonna 1998 M. Filaseta ja S. Konyagin osoittivat edellisten tulosten inspiroimana, että joukolla  $\mathcal{L}$  on kasaantumispiste puoliavoimella välillä  $[1, \frac{3}{2})$  [18].

**Lause 3.4.14** (Filaseta, Konyagin).

$$\mathcal{L}' \cap [1, \frac{3}{2}) \neq \emptyset.$$

**Huomautus 3.4.15.** Lauseen 3.4.14 tarkasteluväliä voidaan itse asiassa siirtää vasemmalle hieman todistusta muuttamalla [18, s. 267–268]. Toisin sanoen, voidaan osoittaa, että

$$\mathcal{L}' \cap \left[ \frac{3}{3+\varepsilon}, \frac{3}{2+\varepsilon} \right] \neq \emptyset$$

kaikilla  $\varepsilon \in (0, 1)$ .

Aiemmat tulokset saatiin olettamatta mitään *Abc*-konjektuurin todenperäisyydestä. Osoitetaan sitten, että jos *Abc*-konjektuuri on voimassa, niin  $\mathcal{L}' \subset [\frac{1}{3}, 1]$ . Tarvitaan seuraavaa määritelmää [8, s. 95].

**Määritelmä 3.4.16.** Määritellään joukon  $\mathcal{L}'$  suurin kasautumispiste lukuna

$$\limsup \mathcal{L} = \sup \mathcal{L}' = \sup \{x \in \mathbb{R} : x \text{ on joukon } \mathcal{L} \text{ kasautumispiste}\}.$$

**Huomautus 3.4.17.** Supremumin määritelmän perusteella

- (i)  $x \leq \sup \mathcal{L}'$  kaikilla  $x \in \mathcal{L}'$  [66, s. 4],
- (ii)  $L$ -arvojen jonolle  $(L_n)_{n \in \mathbb{N}}$  on olemassa yksikäsitteinen luku  $\limsup \mathcal{L} \in \mathbb{R} \cup \{\infty\}$  siten, että kaikilla  $\varepsilon > 0$  pätee

$$L_n < \limsup \mathcal{L} + \varepsilon$$

lähtien jostain indeksistä  $n \geq k$ ,  $k \in \mathbb{N}$ , sekä

$$L_n > \limsup \mathcal{L} - \varepsilon$$

äärettömän monelle indeksille  $n$  [66, s. 187–188].

Seuraava esitys perustuu lähteisiin [56, s. 12] ja [71, s. 25–27].

**Lause 3.4.18.** *Konjektuuri 3.2.1 on totta, jos ja vain jos  $\limsup \mathcal{L} = 1$ .*

*Todistus.* Oletetaan ensin, että Konjektuuri 3.2.1 on totta. Tarkastellaan nyt  $abc$ -kolmikoiden jonoa  $(a_n, b_n, c_n)_{n \in \mathbb{N}}$ , missä  $c_n \leq c_{n+1}$ .  $L$ -arvolle saadaan nyt oletuksen nojalla lauseke

$$\begin{aligned} L(a_n, b_n, c_n) &= \frac{\log c_n}{\log \operatorname{rad}(a_n b_n c_n)} \\ &\leq \frac{\log (C(\varepsilon) \operatorname{rad}(a_n b_n c_n)^{1+\varepsilon})}{\log \operatorname{rad}(a_n b_n c_n)} \\ &= \frac{\log C(\varepsilon)}{\log \operatorname{rad}(a_n b_n c_n)} + 1 + \varepsilon. \end{aligned}$$

Lauseen 3.1.14 nojalla  $\operatorname{rad}(a_n b_n c_n)$  kasvaa rajatta, kun  $n \rightarrow \infty$ . Näin ollen Huomautuksen 3.4.17 kohtaa (ii) soveltamalla saadaan  $\limsup \mathcal{L} \leq 1$ .

Muodostetaan sitten ääretön jono  $abc$ -kolmikoita asettamalla kaikilla  $n \in \mathbb{N}$

$$a_n = 1, \quad b_n = 2^n - 1 \quad \text{ja} \quad c_n = 2^n.$$

Radikaalille saadaan siten kaikilla  $n \in \mathbb{N}$  arvio

$$\operatorname{rad}(2^n(2^n - 1)) = 2 \operatorname{rad}(2^n - 1) \leq 2 \cdot 2^n = 2^{n+1},$$

jota edelleen  $L$ -arvoon soveltamalla saadaan

$$L(a_n, b_n, c_n) = \frac{\log 2^n}{\log \operatorname{rad}(2^n(2^n - 1))} \geq \frac{n \log 2}{(n+1) \log 2} = \frac{n}{n+1} \rightarrow 1,$$

kun  $n \rightarrow \infty$ . Lauseen 3.4.8 nojalla joukolla  $\mathcal{L}$  on kasaantumispiste, joka on vähintään yksi. Huomautuksen 3.4.17 (i)-kohdan nojalla siten  $\limsup \mathcal{L} \geq 1$ . Yhdistämällä epäyhtälöt saadaan  $\limsup \mathcal{L} = 1$ .

Oletetaan kääntäen, että  $\limsup \mathcal{L} = 1$ . Tällöin Huomautuksen 3.4.17 (ii)-kohdan nojalla kaikilla  $\varepsilon > 0$  pätee

$$L(a_n, b_n, c_n) = \frac{\log c_n}{\log \operatorname{rad}(a_n b_n c_n)} \leq 1 + \varepsilon$$

aina kun  $n \geq k$  jollekin  $k \in \mathbb{N}$ . Toisin sanoen, kaikilla  $n \geq k$  pätee

$$c_n \leq \operatorname{rad}(a_n b_n c_n)^{1+\varepsilon}.$$

Valitaan sitten vakiot  $C_1(\varepsilon), C_2(\varepsilon), \dots, C_{k-1}(\varepsilon)$  siten, että epäyhtälö

$$c_i \leq C_i(\varepsilon) \operatorname{rad}(a_i b_i c_i)^{1+\varepsilon}$$

toteutuu kaikilla  $i = 1, 2, \dots, k-1$ . Määritellään

$$C(\varepsilon) = \max_{1 \leq i \leq k-1} \{C_i(\varepsilon), 1\},$$

jolloin epäyhtälö

$$c_n \leq C(\varepsilon) \operatorname{rad}(a_n b_n c_n)^{1+\varepsilon}$$

on voimassa kaikilla  $n \in \mathbb{N}$ . Väite seuraa. □

Paras joukkoon  $\mathcal{L}'$  liittyvä tulos on siten seuraava [7]:

**Lause 3.4.19.** *Konjektuuri 3.2.1 on totta, jos ja vain jos*

$$\mathcal{L}' = \left[ \frac{1}{3}, 1 \right].$$

### 3.5 Abc-konjektuurin efektiivisistä muodosta

Lauseessa 3.4.18 todettiin *Abc*-konjektuurin olevan yhtäpitävää sen kanssa, että  $L$ -arvojen joukon kasaantumispisteiden supremum on yksi. Herääkin kysymys, onko myös  $L$ -arvojen joukolla ylärajaa. Toisin sanoen, onko olemassa *abc*-kolmikko, joka antaa maksimaalisen  $L$ -arvon ja onko se jo löydetty? Tällä hetkellä korkein tunnettu  $L$ -arvo ([61], Liite A) on edelleenkin Eric Reyssatin vuonna 1987 löytämällä kolmikolla

$$(a, b, c) = (2, 3^{10}109, 23^5),$$

jonka  $L(a, b, c) = 1,6299117$ . Maksimaaliselle  $L$ -arvolle saadaan *Abc*-konjektuurin avulla seuraava A. Nitaj'n vuonna 1996 osoittama ehdollinen tulos [47, s. 17].

**Lause 3.5.1.** *Jos Konjektuurin 3.2.1 on totta, niin on olemassa maksimaalisen  $L$ -arvon antava *abc*-kolmikko  $(a, b, c) \in \mathbb{N}^3$ .*

*Todistus.* Oletetaan, että Konjektuuri 3.2.1 on totta. Oletetaan vastoin väitettä, että ei ole olemassa sellaista *abc*-kolmikkoa  $(a, b, c) \in \mathbb{N}^3$ , joka antaa maksimaalisen  $L$ -arvon. Olkoon  $(a_0, b_0, c_0) \in \mathbb{N}^3$  *abc*-kolmikko, jolle  $L(a_0, b_0, c_0) > 1$ . Konstruoidaan ääretön eri *abc*-kolmi-koista muodostuva jono  $(a_n, b_n, c_n)_{n \in \mathbb{N}}$  siten, että

$$L(a_n, b_n, c_n) > L(a_{n-1}, b_{n-1}, c_{n-1})$$

kaikilla  $n \in \mathbb{N}$ . Konjektuurin nojalla kaikilla  $\varepsilon > 0$  on olemassa vakio  $C(\varepsilon) > 0$  siten, että epäyhtälö

$$L(a_n, b_n, c_n) \leq 1 + \varepsilon + \frac{\log C(\varepsilon)}{\log \text{rad}(a_n b_n c_n)}.$$

toteutuu kaikilla  $n \in \mathbb{N}$ . Valitaan luku  $\varepsilon$  siten, että  $1 + \varepsilon < L(a_0, b_0, c_0)$ . Lauseen 3.1.14 nojalla radikaali  $\text{rad}(a_n b_n c_n)$  kasvaa rajatta, kun  $n \rightarrow \infty$ . Näin ollen saadaan

$$\lim_{n \rightarrow \infty} L(a_n, b_n, c_n) \leq 1 + \varepsilon < L(a_0, b_0, c_0),$$

mikä on ristiriita. □

Lauseen 3.5.1 tulosta *Abc*-konjektuuriin soveltamalla pystytään ohittamaan vaikeasti määritettävä vakio  $C(\varepsilon)$  ja saadaan efektiiviset tulokset mahdollistava muoto otaksumasta. Monien mielestä seuraava heikko konjektuuri pitää paikkansa [4, s. 403].

**Konjektuuri 3.5.2.** *Kaikilla *abc*-kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  pätee epäyhtälö*

$$c < \text{rad}(abc)^2.$$

**Huomautus 3.5.3.** Konjektuurin 3.5.2 avulla voidaan osoittaa Fermat'n suuri lause: Konjektuuri 3.5.2 implikoi lauseen väitteen tapauksessa  $n > 5$  ja tapauksille  $n = 3, 4, 5$  on olemassa todistukset [16]. Fermat'n suurta lausetta on käsitelty enemmän alaluvussa 3.9.

E. Reyssatin löytämän *abc*-kolmikokan sekä muiden laskettujen  $L$ -arvojen perusteella A. Nitaj esitti vuonna 1996 seuraavan vieläkin tarkemman heikon konjektuurin [47, s. 19].

**Konjektuuri 3.5.4.** *Kaikilla *abc*-kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  pätee epäyhtälö*

$$c < \text{rad}(abc)^{1,63}.$$

### 3.6 Abc-osumien lukumäärästä

*Abc*-konjektuuri voidaan esittää muodossa, jonka mukaan jokaisella  $\varepsilon > 0$  on olemassa korkeintaan äärellisen monta epäyhtälön

$$c > \text{rad}(abc)^{1+\varepsilon}. \quad (3.8)$$

toteuttavaa *abc*-kolmikkoa  $(a, b, c) \in \mathbb{N}^3$  (Konjektuuri 3.2.4). Tässä alaluvussa tarkastellaan yhtälön (3.8) arvolla  $\varepsilon = 0$  toteuttavia *abc*-kolmikoita sekä niiden lukumäärää. Tällaisia *abc*-kolmikoita kutsutaan *abc*-osumiksi [14, s. 1864].

**Määritelmä 3.6.1.** *Abc*-kolmikkoa  $(a, b, c) \in \mathbb{N}^3$  kutsutaan *abc*-osumaksi, jos  $\text{rad}(abc) < c$ .

**Huomautus 3.6.2.** Määritelmän 3.6.1 mukaan kaikkien *abc*-osumien  $L$ -arvolle pätee

$$L(a, b, c) = \frac{\log c}{\log \text{rad}(abc)} > 1.$$

Suurin osa *abc*-kolmikoista ei ole *abc*-osumia. Esimerkiksi 14 pienimmän *abc*-kolmikojoukosta ainoastaan yksi,  $(1, 8, 9)$ , on *abc*-osuma (Taulukko 3). Kyseisen kolmikojoukon ajatusta yleistämällä voidaan kuitenkin helposti osoittaa, että *abc*-osumia on äärettömästi.

No.	$a$	$b$	$c$	$\text{rad}(abc)$
1	1	1	2	2
2	1	2	3	6
3	1	3	4	6
4	1	4	5	10
5	2	3	5	30
6	1	5	6	30
7	1	6	7	42
8	2	5	7	70
9	3	4	7	42
10	1	7	8	14
11	3	5	8	30
12	1	8	9	6
13	2	7	9	42
14	4	5	9	30

Taulukko 3: Kolmikot  $(a, b, c) \in \mathbb{N}^3$ , joille  $a + b = c$ ,  $\text{syt}(a, b, c) = 1$  ja  $a \leq b < c < 10$ .

**Lause 3.6.3.** *Abc*-osumia on äärettömästi.

*Todistus.* Konsturoidaan ääretön jono *abc*-kolmikoita  $(a_n, b_n, c_n)$  asettamalla

$$a_n = 1, \quad b_n = 9^n - 1 \quad \text{ja} \quad c_n = 9^n$$

jokaisella  $n \in \mathbb{N}$ . Osoitetaan, että kyseiset kolmikot ovat *abc*-osumia.



Esimerkin 2.1.3 nojalla luku  $b_n$  voidaan kirjoittaa muodossa  $b_n = 2^3 j$ , jolloin edelleen  $\text{rad}(b_n) \leq 2j$  jollekin  $j \in \mathbb{N}$ . Koska tulolla  $a_n c_n$  on vain alkutekijä 3, saadaan

$$\text{rad}(a_n b_n c_n) \leq 2j \cdot 3 = 6j < 8j + 1 = c_n.$$

Näin ollen kolmikko  $(a_n, b_n, c_n)$  on  $abc$ -osuma kaikilla  $n \in \mathbb{N}$ . □

**Huomautus 3.6.4.** Lause 3.6.3 vahvistaa vielä sen, mitä jo Lauseen 3.2.13 nojalla tiedetään:  $abc$ -konjektuuri ei ole voimassa ilman lukua  $\varepsilon > 0$ . Tämä voidaan tulkita myös siten, että on olemassa äärettömästi  $abc$ -kolmikoita, joiden  $L$ -arvo on suurempi kuin yksi.

Lauseen 3.6.3 todistuksessa nähdään eräs keino konstruoida äärettömästi  $abc$ -osumia. S. Dahmen esittää artikkelissaan [14, s. 1865] seuraavan yleisemmän menetelmän.

**Lemma 3.6.5.** *Olkoot  $s \in \mathbb{N} \setminus \{1\}$  ja  $p$  alkuluku siten, että  $p \nmid s$ . Tällöin kolmikot*

$$(a_n, b_n, c_n) = (1, s^{(p-1)p^n} - 1, s^{(p-1)p^n})$$

*ovat  $abc$ -osumia tarpeeksi suurilla luvun  $n \in \mathbb{N}$  arvoilla.*

*Todistus.* Lemman 2.1.29 ja Eulerin lauseen (Lause 2.1.32) nojalla pätee kongruenssi

$$s^{(p-1)p^n} = s^{p^{n+1}-p^n} = s^{\phi(p^{n+1})} \equiv 1 \pmod{p^{n+1}},$$

jolloin siis  $p^{n+1} \mid b_n$ . Näin ollen tulon  $a_n b_n c_n$  radikaalille saadaan arvio

$$\text{rad}(a_n b_n c_n) \leq \frac{b_n}{p^n} \cdot 1 \cdot s \leq \frac{s}{p^n} c_n < c_n,$$

missä viimeinen epäyhtälö on voimassa aina, kun  $\frac{s}{p^n} < 1$ , ts. kaikilla  $n > \frac{\log s}{\log p}$ . Tarpeeksi suurilla luvun  $n$  arvoilla kaikki edellä olevan muotoiset  $abc$ -summat ovat siis  $abc$ -osumia. □

**Huomautus 3.6.6.** Vastaavanlaista konstruktiota ei ole pystytty esittämään sellaisille  $abc$ -osumille, joiden termistä mikään ei ole arvoltaan yksi.

$abc$ -osumia tiedetään siis olevan ääretön määrä. Empiirisesti  $abc$ -osumia on etsitty varsinkin Leidenin yliopiston BOINC-pohjaisen hajautetun laskennan projektin ABC@Homen [40] avulla. Havainnollisuuden vuoksi ensimmäiset 31  $abc$ -osumaa on esitetty taulukkona Liitteessä D. Varsinaisia algoritmeja  $abc$ -osumien tai *hyvien*  $abc$ -osumien ( $L$ -arvo vähintään 1,4) löytämiseksi ei tässä tutkielmassa kuitenkaan käsitellä, ks. [40], [46] tai [48].

$abc$ -osumien lukumäärän kuvaamiseksi otetaan käyttöön seuraava merkintä [14, s. 1865].

**Merkintä 3.6.7.** Merkitään  $abc$ -osumien lukumäärää funktiolla  $N : \mathbb{R}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ ,

$$N(X) = |\{abc\text{-osuma } (a,b,c) \in \mathbb{N}^3 \mid c \leq X\}|.$$

**Huomautus 3.6.8.**  $abc$ -osumien lukumäärälle ei ole esitetty asympotoottista kasvua kuvaavaa alkulukulauseen (Lause 2.8.4) kaltaista tulosta eikä yhteyttä alkulukujen lukumäärään. Empiiristen tulosten [40] perusteella  $abc$ -osumat näyttäisivät olevan alkulukuja huomattavasti harvemmassa, ks. Liite C.

S. Dahmen esitti vuonna 2008  $abc$ -osumien lukumäärällä olevan seuraavan alarajan [14]:

**Lause 3.6.9.** *Jokaista  $\varepsilon > 0$  kohti on olemassa  $X_0 > 0$  siten, että kaikilla  $X \geq X_0$  pätee*

$$N(X) \geq \exp((\log X)^{\frac{1}{2}-\varepsilon}).$$

*Todistus.* Olkoon  $q = \frac{b}{c} \in \mathbb{Q} \setminus \{0\}$  siten, että  $b, c \in \mathbb{Z} \setminus \{0\}$  ja  $\text{syt}(b, c) = 1$ . Määritellään luvun  $q$  korkeus funktiolla  $h : \mathbb{Q} \rightarrow \mathbb{R}$ ,

$$h(q) = \log(\max(|b|, |c|)),$$

missä merkinnällä  $|\cdot|$  tarkoitetaan standardin itseisarvon muodostamaa metriikkaa. Olkoon  $x \geq 5$  ja merkitään luvulla

$$n = \pi(x) - 1$$

lukumäärää parittomille alkuluvuille, jotka ovat korkeintaan yhtä suuria kuin  $x$ . Merkitään  $p_1, \dots, p_n$   $n$  ensimmäistä paritonta alkulukua. Tarkastellaan niiden virittämää joukon  $\mathbb{Q}_{>0}$  osajoukkoa

$$\mathcal{Q}_n := \{p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n} \mid a_i \in \mathbb{Z}\}$$

sekä rajoitettujen alkioiden muodostamaa osajoukkoa

$$\mathcal{B}_x := \{q \in \mathcal{Q}_n \mid h(q) \leq B(x)\},$$

missä  $B : \mathbb{R}_{>0} \rightarrow \mathbb{R}_{>0}$  on myöhemmin määritettävä muuttujan  $x$  funktio. Määritellään injektiivinen joukkohomomorfismi  $\varphi_n : \mathcal{Q}_n \rightarrow \mathbb{R}^n$ ,

$$\varphi_n(p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}) = (a_1 \log p_1, a_2 \log p_2, \dots, a_n \log p_n).$$

Tällöin joukko

$$\Lambda_n = \varphi_n(\mathcal{Q}_n) = \{(a_1 \log p_1, \dots, a_n \log p_n) \in \mathbb{R}^n \mid a_i \in \mathbb{Z}\}$$

on avaruuden  $\mathbb{R}^n$  täysiasteinen hila. Käytetään rajoitettujen alkioiden joukosta  $\mathcal{B}_x$  muodostetulle hilalle merkintää  $L_x = \varphi_n(\mathcal{B}_x)$ , toisin sanoen

$$L_x = \left\{ y \in \Lambda_n \mid \sum_{\substack{i=1 \\ y_i > 0}}^n y_i \leq B(x) \text{ ja } \sum_{\substack{i=1 \\ y_i < 0}}^n |y_i| \leq B(x) \right\},$$

sekä avaruuden  $\mathbb{R}^n$  rajoitettujen alkioiden joukolle merkintää

$$V_x = \left\{ y \in \mathbb{R}^n \mid \sum_{\substack{i=1 \\ y_i > 0}}^n y_i \leq B(x) \text{ ja } \sum_{\substack{i=1 \\ y_i < 0}}^n |y_i| \leq B(x) \right\}.$$

Näin ollen  $L_x \subset V_x$  ja joukon  $V_x$  tilavuus tunnetaan Huomautuksen 2.3.10 nojalla.

Todistuksessa tarkastellaan osamääränä  $\frac{b}{c}$  esitettyjä  $abc$ -kolmikoita  $(a, b, c) \in \mathbb{N}^3$ .  $abc$ -kolmikoiden  $(a, b, c) \in \mathbb{N}^3$ , joille  $\text{rad}(bc) \mid \prod_{i=1}^n p_i$ , ja järjestämättömien pariien  $\pm y \in \Lambda_n \setminus \{0\}$  välillä on nimittäin bijektiivinen kuvaus

$$(a, b, c) \mapsto \left\{ \varphi_n\left(\frac{b}{c}\right), -\varphi_n\left(\frac{b}{c}\right) \right\}.$$

Samana bijektiivisen kuvauksen nojalla parit  $\pm y \in L_x \setminus \{0\}$  vastaavat  $abc$ -kolmikoita  $(a, b, c)$ , joille  $\text{rad}(bc) \mid \prod_{i=1}^n p_i$  ja  $\log c \leq B(x)$ . Todistus perustuu oleellisesti pariien  $\pm y \in L_x \setminus \{0\}$  ja  $abc$ -kolmikoiden väliseen yhteyteen.

Määritellään joukon  $\mathcal{Q}_n$  osajoukko

$$\mathcal{Q}_{n,m} = \left\{ \frac{b}{c} \in \mathcal{Q}_n \mid b \equiv c \pmod{2^m}, \text{syt}(b, c) = 1 \right\}.$$

ja sitä vastaava hila  $\Lambda_{n,m} = \varphi_n(\mathcal{Q}_{n,m})$ . Lauseen 2.4.16 nojalla alkio 3 ja 5 virittävät ryhmän  $(\mathbb{Z}/2^m\mathbb{Z})^*$ . Esimerkkien 2.4.20 ja 2.4.31 mukaan on siten olemassa surjektiivinen homomorfismi  $\mathcal{Q}_n \rightarrow (\mathbb{Z}/2^m\mathbb{Z})^*$ , jonka ydin on ryhmä  $\mathcal{Q}_{n,m}$ . Näin ollen on ryhmät  $\mathcal{Q}_n/\mathcal{Q}_{n,m}$  ja  $(\mathbb{Z}/2^m\mathbb{Z})^*$  ovat isomorfiset. Esimerkin 2.4.33 nojalla siten  $|\mathcal{Q}_n/\mathcal{Q}_{n,m}| = 2^{m-1}$ , ja näin ollen vastaavalle hilalla pätee

$$|\Lambda_n/\Lambda_{n,m}| = 2^{m-1}. \quad (3.9)$$

Olkoon sitten  $\alpha \in \mathbb{Q} \cap (0, 1)$  ja olkoon  $\beta := 1 - \alpha$  sekä merkitään luvun  $\alpha$  nimittäjää luvulla  $d \in \mathbb{N}$ . Valitaan luku  $m \in \mathbb{N}$  siten, että  $d \mid m$  ja

$$2^{m-d} < \frac{\text{vol}_n V_x}{2^n \det \Lambda_n} \leq 2^m. \quad (3.10)$$

Jatkossa tarkastellaan joukon  $V_x$  sisään jäävien hilapisteiden  $\pm y \in L_x \setminus \{0\}$  lukumäärää soveltamalla Minkowskin konveksin kappaleen lausetta (Lause 2.3.7).

Tarkastellaan ensin epäyhtälön (3.10) ylärajaa. Lemman 2.3.9, Huomautuksen 2.3.10 sekä tiedon  $\det \Lambda_n = \prod_{i=1}^n \log p_i$  (Esimerkki 2.3.12) nojalla saadaan

$$\begin{aligned} 2^m &\geq \frac{\text{vol}_n V_x}{2^n \det \Lambda_n} = \frac{(2n)! B(x)^n}{(n!)^3 2^n \prod_{i=1}^n \log p_i} \\ &= \exp \left( \log \left( \left( \frac{(2n)! B(x)^n}{(n!)^3 2^n} \right) \left( \prod_{i=1}^n \log p_i \right)^{-1} \right) \right) \\ &= \exp \left( \log \left( \frac{(2n)! B(x)^n}{(n!)^3 2^n} \right) - \sum_{i=1}^n \log \log p_i \right). \end{aligned} \quad (3.11)$$

Lemman 2.7.17 nojalla

$$\log \left( \frac{(2n)!}{(n!)^3 2^n} \right) = n \log \left( \frac{2e}{n} \right) + \mathcal{O}(\log n).$$

Edellä olevan sekä Lemman 2.8.10 nojalla saadaan epäyhtälöstä (3.11) siten

$$\begin{aligned} 2^m &\geq \exp \left( \log \left( \frac{(2n)!}{(n!)^3 2^n} B(x)^n \right) - \sum_{i=1}^n \log \log p_i \right) \\ &\geq \exp \left( n \log \left( \frac{2e B(x)}{x} \right) + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right). \end{aligned} \quad (3.12)$$

Tarkastellaan sitten epäyhtälön (3.10) alarajaa. Aiemmin asetettiin  $m = kd$  jollekin  $k \in \mathbb{N}$  ja  $\alpha = \frac{k'}{d}$  jollekin  $k' \in \mathbb{N}$ ,  $k' < d$ , jolloin

$$\alpha m = \frac{k'}{d} \cdot kd = kk' \quad \text{ja} \quad \beta m = (1 - \alpha)m = k(d - k'),$$

toisin sanoen  $\alpha m, \beta m \in \mathbb{N}$ . Koska  $m = m(1 - \alpha) + \alpha m = \beta m + 1 + \alpha m - 1$ , epäyhtälöstä (3.10) saadaan

$$\text{vol}_n(V_x) > 2^{m-d} 2^n \det \Lambda_n = 2^{\beta m + 1 - d} 2^n 2^{\alpha m - 1} \det \Lambda_n = 2^{\beta m + 1 - d} 2^n \det \Lambda_{n, \alpha m}, \quad (3.13)$$

missä viimeinen yhtäsuuruus seuraa Huomautuksesta 2.4.27, Esimerkistä 2.4.38 sekä yhtälöstä (3.9). Myöhemmin todistuksessa nähdään, että  $2^m \rightarrow \infty$ , kun  $x \rightarrow \infty$ , joten riittävän suurella muuttujan  $x$  arvolla  $2^{\beta m + 1 - d} \in \mathbb{N}$ . Soveltamalla epäyhtälöön (3.13) Minkowskin konveksin kappaleen lausetta (Lause 2.3.7) nähdään, että tarpeeksi suurella muuttujan  $x$  arvolla on ainakin  $2^{\beta m + 1 - d}$  erilaista nollasta eroavaa paria  $\pm y \in \Lambda_{n, m}$ , jotka sisältyvät joukkoon  $V_x$  ja siten myös joukkoon  $L_x$ . Aiemmin mainitun bijektio nojalla nämä pisteparit vastaavat  $2^{\beta m + 1 - d}$  eri  $abc$ -kolmikkoo  $(a, b, c) \in \mathbb{N}^3$ , joille  $\log c \leq B(x)$  sekä

$$\text{rad}(bc) \mid \prod_{i=1}^n p_i \quad \text{ja} \quad 2^{\alpha m} \mid c - b = a. \quad (3.14)$$

Jälkimmäinen tieto seuraa joukon  $\mathcal{Q}_{n, m}$  määritelmästä.

Osoitetaan seuraavaksi, että tarpeeksi suurilla muuttujan  $x$  arvoilla edellä mainitut  $abc$ -kolmikot ovat itse asiassa  $abc$ -osumia. Soveltamalla radikaaliin tietoja (3.14), arvioita  $a = c - b \leq c$  ja (3.12) sekä Lemmaa 2.8.11 saadaan

$$\begin{aligned} \text{rad}(abc) &\leq \frac{a}{2^{\alpha m}} \prod_{i=1}^n p_i \leq c \left( \frac{1}{2^m} \right)^\alpha \prod_{i=1}^n p_i \\ &\leq c \exp \left( n \log \left( \frac{x}{e} \left( \frac{x}{2eB(x)} \right)^\alpha \right) - \frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right). \end{aligned}$$

Yksinkertaistetaan radikaalille saatua arviota määrittelemällä rajoitefunktio  $B$  siten, että

$$\frac{x}{e} \left( \frac{x}{2eB(x)} \right)^\alpha = 1, \quad (3.15)$$

toisin sanoen

$$B(x) = \frac{1}{2} \left( \frac{x}{e} \right)^{1 + \frac{1}{\alpha}}.$$

Näin ollen riittävän suurilla muuttujan  $x$  arvoilla pätee epäyhtälö

$$\text{rad}(abc) \leq c \exp \left( -\frac{x}{\log^2 x} + \mathcal{O} \left( \frac{x}{\log^3 x} \right) \right) < c,$$

jolloin kyseessä olevat  $abc$ -kolmikot ovat todella  $abc$ -osumia. Koska joukkoon  $L_x$  kuuluville  $abc$ -kolmikoille pätee  $\log c \leq B(x)$ , toisin sanoen  $c \leq \exp(B(x))$ ,  $abc$ -osumien lukumäärä-funktion  $N$  määritelmän mukaan siten tarpeeksi suurilla muuttujan  $x$  arvoilla pätee

$$N(\exp(B(x))) \geq 2^{\beta m + 1 - d}. \quad (3.16)$$

Arviossa (3.16) on siis huomioitu myös sellaiset  $abc$ -osumia vastaavat nolasta eroavat parit  $\pm y \in \Lambda_{n,m}$ , joille  $2^{\alpha m} \nmid c - b = a$ .

Arvioidaan sitten epäyhtälöä (3.16) siten, että saadaan viimein lauseen väite. Kirjoittamalla yhtälö (3.15) muodossa

$$\frac{2eB(x)}{x} = \left(\frac{x}{e}\right)^{\frac{1}{\alpha}}$$

saadaan luvulle  $2^m$  epäyhtälöä (3.12) soveltamalla Lemman 2.8.12 mukaisesti arvio

$$2^m \geq \exp\left(\frac{x}{\alpha} \left[1 + \frac{1}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right)\right]\right).$$

Näin ollen nähdään, että  $2^m \rightarrow \infty$ , kun  $x \rightarrow \infty$ . Soveltamalla saatua arviota epäyhtälöön (3.16) saadaan tarpeeksi suurille muuttujan  $x$  arvoille edelleen arvio

$$\begin{aligned} N(\exp(B(x))) &\geq \exp(\log 2^{m\beta+1-d}) = \exp(\beta \log 2^m + (1-d) \log 2) \\ &\geq \exp\left(\beta \log \left[\exp\left(\frac{x}{\alpha} \left[1 + \frac{1}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right)\right]\right)\right] + (1-d) \log 2\right) \\ &= \exp\left(\frac{\beta}{\alpha} x \left[1 + \frac{1}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right) + \frac{\alpha}{\beta x} (1-d) \log 2\right]\right) \\ &\geq \exp\left(\frac{\beta}{\alpha} x\right). \end{aligned}$$

Sijoittamalla sitten tieto  $\beta = 1 - \alpha$  sekä yhtälöstä (3.15) saatu  $x = e(2B(x))^{\frac{\alpha}{\alpha+1}}$  saadaan

$$N(\exp(B(x))) \geq \exp\left(\frac{1-\alpha}{\alpha} e(2B(x))^{\frac{\alpha}{\alpha+1}}\right) = \exp(C'_\alpha B(x)^{\frac{\alpha}{\alpha+1}}),$$

missä  $C'_\alpha := e(\frac{1}{\alpha} - 1)2^{\frac{\alpha}{\alpha+1}} > 0$ . Koska kuvaus  $x \mapsto \exp(B(x)) : (0, \infty) \rightarrow (1, \infty)$  on surjektio ja monotonisesti kasvava, voidaan tehdä muuttujanvaihto asettamalla  $\exp(B(x)) = X$ , toisin sanoen  $B(x) = \log X$ . Näin ollen edellisen nojalla tarpeeksi suurilla muuttujan  $X$  arvoilla pätee

$$N(X) \geq \exp(C'_\alpha (\log X)^{\frac{\alpha}{\alpha+1}}).$$

Koska  $0 < \frac{\alpha}{\alpha+1} < \frac{1}{2}$  tarkasteltavalla välillä  $0 < \alpha < 1$ , voidaan osamäärä  $\frac{\alpha}{\alpha+1}$  esittää luvun  $\varepsilon > 0$  avulla asettamalla  $\frac{\alpha}{\alpha+1} = \frac{1}{2} - \varepsilon$ , jolloin myös vakio  $C'_\alpha$  korvataan vastaavalla luvulla  $C_\varepsilon$ . Tällöin jostaista  $\varepsilon > 0$  kohden on olemassa luku  $C_\varepsilon > 0$  siten, että tarpeeksi suurilla muuttujan  $X$  arvoilla

$$N(X) \geq \exp(C_\varepsilon (\log X)^{\frac{1}{2}-\varepsilon}).$$

Lopuksi nähdään, että jokaisella  $\varepsilon > 0$  ja riittävän suurella muuttujan  $X$  arvolla pätee

$$\log N(X) \geq C_\varepsilon (\log X)^{\frac{1}{2}-\varepsilon} = C_\varepsilon (\log X)^{\frac{1}{2}} (\log X)^{\frac{1}{2}-\varepsilon} \geq (\log X)^{\frac{1}{2}-\varepsilon},$$

mistä väite seuraa. □

**Huomautus 3.6.10.** Lauseen 3.6.9 antama alaraja ei ole paras mahdollinen. Todistus perustuu oleellisesti siihen, että tarkasteltavien  $abc$ -kolmikoiden luku  $a$  on jaollinen jollain luvun 2 suurella potenssilla. Tällöin tarkastelun ulkopuolella jää monta  $abc$ -kolmikkoa. Lauseen 3.6.9 tulos ei kuitenkaan välttämättä parane, vaikka käytettäisiin menetelmää, jossa huomioidaan luvun  $a$  olevan jaollinen joidenkin muiden lukujen suurilla potensseilla. Dahmen kuitenkin uskoo, että alarajaa voidaan oleellisesti samalla päättelyllä parantaa korvaamalla  $(\log X)^\varepsilon$  jollakin funktion  $\log \log X$  potenssilla. [14]

Lauseen 3.6.9 perusteella on luonnollista kysyä, kuinka hyvin alarajafunktio approksimoi  $abc$ -osumien lukumääräfunktiota  $N(X)$ . Alustavan arvion saamiseksi voidaan käyttää Leidenin yliopiston BOINC-pohjaisen hajautetun laskennan projektin ABC@Homen [40] tuloksena marraskuussa 2011 saatua listaa kaikista  $abc$ -osumista, joille  $a < b < c < 10^{18}$ . Kuvassa 3 nähdään tilanne arvoilla  $X \leq 10^6$ .

Jo arvoilla  $X \leq 10^6$  nähdään alarajafunktion olevan todella löysä. Toki kyseessä on hyvin lyhyt väli eikä asymptoottisesta käyttäytymisestä voida vielä sen perusteella sanoa paljoa, mutta selvästikään ei voida vielä puhua approksimaatiosta. Suurin syy tähän lienee jo aiemmin mainittu huomio, että Lauseen 3.6.9 alarajafunktio ei huomioi kaikkia mahdollisia  $abc$ -osumia. Kuvassa 4 on graafisesti haettu lukumääräfunktiolle  $N(X)$  parempaa approksimaatiota arvoilla  $X \leq 10^{10}$  käyttämällä funktioita

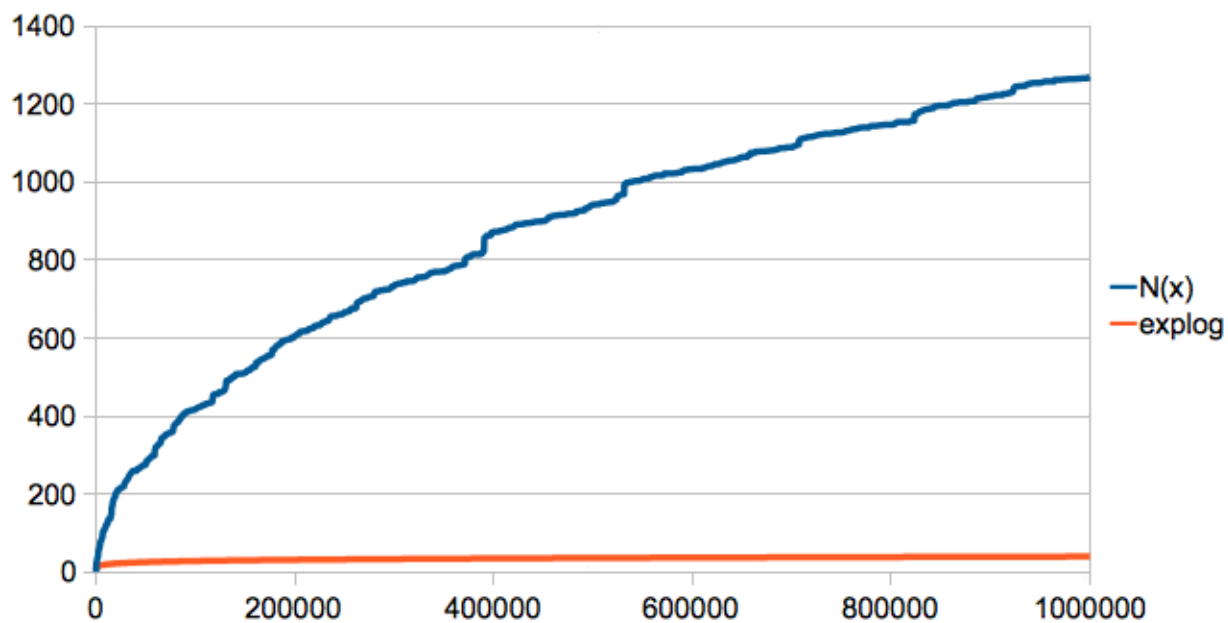
$$\begin{array}{ll} \sqrt{x} & (\text{sqrt\_x}), \\ \exp((\log X)^{\frac{1}{2}}) & (\text{explog}), \\ \exp((\log X)^{\frac{1}{2}}(\log \log X)^{\frac{1}{2}}) & (\text{exploglog}), \\ \exp((\log X)^{\frac{1}{2}}(\log \log X)^{\frac{7}{10}}) & (\text{exploglog7/10}). \end{array}$$

Kuvasta 4 nähdään, että varsinkin viimeisimmäksi mainittu funktio antaa jo kohtalaisen approksimaation funktiolle  $N(X)$  kyseisillä muuttujan  $X$  arvoilla.

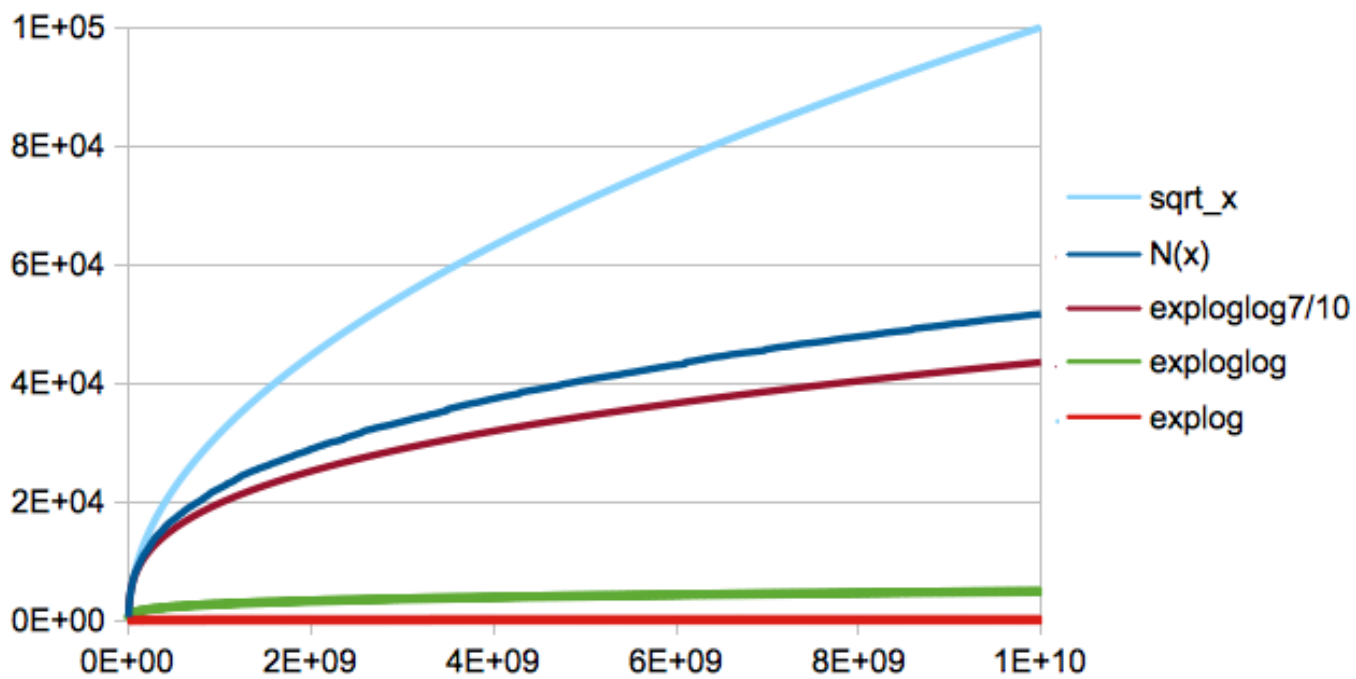
$abc$ -osumien ylärajalle ei ole osoitettu olevan mitään rajoittavaa funktiota. ABC@Homen laskentatulosten perusteella artikkelissa [22] ehdotetaan funktion  $X^{\frac{2}{3}}$  olevan eräs tällainen ylärajafunktio. Kuvan 4 perusteella voidaan kuitenkin ehdottaa Lausetta 3.6.9 ja artikkelia [14] mukaillen vielä tiukempaa ylärajaa:

**Konjektuuri 3.6.11.** *Jokaista  $\varepsilon > 0$  kohti on olemassa  $X_0 > 0$  siten, että kaikilla  $X \geq X_0$  pätee*

$$N(X) \leq X^{\frac{1}{2}+\varepsilon}.$$



Kuva 3: *Abc*-osumien lukumääräfunktio  $N(X)$  ja alarajafunktio  $\exp((\log X)^{\frac{1}{2}})$ .



Kuva 4: *Abc*-osumien lukumääräfunktio  $N(X)$  ja sitä rajoittavia funktioita.

### 3.7 Logaritmisten abc-osumien lukumäärästä

Edellisessä alaluvussa todettiin olevan äärettömästi  $abc$ -osumia, toisin sanoen epäyhtälön

$$c > \text{rad}(abc)$$

toteuttavia  $abc$ -kolmikoita  $(a, b, c) \in \mathbb{N}^3$ . Seuraavassa tarkastellaan  $abc$ -kolmikoille asetettua vieläkin tiukempaa ehtoa, jonka tarkoituksena on muodostaa rakenteellista yhteneväisyyttä kokonaislukujen ja funktioteorian välille, ks. alaluku 5.4. Tämä alaluku sisältää kirjallisuudessa aiemmin julkaisematonta tietoa ja perustuu allekirjoittaneen sekä professori Risto Korhosen välisiin keskusteluihin.

**Määritelmä 3.7.1.**  $abc$ -kolmikka  $(a, b, c) \in \mathbb{N}^3$  kutsutaan *logaritmiseksi abc-osumaksi*, jos

$$\text{rad}(abc) < \frac{c}{\log c}.$$

**Huomautus 3.7.2.** Kaikki logaritmiset  $abc$ -osumat ovat myös “tavallisia“  $abc$ -osumia, sillä kaikilla  $c > e$  logaritmisille  $abc$ -osumille pätee epäyhtälöketju

$$\text{rad}(abc) < \frac{c}{\log c} < c.$$

Logaritmiehdon asettaminen  $abc$ -kolmikoille pienentää todella tehokkaasti tarkasteltavien osumien määrää, sillä nyt radikaalin täytyy olla jo huomattavasti kolmikön suurinta lukua pienempi. Ensimmäinen logaritmisen  $abc$ -osuma onkin vasta

$$(1, 2400, 2401) = (1, 2^5 3 \cdot 5^2, 7^4),$$

ja seuraavien logaritmisten  $abc$ -osumien suurimman luvun arvo kasvaa nopeasti, ks. liite E. Kuten  $abc$ -osumien tapauksessa, myös logaritmisten  $abc$ -osumien kohdalla voidaan pienimmästä kolmikön ajatusta yleistämällä osoittaa tarkasteltavia osumia olevan ääretön määrä.

**Lause 3.7.3.** *Logaritmisiä abc-osumia on äärettömästi.*

*Todistus.* Osoitetaan väite konstruoimalla ääretön jono  $abc$ -kolmikoita  $(a_n, b_n, c_n)$  asettamalla

$$a_n = 1, \quad b_n = 7^{2^n} - 1, \quad \text{ja} \quad c_n = 7^{2^n},$$

jokaisella  $n \in \mathbb{N}$ . Osoitetaan, että arvosta  $n = 2$  lähtien kyseiset kolmikot ovat logaritmisiä  $abc$ -osumia.

Esimerkin 2.1.22 nojalla arvoilla  $n \geq 2$  pätee  $2^{n+3} 5^2 \mid b_n$ . Näin ollen saadaan arvio

$$\text{rad}(a_n b_n c_n) \leq 1 \cdot \frac{b_n}{2^{n+2} 5} \cdot 7 \leq \frac{7}{2^{n+2} 5} c_n \leq \frac{7}{2^{n+2} 4} c_n = \frac{7}{2^{n+4}} c_n.$$

Lauseen väitteen todistamiseksi riittää näyttää, että

$$\frac{7}{2^{n+4}} < \frac{1}{\log c_n} = \frac{1}{2^n \log 7}.$$

kaikilla  $n \geq 2$ . Ristiinkertomalla ja termejä järjestelemällä saadaan ekvivalentti epäyhtälö

$$2^{n+4} - 7 \cdot 2^n \log 7 = 2^n (2^4 - 7 \log 7) > 0.$$

Koska  $2^n > 0$  kaikilla  $n \geq 2$  ja  $2^4 - 7 \log 7 \approx 2,38 > 0$ , epäyhtälön vasen puoli on positiivinen kaikilla  $n \geq 2$ .  $\square$



**Huomautus 3.7.4.** Lauseen 3.7.3 todistuksen  $abc$ -kolmikolle ehto

$$\frac{7}{2^{n+4}} < \frac{1}{\log c_n}$$

on paras mahdollinen tai ainakin hyvin lähellä sitä, sillä ehtoa ei voida enää tiukentaa korvaamalla termi  $\log c_n$  termillä  $(\log c_n)^{1+\delta}$ , missä  $\delta > 0$ . Tällöin nimittäin saadaan epäyhtälö

$$2^{n+4} - 7(2^n \log 7)^{1+\delta} = 2^{n+4} - 7 \cdot 2^{n(1+\delta)} (\log 7)^{1+\delta} = 2^n (2^4 - 7 \cdot 2^{n\delta} (\log 7)^{1+\delta}) > 0,$$

jonka vasen puoli ei enää ole positiivinen kaikilla muuttujan  $n \geq 2$  arvoilla.

Tiukentamalla  $abc$ -osumille asetettua ehtoa saadaan siis vielä äärettömästi osumia  $abc$ -kolmikoiden joukosta. Koska logaritmiset  $abc$ -osumat ovat myös tavallisia  $abc$ -osumia, voidaan edellisiä etsiä jälkimmäisten joukosta käyttämällä hyväksi aiemmin mainittun Leidenin yliopiston hajautetun laskennan projektin ABC@Homen [40] tuloksia. Logaritmisten  $abc$ -osumien löytämiseen käytetty java-algoritmi on esitetty Liitteessä F ja sen tuloksena saadut 31 ensimmäistä logaritmistä  $abc$ -osumaa on esitetty taulukkona Liitteessä E.

Logaritmisten  $abc$ -osumien lukumäärän kuvaamiseksi otetaan käyttöön seuraava tavallisten  $abc$ -osumien kanssa analoginen merkintä:

**Merkintä 3.7.5.** Merkitään logaritmisten  $abc$ -osumien lukumäärää analogisesti funktiolla  $N_{\log} : \mathbb{R}_{\geq 0} \rightarrow \mathbb{Z}_{\geq 0}$ ,

$$N_{\log}(X) = |\{\text{logaritminen } abc\text{-osuma } (a,b,c) \in \mathbb{N}^3 \mid c \leq X\}|.$$

Logaritmisten  $abc$ -osumien lukumäärän kasvu on tiukemmista ehdoista johtuen huomattavasti  $abc$ -osumien lukumäärän kasvua hitaampaa. Tämän voi nähdä vertaamalla funktion  $N_{\log}$  arvoja funktion  $N$  arvoihin (Taulukko 4). Voidaan kuitenkin osoittaa, että S. Dahmenin  $abc$ -osumien lukumäärälle osoittama alaraja (Lause 3.6.9) pätee myös logaritmisten  $abc$ -osumien lukumäärälle.

$X$	$N_{\log}(X)$	$N(X)$
10	0	1
$10^2$	0	6
$10^3$	0	31
$10^4$	4	120
$10^5$	10	418
$10^6$	40	1268
$10^7$	129	3499
$10^8$	312	8987
$10^9$	756	22 316
$10^{10}$	1661	51 677
$10^{11}$	3776	116 978
$10^{12}$	7838	252 856

Taulukko 4: Logaritmisten ja tavallisten  $abc$ -osumien lukumääräfunktioiden arvoja.

**Lause 3.7.6.** Jokaista  $\varepsilon > 0$  kohti on olemassa  $X_0 > 0$  siten, että kaikilla  $X \geq X_0$  pätee

$$N_{\log}(X) \geq \exp((\log X)^{\frac{1}{2}-\varepsilon}).$$

*Todistus.* Lauseen 3.6.9 todistuksessa määriteltiin rajoitefunktio  $B$  yhtälöllä (3.15) siten, että riittävän suurilla muuttujan  $x$  arvoilla tarkastelluille  $abc$ -kolmikoille pätee

$$\text{rad}(abc) \leq c \exp\left(-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right)\right) < c.$$

Osoitetaan, että tarkasteltavat  $abc$ -kolmikot ovat itse asiassa logaritmisia  $abc$ -osumia. Toisin sanoen osoitetaan, että riittävän suurilla muuttujan  $x$  arvoilla pätee ehto

$$\exp\left(-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right)\right) < \frac{1}{\log c}. \quad (3.17)$$

Todistus perustuu epäyhtälön (3.17) eksponenttifunktion sisäfunktiolle riittävän suurilla muuttujan  $x$  arvoilla saatavaan arvioon

$$-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) < \log\left(\frac{1}{B(x)}\right) \leq \log\left(\frac{1}{\log c}\right), \quad (3.18)$$

missä viimeinen epäyhtälö on voimassa Lauseen 3.6.9 todistuksessa tarkasteltaville  $abc$ -kolmikoille asetetun ehdon  $\log c \leq B(x)$  nojalla.

Sijoittamalla nyt yhtälöllä (3.15) määrätty rajoitefunktio  $B$  epäyhtälöön (3.18) saadaan

$$-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) < \log\left(\frac{1}{B(x)}\right) = -\log B(x) = -\log\left[\frac{1}{2}\left(\frac{x}{e}\right)^{1+\frac{1}{\alpha}}\right],$$

josta termejä järjestelemällä ja sieventämällä saadaan edelleen

$$\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) - \left(1 + \frac{1}{\alpha}\right) \log x - \log C''_{\alpha} > 0, \quad (3.19)$$

missä  $C''_{\alpha} = (2e^{1+\frac{1}{\alpha}})^{-1}$  on vakio. Osoitetaan lauseen väite näyttämällä, että epäyhtälön (3.19) vasen puoli kasvaa rajatta muuttujan  $x$  kasvaessa rajatta.

Tarkastellaan osamäärää

$$\frac{\frac{x}{\log^2 x}}{\mathcal{O}\left(\frac{x}{\log^3 x}\right) + \left(1 + \frac{1}{\alpha}\right) \log x + \log C''_{\alpha}}$$

ja asetetaan nimittäjä mahdollisimman suureksi, toisin sanoen käytetään termille  $\mathcal{O}\left(\frac{x}{\log^3 x}\right)$  arviota  $K \frac{x}{\log^3 x}$ , missä  $K > 0$  on jokin vakio. Antamalla muuttujan  $x$  kasvaa rajatta saadaan toistuvasti L'Hospitalin lausetta (Lause 2.7.3 ja Huomautus 2.7.4) soveltamalla

$$\begin{aligned}
\lim_{x \rightarrow \infty} \frac{\frac{x}{\log^2 x}}{K \frac{x}{\log^3 x} + (1 + \frac{1}{\alpha}) \log x + \log C''_{\alpha}} &= \lim_{x \rightarrow \infty} \frac{x \log x}{Kx + (1 + \frac{1}{\alpha}) \log^4 x + \log C''_{\alpha} \log^3 x} \\
&= \lim_{x \rightarrow \infty} \frac{x \log x + x}{Kx + 4(1 + \frac{1}{\alpha}) \log^3 x + 3 \log C''_{\alpha} \log^2 x} \\
&= \lim_{x \rightarrow \infty} \frac{x \log x + 2x}{Kx + 12(1 + \frac{1}{\alpha}) \log^2 x + 6 \log C''_{\alpha} \log x} \\
&= \lim_{x \rightarrow \infty} \frac{x \log x + 3x}{Kx + 24(1 + \frac{1}{\alpha}) \log x + 6 \log C''_{\alpha}} \\
&= \lim_{x \rightarrow \infty} \frac{\log x + 4}{K + 4!(1 + \frac{1}{\alpha}) \frac{1}{x}} \\
&= \infty.
\end{aligned}$$

Näin ollen osamäärän osoittaja kasvaa nimittäjää nopeammin. Raja-arvon määritelmän nojalla on tällöin olemassa luku  $x_0 > 0$  siten, että epäyhtälö (3.19) on voimassa kaikilla  $x > x_0$ . Tällöin myös epäyhtälöt (3.18) ja (3.17) ovat voimassa tarpeeksi suurilla muuttujan  $x$  arvoilla. Lauseen väite seuraa analogisesti Lauseen 3.6.9 todistuksesta.  $\square$

**Huomautus 3.7.7.** Lauseen 3.7.6 antama alaraja logaritmisille  $abc$ -osumille tuskin on paras mahdollinen. Huomautusta 3.6.10 soveltamalla voidaankin esittää, että termi  $(\log X)^{\epsilon}$  voitaneen korvata jollain termin  $\log \log X$  potenssilla.

**Huomautus 3.7.8.** Lauseen 3.7.6 todistus herättää kysymyksen, voidaanko  $abc$ -osumille esittää vielä logaritmiehtoakin tiukempi ehto, jonka toteuttaville  $abc$ -kolmikoille voidaan osoittaa olevan voimassa Lauseiden 3.6.9 ja 3.7.6 mukainen alaraja.

Logaritmistien  $abc$ -osumien kerrointa  $\frac{1}{\log c}$  ei esimerkiksi voida todistuksessa korvata kertoimella  $c^{-\delta}$ ,  $\delta \in (0, 1)$ . Oletuksen  $\log c \leq B(x)$  nojalla nimittäin  $-\log c \geq -B(x)$ , joten voidaan tarkastella epäyhtälöketjua (3.18) vastaavaa epäyhtälöketjua

$$-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) < -\delta B(x) \leq -\delta \log c.$$

Sijoittamalla yhtälöllä (3.15) määrätty rajoitefunktio  $B$  ensimmäiseen epäyhtälöön saadaan

$$\frac{x}{\log^2 x} - \epsilon B(x) + \mathcal{O}\left(\frac{x}{\log^3 x}\right) = \frac{x}{\log^2 x} - \frac{\delta}{2} \left(\frac{x}{e}\right)^{1+\frac{1}{\alpha}} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) > 0.$$

Koska  $0 < \alpha < 1$ , niin  $1 + \frac{1}{\alpha} > 2$ . Termi  $x^2$  kasvaa vakiolla  $\delta$  skaalauksesta huolimatta nopeammin kuin termi  $\frac{x}{\log^2 x}$ , joten epäyhtälö ei toteudu enää tarpeeksi suurilla muuttujan  $x$  arvoilla.

Lauseen 3.6.9 tapauksen mukaisesti voidaan tässäkin tapauksessa kysyä, kuinka hyvin Lauseen 3.7.6 alaraja approksimoi logaritmistien  $abc$ -osumien lukumääräfunktiota  $N_{\log}(X)$ . Alustava arvio saadaan soveltamalla Liitteen F algoritmiä jo aiemmin mainittuihin Leidenin yliopiston ABC@Home-laskentaprojektin tuloksiin [40].

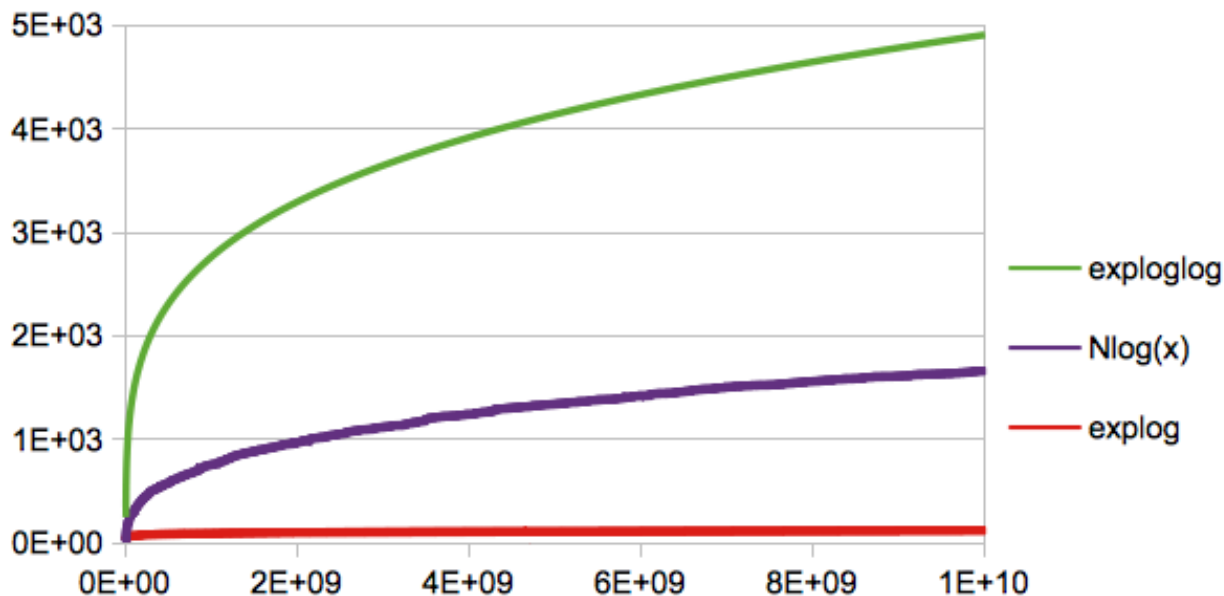
Kuvasta 5 nähdään, että alarajafunktio antaa jo huomattavasti paremman approksimaation funktiolle  $N_{\log}(X)$  kuin mitä funktiolle  $N(X)$ , ks. Kuva 4. Tätä selittää myös logaritmisten  $abc$ -osumien huomattavasti pienempi tiheys. Tiukemmasta ehdosta johtuen on lisäksi vaikeaa konstruoida äärettömästi logaritmisiä  $abc$ -osumia Lemman 3.6.5 tapaisesti. Kuvassa 5 funktion  $N_{\log}(X)$  kasvua välillä  $0 \leq X \leq 10^{10}$  on verrattu funktioihin

$$\begin{aligned} \exp((\log X)^{\frac{1}{2}}) & \quad (\text{explog}), \\ \exp((\log X)^{\frac{1}{2}}(\log \log X)^{\frac{1}{2}}) & \quad (\text{exploglog}). \end{aligned}$$

Kuvan 5 perusteella voidaan ehdottaa lukumääräfunktiolle  $N_{\log}(X)$  seuraavaa ylärajaa:

**Konjektuuri 3.7.9.** *Jokaista  $\varepsilon > 0$  kohti on olemassa  $X_0 > 0$  siten, että kaikilla  $X \geq X_0$  pätee*

$$N_{\log}(X) \leq \exp((\log X)^{\frac{1}{2}}(\log \log X)^{\frac{1}{2}}).$$



Kuva 5: Logaritmisten  $abc$ -osumien lukumääräfunktio  $N_{\log}(X)$  ja sitä rajoittavia funktioita.

### 3.8 Szpiron konjektuureista

Fermat'n suuren lauseen lisäksi  $Abc$ -konjektuurin syntyyn ovat vaikuttaneet suuresti 1980-luvulla esitetyt Szpiron konjektuurit sekä Stothers-Masonin lause. Tässä alaluvussa tarkastellaan Szpiron elliptisille käyrille esittämiä konjektuureja sekä niiden yhteyttä  $Abc$ -konjektuuriin, josta tässä yhteydessä käytetään ilman erillistä mainintaa yleisempää muotoa (Konjektuuri 3.2.2). Elliptisiä käyriä tarkastellaan seuraavassa kerroinkunnassa  $\mathbb{Q}$  ja niihin liittyvää teoriaa on käsitelty tarkemmin alaluvussa 2.6.

Aloitetaan L. Szpiron vuonna 1983 esittämällä alkuperäisellä konjektuurilla [49, s. 167].

**Konjektuuri 3.8.1** (Szpiro, heikko muoto). *On olemassa luvut  $\alpha > 0$  ja  $\beta > 0$  siten, että jokaiselle puolivakaalle elliptiselle käyrälle  $E$  pätee epäyhtälö*

$$|\Delta| \leq \alpha N_E^\beta.$$

Kokonaisluvuille saadaan analoginen tulos:

**Konjektuuri 3.8.2.** *On olemassa luvut  $\alpha' > 0$  ja  $\beta' > 0$  siten, että kaikille  $abc$ -kolmikoille  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$ , pätee epäyhtälö*

$$|abc| \leq \alpha' \text{rad}(abc)^{\beta'}.$$

**Huomautus 3.8.3.** Konjektuuri 3.8.2 voidaan esittää myös pelkän radikaalin avulla [50]: On olemassa luku  $s > 0$  siten, että kaikille  $abc$ -kolmikoille  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$ , pätee epäyhtälö

$$|abc| \leq \text{rad}(abc)^s.$$

Tämä nähdään soveltamalla työn [56, s. 26] ajatusta seuraavasti: valitaan luku  $r > 0$  siten, että  $2^r \geq \alpha'$ . Koska kaikilla  $abc$ -kolmikoilla  $\text{rad}(abc) \geq 2$ , saadaan tällöin  $\alpha' \leq \text{rad}(abc)^r$ . Väite seuraa valitsemalla  $s = \beta' + r$ .

Vuonna 1988 Oesterlé huomautti, että mikäli Konjektuuriin 3.8.2 lisätään ehto  $16 \mid abc$ , niin se seuraa Szpiron konjektuurin heikosta muodosta [49, s. 167]. Osoitetaan seuraavaksi, että Konjektuuri 3.8.2 seuraa helposti  $Abc$ -konjektuurista.

**Lause 3.8.4.** *Konjektuurista 3.2.2 seuraa Konjektuuri 3.8.2.*

*Todistus.* Oletetaan, että Konjektuuri 3.2.2 on voimassa. Tällöin Huomautuksen 3.2.14 nojalla luku  $C(\varepsilon)$ ,

$$C(\varepsilon) = \sup \left\{ \frac{\max\{|a|, |b|, |c|\}}{\text{rad}(abc)^{1+\varepsilon}} : \text{syt}(a, b) = 1, a + b = c \right\},$$

on äärellinen jokaisella  $\varepsilon > 0$ . Näin ollen Konjektuuria 3.2.2 soveltamalla saadaan

$$|abc| \leq (\max\{|a|, |b|, |c|\})^3 \leq (C(\varepsilon) \text{rad}(abc)^{1+\varepsilon})^3,$$

mistä väite seuraa valitsemalla  $\alpha' = C(\varepsilon)^3$  ja  $\beta' = 3(1 + \varepsilon)$ . □

Konjektuurissa 3.8.1 ei aseteta tarkemmin rajaa luvulle  $\beta$ . Vuonna 1988 Oesterle osoitti edellä mainittua ehtoa  $16 \mid abc$  ja Konjektuuria 3.8.2 soveltamalla, että Konjektuurissa 3.8.1 täytyy olla  $\beta > 6$  [49, s. 168]. Näin saadaan *vahva Szpiron konjektuuri*.

**Konjektuuri 3.8.5** (Szpiro, vahva muoto). *Kaikilla  $\varepsilon > 0$  on olemassa vakio  $C(\varepsilon) > 0$  siten, että jokaiselle puolivakaaalle elliptisille käyrälle  $E$  pätee epäyhtälö*

$$|\Delta| \leq C(\varepsilon)N_E^{6+\varepsilon}.$$

**Huomautus 3.8.6.** Konjektuuri 3.8.5 ei ole voimassa ilman lukua  $\varepsilon > 0$ . Tämän nähdään lähteistä [49, s. 168] ja [46, s. 4–5]. Näin ollen Konjektuurin 3.8.5 väite on paras mahdollinen, jos se ylipäättään on voimassa.

Triviaalisti Szpiron konjektuurin vahva muoto implikoi heikon muodon. Vahvan muodon avulla voidaan osoittaa myös seuraavan  $abc$ -kolmikoihin liittyvän konjektuurin olevan voimassa [46, s. 7–8].

**Konjektuuri 3.8.7.** *Jokaista lukua  $\varepsilon > 0$  kohden on olemassa luku  $C(\varepsilon)$  siten, että kaikille  $abc$ -kolmikoille  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$  ja  $16 \mid abc$ , pätee epäyhtälö*

$$|abc| \leq C(\varepsilon) \operatorname{rad}(abc)^{3+\varepsilon}.$$

**Huomautus 3.8.8.** Konjektuurin 3.8.7 mukaan osamäärä

$$\rho = \rho(a, b, c) = \frac{\log |abc|}{\log \operatorname{rad}(abc)} \tag{3.20}$$

on rajoitettu. Osamäärää (3.20) kutsutaan  $abc$ -kolmikon *Szpiron osamääräksi* (engl. Szpiro ratio) ja sillä on läheinen yhteys aiemmin määriteltyn  $L$ -arvoon (Määritelmä 3.2.15). Szpiro-laadultaan hyviä  $abc$ -kolmikoita, joilla  $\rho(a, b, c) > 4$ , on taulukoitu Liitteessä B.

**Lause 3.8.9.** *Konjektuuri 3.8.5 implikoi Konjektuurin 3.8.7*

*Todistus.* Oletetaan, että nollostasta eroaville luvuille  $a, b$  ja  $c$  pätee ehdot

$$a + b + c = 0, \quad a \equiv -1 \pmod{4}, \quad 16 \mid b.$$

Lemman 2.6.8 nojalla tällöin puolivakaa elliptinen käyrä

$$E_{abc}: y^2 + xy = x^3 + \frac{b-a-1}{4}x^2 - \frac{ab}{16}x$$

on minimaalimalli, jolloin Huomautusta 2.6.9 ja Konjektuuria 3.8.5 soveltamalla sekä ylöspäin arvioimalla saadaan

$$\left(\frac{abc}{16}\right)^2 \leq C_1(\varepsilon) \operatorname{rad}\left(\frac{abc}{16}\right)^{6+\varepsilon} \leq C_1(\varepsilon) \operatorname{rad}(abc)^{6+\varepsilon}.$$

Puolittain neliöjuuri ottamalla sekä luvulla 16 kertomalla saadaan edelleen

$$|abc| \leq 16C_1(\varepsilon)^{\frac{1}{2}} \operatorname{rad}(abc)^{3+\frac{\varepsilon}{2}},$$

mistä väite seuraa merkitsemällä  $\varepsilon' = \frac{\varepsilon}{2}$  ja  $C(\varepsilon') = 16C_1(\varepsilon)^{\frac{1}{2}}$ . □

Hallin konjektuurin (Konjektuuri 4.5.1) pohjalta S. Lang esitti vuonna 1990 seuraavan *yleistetyn Szpiro konjektuurin*, jota jossain yhteyksissä kutsutaan myös *Lang-Szpiro konjektuuriksi* [36, s. 44], [47, s. 6].

**Konjektuuri 3.8.10** (Szpiro, yleistetty). *Olkoon  $\varepsilon > 0$  ja olkoot  $A, B \in \mathbb{Z}$  suhteellisia alkulukuja. Tällöin on olemassa vakio  $c(\varepsilon, A, B) > 0$  siten, että mikäli luvut  $u, v, k \in \mathbb{Z}$  toteuttavat ehdot*

$$\text{syt}(Au, Bv) = 1 \quad \text{ja} \quad k = Au^3 + Bv^2, \quad (3.21)$$

*niin tällöin*

$$|u| \leq c(\varepsilon, A, B) \text{rad}(k)^{2+\varepsilon} \quad \text{ja} \quad |v| \leq c(\varepsilon, A, B) \text{rad}(k)^{3+\varepsilon}$$

Osoitetaan, että yllä oleva konjektuuri on yhtäpitävä *Abc*-konjektuurin kanssa. Todistus perustuu lähteisiin [47, s. 6–7] ja [56, s. 20–21].

**Lause 3.8.11.** *Konjektuuri 3.2.2 ja Konjektuuri 3.8.10 ovat ekvivalentteja.*

*Todistus.* Oletetaan ensin, että Konjektuuri 3.2.2 on voimassa. Olkoot  $A, B \in \mathbb{Z}$  suhteellisia alkulukuja ja  $u, v, k \in \mathbb{Z}$  ehdot (3.21) toteuttavia lukuja. Konjektuurin 3.2.2 nojalla saadaan

$$|Bv^2| \leq \max\{|Au^3|, |Bv^2|, |k|\} \leq C_1(\varepsilon) \text{rad}(ABuvk)^{1+\varepsilon} \leq C_1(\varepsilon) |ABuv|^{1+\varepsilon} \text{rad}(k)^{1+\varepsilon},$$

josta edelleen

$$|v|^2 \leq \frac{C_1(\varepsilon) |AB|^{1+\varepsilon}}{|B|} |uv|^{1+\varepsilon} \text{rad}(k)^{1+\varepsilon} = C_2(\varepsilon, A, B) |uv|^{1+\varepsilon} \text{rad}(k)^{1+\varepsilon}, \quad (3.22)$$

missä  $C_2(\varepsilon, A, B) = C_1(\varepsilon) |A|^{1+\varepsilon} |B|^\varepsilon$ .

Oletetaan sitten, että  $|Au^3| \leq |Bv^2|$ . Tällöin  $|u| \leq C_3(A, B) |v|^{\frac{2}{3}}$ , missä  $C_3 = \left|\frac{B}{A}\right|^{\frac{1}{3}}$ . Soveltamalla tätä epäyhtälöön (3.22) saadaan

$$|v|^2 \leq C_2(\varepsilon, A, B) C_3(A, B)^{1+\varepsilon} |v|^{\frac{5}{3}(1+\varepsilon)} \text{rad}(k)^{1+\varepsilon},$$

josta edelleen puolittain termillä  $|v|^{\frac{5}{3}(1+\varepsilon)}$  jakamalla

$$|v|^{\frac{1-5\varepsilon}{3}} \leq C_4(\varepsilon, A, B) \text{rad}(k)^{1+\varepsilon}, \quad (3.23)$$

missä  $C_4(\varepsilon, A, B) = C_2(\varepsilon, A, B) C_3(A, B)^{1+\varepsilon}$ . Valitaan nyt  $\varepsilon$  väliltä  $(0, \frac{1}{5})$ , jolloin  $1 - 5\varepsilon > 0$ , ja määritellään  $\varepsilon' = \frac{18\varepsilon}{1-5\varepsilon}$ , jolloin  $3 + \varepsilon' = \frac{3(1+\varepsilon)}{1-5\varepsilon}$ . Tällöin  $\varepsilon' > 0$  ja epäyhtälöstä (3.23) saadaan

$$|v| \leq (C_4(\varepsilon, A, B))^{\frac{3}{1-5\varepsilon}} \text{rad}(k)^{\frac{3}{1-5\varepsilon}(1+\varepsilon)} = C_5(\varepsilon', A, B) \text{rad}(k)^{3+\varepsilon'},$$

missä  $C_5(\varepsilon', A, B) = (C_4(\varepsilon, A, B))^{\frac{3}{1-5\varepsilon}}$ . Epäyhtälöstä  $|u| \leq C_3(A, B) |v|^{\frac{2}{3}}$  saadaan edelleen

$$|u| \leq C_3(A, B) (C_5(\varepsilon', A, B) \text{rad}(k)^{3+\varepsilon'})^{\frac{2}{3}} \leq C_6(\varepsilon', A, B) \text{rad}(k)^{2+\varepsilon},$$

missä  $C_6(\varepsilon', A, B) = C_3(A, B) (C_5(\varepsilon', A, B))^{\frac{2}{3}}$ . Näin ollen Konjektuuri 3.8.10 on voimassa. Tapauksessa  $|Au^3| \geq |Bv^2|$  päättely on oleellisesti samanlainen.

Oletetaan kääntäen, että Konjektuuri 3.8.10 on voimassa. Muodostetaan mielivaltaiseta  $abc$ -kolmikosta  $(a, b, c) \in \mathbb{Z}^3$ ,  $abc \neq 0$ , lukuja tarvittaessa uudelleen määrittelemällä kolmikko  $(a, b, c) \in \mathbb{N}^3$ ,  $0 < a < b < c$ , ja sitä vastaava elliptinen käyrä  $E$  asettamalla

$$E : y^2 = x(x - a)(x + b) = x^3 + (b - a)x^2 - abx.$$

Esimerkin 2.6.6 nojalla luvut  $c_4$  ja  $c_6$  sekä käyrän diskriminantti ovat tällöin

$$\begin{aligned} c_4 &= 16(a^2 + ab + b^2) \\ c_6 &= -32(b - a)(a + 2b)(2a + b) \\ \Delta &= 16(ab(a + b))^2 \end{aligned}$$

Lemman 2.6.5 mukaan  $1728\Delta = c_4^3 - c_6^2$ , joten sijoittamalla yllä olevat luvut ja jakamalla luvulla 4096 saadaan yhtälö

$$(a^2 + ab + b^2)^3 - \left(\frac{1}{2}(b - a)(a + 2b)(2a + b)\right)^2 = 3^3 \left(\frac{1}{2}ab(a + b)\right)^2.$$

Koska  $\text{syta}(a, b) = 1$ , niin Lemmaa 2.1.7 toistuvasti käyttämällä yhtälön toiseen ja kolmanteen termiin nähdään yhtälön termien suurimman yhteisen tekijän olevan joko  $3^3$  tai 1. Jos nimittäin  $b - a \equiv 0 \pmod{3}$ , niin  $a^2 + ab + b^2 = (b - a)^2 + 3ab \equiv 0 \pmod{3}$  sekä

$$a + 2b = 2(b - a) + 3a \equiv 0 \pmod{3} \quad \text{ja} \quad 2a + b = -2(b - a) + 3b \equiv 0 \pmod{3}.$$

Tässä tapauksessa jaetaan yhtälö luvulla  $3^3$  ja valitaan  $k = \left(\frac{1}{2}ab(a + b)\right)^2$ . Mikäli taas suurin yhteinen tekijä on yksi, valitaan  $k = 3^3 \left(\frac{1}{2}ab(a + b)\right)^2$ . Tällöin yhtälö toteuttaa ehdot (3.21) arvoilla  $A = 1$  ja  $B = -1$ , jolloin Konjektuuria 3.8.10 soveltamalla saadaan

$$a^2 \leq a^2 + ab + b^2 \leq C_1(\varepsilon, 1, -1) \text{rad}(k)^{2+\varepsilon} \leq 3C_1(\varepsilon, 1, -1) \text{rad}(abc)^{2+\varepsilon}, \quad (3.24)$$

josta edelleen

$$a \leq C_2(\varepsilon) \text{rad}(abc)^{1+\frac{\varepsilon}{2}}, \quad (3.25)$$

missä  $C_2(\varepsilon) = (3C_1(\varepsilon, 1, -1))^{\frac{1}{2}}$ . Samanlaisella päättelyllä saadaan vastaava epäyhtälö luvulle  $b$ . Kun nyt merkitään  $\varepsilon' = \frac{\varepsilon}{2}$  ja  $C(\varepsilon') = \frac{1}{2}C_2(\varepsilon)$ , saadaan yhtälöt puolittain summaamalla

$$c = a + b \leq C(\varepsilon') \text{rad}(abc)^{1+\varepsilon'}.$$

Näin ollen Konjektuuri 3.2.2 on voimassa. □

**Huomautus 3.8.12.** Yleistetystä Szpiron konjektuurista seuraa vahva Szpiron konjektuuri [49, s. 169]. Tämä näytetään tietyin lisäoletuksin työssä [56, s. 21–22]. Näin ollen nähdään toista kautta, että luku  $\varepsilon > 0$  on tarpeellinen Szpiron vahvassa konjektuurissa. Lauseen 3.2.13 mukaan nimittäin  $Abc$ -konjektuuri ei ole voimassa ilman lukua  $\varepsilon > 0$ , joten myöskään Konjektuurit 3.8.10 ja 3.8.5 eivät ole voimassa ilman lukua  $\varepsilon > 0$ .

Osoitetaan vielä kirjaan [59, s. 259–260] perustuen, että  $Abc$ -konjektuuri implikoi suoraan Szpiron konjektuurin vahvan muodon.

**Lause 3.8.13.** *Konjektuurista 3.2.2 seuraa Konjektuuri 3.8.5.*



*Todistus.* Olkoon  $E$  elliptinen käyrä, joka saadaan minimaalisesta Weierstrassin yhtälöstä. Tällöin käyrän diskriminantin ja lukujen  $c_4$  sekä  $c_6$  välillä on yhteys

$$1728\Delta = c_4^3 - c_6^2.$$

Merkitään  $d = \text{syt}(c_4^3, c_6^2)$ . Soveltamalla nyt yleistettyä  $Abc$ -konjektuuria arvoilla

$$a = \frac{c_4^3}{d}, \quad b = -\frac{c_6^2}{d} \quad \text{ja} \quad c = \frac{1728\Delta}{d}$$

saadaan

$$\max\{|c_4^3|, |c_6^2|, |1728\Delta|\} \leq C(\varepsilon)d \text{rad}(c_4^3 c_6^2 1728\Delta)^{1+\varepsilon}.$$

Määritelmää 2.6.11 ja huomiota  $1728 = 2^6 3^3$  soveltamalla saadaan radikaalille edelleen arvio

$$\text{rad}(c_4^3 c_6^2 1728\Delta)^{1+\varepsilon} \leq 6|c_4 c_6 N_E|^{1+\varepsilon}.$$

Merkitsemällä  $C_1(\varepsilon) = 6C(\varepsilon)d$  saadaan siten  $abc$ -kolmikon luvuille epäyhtälöt

$$\begin{aligned} |c_4|^{2-\varepsilon} &\leq C_1(\varepsilon)|c_6 N_E|^{1+\varepsilon} \\ |c_6|^{1-\varepsilon} &\leq C_1(\varepsilon)|c_4 N_E|^{1+\varepsilon} \\ |\Delta| &\leq C_1(\varepsilon)|c_4 c_6 N_E|^{1+\varepsilon} \end{aligned}$$

Korottamalla nyt ensimmäinen epäyhtälö potenssiin  $2 + 2\varepsilon$ , toinen epäyhtälö potenssiin  $3 + 3\varepsilon$  ja kolmas potenssiin  $1 - 5\varepsilon$  sekä kertomalla saadut epäyhtälöt keskenään saadaan

$$\begin{aligned} |c_4|^{4+2\varepsilon-2\varepsilon^2} |c_6|^{3-3\varepsilon^2} |\Delta|^{1-5\varepsilon} &\leq C_1(\varepsilon)^6 |c_6 N_E|^{2+4\varepsilon+2\varepsilon^2} |c_4 N_E|^{3+6\varepsilon+3\varepsilon^2} |c_4 c_6 N_E|^{1-4\varepsilon-5\varepsilon^2} \\ &\leq C_1(\varepsilon)^6 |c_4|^{4+2\varepsilon-2\varepsilon^2} |c_6|^{3-3\varepsilon^2} |N_E|^{6+6\varepsilon}, \end{aligned}$$

josta puolittain jakamalla saadaan lopulta

$$|\Delta|^{1-5\varepsilon} \leq C_1(\varepsilon)^6 |N_E|^{6+6\varepsilon}. \quad (3.26)$$

Yhtälö (3.26) on vain luvun  $\varepsilon$  säätöä vaille sama kuin Szpiron konjektuurissa.  $\square$

**Huomautus 3.8.14.** Lauseen 3.8.13 käänteinen väite ei suoraan ole voimassa. Voidaan kuitenkin helposti osoittaa, että vahva Szpiron konjektuuri implikoi  $Abc$ -konjektuurin, jossa luku  $1 + \varepsilon$  on korvattu luvulla  $\frac{3}{2} + \varepsilon$  [59, s. 259]. Paras tämänlaatuinen tulos on Oesterlén vuonna 1988 esittämä tiukempi yläraja  $\frac{6}{5} + \varepsilon$  [49, s. 169].

Koontina voidaan sanoa, että  $Abc$ -konjektuurista seuraa yleistetty Szpiron konjektuuri, josta puolestaan seuraa sekä Szpiron konjektuurin vahva että heikko muoto. Szpiron konjektuurin vahva muoto implikoi edelleen  $Abc$ -konjektuurin radikaalin eksponentilla  $\frac{6}{5} + \varepsilon$ . Tämän alaluvun tulokset perustuvat oleellisesti Lemmassa 2.6.13 esitettyyn Freyn käyrään, jonka avulla voidaan luoda yhteys Diophantoksen yhtälöiden ja elliptisten käyrien välille.

### 3.9 Fermat'n suuri lause

Lukuteorian kuuluisimpiin tuloksiin kuuluu Fermat'n suuri lause, jonka todistaminen on innostanut ja turhauttanut matemaatikoita jo reilun kolmen vuosisadan ajan [16]. Tämä A. Wilesin viimein vuonna 1995 todistama tulos [70] on myös suurimpia *Abc*-konjektuurin synnyn innoittajia, joten on perusteltua käsitellä sitä vielä erikseen. Fermat'n suuren lauseen yleistettyä muotoa on käsitelty erikseen alaluvussa 4.6.

Aloitetaan toteamalla kuuluisa lause moderneilla merkinnöillä [16, s. 2]:

**Lause 3.9.1** (Fermat'n suuri lause). *Yhtälöllä*

$$x^n + y^n = z^n, \quad (3.27)$$

*ei ole kokonaislukuratkaisuja*  $(x, y, z) \in \mathbb{N}^3$  *luonnollisilla luvuilla*  $n \geq 3$ .

**Huomautus 3.9.2.** Jos yhtälöllä (3.27) on kokonaislukuratkaisu, niin sillä on ratkaisu myös suhteellisilla alkuluvuilla. Nimittäin, jos kolmikko  $(x, y, z) \in \mathbb{N}^3$  toteuttaa yhtälön (3.27) ja jokin alkuluku  $p$  jakaa luvut  $x$  ja  $y$ , niin  $p$  jakaa myös luvun  $z$ . Näin ollen kolmikko  $(\frac{x}{p}, \frac{y}{p}, \frac{z}{p})$  toteuttaa myös kyseisen yhtälön.

Vaikkei *Abc*-konjektuurin avulla pystytäkään todistamaan koko Fermat'n suurta lausetta, voidaan sen avulla osoittaa seuraava asymptoottinen tulos [43, s. 185–186]:

**Lause 3.9.3.** *Konjektuurin 3.2.2 nojalla on olemassa*  $n_0 \in \mathbb{N}$  *siten, että yhtälöllä (3.27) ei ole suhteellisia alkulukuratkaisuja arvoilla*  $n \geq n_0$ .

*Todistus.* Huomautuksen 3.9.2 nojalla riittää tarkastella yhtälön (3.27) jollakin  $n \in \mathbb{N}$  toteuttavia positiivisia suhteellisia alkulukuja  $x, y$  ja  $z$ . Radikaalille saadaan tällöin arvio

$$\text{rad}(x^n y^n z^n) = \text{rad}(xyz) \leq xyz < z^3.$$

Jos nyt  $n \geq 2$ , niin  $z \geq 3$ . Konjektuuria 3.2.2 arvoilla  $\varepsilon = 1$  ja  $C_1 = \max\{1, C(1)\}$  soveltamalla saadaan

$$z^n = \max\{x^n, y^n, z^n\} \leq C_1 \text{rad}(x^n y^n z^n)^2 < C_1 z^6,$$

josta edelleen

$$n < 6 + \frac{\log C_1}{\log z} \leq 6 + \frac{\log C_1}{\log 3}.$$

Väite seuraa. □

**Huomautus 3.9.4.** *Abc*-konjektuurin soveltamisen kannalta suurimman haasteen aiheuttaa se, ettei lukua  $C(\varepsilon) > 0$  ole mitenkään tarkemmin määritelty. Jos kuitenkin pystytään esittämään *Abc*-konjektuuri efektiivisessä muodossa, saadaan myös Fermat'n suuren lauseen eksponentille  $n$  efektiivinen yläraja. Soveltamalla esimerkiksi alaluvussa 3.5 esitettyä otaksumaa, jonka mukaan kaikilla *abc*-kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  pätee

$$c < \text{rad}(abc)^2,$$

nähdään, ettei yhtälöllä (3.27) ei ole kokonaislukuratkaisuja arvoilla  $n \geq 6$ .

Parhaan efektiivisen tuloksen antaa alaluvun 3.5 Konjektuuri 3.5.4.

**Lause 3.9.5.** *Konjektuurin 3.5.4 nojalla yhtälöllä (3.27) ei ole suhteellisia alkulukuratkaisuja arvoilla  $n \geq 5$ .*

**Huomautus 3.9.6.** Mikäli Lause 3.9.5 on totta, Fermat'n suurelle lauseelle voidaan esittää paljon Wilesin todistusta alkeellisempi todistus. Euler nimittäin osoitti, ettei yhtälöllä (3.27) ole ratkaisuja arvolla  $n = 3$  [16, s. 39–58], ja Pythagoraan primitiivisiä kolmikoita sekä Fermat'n kehittämää äärettömän laskeutumisen periaatetta käyttämällä voidaan osoittaa sama tilanne arvolla  $n = 4$  [16, s. 9–10].

Edellisessä alaluvussa osoitettiin  $Abc$ -konjektuurin ja Szpiron konjektuurien välillä oleva yhteys. Näin ollen luonnollisesti myös Fermat'n suuren lauseen ja elliptisten käyrien välillä on yhteys. Osoitetaan lopuksi vahvan Szpiron konjektuurin avulla seuraava asymptoottinen tulos [59, s. 256–257]:

**Lause 3.9.7.** *Konjektuurin 3.8.5 nojalla on olemassa luku  $n_0 \in \mathbb{N}$  siten, että yhtälöllä (3.27) ei ole suhteellisia alkulukuratkaisuja arvoilla  $n \geq n_0$ .*

*Todistus.* Olkoon  $n \in \mathbb{N}$  ja olkoot  $a, b, c \in \mathbb{N}$ ,  $a < b < c$ , siten, että  $a^n + b^n = c^n$  ja  $\text{syt}(a, b, c) = 1$ . Tarkastellaan puolivakaata elliptistä käyrää  $E$ ,

$$E : y^2 = x(x + a^n)(x - b^n),$$

jonka diskriminantiksi saadaan Esimerkkiä 2.6.6 soveltamalla

$$\Delta = 16(a^n b^n (a^n + b^n))^2 = 16(abc)^{2n}.$$

Oletusten nojalla siis  $\Delta \neq 0$ , joten kyseessä todella on elliptinen käyrä. Lemmaa 2.6.13 soveltamalla tiedetään, että käyrän  $E$  minimaalidiskriminantille  $\Delta_{\min}$  pätee joko

$$|\Delta_{\min}| = 2^4 |abc|^{2n} \quad \text{tai} \quad |\Delta_{\min}| = 2^{-8} |abc|^{2n}.$$

Erityisesti on voimassa  $|\Delta_{\min}| \geq 2^{-8} |abc|^{2n}$ . Koska minimaalidiskriminantti on aina kokonaisluku, saadaan yllä olevaa tietoa käyttämällä käyrän  $E$  johtajalle  $N_E$  arvio

$$N = \prod_{p|\Delta_{\min}} p \leq \prod_{p|2abc} p^2 \leq |2abc|^2,$$

missä  $p$  on alkuluku. Soveltamalla Konjektuuria 3.8.5 arvolla  $\varepsilon = 1$  saadaan epäyhtälöketju

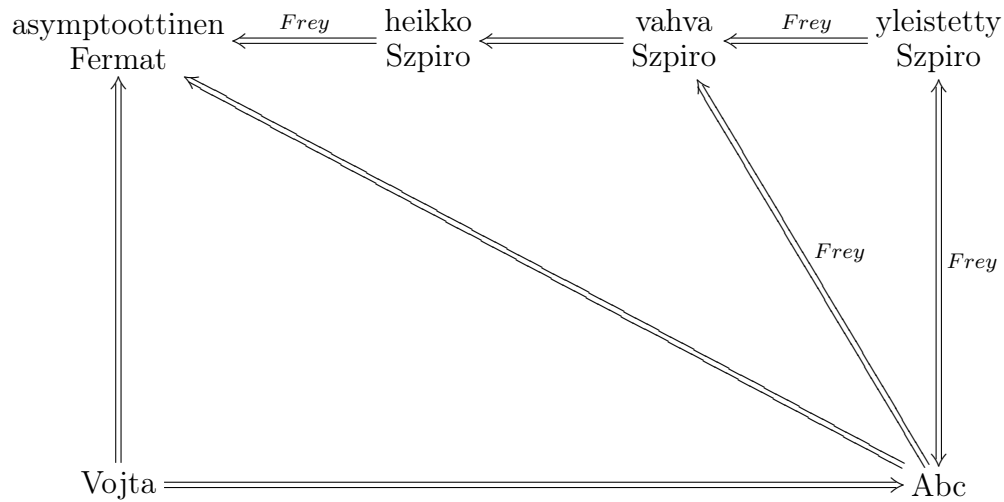
$$\frac{|abc|^{2n}}{2^8} \leq |\Delta_{\min}| \leq C(1)N^7 \leq C(1)|2abc|^{14},$$

missä  $C(1)$  on jokin absoluuttinen vakio. Tästä saadaan edelleen epäyhtälö

$$|abc|^{2n-14} \leq 2^{22} C(1),$$

josta tiedon  $|abc| \geq 2$  nojalla nähdään, että luvulla  $n$  on olemassa jokin absoluuttinen yläraja.  $\square$

**Huomautus 3.9.8.** Lauseen 3.9.7 todistus perustui Freyn käyrien teoriaan, jonka avulla pystytään tulkitsemaan kokonaislukuyhtälö elliptisenä käyränä. Kuvassa 6 on yhteenvetona esitetty tässä sekä edellisessä aluvuossa tarkasteltujen konjektuurien välisiä yhteyksiä. Kuvassa on mainittu lähettä [36, s. 47] mukaillen vielä Vojtan konjektuurin yhteys käsiteltyihin konjektuureihin. Vojtan konjektuuria ei tässä tutkielmassa kuitenkaan mainintaa enempää tarkastella, perusteellinen esitys aiheesta löytyy esimerkiksi kirjasta [68].



Kuva 6: Eri konjektuurien välisiä implikaatioita.

## 4 Abc-konjektuurin seurauksia

Tässä luvussa oletetaan  $Abc$ -konjektuurin pitävän paikkansa ja tarkastellaan sen implikoi-mia lukuteorian tuloksia. Täydellisempi lista seurauksista löytyy mm. internetsivuilta [48].  $Abc$ -konjektuurista käytetään ilman erillistä mainintaa Lauseen 3.2.1 mukaista versiota ole-tuksella  $0 < a < b < c$ :

**$Abc$ -konjektuuri.** *Jokaista reaalityyppistä luvua  $\varepsilon > 0$  kohden on olemassa luku  $C(\varepsilon) > 0$  siten, että kaikilla  $abc$ -kolmikoilla  $(a, b, c) \in \mathbb{N}^3$  on voimassa epäyhtälö*

$$c \leq C(\varepsilon) \operatorname{rad}(abc)^{1+\varepsilon}.$$

Yksinkertainen neljän askeleen ajatusketju konjektuurin soveltamiseen on seuraavanlainen:

1. Muodostetaan summa  $a + b = c$ , jolla  $\operatorname{syt}(a, b, c) = 1$  (tarvittaessa jaetaan termit luvulla  $d = \operatorname{syt}(a, b, c) \geq 2$ )
2. Sovelletaan  $Abc$ -konjektuuria, jolloin saadaan epäyhtälö
3. Arvioidaan epäyhtälön oikeaa puolta (ylärajaa) siten, että tu-loksena on vakio tai vakio kertaa tarkasteltava summan termi
4. Yhdistetään termit, kiinnitetään luku  $\varepsilon > 0$  ja todetaan ter-min arvojen olevan ylhäältä rajoitettuja

Haasteita aiheuttaa usein kohta 3, kun pelkkä radikaalin arvioiminen Lemman 3.1.7 mukaan ei riitä ja on käytettävä apuna muita tuloksia. Hyvin käyttökelpoisia aputuloksia ovat usein arviot  $\frac{n^n}{e^n} \leq n!$  (Lemma 2.7.14) sekä  $\prod_{p \leq n} p < 4^n$  (Lemma 2.8.1).

$Abc$ -konjektuurin avulla johdetut tulokset ovat usein asympotoottisia. Mikäli luvusta  $\varepsilon > 0$  riippuva vakio  $C(\varepsilon)$  voitaisiin määrittää efektiivisesti, ratkaisujen lukumäärälle saataisiin selkeä numeerinen yläraja nykyisen “äärellisen määrän” sijaan. Käsittelemällä poikkeus-tapaukset tietokoneavusteisesti voitaisiin  $Abc$ -konjektuurin voimaa tehostaa entisestään.

Tässä luvussa esiteltävien seurausten pääasiallisena lähteenä on käytetty Abderrahmane Nitaj’n väitöskirjaa [46] sekä suuntaa antavasti internetsivua [48]. Mahdollisuuksien mukaan alkuperäislähteitä on kuitenkin käytetty ensisijaisina lähteinä.

### 4.1 $Abc$ -kolmikoihin liittyviä tuloksia

Väitöskirjassaan [46, s. 13–15] Nitaj osoitti  $Abc$ -konjektuurin avulla seuraavat kolme melko yksinkertaista mutta hyvin erilaista  $abc$ -kolmikoihin liittyvää tulosta.

**Lause 4.1.1.**  *$Abc$ -konjektuurin nojalla kaikilla  $\varepsilon > 0$  on olemassa vakio  $C(\varepsilon)$  siten, että kaikilla  $abc$ -kolmikoilla  $(x_1, x_2, x_3) \in \mathbb{N}^3$  on voimassa epäyhtälö*

$$x_i \leq C(\varepsilon) \operatorname{rad}(x_i)^{3+\varepsilon}$$

jollakin  $i = 1, i = 2$  tai  $i = 3$ .

*Todistus.*  $Abc$ -konjektuurin nojalla kaikilla  $i = 1, 2, 3$  pätee  $x_i \leq C(\varepsilon) \operatorname{rad}(x_1 x_2 x_3)^{1+\varepsilon}$ , joten kertomalla puolittain epäyhtälöt saadaan

$$x_1 x_2 x_3 \leq C(\varepsilon)^3 \operatorname{rad}(x_1 x_2 x_3)^{3+\varepsilon}. \tag{4.1}$$

Mikäli kaikilla  $i = 1, 2, 3$  pätee

$$x_i > C(\varepsilon) \operatorname{rad}(x_i)^{3+\varepsilon},$$

kertomalla epäyhtälöt puolittain saadaan

$$x_1 x_2 x_3 > C(\varepsilon)^3 (\operatorname{rad}(x_1) \operatorname{rad}(x_2) \operatorname{rad}(x_3))^{3+\varepsilon} \geq C(\varepsilon)^3 \operatorname{rad}(x_1 x_2 x_3)^{3+\varepsilon},$$

mikä on ristiriita epäyhtälön (4.1) kanssa. Näin ollen on olemassa ainakin yksi indeksi  $i$ ,  $i \in \{1, 2, 3\}$ , jolla väite on voimassa.  $\square$

Toinen tulos antaa eräänlaisen arvion lukujen potensseille:

**Lause 4.1.2.** *Abc-konjektuurin nojalla kaikilla  $\varepsilon > 0$  on olemassa vakio  $C_0(\varepsilon) > 0$  siten, että kaikilla  $x, n \in \mathbb{N}_{\geq 2}$*

$$x^{n-1} \leq C_0(\varepsilon) \operatorname{rad}(x^n - 1)^{1+\varepsilon}.$$

*Todistus.* Valitaan luku  $\varepsilon$  siten, että  $0 < \varepsilon < \frac{1}{2}$ . Soveltamalla *Abc*-konjektuuria summaan  $(x^n - 1) + 1 = x^n$  saadaan

$$x^n \leq C(\varepsilon) \operatorname{rad}((x^n - 1)x^n)^{1+\varepsilon} \leq C(\varepsilon) \operatorname{rad}(x^n - 1)^{1+\varepsilon} x^{1+\varepsilon},$$

josta puolittain luvulla  $x^{1+\varepsilon}$  jakamalla saadaan edelleen

$$x^{n-(1+\varepsilon)} = x^{n-1-\varepsilon} = (x^{n-1})^{1-\frac{\varepsilon}{n-1}} \leq C(\varepsilon) \operatorname{rad}(x^n - 1)^{1+\varepsilon}.$$

Korottamalla nyt epäyhtälö puolittain potenssiin  $(1 - \frac{\varepsilon}{n-1})^{-1} = \frac{n-1}{n-1-\varepsilon}$  saadaan

$$x^{n-1} \leq C(\varepsilon)^{\frac{n-1}{n-1-\varepsilon}} \operatorname{rad}(x^n - 1)^{\frac{(1+\varepsilon)(n-1)}{n-1-\varepsilon}}.$$

Vakion  $C(\varepsilon)$  ja radikaalin eksponentteja tarkastelemalla nähdään, että  $\frac{n-1}{n-1-\varepsilon} < 2$ , mikä seuraa suoraan epäyhtälöstä  $n - 1 - 2\varepsilon > 0$  sekä oletuksista  $0 < \varepsilon < \frac{1}{2}$  ja  $n \geq 2$ . Lisäksi

$$\frac{(n-1)(1+\varepsilon)}{n-1-\varepsilon} = \frac{1+\varepsilon}{1-\frac{\varepsilon}{n-1}} \leq \frac{1+\varepsilon}{1-\varepsilon} = \frac{1-\varepsilon+2\varepsilon}{1-\varepsilon} = 1+\varepsilon',$$

missä  $\varepsilon' = \frac{2\varepsilon}{1-\varepsilon}$ . Näin ollen väite seuraa, kun valitaan  $C_0(\varepsilon) = C(\varepsilon)^2$ .  $\square$

Kolmas tulos antaa ylärajan *abc*-kolmikon suurimmalle termille muiden termien kautta:

**Lause 4.1.3.** *Olkoon kolmikko  $(x_1, x_2, x_3) \in \mathbb{N}^3$  siten, että  $x_1 < x_2 < x_3$  ja  $x_1 + x_2 = x_3$ . Tällöin *Abc*-konjektuurin nojalla kaikilla  $i = 1, 2, 3$*

$$x_3 \leq C(\varepsilon) \left( x_i \operatorname{rad} \left( \frac{x_1 x_2 x_3}{x_i} \right) \right)^{1+\varepsilon}.$$

*Todistus.* Olkoon  $d = \operatorname{syt}(x_1, x_2, x_3)$ . Soveltamalla *Abc*-konjektuuria kolmikkoon  $(\frac{x_1}{d}, \frac{x_2}{d}, \frac{x_3}{d})$  saadaan

$$\begin{aligned} \frac{x_3}{d} &\leq C(\varepsilon) \operatorname{rad} \left( \frac{x_1 x_2 x_3}{d^3} \right)^{1+\varepsilon} \leq C(\varepsilon) \operatorname{rad} \left( \frac{x_1 x_2 x_3}{d} \right)^{1+\varepsilon} \\ &\leq C(\varepsilon) \operatorname{rad} \left( \frac{x_1 x_2 x_3}{d} \cdot \frac{x_i}{x_i} \right)^{1+\varepsilon} \leq C(\varepsilon) \left( \frac{x_i}{d} \right)^{1+\varepsilon} \operatorname{rad} \left( \frac{x_1 x_2 x_3}{x_i} \right)^{1+\varepsilon}. \end{aligned}$$

Väite seuraa käyttämällä arviota  $d \leq d^{1+\varepsilon}$  epäyhtälön oikean puolen nimittäjään ja kertomalla epäyhtälö puolittain luvulla  $d$ .  $\square$

## 4.2 Aritmeettisista lukujonoista

Olkoot  $m, d, k \in \mathbb{N}$  siten, että  $\text{sy}(m, d) = 1$  ja  $k \geq 3$ . Tarkstellaan tuloa

$$\Pi = m(m+d)(m+2d) \cdots (m+(k-1)d),$$

joka koostuu  $k$ :sta peräkkäisestä aritmeettisen lukujonon  $m, m+d, \dots, m+(k-1)d$  termistä. Vuonna 1975 P. Erdős ja J. L. Selfridge osoittivat, että jos  $d = 1$ , niin  $\Pi$  ei voi olla muotoa  $y^n$ , missä  $y, n \geq 2$ . 1985 R. Marzsalek osoitti, että muoto  $\Pi = y^n$  on mahdollinen  $d$ :n valinnasta riippuvalle rajoitetulle määrälle lukuja  $k$ , kun  $y, n \geq 2$ . Sovelletaan tilanteeseen *Abc*-konjektuuria seuraavalla aputuloksella. [46, s. 36–37]

**Lemma 4.2.1.** *Olkoot  $i, j \in \mathbb{N}$  siten, että  $0 \leq i < j \leq k-1$ . Tällöin  $\text{sy}(m+id, m+jd) < k$ .*

*Todistus.* Lauseen 2.1.5 nojalla  $g = \text{sy}(m+id, m+jd) = m+jd - (m+id) = (j-i)d$ . Jos  $p$  on luvun  $g$  alkutekijä, niin Lemman 2.1.13 nojalla joko  $p \mid (j-i)$  tai  $p \mid d$ . Jos  $p \mid d$ , niin ehdoista  $g \mid (m+id)$  ja  $p \mid g$  seuraa  $p \mid m$ , jolloin oletuksen  $\text{sy}(m, d) = 1$  nojalla täytyy olla  $p = 1$ . Jos taas  $p \mid (j-i) < k$ , niin myös  $g < k$ . Tämä osoittaa, että termeillä  $m+id$  ja  $m+jd$  ei ole yhteisiä alkutekijöitä  $p$ , joille  $p \geq k$   $\square$

**Huomautus 4.2.2.** Olkoon  $i \in \mathbb{N}$ . Edellisen Lemman mukaan

(i) jos  $0 \leq i \leq k-2$ , niin  $\text{sy}(m+id, m+(i+1)d) = 1$ .

(ii) jos  $0 \leq i \leq k-3$ , niin  $\text{sy}(m+id, m+(i+2)d) \leq 2$ .

**Konjektuuri 4.2.3.** *Olkoot  $m, k, y, n \in \mathbb{N}$  siten, että  $k \geq 3$  ja  $n \geq 2$ . Tällöin kaikilla  $d \in \mathbb{N}$  yhtälöllä*

$$m(m+d)(m+2d) \cdots (m+(k-1)d) = y^n$$

*on vain äärellinen määrä ratkaisuja.*

**Lause 4.2.4.** *Abc-konjektuurin nojalla Konjektuuri 4.2.3 on voimassa arvolla  $k = 3$ .*

*Todistus.* Lemmaa 4.2.1 soveltamalla kaikilla  $i, i \in \{0, 1, 2\}$ , voidaan kirjoittaa

$$m = a_0 y_0^n, \quad m+d = a_1 y_1^n \quad \text{ja} \quad m+2d = a_2 y_2^n,$$

missä luku  $a_i$  koostuu lukua  $k = 3$  pienemmistä alkutekijöistä ja luku  $y_i$  koostuu suuruudeltaan vähintään lukua 3 olevista alkutekijöistä tai  $y_i = 1$ . Huomautuksen 4.2.2 mukaan  $\text{sy}(m+d, m(m+2d)) = 1$ , jolloin  $a_1 = 1$  ja  $y_1 \geq 2$ . Yhtälöstä  $(m+d)^2 = d^2 + m(m+2d)$  saadaan siten *abc*-summa

$$a_1 y_1^{2n} = d^2 + a_0 a_2 y_0^n y_2^n. \tag{4.2}$$

Soveltamalla *Abc*-konjektuuria ja arvioimalla ylöspäin saadaan

$$y_1^{2n} \leq C(\varepsilon) \text{rad}(d^2 a_0 a_1 a_2 y_0 y_1 y_2)^{1+\varepsilon} \leq C_1(\varepsilon) y_1^{3(1+\varepsilon)},$$

missä  $C_1(\varepsilon) = C(\varepsilon) d a_0 a_1 a_2$ . Edelleen

$$y_1^{2n-3(1+\varepsilon)} \leq C(\varepsilon),$$

josta nähdään luku  $\varepsilon$  kiinnittämällä, että  $n$  on rajoitettu. Lisäksi yhtälön (4.2) nojalla kaikilla  $n \geq 2$  myös luvut  $y_0, y_1$  ja  $y_2$  ovat rajoitettuja.  $\square$

### 4.3 Luvuista, joilla on samat alkutekijät

Vuonna 1999 T. Cochrane ja R. Dressler [12] julkaisivat hyvin läheisesti Bertrandin postulaattia muistuttavat kaksi otaksumaa:

**Konjektuuri 4.3.1** (Dressler). *Olkoot  $a, c \in \mathbb{N}$ ,  $a < c$ , siten, että luvuilla  $a$  ja  $c$  on samat alkutekijät. Tällöin on olemassa alkuluku  $p$ , jolle pätee*

$$a \leq p < c.$$

**Konjektuuri 4.3.2.** *Olkoot  $a, c \in \mathbb{N}$ ,  $a < c$ , siten, että luvuilla  $a$  ja  $c$  on samat alkutekijät. Tällöin jokaista  $\varepsilon > 0$  kohti on olemassa luku  $C(\varepsilon) > 0$  siten, että*

$$c - a \geq C(\varepsilon)c^{\frac{1}{2}-\varepsilon}.$$

Konjektuuri 4.3.1 seuraa Konjektuurista 4.3.2, mikäli tiedetään enemmän vakiosta  $C(\varepsilon)$  ja kahden peräkkäisen alkuluvun maksimaalisen välin pituudesta. Konjektuuri 4.3.2 on puolestaan helppo seuraus *Abc*-konjektuurista. [12]

**Lause 4.3.3.** *Abc-konjektuurista seuraa Konjektuuri 4.3.2.*

*Todistus.* Oletetaan, että luvut  $a$  ja  $c$  ovat Konjektuurin 4.3.2 oletukset täyttäviä lukuja, jolloin siis  $\text{rad}(a) = \text{rad}(c)$ . Asetetaan  $b = c - a$  ja  $d = \text{syt}(a, b, c)$ . Tällöin kolmikko  $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$  muodostaa *abc*-summan. Lukujen  $a$  ja  $c$  radikaalille pätee  $\text{rad}(a) \mid b$ , joten saadaan arvio

$$\text{rad}\left(\frac{a}{d} \frac{b}{d} \frac{c}{d}\right) \leq \text{rad}(ac) \text{rad}\left(\frac{b}{d}\right) \leq \text{rad}(a) \cdot \frac{b}{d} \leq \frac{b^2}{d}.$$

Soveltamalla *Abc*-konjektuuria ja edellä saatua arviota *abc*-summaan  $\frac{a}{d} + \frac{b}{d} = \frac{c}{d}$  saadaan

$$\frac{c}{d} \leq C(\varepsilon) \left(\frac{b^2}{d}\right)^{1+\varepsilon},$$

josta edelleen

$$c \leq C(\varepsilon)b^{2(1+\varepsilon)}.$$

Näin ollen

$$b \geq \left(\frac{c}{C(\varepsilon)}\right)^{\frac{1}{2(1+\varepsilon)}} = C'(\varepsilon)c^{\frac{1+\varepsilon-\varepsilon}{2(1+\varepsilon)}} = C'(\varepsilon)c^{\frac{1}{2}-\frac{\varepsilon}{2(1+\varepsilon)}} \geq C'(\varepsilon)c^{\frac{1}{2}-\varepsilon}$$

missä  $C'(\varepsilon) = C(\varepsilon)^{-\frac{1}{2(1+\varepsilon)}}$ . Koska  $b = c - a$ , väite seuraa.  $\square$

Itse asiassa seuraava Lauseeseen 3.3.3 perustuva Konjektuurin 4.3.2 mukainen tulos on voimassa ilman oletuksia *Abc*-konjektuurin todenperäisyydestä [12].

**Lause 4.3.4.** *Olkoot  $a, c \in \mathbb{N}$ ,  $a < c$ , siten, että luvuilla  $a$  ja  $c$  on samat alkutekijät. Tällöin jokaista  $\varepsilon > 0$  kohti on olemassa luku  $C(\varepsilon) > 0$  siten, että*

$$c - a \geq C(\varepsilon)(\log c)^{\frac{3}{4}-\varepsilon}.$$



## 4.4 Catalanin ja Pillain konjektuurit

Vuonna 1844 E. C. Catalan esitti konjektuurin, jonka mukaan 8 ja 9 ovat ainoat peräkkäiset kokonaislukupotenssit [58, s. 201]. Formaalisimmin konjektuuri voidaan esittää muodossa

**Konjektuuri 4.4.1** (Catalan). *Olkoot  $x, y, m, n \in \mathbb{N} \setminus \{1\}$ . Tällöin yhtälöllä*

$$x^m - y^n = 1 \quad (4.3)$$

*on vain ratkaisu  $(x, y, m, n) = (3, 2, 2, 3)$ .*

**Huomautus 4.4.2.** Aiemmin on pystytty osoittamaan muun muassa, että yhtälöllä (4.3) ei ole ratkaisuja arvolla  $n = 2$  (Lebesgue, 1850) ja arvolla  $m = 2$  on vain ratkaisu  $(x, y, m, n) = (3, 2, 2, 3)$  (Chao Ko, 1965) [58, s. 216-217]. Viimein vuonna 2002 P. Mihăilescu osoitti konjektuurin todeksi käyttämällä hyväksi syklotomisten kuntien teoriaa [41].

Näytetään seuraavaksi kirjaan [43, s. 186-187] perustuen, että *Abc*-konjektuuri implikoi Catalanin konjektuurin asymptoottisen version.

**Lause 4.4.3.** *Abc-konjektuurin nojalla yhtälöllä (4.3) on vain äärellisen monta ratkaisua.*

*Todistus.* Olkoon  $(x, y, m, n)$  yhtälön (4.3) ratkaisu. Huomautuksen 4.4.2 nojalla riittää tarkastella tilannetta  $\min\{m, n\} \geq 3$ . Lauseen 2.1.5 mukaan  $\text{syt}(x, y) = 1$ . Soveltamalla *Abc*-konjektuuria arvolla  $\varepsilon = \frac{1}{4}$  ja vakiolla  $K_2 = C(\frac{1}{4})$  saadaan

$$y^n < x^m \leq K_2 \text{rad}(x^m y^n)^{\frac{5}{4}} = K_2 \text{rad}(xy)^{\frac{5}{4}} \leq K_2 (xy)^{\frac{5}{4}},$$

josta seuraa yhtälöt

$$m \log x \leq \log K_2 + \frac{5}{4}(\log x + \log y) \quad (4.4)$$

$$n \log y < \log K_2 + \frac{5}{4}(\log x + \log y). \quad (4.5)$$

Laskemalla yhtälöt (4.4) ja (4.5) puolittain yhteen saadaan

$$m \log x + n \log y < 2 \log K_2 + \frac{5}{2}(\log x + \log y),$$

josta edelleen termejä järjestelemällä

$$\left(m - \frac{5}{2}\right) \log x + \left(n - \frac{5}{2}\right) \log y < 2 \log K_2. \quad (4.6)$$

Koska oletuksen nojalla  $x \geq 2$  ja  $y \geq 2$ , saadaan arvio alaspäin

$$(m + n - 5) \log 2 = \left(m - \frac{5}{2}\right) \log 2 + \left(n - \frac{5}{2}\right) \log 2 \leq \left(m - \frac{5}{2}\right) \log x + \left(n - \frac{5}{2}\right) \log y,$$

jota käyttämällä yhtälö (4.6) sievenee muotoon

$$m + n < \frac{2 \log K_2}{\log 2} + 5.$$

Koska epäyhtälön oikea puoli on vakio, yhtälöllä (4.3) on vain äärellinen määrä ratkaisuja eksponenttiparilla  $(m, n)$ . Näin ollen kiinnitettyillä eksponenteilla  $m \geq 3$  ja  $n \geq 3$  yhtälöllä (4.6) on vain äärellisen monta positiivista kokonaislukuratkaisua  $x$  ja  $y$ , mistä väite seuraa.  $\square$

Catalanin konjektuurin yleisti Pillai vuonna 1945 [58, s. 201]:

**Konjektuuri 4.4.4** (Pillai). *Olkoot  $A, B, k \in \mathbb{N}$  ja  $x, y, m, n \in \mathbb{N} \setminus \{1\}$  siten, että  $mn > 4$ . Tällöin yhtälöllä*

$$Ax^m - By^n = k \quad (4.7)$$

*on vain äärellinen määrä ratkaisuja.*

Osoitetaan konjektuuri *Abc*-konjektuurin avulla [46, s. 23].

**Lause 4.4.5.** *Konjektuuri 4.4.4 seuraa Abc-konjektuurista.*

*Todistus.* Merkitsemällä  $d = \text{syt}(Ax^m, By^n, k)$  ja soveltamalla *Abc*-konjektuuria summaan  $\frac{Ax^m}{d} = \frac{By^n}{d} + \frac{k}{d}$  saadaan epäyhtälöketju

$$\frac{By^n}{d} \leq \frac{Ax^m}{d} \leq C(\varepsilon) \text{rad}\left(\frac{Ax^m By^n k}{d^3}\right)^{1+\varepsilon},$$

josta edelleen ylöspäin arvioimalla saadaan

$$By^n \leq Ax^m \leq C(\varepsilon) \left(d \cdot \frac{ABk}{d} \text{rad}(x^m y^n)\right)^{1+\varepsilon} \leq C_1(\varepsilon, A, B, k)(xy)^{1+\varepsilon},$$

missä  $C_1(\varepsilon, A, B, k) = C(\varepsilon)(ABk)^{1+\varepsilon}$ . Näin ollen saadaan epäyhtälöt

$$x^m \leq C_2(\varepsilon, A, B, k)(xy)^{1+\varepsilon}, \quad (4.8)$$

$$y^n \leq C_3(\varepsilon, A, B, k)(xy)^{1+\varepsilon}, \quad (4.9)$$

missä  $C_2(\varepsilon, A, B, k) = C(\varepsilon)(Bk)^{1+\varepsilon}A^\varepsilon$  ja  $C_3 = C(\varepsilon)(Ak)^{1+\varepsilon}B^\varepsilon$ .

Oletetaan nyt  $x^m \leq y^n$ , jolloin  $x \leq y^{\frac{n}{m}}$ . Tällöin yhtälöstä (4.9) saadaan

$$y^n \leq C_3(\varepsilon, A, B, k)y^{(1+\frac{n}{m})(1+\varepsilon)},$$

josta edelleen

$$y^{n-(1+\frac{n}{m})(1+\varepsilon)} = (y^n)^{1-(\frac{1}{n}+\frac{1}{m})(1+\varepsilon)} \leq C_3(\varepsilon, A, B, k). \quad (4.10)$$

Koska  $m \geq 2$  ja  $n \geq 2$  siten, että  $mn > 4$ , täytyy tulo  $mn \geq 6$ , jolloin

$$\frac{1}{n} + \frac{1}{m} \leq \frac{1}{2} + \frac{1}{3} = \frac{5}{6}.$$

Näin ollen valinta  $0 < \varepsilon < \frac{1}{5}$  toteuttaa epäyhtälön

$$\left(\frac{1}{n} + \frac{1}{m}\right)(1+\varepsilon) < 1,$$

jolloin edelleen epäyhtälön (4.10) nojalla  $y$  ja  $n$  ovat rajoitettuja. Oletuksesta  $x^m \leq y^n$  seuraa, että myös  $x$  ja  $m$  ovat rajoitettuja.

Tapauksessa  $y^n \leq x^m$  päättely on täysin analoginen. Väite seuraa.  $\square$

Tarkastellaan vielä Pillain konjektuurin ulkopuolelle jäänyttä hieman Pellin yhtälöä muistuttavaa tilannetta  $m = n = 2$  [46, s. 23–24]:

**Lause 4.4.6.** Olkoot  $A, B, k \in \mathbb{N}$  ja  $x, y \in \mathbb{N} \setminus \{1\}$ .  $abc$ -konjektuurin nojalla yhtälöllä

$$Ax^2 - By^2 = k. \quad (4.11)$$

on vain äärellinen määrä ratkaisuja, kun  $\text{rad}(y)$  on rajoitettu.

*Todistus.* Merkitsemällä  $d = \text{syt}(Ax^2, By^2, k)$  ja soveltamalla  $abc$ -konjektuuria summaan  $\frac{Ax^2}{d} = \frac{By^2}{d} + \frac{k}{d}$  saadaan epäyhtälö

$$\frac{Ax^2}{d} \leq C(\varepsilon) \text{rad}\left(\frac{ABkx^2y^2}{d^3}\right)^{1+\varepsilon},$$

josta edelleen

$$Ax^2 \leq C(\varepsilon) \left(d \cdot \frac{ABk}{d} \text{rad}(x^2y^2)\right)^{1+\varepsilon} \leq C(\varepsilon) (ABk)^{1+\varepsilon} \text{rad}(xy)^{1+\varepsilon}.$$

Jakamalla puolittain luvulla  $A$  ja arvioimalla radikaalia saadaan siten

$$x^2 \leq C(\varepsilon) (Bk)^{1+\varepsilon} A^\varepsilon x^{1+\varepsilon} \text{rad}(y)^{1+\varepsilon},$$

josta edelleen

$$x^{1-\varepsilon} \leq C(\varepsilon) (Bk)^{1+\varepsilon} A^\varepsilon \text{rad}(y)^{1+\varepsilon}.$$

Koska oletuksen mukaan  $\text{rad}(y)$  on rajoitettu, valitsemalla  $0 < \varepsilon < 1$  nähdään, että myös luku  $x$  on rajoitettu. Näin ollen yhtälöllä (4.11) on vain äärellinen määrä ratkaisuja.  $\square$

**Huomautus 4.4.7.** Lauseen 4.4.6 todistusta imitoimalla saadaan samanlainen tulos myös olettamalla, että  $\text{rad}(x)$  on rajoitettu.

## 4.5 Hallin konjektuuri

Vuonna 1971 M. Hall esitti täydellisten neliöiden ja täydellisten kuutioiden erotuksella olevan tietynlainen alarajan [57, s. 205]:

**Konjektuuri 4.5.1** (Hall, alkuperäinen). *On olemassa vakio  $C > 0$  siten, että kaikilla  $x, y \in \mathbb{N}$ ,  $x^2 \neq y^3$ , on voimassa epäyhtälö*

$$|x^2 - y^3| > Cy^{\frac{1}{2}}.$$

$abc$ -konjektuuri implikoi ns. Hallin konjektuurin heikon muodon [57, s. 205–206]:

**Konjektuuri 4.5.2** (Hall, heikko). *Jokaista lukua  $\varepsilon > 0$  kohti on olemassa luku  $C(\varepsilon) > 0$  siten, että epäyhtälö*

$$|x^2 - y^3| > C(\varepsilon)y^{\frac{1}{2}-\varepsilon}.$$

*toteutuu kaikilla  $x, y \in \mathbb{N}$ ,  $x^2 \neq y^3$ .*

**Lause 4.5.3.**  $abc$ -konjektuurista seuraa Konjektuuri 4.5.2.

*Todistus.* Asetetaan  $d = \text{syt}(x^2, y^3)$  sekä  $a = \frac{x^2}{d}$ ,  $b = -\frac{y^3}{d}$  ja  $c = \frac{x^2 - y^3}{d}$ . Tällöin summaan  $a + b = c$  voidaan soveltaa  $Abc$ -konjektuurin yleistä muotoa (Konjektuuri 3.2.2), jolloin saadaan epäyhtälöt

$$|b| = \frac{y^3}{d} \leq \max\{|a|, |b|, |c|\} \leq C(\varepsilon) \text{rad}(abc)^{1+\varepsilon}$$

$$a = \frac{x^2}{d} \leq \max\{|a|, |b|, |c|\} \leq C(\varepsilon) \text{rad}(abc)^{1+\varepsilon}.$$

Kertomalla epäyhtälöt puolittain ja arvioimalla saadaan

$$\frac{x^2 y^3}{d^2} \leq C(\varepsilon)^2 \text{rad}(abc)^{2+2\varepsilon} \leq C(\varepsilon)^2 x^{2+2\varepsilon} y^{2+2\varepsilon} \frac{|x^2 - y^3|^{2+2\varepsilon}}{d^{2+2\varepsilon}},$$

josta edelleen

$$x^2 y^3 \leq C(\varepsilon)^2 x^{2+2\varepsilon} y^{2+2\varepsilon} |x^2 - y^3|^{2+2\varepsilon}.$$

Näin ollen epäyhtälö sievenee muotoon

$$|x^2 - y^3|^{2+2\varepsilon} \geq \frac{1}{C(\varepsilon)^2} x^{-2\varepsilon} y^{1-2\varepsilon},$$

josta tarkastelu jakautuu kahteen osaan.

Jos  $x \leq 2y^2$ , niin tällöin

$$|x^2 - y^3|^{2+2\varepsilon} \geq \frac{1}{C(\varepsilon)^2} \frac{1}{(2y^2)^{2\varepsilon}} y^{1-2\varepsilon} = \frac{1}{4^\varepsilon C(\varepsilon)^2} \frac{y^{1-2\varepsilon}}{y^{4\varepsilon}} = \frac{1}{4^\varepsilon C(\varepsilon)^2} y^{1-6\varepsilon},$$

josta edelleen

$$|x^2 - y^3| \geq \left( \frac{1}{4^\varepsilon C(\varepsilon)^2} \right)^{\frac{1}{2+2\varepsilon}} y^{\frac{1-6\varepsilon}{2+2\varepsilon}} = C_1(\varepsilon) y^{\frac{1+\varepsilon-7\varepsilon}{2(1+\varepsilon)}} = C_1(\varepsilon) y^{\frac{1}{2} - \frac{7\varepsilon}{2(1+\varepsilon)}} > C_1(\varepsilon) y^{\frac{1}{2} - 7\varepsilon},$$

missä  $C_1(\varepsilon) = (4^\varepsilon C(\varepsilon)^2)^{-\frac{1}{2+2\varepsilon}}$ . Merkitsemällä  $\varepsilon' = 7\varepsilon$  saadaan epäyhtälö lopulta haluttuun muotoon

$$|x^2 - y^3| > C_1(\varepsilon') y^{\frac{1}{2} - \varepsilon'}.$$

Jos taas  $x > 2y^2$ , niin tällöin suoraan erotusta arvioimalla saadaan

$$|x^2 - y^3| > 4y^4 - y^4 = 3y^4 > C_2(\varepsilon) y^{\frac{1}{2} - \varepsilon},$$

missä esimerkiksi  $C_2(\varepsilon) = \max\{1, C_1(\varepsilon)\}$ . Molemmissa tapauksissa väite seuraa.  $\square$

**Huomautus 4.5.4.** Hallin konjektuurin voidaan ajatella olevan Pillain konjektuurin erikoistapaus, asettamalla nimittäin Konjektuurissa 4.4.4  $(A, B, m, n) = (1, 1, 2, 3)$  muuntuu tarkasteltava yhtälö (4.7) muotoon

$$x^2 - y^3 = k.$$

Mainitaan vielä, että työssään [46, s. 20–21] Nitaj osoittaa  $Abc$ -konjektuurin implikoivan myös seuraavanlaisen version heikosta Hallin konjektuurista.

**Konjektuuri 4.5.5.** *Jokaista lukua  $\varepsilon > 0$  kohti on olemassa luku  $C(\varepsilon) > 0$  siten, että epäyhtälö*

$$|x^2 - y^3| \geq C(\varepsilon) \max(x^2, y^3)^{\frac{1}{6} - \varepsilon}.$$

*toteutuu kaikilla  $x \in \mathbb{N}$  ja  $y \in \mathbb{N} \setminus \{1\}$ .*

## 4.6 Fermat-Catalanin konjektuuri

Yhdistämällä Fermat'n suuren lauseen ja Catalanin konjektuurin ideat saadaan seuraava Fermat-Catalanin konjektuuriksi kutsuttu otaksuma [15]:

**Konjektuuri 4.6.1** (Fermat-Catalan). *Olkoot  $x, y, z, p, q, r \in \mathbb{N}$  siten, että  $\text{sy}(x, y, z) = 1$  ja  $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ . Tällöin yhtälöllä*

$$x^p + y^q = z^r$$

*on vain äärellinen määrä ratkaisuja.*

**Huomautus 4.6.2.** Tällä hetkellä tunnetaan vain ratkaisut

$$\begin{array}{ll} 1^p + 2^3 = 3^2 & 2^5 + 7^2 = 3^4 \\ 7^3 + 13^2 = 2^9 & 2^7 + 17^3 = 71^2 \\ 3^5 + 11^4 = 122^2 & 17^7 + 76271^3 = 21063928^2 \\ 1414^3 + 2213459^2 = 65^7 & 9262^3 + 15312283^2 = 113^7 \\ 43^8 + 96222^3 = 30042907^2 & 33^8 + 1549034^2 = 15613^3. \end{array}$$

Ensimmäisessä yhtälössä valitsemalla  $p \geq 6$  saadaan äärettömästi ratkaisuja, mutta konjektuurin valossa tarkastellaan sitä kuitenkin vain yhtenä ratkaisuna. [15]

*Abc*-konjektuurin avulla voidaan osoittaa seuraava yleisempi tulos [46, s. 24–25].

**Lause 4.6.3.** *Olkoot  $A, B, C, x, y, z, p, q, r \in \mathbb{N}$  siten, että  $\text{sy}(x, y, z) = 1$  ja  $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$ . Tällöin *Abc*-konjektuurin nojalla yhtälöllä*

$$Ax^p + By^q = Cz^r \tag{4.12}$$

*on vain äärellinen määrä ratkaisuja.*

*Todistus.* Voidaan olettaa  $z \geq 2$ , sillä tapauksessa  $z = 1$  väite seuraa Pillain konjektuurista (Konjektuuri 4.4.4). Asettamalla  $d = \text{sy}(Ax^p, By^q, Cz^r)$  ja soveltamalla *Abc*-konjektuuria summaan  $\frac{Ax^p}{d} + \frac{By^q}{d} = \frac{Cz^r}{d}$  saadaan

$$\frac{Cz^r}{d} \leq C(\varepsilon) \text{rad}\left(\frac{ABCx^p y^q z^r}{d^3}\right)^{1+\varepsilon},$$

josta edelleen ylöspäin arvioimalla

$$z^r \leq \frac{1}{C} \cdot C(\varepsilon) \left(d \cdot \frac{ABC}{d} \text{rad}(x^p y^q z^r)\right)^{1+\varepsilon} \leq C_1(\varepsilon, A, B, C)(xyz^r)^{1+\varepsilon},$$

missä  $C_1(\varepsilon, A, B, C) = \frac{1}{C} \cdot C(\varepsilon)(ABC)^{1+\varepsilon}$ . Koska  $Ax^p < Cz^r$  ja  $By^q < Cz^r$ , niin  $x < (\frac{Cz^r}{A})^{\frac{1}{p}}$  ja  $y < (\frac{Cz^r}{B})^{\frac{1}{q}}$ , ja siten

$$z^r \leq C_2(\varepsilon, A, B, C)(z^r)^{(1+\varepsilon)(\frac{1}{r} + \frac{1}{p} + \frac{1}{q})},$$

missä  $C_2(\varepsilon, A, B, C) = C_1(\varepsilon, A, B, C) \left(\left(\frac{C}{A}\right)^{\frac{1}{p}} \left(\frac{C}{B}\right)^{\frac{1}{q}}\right)^{1+\varepsilon}$ . Tästä saadaan edelleen

$$(z^r)^{1-(1+\varepsilon)(\frac{1}{r} + \frac{1}{p} + \frac{1}{q})} \leq C_2(\varepsilon, A, B, C).$$

Valitsemalla nyt  $\varepsilon > 0$  siten, että  $1 - (1 + \varepsilon)(\frac{1}{r} + \frac{1}{p} + \frac{1}{q}) > 0$ , nähdään termin  $z^r$  olevan ylhäältä rajoitettu vakiolla  $C_2(\varepsilon, A, B, C)$ . Näin ollen myös luvut  $z, x, y, p, q, r$  ovat rajoitettuja.  $\square$

**Huomautus 4.6.4.** Yhtälöä (4.12) kutsutaan yleistetyksi Fermat'n yhtälöksi [15].

## 4.7 Shorey-Tijdemanin konjektuuri

Vuonna 1986 T. N. Shorey ja R. Tijdeman esittivät seuraavan konjektuurin [58, s. 202]:

**Konjektuuri 4.7.1** (Shorey-Tijdeman). *Olkoot  $x, y, v, w \in \mathbb{N}$  ja  $m, n \in \mathbb{N} \setminus \{1\}$  siten, että  $\text{syt}(x, v) = \text{syt}(y, w) = 1$  ja  $mn > 4$ . Tällöin yhtälöllä*

$$\left(\frac{x}{v}\right)^m - \left(\frac{y}{w}\right)^n = 1 \quad (4.13)$$

*on vain äärellinen määrä ratkaisuja.*

Teoksen [58] samassa yhteydessä osoitetaan, että konjektuuri pitää paikkansa, mikäli jokin luvuista  $v, w, x, y$  on kiinnitettyjen alkulukujen tulo. *Abc*-konjektuurin avulla voidaan konjektuuri osoittaa todeksi asettamalla lisäoletus eksponenteille  $m$  ja  $n$  [46, s. 25–26].

**Lause 4.7.2.** *Abc-konjektuurin nojalla Konjektuuri 4.7.1 on voimassa.*

*Todistus.* Oletetaan  $(v, w) \neq (1, 1), (1, 2), (2, 1)$ , sillä muuten väite seuraa Catalanin ja Pillain konjektuureista (Konjektuurit 4.4.1 ja 4.4.4). Nyt yhtälö (4.13) saadaan muotoon

$$w^n x^m - v^m y^n = v^m w^n, \quad (4.14)$$

josta edelleen saadaan yhtälöt

$$w^n x^m = v^m (y^n + w^n), \quad (4.15)$$

$$v^m y^n = w^n (x^m - v^m). \quad (4.16)$$

Määritelmän 2.1.1 ja yhtälön (4.15) mukaan  $v^m \mid w^n x^m$ , jolloin oletuksesta  $\text{syt}(x, v) = 1$  ja Eukleideen lemmasta (Lemma 2.1.12) seuraa  $v^m \mid w^n$ . Vastaavalla päättelyllä yhtälöstä (4.16) seuraa  $w^n \mid v^m$ , ja oletuksesta  $v, w \in \mathbb{N}$  edelleen  $v^m = w^n$ . Aritmetiikan peruslauseen (Lause 2.1.14) yksikäsitteisyyden nojalla voidaan asettaa luku  $z \in \mathbb{N} \setminus \{1\}$  siten, että

$$v^m = w^n = z^{\text{pym}(n, m)}, \quad (4.17)$$

missä  $\text{pym}(n, m)$  on lukujen  $n$  ja  $m$  pienin yhteinen monikerta. Yhtälö (4.14) sievenee tällöin yhtälöä (4.17) soveltamalla muotoon

$$x^m - y^n = z^{\text{pym}(m, n)}. \quad (4.18)$$

Soveltamalla nyt *Abc*-konjektuuria Lauseen 4.6.3 mukaisesti saadaan, että yhtälöllä 4.18 on äärellinen määrä ratkaisuja aina kun

$$\frac{1}{m} + \frac{1}{n} + \frac{1}{\text{pym}(m, n)} < 1. \quad (4.19)$$

Yhtälö (4.19) on voimassa kaikilla  $m, n \geq 2$  ja  $mn > 4$  lukuunottamatta lukupareja  $(m, n) = (2, 3), (3, 2), (3, 3), (2, 4), (4, 2)$ . Tarkastellaan nämä tilanteet erikseen:

1.  $(m, n) = (2, 3)$  ja  $(m, n) = (3, 2)$ : Yhtälöillä  $x^2 - y^3 = z^6$  ja  $x^3 - y^2 = z^6$  on vain äärellinen määrä ratkaisuja, sillä vastaavilla elliptisillä käyrillä on vain äärellinen määrä rationaaliratkaisuja [46, s. 26]
2.  $(m, n) = (3, 3)$ : Yhtälöllä  $x^3 - y^3 = z^3$  ei ole ei-triviaaleja ratkaisuja [16, s. 40–54], [70]
3.  $(m, n) = (2, 4)$ : Yhtälöllä  $x^2 - y^4 = z^4$  ei ole ei-triviaaleja ratkaisuja [42, s. 16]
4.  $(m, n) = (4, 2)$ : Yhtälöllä  $x^4 - y^2 = z^4$  ei ole ei-triviaaleja ratkaisuja [42, s. 17].

Väite seuraa. □

## 4.8 Erdős-Stewartin konjektuuri

Merkitään  $p_k$ :lla  $k$ :ttä alkulukua, missä  $k \in \mathbb{N}$ . P. Erdős ja C.L. Stewart asettivat seuraavan konjektuurin [27, Problem A2, s. 7]:

**Konjektuuri 4.8.1** (Erdős-Stewart). *Olkoot  $a, b \in \mathbb{Z}_{\geq 0}$  ja olkoon  $n \in \mathbb{N}$  siten, että  $p_{k-1} \leq n < p_k$ . Tällöin yhtälöllä*

$$n! + 1 = p_k^a p_{k+1}^b \quad (4.20)$$

*on ainoastaan ratkaisut*

$$1! + 1 = 2, \quad 2! + 1 = 3, \quad 3! + 1 = 7, \quad 4! + 1 = 5^2, \quad 5! + 1 = 11^2.$$

Vuonna 2001 F. Luca todisti konjektuurin osoittamalla ensin ettei yhtälöllä (4.20) ole ratkaisuja arvoilla  $n > 7\,242\,115$  ja tarkistamalla sitten loput tapaukset tietokoneavusteisesti [39]. Osoitetaan kuitenkin vielä *Abc*-konjektuurin avulla, että yhtälöllä (4.22) on vain äärellinen määrä ratkaisuja. Todistus perustuu työhön [46, s. 32–33] ja siinä tarvitaan seuraavaa tulosta [28, s. 455–457]:

**Lause 4.8.2** (Bertrandin postulaatti). *Olkoon  $n \in \mathbb{N}$ . Tällöin on olemassa ainakin yksi alkuluku  $p$  siten, että*

$$n < p \leq 2n.$$

*Toisin sanoen kaikilla  $k \in \mathbb{N}$*

$$p_{k+1} < 2p_k.$$

**Lause 4.8.3.** *Abc-konjektuurin nojalla yhtälöllä (4.20) on vain äärellisen monta ratkaisua.*

*Todistus.* Lauseen 2.1.5 nojalla  $\text{syt}(n!, p_k^a p_{k+1}^b) = 1$ . Soveltamalla *Abc*-konjektuuria *abc*-summaan (4.20) saadaan

$$n! \leq p_k^a p_{k+1}^b \leq C(\varepsilon) \text{rad}(n! p_k p_{k+1})^{1+\varepsilon} = C(\varepsilon) \left( \prod_{p \leq p_{k+1}} p \right)^{1+\varepsilon}. \quad (4.21)$$

Bertrandin postulaatin ja oletuksen  $p_{k-1} \leq n$  mukaan  $p_{k+1} < 2p_k < 4p_{k-1} \leq 4n$ , jolloin arvioita  $\frac{n^n}{e^n} \leq n!$  (Lemma 2.7.14) ja  $\prod_{p \leq n} p < 4^n$  (Lemma 2.8.1) soveltamalla saadaan epäyhtälö (4.21) muotoon

$$\left(\frac{n}{e}\right)^n \leq C(\varepsilon) 4^{p_{k+1}(1+\varepsilon)} \leq C(\varepsilon) 4^{4n(1+\varepsilon)} \leq (C(\varepsilon) 4^{4(1+\varepsilon)})^n,$$

josta puolittain  $n$ :s juuri ottamalla ja  $\varepsilon$  kiinnittämällä nähdään, että luku  $n$  on rajoitettu.  $\square$

Työssä [46, s. 32–33] huomautetaan vielä, että *Abc*-konjektuurin avulla voidaan äärellistä määrää poikkeuksia lukuunottamatta osoittaa todeksi myös seuraava yleisempi konjektuuri:

**Konjektuuri 4.8.4.** *Olkoot  $a, b \in \mathbb{Z}_{\geq 0}$ ,  $u \in \mathbb{N}$ , ja  $n \in \mathbb{N} \setminus \{1\}$  siten, että  $p_{k-u} \leq n < p_k$ . Tällöin yhtälöllä*

$$n! + 1 = p_k^a p_{k+1}^b$$

*on vain äärellinen määrä ratkaisuja.*

## 4.9 Erdős-Woodsin konjektuuri arvolla $k = 3$

Vuonna 1981 A. Woods [73, s. 53] otaksui P. Erdősin ajatuksien pohjalta seuraavaa:

**Konjektuuri 4.9.1** (Erdős-Woods). *On olemassa luku  $k \in \mathbb{N}$  siten, että jokainen luku  $x \in \mathbb{N}$  voidaan määritellä yksikäsitteisesti (toisistaan eroavista) alkutekijöistä  $p$  muodostuvien joukkojen jonona  $S_0, S_1, S_2, \dots, S_k$ , missä*

$$S_i = \{p : p \mid x + i\}.$$

Esitetään konjektuuri seuraavassa ekvivalentissa muodossa:

**Konjektuuri 4.9.2.** *On olemassa vakio  $k \in \mathbb{N}$  siten, että jos luvuille  $x, y \in \mathbb{N}$  pätee*

$$\text{rad}(x + i) = \text{rad}(y + i) \tag{4.22}$$

*kaikilla  $i = 1, \dots, k$ , niin tällöin  $x = y$ .*

**Huomautus 4.9.3.** Konjektuuri 4.9.2 ei toteudu luvulla  $k = 2$ . Tämä nähdään esimerkiksi valitsemalla  $x = 74$  ja  $y = 1214$ , jolloin

$$\begin{aligned} x + 1 &= 75 = 3 \cdot 5^2, & x + 2 &= 76 = 2^2 \cdot 19, \\ y + 1 &= 1215 = 3^5 \cdot 5, & y + 2 &= 1216 = 2^6 \cdot 19. \end{aligned}$$

Vastaesimerkkejä voidaan itse asiassa konstruoida äärettömästi asettamalla

$$x_n = 2^n - 3 \quad \text{ja} \quad y_n = 2^{2n} - 2^{n+1} - 1.$$

Tällöin nimittäin

$$\begin{aligned} x_n + 1 &= 2(2^{n-1} - 1), & x_n + 2 &= 2^n - 1, \\ y_n + 1 &= 2^{2n} - 2^{n+1} = 2^{n+1}(2^{n-1} - 1), & y_n + 2 &= 2^{2n} - 2^{n+1} + 1 = (2^n - 1)^2. \end{aligned}$$

Vastaavanlaisia esimerkkejä ei tunneta luvuille  $k \geq 3$ . [46, s. 18-19]

1993 M. Langevin osoitti todeksi lukua  $k = 3$  koskevan konjektuurin [46, s. 19–20]:

**Lause 4.9.4.** *Abc-konjektuurin nojalla Konjektuuri 4.9.2 on voimassa arvolla  $k = 3$  äärellistä määrää poikkeuksia lukuunottamatta.*

*Todistus.* Olkoot  $x, y \in \mathbb{N}$  siten, että  $x < y$  ja yhtälö (4.22) toteutuu arvoilla  $i = 1, 2, 3$ . Triviaalisti  $\text{rad}(y + i) \mid (y + i)$  ja oletusten mukaan

$$\text{rad}(y + i) = \text{rad}(x + i) \mid (x + i)$$

sekä

$$\text{rad}(y + i) \mid (y - x)$$

kaikilla  $i = 1, 2, 3$ , sillä  $y - x = (y + i) - (x + i)$ . Näin ollen saadaan

$$\text{rad}((y + 1)(y + 2)(y + 3)) \mid (y - x).$$



Koska  $\text{sy}(y+1, y+2) = \text{sy}(y+2, y+3) = 1$ , saadaan *Abc*-konjektuuria summaan

$$1 + (y+1)(y+3) = (y+2)^2$$

soveltamalla ja aiempaa jaollisuushuomiota käyttämällä arvio

$$y^2 < (y+2)^2 \leq C(\varepsilon) \text{rad}((y+1)(y+2)(y+3))^{1+\varepsilon} \leq C(\varepsilon)(y-x)^{1+\varepsilon} < C(\varepsilon)y^{1+\varepsilon},$$

jolloin siis

$$y^{1-\varepsilon} < C(\varepsilon).$$

Valitsemalla  $0 < \varepsilon < 1$  nähdään, että epäyhtälön oikea puoli antaa luvulle  $y$  vain luvusta  $\varepsilon$  riippuvan ylärajan. Näin ollen kaikilla  $\varepsilon > 0$  on olemassa vakio  $C_0(\varepsilon) > 0$  siten, että jos luvuilla  $x, y$  toteutuu yhtälö (4.22) kaikilla  $i = 1, 2, 3$  ja  $y > C_0(\varepsilon)$ , niin  $x = y$ . Konjektuuri 4.9.2 on siis voimassa lukuunottamatta äärellistä määrää lukuja  $x, y$ , joille  $x < y \leq C_0(\varepsilon)$ .  $\square$

**Huomautus 4.9.5.** Konjektuurin 4.9.2 yleisessä tapauksessa voidaan osoittaa *Abc*-konjektuurista riippumaton tulos, jonka mukaan arvolla  $k \geq 2$  jokaista lukua  $x \in \mathbb{N}$  kohti on korkeintaan äärellinen määrä yhtälön (4.22) toteuttavia lukuja  $y$  [46, s. 19].

## 4.10 Richardin konjektuuri

D. Richard esitti vuonna 1989 seuraavan konjektuurin [46, s. 38]:

**Konjektuuri 4.10.1** (Richard). *Jos kaikilla  $n \in \mathbb{Z}_{\geq 0}$  luvuille  $x, y \in \mathbb{N}$  on voimassa yhtälö*

$$\text{rad}(x^{2^n} - 1) = \text{rad}(y^{2^n} - 1), \quad (4.23)$$

*niin tällöin  $x = y$ .*

Osoitetaan työhön [46, s. 38] perustuen, että Richardin konjektuuri on *Abc*-konjektuurin seuraus. Tarvitaan seuraavaa aputulosta.

**Lemma 4.10.2.** *Abc-konjektuurin nojalla kaikilla  $\varepsilon > 0$  on olemassa vakio  $C(\varepsilon) > 0$  siten, että kaikilla  $x \in \mathbb{N} \setminus \{1\}$  ja  $n \in \mathbb{N}$  on voimassa*

$$\text{rad}(x^n - 1) \geq C(\varepsilon)x^{n(1-\varepsilon)-1}.$$

*Todistus.* Soveltamalla *abc*-summaan  $(x^n - 1) + 1 = x^n$  Konjektuuria 3.2.6 saadaan

$$C(\varepsilon)(x^n)^{1-\varepsilon} \leq \text{rad}((x^n - 1)x^n) \leq x \text{rad}(x^n - 1),$$

mistä väite seuraa jakamalla puolittain luvulla  $x$ .  $\square$

**Lause 4.10.3.** *Abc-konjektuurin nojalla Konjektuuri 4.10.1 on totta.*

*Todistus.* Oletetaan, että luvuilla  $x, y \in \mathbb{N} \setminus \{1\}$  pätee kaikilla  $n \in \mathbb{Z}_{\geq 0}$  yhtälö (4.23). Valitaan luvut  $\varepsilon > 0$  ja  $n$  siten, että

$$x^{1-\varepsilon(x)} = (x(x-1))^{\frac{1}{2}} \quad \text{ja} \quad (x-1)^{2^{n-1}} < C(\varepsilon)x^{2^{n-1}-1}. \quad (4.24)$$

Toisin sanoen valitaan luku  $n$  siten, että epäyhtälö  $(1 - \frac{1}{x})^{2^{n-1}} x < C(\varepsilon)$  toteutuu.

Oletetaan vastoin väitettä, että  $y < x$ , jolloin  $y^{2^n} - 1 < y^{2^n} \leq (x-1)^{2^n}$ . Näin olen ylöspäin arvioimalla, valintoja (4.24) sekä *Abc*-konjektuuria Lemman 4.10.2 mukaisesti soveltamalla saadaan

$$y^{2^n} - 1 < (x-1)^{2^n} < C(\varepsilon)x^{2^{n-1}-1}(x-1)^{2^{n-1}} = C(\varepsilon)x^{2^n(1-\varepsilon)-1} \leq \text{rad}(x^{2^n} - 1).$$

Siten oletuksen (4.23) nojalla saadaan epäyhtälö

$$y^{2^n} - 1 < \text{rad}(y^{2^n} - 1),$$

joka ei ole voimassa millään  $y \in \mathbb{N} \setminus \{1\}$ . Tämä on ristiriita, joten täytyy olla  $x = y$ .  $\square$

## 4.11 Brocard-Ramanujan yhtälö $n! + 1 = m^2$

Toisistaan tietämättä H. Brocard (1876 ja 1885) ja S. Ramanujan (1913) esittivät ongelman kaikkien positiivisten kokonaislukuratkaisujen löytämiseksi yhtälölle

$$n! + 1 = m^2.$$

Ongelma on edelleenkin avoin. Tällä hetkellä tunnettuja ratkaisuja  $(n, m)$  arvoon  $n = 10^9$  asti ovat ainoastaan  $(4, 5)$ ,  $(5, 11)$ ,  $(7, 71)$ . [5]

Vuonna 1993 M. Overholt todisti, että *Abc*-konjektuurin nojalla yhtälöllä on vain äärellinen määrä ratkaisuja [50]. Esitetään seuraavaksi Overholtin tulos käyttämällä todistuksessa Overholtin tavoin seuraavaa *Abc*-konjektuurin implikoimaa Szpiron konjektuurin heikon muodon (Konjektuuri 3.8.1) analogiaa kokonaisluvuille (Huomautus 3.8.3):

**Konjektuuri 4.11.1.** *On olemassa luku  $s > 0$  siten, että kaikille kolmikoille  $(a, b, c) \in \mathbb{Z}^3$ , joille  $abc \neq 0$ ,  $\text{syt}(a, b, c) = 1$  ja  $a + b = c$ , pätee epäyhtälö*

$$|abc| \leq \text{rad}(abc)^s.$$

**Lause 4.11.2.** *Olko  $n, m \in \mathbb{N}$ . Konjektuurin 4.11.1 nojalla yhtälöllä*

$$n! + 1 = m^2 \quad (4.25)$$

*on vain äärellinen määrä ratkaisuja.*

*Todistus.* Luvut  $1! + 1 = 2$ ,  $2! + 1 = 3$  ja  $3! + 1 = 7$  eivät ole minkään luonnollisen luvun neliöitä, joten voidaan olettaa, että  $n \geq 4$ . Lisäksi kertoma  $n!$  on parillinen, jolloin luvun  $m$  täytyy olla pariton.

Merkitsemällä nyt  $m = 2k + 1$  jollekin  $k \in \mathbb{N}$ , saadaan yhtälö (4.25) muotoon

$$n! = (2k + 1)^2 - 1 = 4k(k + 1),$$

josta edelleen

$$\frac{1}{4}n! = k(k+1). \quad (4.26)$$

Soveltamalla nyt Konjektuuria 4.11.1  $abc$ -summaan  $1+k = k+1$  sekä arvioita  $\left(\frac{e}{n}\right)^n < n!$  (Lemma 2.7.14) ja  $\prod_{p \leq n} p < 4^n$  (Lemma 2.8.1) käyttämällä saadaan yhtälöstä (4.26) edelleen

$$\frac{1}{4} \left(\frac{n}{e}\right)^n < \frac{1}{4}n! = k(k+1) \leq \text{rad}(k(k+1))^s = \text{rad}\left(\frac{n!}{4}\right)^s \leq \left(\prod_{p \leq n} p\right)^s < 4^{sn}.$$

Kertomalla puolittain luvulla  $4e^n$  saadaan

$$n^n < 4^{sn+1}e^n \leq 4^{sn+n}e^n = (4^{s+1}e)^n,$$

josta edelleen

$$n < 4^{s+1}e.$$

Koska  $s$  on vakio, nähdään näin ollen että yhtälön (4.25) toteuttavia lukuja  $n$  on vain äärellinen määrä.  $\square$

Yleisemmän tuloksen esitti A. Dabrowski vuonna 1996 [13]:

**Lause 4.11.3.** *Olkoot  $n, m, A \in \mathbb{N}$ . Konjektuurin 4.11.1 nojalla yhtälöllä*

$$n! + A = m^2 \quad (4.27)$$

*on vain äärellinen määrä ratkaisuja, kun  $A = k^2$  jollekin  $k \in \mathbb{N}$ .*

**Huomautus 4.11.4.** Tapauksessa  $A \neq k^2$  kaikilla  $k \in \mathbb{N}$  voidaan osoittaa ilman  $abc$ -konjektuuria, että yhtälöllä (4.27) on vain äärellinen määrä ratkaisuja [13].

## 4.12 Simmons'n yhtälö $n! = m(m^2 - 1)$

Kirjassa [27, Problem D25, s. 193] Simmons kysyy, onko mahdollista esittää luvun  $n \in \mathbb{N}$  kertoma kolmen peräkkäisen luvun tulona kun  $n > 6$ . Toisin sanoen, onko yhtälöllä

$$n! = (m-1)m(m+1) = m(m^2 - 1)$$

muita ratkaisuja kuin  $(n, m) = (3, 2), (4, 3), (5, 5), (6, 9)$ ? Lisäksi hän kysyy, onko yleisellä tapauksella

$$n! = m(m^k - 1)$$

ratkaisuja.

Osoitetaan työhön [46, s. 34] perustuen, että  $abc$ -konjektuurin nojalla päästään käsiksi vielä yleisempään tapaukseen.

**Lause 4.12.1.** *Olkoot  $n, m, k \in \mathbb{N} \setminus \{1\}$ .  $abc$ -konjektuurin nojalla yhtälöllä*

$$n! = m(m^k \pm 1) \quad (4.28)$$

*on vain äärellinen määrä ratkaisuja.*

*Todistus.* Kirjoitetaan yhtälö (4.28) muodossa

$$m^k \pm 1 = \frac{n!}{m}, \quad (4.29)$$

josta nähdään  $\text{syt}(m^k, \frac{n!}{m}) = 1$ . Soveltamalla summaan (4.29) *Abc*-konjektuurin yleistä muotoa (Konjektuuri 3.2.2) sekä ylöspäin arvioimalla saadaan

$$\frac{n!}{m} \leq C(\varepsilon) \text{rad} \left( 1 \cdot m^k \cdot \frac{n!}{m} \right)^{1+\varepsilon} \leq C(\varepsilon) \text{rad} (n!)^{1+\varepsilon}. \quad (4.30)$$

Yhtälöstä (4.29) saadaan ylöspäin arvioimalla  $m^k \leq \frac{2n!}{m}$ , josta edelleen

$$m \leq (2n!)^{\frac{1}{k+1}}. \quad (4.31)$$

Soveltamalla epäyhtälöön (4.30) arvioita (4.31) ja  $\prod_{p \leq n} p < 4^n$  (Lemma 2.8.1) saadaan

$$\frac{n!}{(2n!)^{\frac{1}{k+1}}} \leq \frac{n!}{m} \leq C(\varepsilon) 4^{n(1+\varepsilon)}.$$

Kirjoittamalla epäyhtälön vasemmanpuoleinen termi muodossa

$$\frac{n!}{(2n!)^{\frac{1}{k+1}}} = \frac{(n!)^{1-\frac{1}{k+1}}}{2^{\frac{1}{k+1}}} = \frac{(n!)^{\frac{k}{k+1}}}{2^{\frac{1}{k+1}}}$$

ja käyttämällä arviota  $\frac{n^n}{e^n} \leq n!$  (Lemma 2.7.14) saadaan

$$\left(\frac{n}{e}\right)^{n \cdot \frac{k}{k+1}} \leq (n!)^{\frac{k}{k+1}} \leq C(\varepsilon) 2^{\frac{1}{k+1}} 4^{n(1+\varepsilon)},$$

josta edelleen

$$\left(\frac{n}{e}\right)^{\frac{k}{k+1}} \leq C(\varepsilon)^{\frac{1}{n}} 2^{\frac{1}{n(k+1)}} 4^{(1+\varepsilon)} \leq C(\varepsilon) 2^{\frac{1}{8}} 4^{(1+\varepsilon)},$$

mistä nähdään luku  $\varepsilon$  kiinnittämällä, että luku  $n$  on rajoitettu. Näin ollen myös luvut  $m$  ja  $k$  ovat rajoitettuja.  $\square$

### 4.13 Gandhin yhtälö $x^n + y^n = n!z^n$

Kirjassa [27, Problem D 2, s. 145] J. M. Gandhi esittää avoimen kysymyksen ratkaisuihin yhtälölle

$$x^n + y^n = n!z^n, \quad (4.32)$$

kun  $x, y, z \in \mathbb{Z}$  ja  $n \in \mathbb{N}_{\geq 3}$ . Sovelletaan tapaukseen *Abc*-konjektuuria [46, s. 33–34]:

**Lause 4.13.1.** *Olkoot  $x, y, z, n \in \mathbb{N}$ ,  $n \geq 4$ . *Abc*-konjektuurin nojalla yhtälöllä (4.32) on vain äärellinen määrä ratkaisuja.*

*Todistus.* Olkoot  $x, y, z, n$  yhtälön (4.32) toteuttavat luvut. Voidaan olettaa  $\text{sy}(x^n, y^n) = 1$ , jolloin myös  $\text{sy}(x^n, y^n, n!z^n) = 1$  (Huomautus 3.1.2). Soveltamalla *Abc*-konjektuuria *abc*-summaan (4.32) saadaan

$$n!z^n \leq C(\varepsilon) \text{rad}(x^n y^n n!z^n)^{1+\varepsilon} \leq C(\varepsilon)(xyz)^{1+\varepsilon} \text{rad}(n!)^{1+\varepsilon}.$$

Oletuksien  $x, y, z \in \mathbb{N}$  ja  $n \geq 4$  nojalla  $x, y, z \leq (n!z^n)^{\frac{1}{n}}$ , joten saadaan

$$n!z^n \leq C(\varepsilon)(n!z^n)^{\frac{3(1+\varepsilon)}{n}} \text{rad}(n!)^{1+\varepsilon},$$

josta jakamalla puolittain termillä  $(n!z^n)^{\frac{3(1+\varepsilon)}{n}}$  sekä tuloksia  $(\frac{n}{e})^n < n!$  (Lemma 2.7.14) ja  $\prod_{p \leq n} p < 4^n$  (Lemma 2.8.1) käyttämällä edelleen

$$\left(\frac{nz}{e}\right)^{n(1-\frac{3(1+\varepsilon)}{n})} < (n!z^n)^{1-\frac{3(1+\varepsilon)}{n}} \leq C(\varepsilon)4^{n(1+\varepsilon)}.$$

Ottamalla puolittain  $n$ :s juuri saadaan viimein

$$\left(\frac{nz}{e}\right)^{1-\frac{3(1+\varepsilon)}{n}} \leq C(\varepsilon)^{\frac{1}{n}} 4^{1+\varepsilon} \leq C(\varepsilon)4^{1+\varepsilon}.$$

Valitsemalla  $\varepsilon$  siten, että  $\frac{3(1+\varepsilon)}{n} < 1$  nähdään lukujen  $n$  ja  $z$  olevan rajoitettuja, jolloin yhtälöllä (4.32) on vain äärellinen määrä ratkaisuja.  $\square$

**Huomautus 4.13.2.** Tapauksissa  $n = 2$  ja  $n = 3$  yhtälöllä (4.32) on äärettömästi ratkaisuja [46, s. 33]. Tapauksessa  $n = 2$  tämä nähdään valitsemalla luvut  $x_k$  ja  $y_k$  siten, että

$$x_k + y_k\sqrt{2} = (1 + \sqrt{2})^k,$$

jolloin ne toteuttavat myös yhtälön  $x_k - y_k\sqrt{2} = (1 - \sqrt{2})^k$  (vrt. Lemma 2.2.11). Kertomalla yhtälöt puolittain saadaan yhtälö

$$x_k^2 - 2y_k^2 = (-1)^k,$$

josta nähdään, että parittomilla muuttujan  $k \in \mathbb{N}$  arvoilla luvut  $x_k$  ja  $y_k$  toteuttavat yhtälön (4.32) muodossa

$$1 + x_k^2 = 2y_k^2.$$

Tapauksessa  $n = 3$  saadaan äärettömästi ratkaisuja asettamalla

$$x_0 = 37, \quad y_0 = 17 \quad \text{ja} \quad z_0 = 21,$$

jolloin kaikilla  $k \in \mathbb{N}$  saadaan yhtälön (4.32) toteuttavat kolmikot

$$\begin{aligned} x_{k+1} &= x_k (x_k^3 + 2y_k^3), \\ y_{k+1} &= -y_k (2x_k^3 + y_k^3), \\ z_{k+1} &= z_k (x_k^3 - y_k^3). \end{aligned}$$

## 4.14 Voimakkaista luvuista

P. Erdős ja G. Szekers tutkivat lukuja  $n \in \mathbb{N}$ , joille ehdosta  $p \mid n$  seuraa  $p^2 \mid n$ , kun  $p$  on jokin alkuluku. S. Golomb nimesi tällaiset luvut *voimakkaiksi*. [27, Problem B16, s. 70]

**Määritelmä 4.14.1.** Luvun  $n \in \mathbb{N}$  sanotaan olevan *voimakas* (engl. powerful), jos

$$\text{rad}(n)^2 \mid n. \quad (4.33)$$

**Huomautus 4.14.2.** Voimakkaille luvuille  $n \in \mathbb{N}$  pätee  $\text{rad}(n) \leq n^{\frac{1}{2}}$ , sillä ehdosta (4.33) seuraa  $\text{rad}(n)^2 \leq n$ .

Ekvivalentisti voimakas luku voidaan määritellä täydellisen neliön ja kuution tulona.

**Lemma 4.14.3.** *Luku  $m \in \mathbb{N}$  on voimakas, jos ja vain jos  $m = a^2b^3$  joillekin  $a, b \in \mathbb{N}$ .*

*Todistus.* Ohitetaan triviaalin tapauksen tarkastelu ja oletetaan, että  $m, a, b > 1$ .

Jos  $m = a^2b^3$  joillekin  $a, b \in \mathbb{N}$ , niin luvun  $m$  alkutekijäesityksessä jokainen luvun  $m$  alkutekijä on korotettu ainakin potenssiin kaksi, jolloin luku  $m$  on voimakas.

Oletetaan sitten, että  $m \in \mathbb{N}$  on voimakas ja sillä on alkutekijäesitys  $m = \prod p_i^{a_i}$ ,  $a_i \geq 2$ . Määritellään luku  $c_i$  siten, että

$$c_i = \begin{cases} 3, & \text{jos } a_i \text{ on pariton} \\ 0, & \text{jos } a_i \text{ on parillinen} \end{cases}$$

ja asetetaan  $b_i = a_i - c_i$ , jolloin  $b_i \in \mathbb{N}$  on parillinen. Näin ollen voidaan kirjoittaa

$$m = \prod p_i^{a_i} = \prod p_i^{b_i} \prod p_i^{c_i} = \left( \prod p_i^{\frac{b_i}{2}} \right)^2 \left( \prod p_i^{\frac{c_i}{3}} \right)^3.$$

Väite seuraa. □

**Huomautus 4.14.4.** Jos  $n^2 \nmid b$  kaikilla  $n \in \mathbb{N}_{\geq 2}$ , esitys  $m = a^2b^3$  on yksikäsitteinen [52].

Tarkastellaan seuraavaksi voimakkaisiin lukuihin liittyviä konjektuureja P. Ribenboimin artikkelin [52] pohjalta. Mollin ja Walsh esittivät seuraavan konjektuurin tietämättä, että Erdős oli esittänyt sen jo aiemmin:

**Konjektuuri 4.14.5** (Erdős-Mollin-Walsh). *Ei ole olemassa kolmea peräkkäistä voimakasta lukua.*

*Abc*-konjektuurin avulla voidaan osoittaa asymptoottinen tapaus [46, s. 27–28]:

**Lause 4.14.6.** *Abc-konjektuurin nojalla on olemassa vain äärellinen määrä kolmen peräkkäisen voimakkaan luvun joukkoja.*

*Todistus.* Jos  $1 < a < b < c$  ovat kolme peräkkäistä voimakasta lukua, niin tällöin neliöstä

$$(a+1)^2 = a^2 + 2a + 1 = a(a+2) + 1$$

saadaan summa

$$b^2 = ac + 1. \quad (4.34)$$

Soveltamalla  $Abc$ -konjektuuria summaan (4.34), ja käyttämällä arviota  $\text{rad}(abc) \leq (abc)^{\frac{1}{2}}$  (Huomautus 4.14.2) saadaan

$$b^2 \leq C(\varepsilon) \text{rad}(abc)^{1+\varepsilon} \leq C(\varepsilon)(abc)^{\frac{1+\varepsilon}{2}} \leq C(\varepsilon)b^{\frac{3(1+\varepsilon)}{2}}, \quad (4.35)$$

josta edelleen

$$b^{\frac{1-3\varepsilon}{2}} \leq C(\varepsilon).$$

Näin ollen valitsemalla  $0 < \varepsilon < \frac{1}{3}$  nähdään, että luku  $b$  on rajoitettu, jolloin myös luvut  $a$  ja  $c$  ovat rajoitettuja.  $\square$

Seuraavat kaksi konjektuuria liittyvät osaltaan Fermat'n ja Mersennen lukuihin, joten palautetaan mieleen niiden määritelmät. Olkoon  $n \in \mathbb{Z}_{\geq 0}$  ja  $m \in \mathbb{N}$ . Lukuja  $F_n$  ja  $M_m$ ,

$$\begin{aligned} F_n &= 2^{2^n} + 1 \\ M_m &= 2^m - 1, \end{aligned}$$

kutsutaan *Fermat'n luvuiksi* ja *Mersennen luvuiksi*, vastaavasti [54, s. 81, 182].

**Konjektuuri 4.14.7.** Merkitään jokaisella  $k \in \mathbb{N}$   $n_k$ :lla sitä voimakasta lukua, joka on lähinnä lukua  $2^k$  ja  $n_k \neq 2^k$ . Tällöin

$$\lim_{k \rightarrow \infty} |2^k - n_k| = \infty.$$

Tilanteeseen voidaan soveltaa  $Abc$ -konjektuuria seuraavasti [46, s. 28]:

**Lause 4.14.8.**  $Abc$ -konjektuurin nojalla Konjektuuri 4.14.7 on voimassa.

*Todistus.* Lukua  $2^k$  lähinnä oleva voimakas luku on muotoa  $n_k = 2^s n'_k$ , missä  $s = 0$  tai  $1 < s < k$  ja  $n'_k$  on pariton voimakas luku. Soveltamalla sitten  $Abc$ -konjektuuria summaan

$$2^{k-s} - \frac{n_k}{2^s} = z$$

saadaan

$$\frac{n_k}{2^s} \leq 2^{k-s} \leq C(\varepsilon) \text{rad} \left( \frac{2^{k-s} n_k z}{2^s} \right)^{1+\varepsilon} \leq C_1(\varepsilon) \left( |z| \text{rad} \left( \frac{n_k}{2^s} \right) \right)^{1+\varepsilon},$$

missä  $C_1(\varepsilon) = 2^{1+\varepsilon} C(\varepsilon)$ . Kertomalla puolittain luvulla  $2^s$  ja arvioimalla ylöspäin (Huomautus 4.14.2) saadaan

$$n_k \leq C_1(\varepsilon) \left( 2^s |z| \text{rad} \left( \frac{n_k}{2^s} \right) \right)^{1+\varepsilon} \leq C_1(\varepsilon) |2^k - n_k|^{1+\varepsilon} n_k^{\frac{1+\varepsilon}{2}},$$

josta edelleen

$$n_k^{\frac{1-\varepsilon}{2}} \leq C(\varepsilon) |2^k - n_k|^{1+\varepsilon}.$$

Koska  $\lim_{k \rightarrow \infty} n_k = \infty$ , väite seuraa valitsemalla  $0 < \varepsilon < 1$ .  $\square$

$Abc$ -konjektuuri antaa varman vastauksen myös seuraavalle otaksumalle [46, s. 28–29].

**Konjektuuri 4.14.9.** *On olemassa äärettömästi Fermat'n ja Mersennen lukuja, jotka eivät ole voimakkaita.*

**Lause 4.14.10.** *Abc-konjektuurin nojalla konjektuuri 4.14.9 on voimassa.*

*Todistus.* Osoitetaan väite näyttämällä, että Abc-konjektuurin nojalla on olemassa äärellinen määrä voimakkaita Fermat'n ja Mersennen lukuja. Tarkastellaan Diophantoksen yhtälöä

$$2^k \pm 1 = z,$$

missä  $k \in \mathbb{N}$  ja  $z$  on voimakas. Nyt kuitenkin Lauseen 4.14.8 nojalla yhtälöllä on vain äärellinen määrä ratkaisuja. Koska Fermat'n ja Mersennen lukuja on äärettömästi, väite seuraa.  $\square$

Tarkastellaan vielä lopuksi erästä Erdösien konjektuuria [46, s. 29]. Sitä varten tarvitsemme seuraavan yleistyksen [27, Problem B16, s. 70].

**Määritelmä 4.14.11.** Olkoon  $k \in \mathbb{N}_{\geq 2}$ . Luku  $n \in \mathbb{N}$  on *k-voimakas* (engl. *k-ful*), jos

$$\text{rad}(n)^k \mid n.$$

**Huomautus 4.14.12.** *k-voimakkaille luvuille  $n \in \mathbb{N}$  pätee vastaavasti  $\text{rad}(n) \leq n^{\frac{1}{k}}$ .*

**Konjektuuri 4.14.13** (Erdös). *Yhtälöllä*

$$x + y = z$$

*on vain äärellinen määrä ratkaisuja 4-voimakkailta suhteellisilla alkuluvuilla  $x, y$  ja  $z$ .*

Osoitetaan jälleen Abc-konjektuurin voima [46, s. 29].

**Lause 4.14.14.** *Abc-konjektuurin nojalla Erdösien konjektuuri on voimassa.*

*Todistus.* Olkoot  $x, y, z \in \mathbb{N}$  4-voimakkaita lukuja siten, että  $\text{syt}(x, y, z) = 1$  ja  $x + y = z$ . Tällöin Abc-konjektuurin nojalla

$$z \leq C(\varepsilon) \text{rad}(xyz)^{1+\varepsilon} \leq C(\varepsilon)(xyz)^{\frac{1+\varepsilon}{4}} \leq C(\varepsilon)z^{\frac{3(1+\varepsilon)}{4}},$$

josta edelleen

$$z^{\frac{1-3\varepsilon}{4}} \leq C(\varepsilon).$$

Valitsemalla  $0 < \varepsilon < \frac{1}{3}$  nähdään, että  $z$  on rajoitettu.  $\square$

**Huomautus 4.14.15.** Mikäli Konjektuurissa 4.14.13 tarkastellaan 3-voimakkaita lukuja, saadaan äärettömästi ratkaisuja. Nitaj [45] osoitti tämän käyttämällä yhtälön  $x_n^3 + y_n^3 = az_n^3$  toteuttavia kolmikoita (vrt. Huomautus 4.13.2)

$$\begin{aligned} x_{n+1} &= x_n (x_n^3 + 2y_n^3), \\ y_{n+1} &= -y_n (2x_n^3 + y_n^3), \\ z_{n+1} &= z_n (x_n^3 - y_n^3), \end{aligned}$$

alkuarvoilla  $(a, x_0, y_0, z_0) = (6, 1\ 805\ 723, -2\ 237\ 723, -960\ 540)$ , jolloin

$$x_0 + y_0 = -2^7 \cdot 3^4 \cdot 5^3 \cdot 7^3 \cdot 2287^3.$$



## 4.15 Wieferichin alkuluvuista

Vuonna 1909 A. Wieferich todisti Fermat'n suureen lauseeseen liittyen seuraavaa [34]:

**Lause 4.15.1** (Wieferich). *Olkoot  $x, y, z \in \mathbb{Z} \setminus \{0\}$ . Jos parittomalle alkuluvulle  $p \nmid xyz$  on voimassa yhtälö*

$$x^p + y^p + z^p = 0,$$

*luku  $p$  toteuttaa kongruenssin*

$$2^{p-1} \equiv 1 \pmod{p^2}. \quad (4.36)$$

Kongruenssin toteuttavia alkulukuja alettiin kutsua esittäjänsä mukaisesti.

**Määritelmä 4.15.2.** Alkulukua  $p$  sanotaan *Wieferichin alkuluvuksi*, jos se toteuttaa kongruenssin (4.36).

Kongruenssi (4.36) ei toteutu suurimmalla osalla alkuluvuista. Vaikka Wieferichin alkulukuja uskotaan olevan äärettömästi, tällä hetkellä ainoat tunnetut lukua  $1, 25 \cdot 10^{15}$  pienemmät Wieferichin alkuluvut ovat 1093 ja 3511 [34]. Lang ja Trotter otaksuvatkin esiintymistiheydelle seuraavaa [37, s.175]:

**Konjektuuri 4.15.3** (Lang-Trotter). *Olkoon  $x \in \mathbb{R}$ ,  $x > e^e$ . Tällöin*

$$\left| \{p \text{ alkuluku} \mid p \leq x \text{ ja } 2^{p-1} \equiv 1 \pmod{p^2}\} \right| \leq C \log \log x$$

*jollekin vakiolle  $C > 0$ .*

Vuonna 1988 J. Silverman [60] osoitti *Abc*-konjektuurin nojalla olevan olemassa äärettömästi ns. ei-Wieferichin alkulukuja, jotka eivät toteuta kongruenssia (4.36). Osoitetaan tämä kirjaan [43, s. 187–188] perustuen. Tarvitaan seuraava aputulosta.

**Lemma 4.15.4.** *Olkoon  $p$  pariton alkuluku. Jos jollekin  $n \in \mathbb{N}$  pätee*

$$2^n \equiv 1 \pmod{p} \quad \text{mutta} \quad 2^n \not\equiv 1 \pmod{p^2},$$

*niin luku  $p$  ei ole Wieferichin alkuluku.*

*Todistus.* Koska  $p$  on pariton,  $\text{syt}(p, 2) = 1$ . Olkoon  $d$  luvun 2 kertaluku modulo  $p$ , ts.  $d = \text{ord}_p 2$ . Tällöin  $d \mid n$  Lemman 2.1.34 nojalla ja yhtälöstä  $2^n \equiv 1 \pmod{p^2}$  seuraa

$$2^d \not\equiv 1 \pmod{p^2}.$$

Kertaluvun määritelmän nojalla  $2^d = 1 + kp$ , missä  $k \in \mathbb{Z}$  ja  $\text{syt}(k, p) = 1$ . Koska Eulerin lauseen (Lause 2.1.32) nojalla  $2^{p-1} \equiv 1 \pmod{p}$  ja Seurauksen 2.1.35 nojalla  $d \mid p - 1$ , voidaan kirjoittaa  $p - 1 = de$  jollekin kokonaisluvulle  $1 \leq e \leq p - 1$ . Tällöin  $\text{syt}(ek, p) = 1$  ja

$$2^{p-1} = (2^d)^e = (1 + kp)^e \equiv 1 + ekp \not\equiv 1 \pmod{p^2},$$

missä  $(1 + kp)^e \equiv 1 + ekp$  saadaan soveltamalla binomilauseetta termiin  $(1 + kp)^e$  ja tarkastelemalla tulosta modulo  $p^2$ . Näin ollen  $p$  ei ole Wieferichin alkuluku.  $\square$

Seuraavassa todistuksessa käytetään hyväksi voimakkaita lukuja (Määritelmä 4.14.1).

**Lause 4.15.5.** *Abc-konjektuurin nojalla on olemassa äärettömästi alkulukuja, jotka eivät toteuta kongruenssia (4.36).*

*Todistus.* Merkitään ei-Wieferichin alkulukujen joukkoa  $NW$ :lla, toisin sanoen

$$NW = \{p \text{ alkuluku} \mid 2^{p-1} \not\equiv 1 \pmod{p^2}\}.$$

Jokaisella  $n \in \mathbb{N}$  voidaan kirjoittaa

$$2^n - 1 = v_n u_n, \tag{4.37}$$

missä  $v_n$  on suurin voimakas luku, joka jakaa luvun  $2^n - 1$ , ja  $u_n$  on neliövapaa luku, ts.  $k^2 \nmid u_n$  kaikilla  $k \in \mathbb{N} \setminus \{1\}$ , siten, että  $\text{syt}(v_n, u_n) = 1$ .

Mikäli nyt  $p \mid u_n$ , niin tällöin  $p \nmid v_n$  ja edelleen

$$2^n \equiv 1 \pmod{p} \quad \text{mutta} \quad 2^n \not\equiv 1 \pmod{p^2}.$$

Lemman 4.15.4 nojalla siten  $p \in NW$  eli  $u_n$  on jaollinen vain ei-Wieferichin alkuluvuilla.

Oletetaan vastoin väitettä, että joukko  $NW$  on äärellinen. Näin ollen on olemassa vain äärellisen monta neliövapaata kokonaislukua  $u_n$ , joiden alkutekijät kuuluvat joukkoon  $NW$ . Merkitään  $U$ :lla suurinta tällaista lukua  $u_n$ . Koska

$$\lim_{n \rightarrow \infty} 2^n - 1 = \infty,$$

joukko  $\{v_n : n = 1, 2, 3, \dots\}$  puolestaan on tällöin ääretön ja rajoittamaton.

Soveltamalla nyt *Abc*-konjektuuria summaan  $(2^n - 1) + 1 = 2^n$  saadaan

$$2^n \leq C(\varepsilon) \text{rad}(2^n(2^n - 1))^{1+\varepsilon} = C(\varepsilon) \text{rad}(2(2^n - 1))^{1+\varepsilon},$$

josta edelleen yhtälön (4.37) nojalla sekä arvioimalla

$$v_n \leq C(\varepsilon) \text{rad}(2v_n u_n)^{1+\varepsilon} \leq C(\varepsilon) \text{rad}(2u_n)^{1+\varepsilon} \text{rad}(v_n)^{1+\varepsilon}.$$

Käyttämällä arvioita  $U = \max u_n$  ja  $\text{rad}(v_n) \leq v_n^{\frac{1}{2}}$  (Huomautus 4.14.2) saadaan

$$v_n \leq C(\varepsilon)(2U)^{1+\varepsilon} v_n^{\frac{1+\varepsilon}{2}},$$

josta lopulta

$$v_n^{\frac{1-\varepsilon}{2}} \leq C_1(\varepsilon),$$

missä  $C_1(\varepsilon) = C(\varepsilon)(2U)^{1+\varepsilon}$ . Valitsemalla  $0 < \varepsilon < 1$  nähdään, että tällöin myös luvut  $v_n$  ovat rajoitettuja, mikä on ristiriita. Näin ollen joukko  $NW$  on ääretön.  $\square$

Silverman todisti itse asiassa vielä edellistä voimakkaamman tuloksen [60]:

**Lause 4.15.6.** *Abc-konjektuurin nojalla jokaista luonnollista lukua  $a \in \mathbb{N} \setminus \{1\}$  kohden on olemassa äärettömästi alkulukuja  $p$ , jotka toteuttavat ehdon*

$$a^{p-1} \not\equiv 1 \pmod{p^2}$$

*ja joiden lukumäärälle pätee kaikilla  $x > x_0$*

$$|\{p \text{ alkuluku} \mid p \leq x \text{ ja } a^{p-1} \not\equiv 1 \pmod{p^2}\}| > C(a) \log x,$$

*missä  $C(a) > 0$  on vakio.*

## 4.16 Edgarin ja Shorey-Tijdemanin probleema

Kirjassa [27, Problem D10, s. 157] H. Edgar kysyy onko yhtälöllä

$$1 + q + q^2 + \cdots + q^{x-1} = p^y$$

ratkaisun  $(q, x, p, y) = (3, 5, 11, 2)$  lisäksi muita ratkaisuja parittomilla alkuluvuilla  $p$  ja  $q$  ja luonnollisilla luvuilla  $x$  ja  $y$ , kun  $x \geq 5$  ja  $y \geq 2$ . Shorey ja Tijdeman esittivät yleisen tapauksen geometrisen sarjan summan avulla ja asettivat sille seuraavan konjektuurin [58, s. 202-203].

**Konjektuuri 4.16.1.** *Olkoot  $n, x, y \in \mathbb{N}_{\geq 2}$  ja  $m \in \mathbb{N}_{\geq 3}$ . Tällöin yhtälöllä*

$$\frac{x^m - 1}{x - 1} = y^n \tag{4.38}$$

*on vain äärellinen määrä ratkaisuja.*

**Huomautus 4.16.2.** Yhtälölle (4.38) tunnetaan Edgarin ratkaisun lisäksi ratkaisut  $(x, m, y, n) = (7, 4, 20, 2), (18, 3, 7, 3)$ . Tietyillä oletuksilla lukujen  $x, m$  ja  $y$  suhteen voidaan myös osoittaa, että yhtälöllä (4.38) on vain äärellisesti ratkaisuja. [58, s. 203]

Nitaj [46, s. 35] yleisti Konjektuurin 4.16.1 tapauksen ja osoitti, että *Abc*-konjektuurin mukaan saadaan rajoitettu määrä ratkaisuja.

**Lause 4.16.3.** *Olkoot  $x, y, z, n, m \in \mathbb{N}$  siten, että  $x > y$ ,  $\text{sy}(x, y) = 1$ ,  $m > 1$ ,  $n > 3$  ja  $\frac{3}{n} + \frac{1}{m} < 1$ . Tällöin *Abc*-konjektuurin nojalla yhtälöllä*

$$x^{n-1} + x^{n-2}y + \cdots + xy^{n-2} + y^{n-1} = \frac{x^n - y^n}{x - y} = az^m, \tag{4.39}$$

*on vain äärellinen määrä ratkaisuja.*

*Todistus.* Yhtälöketjusta (4.39) saadaan puolittain termillä  $x - y$  kertomalla summa

$$y^n + az^m(x - y) = x^n. \tag{4.40}$$

Ehdosta  $\text{sy}(x, y) = \text{sy}(x^n, y^n) = 1$  saadaan  $\text{sy}(x^n, y^n, az^m(x - y)) = 1$  Lemman 2.1.7 nojalla. Arvioita  $x - y < x$  ja  $z \leq x^{\frac{n}{m}}$  sekä *Abc*-konjektuuria summaan (4.40) soveltamalla saadaan

$$x^n \leq C(\varepsilon) \text{rad}(y^n az^m(x - y)x^n)^{1+\varepsilon} \leq C(\varepsilon)(ayz(x - y)x)^{1+\varepsilon} \leq C_1(\varepsilon, a)x^{(3+\frac{n}{m})(1+\varepsilon)},$$

missä  $C_1(\varepsilon, a) = C(\varepsilon)a^{1+\varepsilon}$ . Edelleen

$$(x^n)^{1-(\frac{3}{n}+\frac{1}{m})(1+\varepsilon)} \leq C_1(\varepsilon, a).$$

Valitsemalla luku  $\varepsilon > 0$  siten, että  $(\frac{3}{n} + \frac{1}{m})(1 + \varepsilon) < 1$  nähdään, että luvut  $x, n$  ja siten myös luvut  $y, z$  ja  $m$  ovat rajoitettuja.  $\square$

## 4.17 Goormaghtighin ja Batemanin ongelma

Goormaghtigh esitti ongelman olemassaolosta luvuille, joilla on samoista numeroista koostuvat esitykset eri lukujärjestelmissä [58, s. 203]. Toisin sanoen, onko olemassa alkulukuja, jotka voidaan esittää kahdella eri tavalla muodossa

$$\frac{x^m - 1}{x - 1} = \frac{y^n - 1}{y - 1}, \quad (4.41)$$

missä  $x, m, y, n \in \mathbb{N}$  siten, että  $m > n > 2$  ja  $y > x > 1$ . Ongelmaan tunnetaan ainakin ratkaisut

$$31 = \frac{2^5 - 1}{2 - 1} = \frac{5^3 - 1}{5 - 1} \quad \text{ja} \quad 8191 = \frac{2^{13} - 1}{2 - 1} = \frac{90^3 - 1}{90 - 1},$$

joista ensimmäinen toteuttaa myös ns. Batemanin ongelman, jossa  $x$  ja  $y$  ovat alkulukuja ja  $m, n \geq 3$ . Batemanin ongelmalle ei ole muita positiivisia ratkaisuja suuruudeltaan korkeintaan  $10^{10}$  olevien alkulukujen joukossa. [27, Problem B25, s. 81]

*Abc*-konjektuurin avulla voidaan osoittaa ratkaisujen lukumäärän äärellisyys [46, s. 36].

**Lause 4.17.1.** *Abc-konjektuurin nojalla yhtälöllä (4.41) on olemassa vain äärellinen määrä ratkaisuja luonnollisilla luvuilla  $m > n > 3$  ja  $y > x > 1$ .*

*Todistus.* Nimittäjillä kertomalla ja termejä siirtämällä saadaan yhtälö (4.41) muotoon

$$x^m(y - 1) = y^n(x - 1) + (y - x).$$

Merkitään  $d = \text{syt}(x^m(y - 1), y^n(x - 1))$ . Soveltamalla summaan  $\frac{y^n(x-1)}{d} + \frac{y-x}{d} = \frac{x^m(y-1)}{d}$  *Abc*-konjektuuria saadaan

$$\frac{x^m(y - 1)}{d} \leq C(\varepsilon) \text{rad} \left( \frac{y^n(x - 1)(y - x)x^m(y - 1)}{d^3} \right)^{1+\varepsilon},$$

josta edelleen ylöspäin arvioimalla saadaan

$$\begin{aligned} x^m(y - 1) &\leq C_1(\varepsilon) \left( (y - x)(y - 1) \text{rad} \left( \frac{x^m y^n (x - 1)}{d} \right) \right)^{1+\varepsilon} \\ &\leq C_1(\varepsilon) ((y - x)(y - 1)xy(x - 1))^{1+\varepsilon} \\ &\leq C_1(\varepsilon) (x^2 y^2 (y - 1))^{1+\varepsilon}. \end{aligned}$$

missä  $C_1(\varepsilon) = C(\varepsilon)d$ . Käytetään epäyhtälön molempiin puoliin arviota  $(y - 1) \leq y$ , jolloin epäyhtälön suunta säilyy ja saadaan

$$x^m y \leq C_1(\varepsilon) (x^2 y^3)^{1+\varepsilon}.$$

Yhtälöä (4.41) soveltamalla nähdään lukujen  $x^{m-1}$  ja  $y^{n-1}$  olevan karkeasti samaa suuruusluokkaa ( $x^{m-1} \approx y^{n-1}$ ), joten saadaan arvio  $x^{\frac{m-1}{n-1}} \approx y$ . Soveltamalla tätä edellä olevaan epäyhtälöön ja huomioimalla siitä aiheutuva epätarkkuus vakiossa  $C_2(\varepsilon)$  saadaan

$$x^{m+\frac{m-1}{n-1}} \leq C_2(\varepsilon) \left( x^{2+3\frac{(m-1)}{n-1}} \right)^{1+\varepsilon},$$

josta viimein

$$x^{\frac{mn-1-(2n+3m-5)(1+\varepsilon)}{n-1}} \leq C_2(\varepsilon).$$

Valitaan nyt  $\varepsilon$  siten, että  $mn - 1 > (2n + 3m - 5)(1 + \varepsilon)$  toteutuu arvoilla  $m > n > 3$ . Näin ollen nähdään, että luku  $x$  on rajoitettu, ja siten myös luvut  $y, m, n$  ovat rajoitettuja.  $\square$

## 4.18 Croftin ongelma

Kirjassa [27, Problem F23, s. 261] Croft esittää avoimen kysymyksen kuinka pieni erotus  $|n! - 2^m|$  voi olla suhteessa lukuun  $2^m$ . *Abc*-konjektuurilla saadaan seuraava arvio [46, s. 39]:

**Lause 4.18.1.** *Abc-konjektuurin nojalla jokaista  $\varepsilon > 0$  kohti on olemassa vakio  $C(\varepsilon) > 0$  siten, että*

$$n \leq C(\varepsilon) \operatorname{rad}(n! - 2^m)^{\frac{1+\varepsilon}{n}}$$

on voimassa kaikilla  $m, n \in \mathbb{N}$ ,  $(m, n) \neq (0, 0), (1, 0), (2, 1)$ .

*Todistus.* Kirjoitetaan  $n!$  muodossa  $n! = 2^s j$ , missä  $j$  on pariton ja  $s < n$ . Jaetaan tarkastelu kahteen osaan riippuen luvun  $s$  suuruudesta.

Jos  $s \geq m$ , niin soveltamalla *Abc*-konjektuuria summaan

$$\frac{n!}{2^m} - 1 = k \tag{4.42}$$

saadaan

$$\frac{n!}{2^n} \leq \frac{n!}{2^m} \leq C(\varepsilon) \operatorname{rad}\left(\frac{n!k}{2^m}\right)^{1+\varepsilon} \leq C(\varepsilon) \operatorname{rad}(n!2^m k)^{1+\varepsilon},$$

jolloin tuloksia  $\left(\frac{n}{e}\right)^n < n!$  (Lemma 2.7.14) ja  $\prod_{p \leq n} p < 4^n$  (Lemma 2.8.1) käyttämällä saadaan

$$\left(\frac{n}{2e}\right)^n \leq C(\varepsilon) 4^{n(1+\varepsilon)} \operatorname{rad}(2^m k)^{1+\varepsilon}.$$

Tästä edelleen puolittain  $n$ :s juuri ottamalla ja yhtälöä (4.42) käyttämällä

$$n \leq 2eC(\varepsilon)^{\frac{1}{n}} 4^{1+\varepsilon} \operatorname{rad}(2^m k)^{\frac{1+\varepsilon}{n}} \leq C_1(\varepsilon) \operatorname{rad}(n! - 2^m)^{\frac{1+\varepsilon}{n}},$$

missä  $C_1(\varepsilon) = 2eC(\varepsilon)4^{1+\varepsilon}$ .

Jos taas  $s < m$ , niin soveltamalla *Abc*-konjektuuria summaan

$$\frac{n!}{2^s} - 2^{m-s} = k$$

saadaan

$$\frac{n!}{2^n} \leq \frac{n!}{2^s} \leq C(\varepsilon) \operatorname{rad}\left(\frac{n!}{2^s} 2^{m-s} k\right)^{1+\varepsilon} \leq C(\varepsilon) \operatorname{rad}(n! 2^{m-s} k)^{1+\varepsilon} = C(\varepsilon) \operatorname{rad}(n! 2^s k)^{1+\varepsilon}.$$

Tämän jälkeen päättely on vastaava kuin edellä. □

Nitaj esittää Lauseen 4.18.1 sekä numeeristen laskelmien pohjalta seuraavan voimakkaamman tuloksen [46, s. 39]

**Konjektuuri 4.18.2.** *On olemassa vakio  $C > 0$  siten, että epäyhtälö*

$$n \leq C \operatorname{rad}(n! - 2^m)^{\frac{1}{n}}$$

on voimassa kaikilla  $m, n \in \mathbb{N}$ ,  $(m, n) \neq (0, 0), (1, 0), (2, 1)$ .

## 4.19 Muita seurauksia

Täydellisyyden vuoksi esitetään vielä lopuksi ilman todistuksia kolme *Abc*-konjektuurin seurausta. Vaikka jo todistettujen Faltingsin ja Rothin lauseen tarkastelu voi tuntua turhalta, *Abc*-konjektuuri tarjoaa kuitenkin yksinkertaisemman ja helpommin seurattavan päätteilyketjun, jossa näkyy paremmin yhteydet eri teorioiden välillä. Lisäksi *Abc*-konjektuurin avulla voidaan osoittaa alkuperäisiä lauseita voimakkaammat tulokset. [21]

Tarvitaan seuraavaa määritelmää [28, s. 203]:

**Määritelmä 4.19.1.** Lukua  $x$  kutsutaan *algebralliseksi luvuksi*, mikäli se toteuttaa jonkun muotoa

$$a_0x^n + a_1x^{n-1} + \cdots + a_n = 0$$

olevan yhtälön, missä  $a_i \in \mathbb{Z}$  ja  $a_j \neq 0$  jollekin  $j \in \{1, \dots, n\}$ .

**Huomautus 4.19.2.** Kahden muuttujan polynomiyhtälön nollakohtien ratkaisujoukko muodostaa *algebrallisen käyrän*.

Vuonna 1922 L. J. Mordell otaksui seuraavan tuloksen, jonka G. Faltings myöhemmin vuonna 1983 todisti [21, s. 56]:

**Lause 4.19.3** (Faltings). *Olkoon  $C$  algebrallinen käyrä, jonka genus  $g \geq 2$ , kerroinkunnassa  $\mathbb{Q}$ . Tällöin käyrällä  $C$  on vain äärellinen määrä rationaalipisteitä.*

Tuloksen osoitti seuraavan myös *Abc*-konjektuurista N. Elkies vuonna 1991 [21]. Todistuksessaan hän käytti Belyin teoriaa sekä yleisissä lukukunnissa määriteltyjen käyrien rationaalipisteiden korkeuteen liittyviä ominaisuuksia [46, s. 17].

Vuonna 1955 K. J. Roth osoitti seuraavan lauseen, joka liittyy algebrallisten lukujen approksimointiin rationaaliluvuilla [21, s. 55]:

**Lause 4.19.4** (Roth). *Olkoon  $\alpha$  algebrallinen luku kerroinkunnassa  $\mathbb{Q}$  ja olkoon  $\varepsilon > 0$ . Tällöin epäyhtälö*

$$\left| \alpha - \frac{s}{t} \right| < \frac{1}{t^{2+\varepsilon}}$$

*toteutuu vain äärellisen monella rationaaliluvulla  $\frac{s}{t}$ ,  $t > 0$ .*

Vaikka Lause 4.19.4 on luonteeltaan kvantitatiivinen, voidaan se kvalitatiivisesti tulkita siten, että algebrallista lukua ei voida kovin hyvin approksimoida äärettömän monella rationaaliluvulla [10, s. 152]. E. Bombieri osoitti tuloksen seuraavan *Abc*-konjektuurista vuonna 1994 [21, s. 45].

Vielä lopuksi mainittakoon A. Granvillen ja H. Starkin [25] vuonna 2000 osoittama analyttiseen lukuteoriaan liittyvä tulos. Sitä ennen tarvitaan vielä muutama selkeyttävä määritelmä [1, s. 224, 249].

**Määritelmä 4.19.5.** *Dirichlet'n  $L$ -sarjaksi* kutsutaan muotoa

$$L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$$

olevaa funktiota, missä  $\chi$  on Dirichlet'n karakteri ja  $s$  on kompleksinen muuttuja, jonka reaaliosa on suurempi kuin yksi. Kun funktio jatketaan analyttisesti meromorfiniseksi funktioksi koko kompleksitasossa, siitä käytetään nimitystä *Dirichlet'n  $L$ -funktio* ja merkintää  $L(s, \chi)$ .

Määritelmässä oleva Dirichlet'n karakteri määritellään seuraavasti [1, s. 138–139]:

**Määritelmä 4.19.6.** Olkoot  $k, m, n \in \mathbb{N}$ . Funktiota  $\chi : \mathbb{N} \rightarrow \mathbb{C}$  kutsutaan *Dirichlet'n karakteriksi modulo  $n$* , mikäli se toteuttaa seuraavat ehdot:

- (i) Jos  $\text{syt}(n, k) > 1$ , niin  $\chi(k) = 0$ ;
- (ii) Jos  $\text{syt}(n, k) = 1$ , niin  $\chi(k) \neq 0$ ;
- (iii) Kaikilla  $k$  ja  $m$  pätee  $\chi(km) = \chi(k)\chi(m)$ ;
- (iv) Kaikilla  $k$  pätee  $\chi(k+n) = \chi(k)$ .

Tarkastellaan hieman yksinkertaistaen sellaisia lukukuntia, joissa ns. perusdiskriminantti on  $-d < 0$ , ks. tarkemmin [25]. Tämä tarkoittaa, että  $-d \in \mathbb{Z}$  ei ole jaollinen millään parittoman alkuluvun neliöllä ja sille pätee

$$-d \equiv 1 \pmod{4} \quad \text{tai} \quad -d \equiv 8 \pmod{16} \quad \text{tai} \quad -d \equiv 12 \pmod{16}.$$

Määritetään Dirichlet'n karakteri  $\chi_d$  asettamalla

$$\chi_d = \left( \frac{-d}{\cdot} \right),$$

jolloin karakterin argumentti määrää karakterin moduloluvun sekä Jacobin symbolin  $\left( \frac{-d}{\cdot} \right)$  arvon. Karakteriin  $\chi_d$  liittyvän Dirichlet'n  $L$ -funktion  $L(s, \chi_d)$  avulla voidaan määrittellä ns. Siegelin nollakohta.

**Määritelmä 4.19.7.** Yhtälön

$$L(s, \chi_d) = \sum_{n=1}^{\infty} \frac{\chi_d(n)}{n^s} = 0$$

reaalista ratkaisua välillä  $1 - \frac{c}{\log d} < s \leq 1$ , missä  $c > 0$  on pieni vakio, kutsutaan "*Siegelin nollakohtaksi*".

Todetaan viimein itse tulos:

**Lause 4.19.8.** *Algebrallisille lukukunnille muotoillun Abc-konjektuurin nojalla Dirichlet'n karakteriin  $\left( \frac{-d}{\cdot} \right)$ ,  $-d < 0$ , liittyvällä  $L$ -funktiolla ei ole "Siegelin nollakohtia".*

## 5 Abc-konjektuurin yleistyksiä

Tässä luvussa tarkastellaan muutamia *Abc*-konjektuurin yleistyksiä, kuten *Abc*-konjektuurin kongruenssiversiota,  $n$ -konjektuuria ja *Abc*-konjektuurin polynomiversiota, Mason-Stotherin lausetta. Lopuksi mainitaan vielä ilman perusteluita meromorfisille funktioille sovelletuista analogioista. Täydellisempi lista yleistyksistä löytyy mm. internetsivuilta [48].

### 5.1 Abc-konjektuurin kongruenssiversio

*Abc*-konjektuurin kongruenssimuotoinen versio määritellään seuraavasti [43, s. 191]:

**Konjektuuri 5.1.1** (*Abc*, kongruenssiversio). *Olkoon  $m \in \mathbb{N} \setminus \{1\}$ . Kaikilla  $\varepsilon > 0$  on olemassa luku  $C(m, \varepsilon) > 0$  siten, että kaikilla  $a, b, c \in \mathbb{Z} \setminus \{0\}$ ,  $\text{syt}(a, b, c) = 1$ , joille*

$$abc \equiv 0 \pmod{m} \quad \text{ja} \quad a + b = c,$$

*on voimassa epäyhtälö*

$$\max(|a|, |b|, |c|) \leq C(m, \varepsilon) \text{rad}(abc)^{1+\varepsilon}.$$

Konjektuurin 5.1.1 väittäjä on kongruenssiehdosta johtuen normaalia *Abc*-konjektuuria heikompi. Kuitenkin voidaan osoittaa, että mikäli Konjektuuri 5.1.1 on voimassa jollakin luvulla  $m \in \mathbb{N} \setminus \{1\}$ , niin tällöin myös varsinainen *Abc*-konjektuuri on voimassa. Ensimmäisenä tämän todisti J. Ellenberg vuonna 2000 [17].

Osoitetaan Ellenbergin tulos kirjan [43, s. 191–195] esitykseen perustuen. Aloitetaan tarkastelu seuraavalla alkeellisellä huomiolla.

**Lemma 5.1.2.** *Olkoon  $(a, b, c) \in \mathbb{N}^3$  abc-summa siten, että  $a < b < c$ .*

(i) *Jos  $c$  on pariton, niin  $b - a$  on pariton;*

(ii) *Jos  $c$  on parillinen, niin  $a$  sekä  $b$  ovat parittomia ja  $b - a$  on parillinen. Lisäksi*

$$4 \mid c \quad \text{tai} \quad 4 \mid (b - a).$$

*Todistus.* Koska  $c = a + b$ , riittää tarkastella lukujen  $a$  ja  $b$  parillisuutta tai parittomuutta. Olkoot  $m, k \in \mathbb{N}$  siten, että  $m < k$ .

Jos luku  $c$  on pariton, niin silloin luvut  $a$  ja  $b$  ovat muotoa  $a = 2m$  ja  $b = 2k + 1$  tai  $a = 2m + 1$  ja  $b = 2k$ . Tällöin molemmissa tapauksissa  $c = 2(m + k) + 1$ . Ensimmäisessä tapauksessa  $b - a = 2(k - m) + 1$  ja toisessa  $b - a = 2(k - m - 1) + 1$ , joten (i) on voimassa.

Jos luku  $c$  on parillinen, niin silloin  $a = 2m + 1$  ja  $b = 2k + 1$ . Tapaus  $a = 2m$  ja  $b = 2k$  johtaa ristiriitaan  $\text{syt}(a, b, c) > 1$ . Nyt  $c = 2(m + k + 1)$  ja  $b - a = 2(k - m)$  eli (ii):n ensimmäinen osa on tämän nojalla voimassa.

Olkoot  $k', m' \in \mathbb{N}$  siten, että  $k' < m'$ . Taulukoidaan kohdan (ii) mahdollisuudet.

$m$	$k$	$c = 2(m + k + 1)$	$b - a = 2(k - m)$
$2m'$	$2k'$	$4(k' + m') + 2$	$4(k' - m')$
$2m' + 1$	$2k' + 1$	$4(k' + m' + 1) + 2$	$4(k' - m')$
$2m' + 1$	$2k'$	$4(k' + m' + 1)$	$4(k' - m' - 1) + 2$
$2m'$	$2k' + 1$	$4(k' + m' + 1)$	$4(k' - m') + 2$

Taulukosta nähdään, että aina joko  $4 \mid c$  tai  $4 \mid (b - a)$ . □



**Huomautus 5.1.3.** Lemman 5.1.2 nojalla nähdään eksplisiittisesti, että kaikilla  $abc$ -summilla  $abc \equiv 0 \pmod{2}$ , sillä ainakin yksi luvuista  $a, b, c$  on parillinen. Näin ollen Konjektuuri 5.1.1 arvolla  $m = 2$  on sama kuin alkuperäinen  $Abc$ -konjektuuri.

Huomautuksen 5.1.3 nojalla riittää siis tarkastella Konjektuuria 5.1.1 arvoilla  $m \geq 3$ . Osoitetaan seuraavaksi, että vanhojen  $abc$ -kolmikoiden avulla voidaan muodostaa uusia  $abc$ -kolmikoita.

**Lemma 5.1.4.** *Olkoon  $n \in \mathbb{N}$  ja olkoon  $(a, b, c) \in \mathbb{N}^3$   $abc$ -kolmikko siten, että  $a < b < c$ . Jos luku  $c$  on pariton, asetetaan*

$$A_n = (b - a)^n, \quad B_n = c^n - (b - a)^n, \quad C_n = c^n.$$

*Jos luku  $c$  on parillinen, asetetaan*

$$A_n = \left(\frac{b - a}{2}\right)^n, \quad B_n = \left(\frac{c}{2}\right)^n - \left(\frac{b - a}{2}\right)^n, \quad C_n = \left(\frac{c}{2}\right)^n.$$

*Tällöin  $(A_n, B_n, C_n)$  muodostaa  $abc$ -kolmikon.*

*Todistus.* Selvästi  $A_n + B_n = C_n$  molemmissa tapauksissa. Oletuksen nojalla  $0 < b - a < c$ , jolloin Lemman 5.1.2 nojalla luvut  $A_n, B_n$  ja  $C_n$  ovat molemmissa tapauksissa luonnollisia lukuja kaikilla  $n \in \mathbb{N}$ . Edelleen nähdään, että  $A_n < C_n$ ,  $B_n < C_n$  ja  $A_n \neq B_n$ , joten luvut  $A_n, B_n, C_n$  ovat eri lukuja ja tarvittaessa uudelleen määrittelemällä saadaan  $A_n < B_n < C_n$ . Riittää siis osoittaa, että  $\text{syt}(A_n, B_n, C_n) = 1$ .

Olkoon  $c$  ensin pariton. Esimerkin 2.1.6 nojalla  $\text{sy}(c, b - a) \leq 2$ . Koska luvut  $c$  ja  $b - a$  ovat parittomia (Lemma 5.1.2), täytyy olla  $\text{sy}(c, b - a) = 1$ . Lemmojen 2.1.11 ja 2.1.7 nojalla edelleen

$$1 = \text{sy}(c^n, (b - a)^n) = \text{sy}(c^n - (b - a)^n, (b - a)^n) = \text{sy}(c^n - (b - a)^n, c^n).$$

Olkoon sitten luku  $c$  parillinen. Tällöin myös  $b - a$  on parillinen (Lemma 5.1.2), joten Esimerkin 2.1.6 nojalla  $\text{sy}(c, b - a) = 2$ . Lemman 2.1.10 nojalla  $\text{sy}\left(\frac{c}{2}, \frac{b - a}{2}\right) = 1$ , jolloin päättely on analoginen yllä olevan kanssa.  $\square$

Lemman 5.1.4 luvuilla  $A_n, B_n, C_n$  on voimassa seuraava kongruenssi:

**Lemma 5.1.5.** *Olkoot  $m \geq 3$  ja  $n = \phi(m)$ . Lemman 5.1.4 kolmikolle  $(A_n, B_n, C_n)$  pätee tällöin*

$$A_n B_n C_n \equiv 0 \pmod{m}. \tag{5.1}$$

*Todistus.* Riittää näyttää, että jos  $p$  on alkuluku ja  $p^r \mid m$  jollekin  $r \in \mathbb{N}$ , niin

$$A_n B_n C_n \equiv 0 \pmod{p^r}.$$

Tällöin väite (5.1) seuraa luvun  $m$  kanonisen esityksen ja Lauseen 2.1.24 nojalla. Todetaan kuitenkin aluksi, että jos alkuluvulle  $p$  pätee  $p^r \mid m$  jollekin  $r \in \mathbb{N}$ , niin  $(p - 1)p^{r-1} \mid n$  (Lemma 2.1.29 ja Lause 2.1.30) ja siten

$$r \leq 2^{r-1} \leq (p - 1)p^{r-1} \leq n.$$

Olkoon  $p$  ensin pariton alkuluku. Jos  $p \mid c$ , niin  $p^n \mid c^n$  ja  $p^n \mid C_n$ . Koska  $r \leq n$ , saadaan  $C_n \equiv 0 \pmod{p^r}$ . Vastaavasti jos  $p \mid (b - a)$ , niin  $A_n \equiv 0 \pmod{p^r}$ . Jos taas  $p \nmid c$  ja  $p \nmid (b - a)$ , niin Lemman 2.1.29 sekä Eulerin lauseen (Lause 2.1.32) nojalla

$$\begin{aligned} c^{(p-1)p^{r-1}} &\equiv 1 \pmod{p^r} \\ (b-a)^{(p-1)p^{r-1}} &\equiv 1 \pmod{p^r}. \end{aligned}$$

Koska  $(p-1)p^{r-1} \mid n$ , saadaan

$$c^n \equiv (b-a)^n \equiv 1 \pmod{p^r},$$

jolloin siis  $B_n \equiv 0 \pmod{p^r}$ . Näin ollen (5.1) pätee kaikilla parittomilla alkuluvuilla.

Olkoon sitten  $p = 2$ . Jos  $2^r \mid m$ , niin  $2^{r-1} \mid n$  ja  $r \leq n$ . Tarkastellaan erikseen tapaukset, missä luku  $c$  on parillinen ja pariton.

Jos  $2 \mid c$ , niin  $2 \mid (b-a)$  ja täsmälleen toinen luvuista  $c$  ja  $b-a$  on jaollinen luvulla 4 (Lemma 5.1.2). Näin ollen joko  $c^n$  tai  $(b-a)^n$  on jaollinen luvulla  $4^n$  eli joko  $2^n \mid C_n$  tai  $2^n \mid A_n$ . Mutta koska  $2^r \mid 2^n$ , kongruenssi (5.1) on voimassa.

Jos  $2 \nmid c$ , niin  $2 \nmid b-a$  (Lemma 5.1.2) jolloin Eulerin lauseen nojalla

$$c^{2^{r-1}} \equiv (b-a)^{2^{r-1}} \equiv 1 \pmod{2^r}.$$

Koska  $2^{r-1} \mid n$ , saadaan

$$c^n \equiv (b-a)^n \equiv 1 \pmod{2^r},$$

joten  $B_n \equiv 0 \pmod{2^r}$ . Näin ollen kongruenssi (5.1) toteutuu alkuluvulla  $p = 2$ . □

Osoitetaan viimein itse väite.

**Lause 5.1.6.** *Olkoon  $m \geq 3$ . Jos Konjektuuri 5.1.1 on voimassa luvulla  $m$ , niin tällöin myös Abc-konjektuuri on voimassa.*

*Todistus.* Olkoon  $0 < \varepsilon < 1$ . Määritellään  $abc$ -summille  $(a, b, c) \in \mathbb{N}^3$  funktio  $\Phi_\varepsilon$  siten, että

$$\Phi_\varepsilon(a, b, c) = \log c - (1 + \varepsilon) \log \text{rad}(abc). \quad (5.2)$$

Kirjoittamalla  $\log c = (1 + \varepsilon)(\log c) - \varepsilon \log c$  saadaan siten

$$\log \text{rad}(abc) = \log c - \frac{\varepsilon \log c}{1 + \varepsilon} - \frac{\Phi_\varepsilon(a, b, c)}{1 + \varepsilon}. \quad (5.3)$$

Oletetaan, että Konjektuuri 5.1.1 on voimassa. Tällöin on olemassa luku  $K(m, \varepsilon) > 0$  siten, että Konjektuurin 5.1.1 ehdot toteuttaville kolmikoille  $(A, B, C)$  pätee

$$\max\{|A|, |B|, |C|\} \leq K(m, \varepsilon) \text{rad}(ABC)^{1+\varepsilon},$$

joka voidaan vaatimuksen  $0 < A < B < C$  ja yhtälön (5.2) nojalla kirjoittaa ekvivalentisti muodossa

$$\Phi_\varepsilon(A, B, C) \leq \log K(m, \varepsilon) = K^*(m, \varepsilon). \quad (5.4)$$

Olkoon  $(a, b, c) \in \mathbb{N}^3$  tavallinen  $abc$ -summa siten, että  $a < b < c$ . Todistetaan väite osoittamalla, että yhtälöä (5.4) soveltamalla nähdään myös luvun  $\Phi_\varepsilon(a, b, c)$  olevan vakiolla rajoitettu.

Asetetaan  $n = \phi(m)$ , joka on parillinen luku oletuksen  $m \geq 3$  ja Huomautuksen 2.1.31 nojalla. Määritellään luvut  $A_n, B_n$  ja  $C_n$  kuten Lemmassa 5.1.4, jolloin niille Lemman 5.1.5 nojalla pätee  $A_n B_n C_n \equiv 0 \pmod{m}$ , ja ne toteuttavat epäyhtälön (5.4). Oletetaan tässä yksinkertaisuuden vuoksi, että luku  $c$  on pariton. Jos  $c$  on parillinen, päättely on oleellisesti samanlainen.

Luvun  $n$  parillisuuden nojalla saadaan Lemmaa 2.2.10 käyttämällä arvio

$$\begin{aligned} B_n &= c^n - (b-a)^n = (b+a)^n - (b-a)^n \\ &= 4ab((b+a)^{n-2} + (b+a)^{n-2}(b-a)^2 + \dots + (b-a)^{n-2}) \\ &\leq 4ab \binom{n}{2} (b+a)^{n-2} \\ &= 2abnc^{n-2}. \end{aligned}$$

Kirjoittamalla

$$A_n B_n C_n = (b-a)^n \left( \frac{abB_n}{ab} \right) c^n = (b-a)^n \left( \frac{B_n}{ab} \right) abc^n,$$

saadaan radikaalille arvio

$$\begin{aligned} \text{rad}(A_n B_n C_n) &= \text{rad} \left( (b-a)^n \left( \frac{B_n}{ab} \right) abc^n \right) = \text{rad} \left( (b-a) \left( \frac{B_n}{ab} \right) abc \right) \\ &\leq \text{rad}(b-a) \text{rad} \left( \frac{B_n}{ab} \right) \text{rad}(abc) \\ &\leq (b-a) \left( \frac{B_n}{ab} \right) \text{rad}(abc) \\ &\leq (b-a) (2nc^{n-2}) \text{rad}(abc) \\ &\leq 2nc^{n-1} \text{rad}(abc). \end{aligned}$$

Ottamalla nyt puolittain logaritmi, sijoittamalla yhtälö (5.3) ja arvioimalla ylöspäin saadaan

$$\begin{aligned} \log \text{rad}(A_n B_n C_n) &\leq (n-1) \log c + \log \text{rad}(abc) + \log 2n \\ &= n \log c - \frac{\varepsilon \log c}{1+\varepsilon} - \frac{\Phi_\varepsilon(a, b, c)}{1+\varepsilon} + \log 2n \\ &= \left( 1 - \frac{\varepsilon}{(1+\varepsilon)n} \right) \log c^n - \frac{\Phi_\varepsilon(a, b, c)}{1+\varepsilon} + \log 2n \\ &\leq \left( 1 - \frac{\varepsilon}{(1+\varepsilon)n} \right) (\log C_n + n \log 2) - \frac{\Phi_\varepsilon(a, b, c)}{1+\varepsilon} + \log 2n \\ &\leq \left( \frac{n+(n-1)\varepsilon}{(1+\varepsilon)n} \right) \log C_n - \frac{\Phi_\varepsilon(a, b, c)}{1+\varepsilon} + 2n \log 2, \end{aligned}$$

kun käytetään arviota

$$\left( 1 - \frac{\varepsilon}{(1+\varepsilon)n} \right) n \log 2 + \log 2n \leq \left( n - \frac{\varepsilon}{(1+\varepsilon)} \right) \log 2 + \log 2^n \leq n \log 2 + n \log 2 = 2n \log 2.$$

Ratkaisemalla  $\Phi_\varepsilon(a, b, c)$ , yhteinen tekijä ottamalla ja arvioimalla  $\varepsilon < 1$  saadaan

$$\begin{aligned}
\Phi_\varepsilon(a, b, c) &\leq \left(\frac{n + (n-1)\varepsilon}{n}\right) \left(\log C_n - \left(\frac{(1+\varepsilon)n}{n + (n-1)\varepsilon}\right) \log \text{rad}(A_n B_n C_n)\right) \\
&\quad + 2(1+\varepsilon)n \log 2 \\
&< 2 \left(\log C_n - \left(\frac{(1+\varepsilon)n}{n + (n-1)\varepsilon}\right) \log \text{rad}(A_n B_n C_n)\right) + 4n \log 2 \\
&= 2(\log C_n - (1+\varepsilon') \log \text{rad}(A_n B_n C_n)) + 4n \log 2,
\end{aligned} \tag{5.5}$$

missä

$$\varepsilon' = \frac{(1+\varepsilon)n}{n + (n-1)\varepsilon} - 1 = \frac{\varepsilon}{\phi(m) + (\phi(m) - 1)\varepsilon}.$$

Koska  $abc$ -summa  $(A_n, B_n, C_n) \in \mathbb{N}^3$  toteuttaa Konjektuurin 5.1.1 oletukset, saadaan yhtälön (5.2) ja epäyhtälön (5.4) nojalla

$$\log C_n - (1 + \varepsilon') \log \text{rad}(A_n B_n C_n) = \Phi_{\varepsilon'}(A_n, B_n, C_n) \leq K^*(\varepsilon', m),$$

jolloin epäyhtälöketju (5.5) sievenee muotoon

$$\Phi_\varepsilon(a, b, c) < 2K^*(\varepsilon', m) + 4\phi(m) \log 2.$$

Näin ollen jokaisella  $\varepsilon > 0$  ja mielivaltaisella  $abc$ -summalla  $(a, b, c) \in \mathbb{N}^3$ ,  $a < b < c$ , funktio  $\Phi_\varepsilon(a, b, c)$  on ylhäältä rajoitettu. Tämä on yhtäpitävää  $Abc$ -konjektuurin kanssa.  $\square$

**Huomautus 5.1.7.** J. Oesterlé [49, s. 169] huomautti jo vuonna 1987, että mikäli Konjektuuri 5.1.1 pätee arvolla  $m = 16$ , niin silloin myös varsinainen  $Abc$ -konjektuuri on voimassa. Yleistä tapausta pidettiin pitkään tunnettuna, vaikka varsinainen todistus esitettiin kirjallisuudessa vasta vuonna 2000 [17].

## 5.2 $n$ -konjektuuri

$Abc$ -konjektuurissa tarkastellaan kolmea kokonaislukua, jotka täyttävät tietyt ehdot. Luonnollinen yleistys otaksumalle onkin tarkastella tilannetta, jossa kokonaislukuja on  $n \geq 3$  kappaletta. Seuraava esitys perustuu J. Brownkinin ja J. Brzezińskiin artikkeliin [6]. Aloiteetaan tarkastelu määrittelemällä  $n$ -summa.

**Määritelmä 5.2.1.** Olkoon  $n \in \mathbb{N}_{\geq 3}$ . Vektoria  $(a_1, a_2, \dots, a_n) \in \mathbb{Z}^n$  kutsutaan  $n$ -summaksi, mikäli seuraavat kolme ehtoa toteutuvat:

- (i)  $\text{synt}(a_1, a_2, \dots, a_n) = 1$ ,
- (ii)  $a_1 + a_2 + \dots + a_n = 0$ ,
- (iii) mikään kohdan (ii) summan aito osasumma ei ole yhtä suuri kuin nolla.

Vuonna 1994 J. Brownkin ja J. Brzeziński esittivät seuraavan otaksuman:

**Konjektuuri 5.2.2** ( $n$ -konjektuuri). *Olkoon  $n \in \mathbb{N}_{\geq 3}$  ja  $\varepsilon > 0$ . Tällöin on olemassa vakio  $C(n, \varepsilon) > 0$  siten, että kaikille  $n$ -summille  $(a_1, \dots, a_n)$  pätee*

$$\max\{|a_1|, \dots, |a_n|\} \leq C(n, \varepsilon) \text{rad}(a_1 \cdots a_n)^{2n-5+\varepsilon}.$$

Käyttämällä  $n$ -summaan liittyviä merkintöjä

$$\begin{aligned} M_n &= \max\{|a_1|, \dots, |a_n|\}, \\ m_n &= \text{rad}(a_1 \cdots a_n), \\ L_n &= L(a_1, \dots, a_n) = \frac{\log M_n}{\log m_n}. \end{aligned}$$

voidaan Konjektuuri 5.2.2 esittää  $L_n$ -arvojen joukon kasaantumispisteiden supremumin  $\limsup L_n$  avulla seuraavassa muodossa:

**Konjektuuri 5.2.3.** *Olkoon  $n \in \mathbb{N}_{\geq 3}$  ja  $\varepsilon > 0$ . Tällöin kaikille  $n$ -summille  $(a_1, \dots, a_n)$  pätee*

$$\limsup L_n = 2n - 5.$$

$n$ -konjektuurin todeperäisyyttä ei ole vielä pystytty osoittamaan. Voidaan kuitenkin osoittaa hieman heikompi tulos, jonka mukaan  $L_n$ -arvojen joukon kasaantumispisteiden supremum on suuruudeltaan ainakin  $2n - 5$ , ts.  $\limsup L_n \geq 2n - 5$ . Tätä varten tarvitaan seuraava aputulos.

**Lemma 5.2.4.** *Jokaista lukua  $k \in \mathbb{Z}_{\geq 0}$  kohti on olemassa  $k$ -asteinen positiivikertoiminen polynomi  $f_k \in \mathbb{Z}[x]$  siten, että*

$$\frac{x^{2k+1} - 1}{x - 1} = x^k f_k \left( \frac{(x - 1)^2}{x} \right). \quad (5.6)$$

*Todistus.* Olkoon  $f_k$  polynomi, jolloin se voidaan kirjoittaa muodossa  $f_k(z) = \sum_{j=0}^k s_j z^j$ . Näin ollen yhtälö (5.6) voidaan geometrisen sarjan summan kaavaa soveltamalla ja tulo auki kirjoittamalla esittää muodossa

$$1 + x + \cdots + x^{2k-1} + x^{2k} = s_0 x^k + s_1 (x-1)^2 x^{k-1} + \cdots + s_{k-1} (x-1)^{2(k-1)} x + s_k (x-1)^{2k}.$$

Yhtälön eri puolien polynomien kertoimia vertailemalla ja polynomiesityksen yksikäsitteisyyttä soveltamalla nähdään, että ratkaisu on ylipäänsä olemassa ja että polynomien  $f_k$  kertoimet  $s_j \in \mathbb{Z}$  kaikilla  $j = 0, 1, \dots, k$ .

Tarkastellaan sitten yhtälön (5.6) vasenta puolta. Asetetaan  $\alpha_j = \frac{2\pi j}{2k+1}$ ,  $j = 1, 2, \dots, k$ . Näin ollen Lemmaa 2.5.12 soveltamalla sekä tuloa muokkaamalla saadaan

$$\begin{aligned} \frac{x^{2k+1} - 1}{x - 1} &= \prod_{j=1}^k (x^2 - 2x \cos \alpha_j + 1) \\ &= \prod_{j=1}^k \left( x^2 - 2x + 1 + 2x - 2x \cos \alpha_j \right) \\ &= x^k \prod_{j=1}^k \left( \frac{(x-1)^2}{x} + 2(1 - \cos \alpha_j) \right), \end{aligned}$$

josta voidaan valita

$$f_k(z) = \prod_{j=1}^k (z + 2(1 - \cos \alpha_j)).$$

Aiemmin todettiin kaikkien polynomien  $f_k$  kerrointen olevan kokonaislukuja. Kaikki kertoimet ovat lisäksi positiivisia, sillä polynomien  $f_k$  juuret ovat negatiivisia lukuja

$$z = -2(1 - \cos \alpha_j)$$

kaikilla  $j = 1, 2, \dots, k$ . Väite seuraa. □

**Huomautus 5.2.5.** Polynomi  $f_k(z)$  voidaan määritellä joko eksplisiittisesti muodossa

$$f_k(z) = \sum_{j=0}^k \frac{2k+1}{k+j+1} \binom{k+j+1}{2j+1} z^j$$

tai induktiivisesti muodossa

$$\begin{aligned} f_0(z) &= 1, \\ f_1(z) &= z + 3, \\ f_{k+1}(z) &= (z+2)f_k(z) - f_{k-1}(z). \end{aligned}$$

Molemmilla tavoilla seuraaviksi polynomeiksi saadaan

$$\begin{aligned} f_2(z) &= z^2 + 5z + 5, \\ f_3(z) &= z^3 + 7z^2 + 14z + 7, \\ f_4(z) &= z^4 + 9z^3 + 27z^2 + 30z + 9, \\ f_5(z) &= z^5 + 11z^4 + 44z^3 + 77z^2 + 55z + 11. \end{aligned}$$

Todistetaan seuraavaksi itse väite.

**Lause 5.2.6.** *Olkoon  $n \in \mathbb{N}_{\geq 3}$  ja  $\varepsilon > 0$ . Tällöin kaikille  $n$ -summille  $(a_1, \dots, a_n)$  pätee*

$$\limsup L_n \geq 2n - 5.$$

*Todistus.* Olkoon  $f_k, f_k(z) = \sum_{j=0}^k s_j z^j$ , Lemman 5.2.4 mukainen polynomi, jolla  $s_j \in \mathbb{N}$  kaikilla  $j = 0, 1, \dots, k$ . Asetetaan yhtälössä (5.6)  $k = n - 3$  ja  $x = -\frac{a_1}{a_2}$ , jolloin yhtälön vasen puoli sievenee muotoon

$$\frac{\left(-\frac{a_1}{a_2}\right)^{2(n-3)+1} - 1}{\left(-\frac{a_1}{a_2}\right) - 1} = \frac{\left(\frac{a_1}{a_2}\right)^{2n-5} + 1}{\left(\frac{a_1}{a_2}\right) + 1} = \frac{a_1^{2n-5} + a_2^{2n-5}}{a_2^{2n-6}(a_1 + a_2)}$$

ja yhtälön oikea puoli muotoon

$$\begin{aligned} \left(-\frac{a_1}{a_2}\right)^{n-3} \cdot \sum_{j=0}^{n-3} s_j \left(\frac{\left(-\frac{a_1}{a_2} - 1\right)^2}{\left(-\frac{a_1}{a_2}\right)}\right)^j &= \left(-\frac{a_1}{a_2}\right)^{n-3} \cdot \sum_{j=0}^{n-3} s_j \left(\frac{\left(\frac{a_1}{a_2} + 1\right)^2}{-\frac{a_1}{a_2}}\right)^j \\ &= \left(-\frac{a_1}{a_2}\right)^{n-3} \cdot \sum_{j=0}^{n-3} s_j \left(\frac{(a_1 + a_2)^2}{-a_1 a_2}\right)^j. \end{aligned}$$

Kertomalla yhtälön (5.6) sievennytty versio puolittain luvulla  $a_2^{2n-6}(a_1 + a_2)$  saadaan

$$\begin{aligned} a_1^{2n-5} + a_2^{2n-5} &= a_2^{2n-6}(a_1 + a_2) \left(-\frac{a_1}{a_2}\right)^{n-3} \cdot \sum_{j=0}^{n-3} s_j \left(\frac{(a_1 + a_2)^2}{-a_1 a_2}\right)^j \\ &= (a_1 + a_2) (-a_1 a_2)^{n-3} \sum_{j=0}^{n-3} s_j \frac{(a_1 + a_2)^{2j}}{(-a_1 a_2)^j} \\ &= \sum_{j=0}^{n-3} s_j (a_1 + a_2)^{2j+1} (-a_1 a_2)^{n-j-3}. \end{aligned}$$

Valitsemalla nyt  $a_1 = 2^i$ ,  $i > 1$ , ja  $a_2 = -1$ , saadaan edellä olevasta yhtälöstä  $n$ :n kokonaisluvun summa

$$2^{i(2n-5)} - 1 - \sum_{j=0}^{n-3} s_j (2^i - 1)^{2j+1} 2^{i(n-j-3)} = 0. \quad (5.7)$$

Summalla ei ole sellaista aitoa osasummaa, joka olisi yhtä suuri kuin nolla, sillä ainoastaan ensimmäinen termi on positiivinen. Koska summan toinen termi on  $-1$ , kaikkien summattavien termien suurin yhteinen tekijä on 1 (Lause 2.1.5). Näin ollen Määritelmän 5.2.1 ehdot ovat voimassa, jolloin kyseessä on  $n$ -summa. Yhtälöstä (5.7) saadaan määrättyä edelleen

$$\begin{aligned} M_{n,i} &= 2^{i(2n-5)}, \\ m_{n,i} &= \text{rad}((2^i - 1)2s_0s_1 \cdots s_{n-3}) = \text{rad}((2^i - 1)c), \end{aligned}$$

missä  $c = 2s_0s_1 \cdots s_{n-3}$ . Soveltamalla radikaalille arviota

$$\text{rad}((2^i - 1)c) \leq \text{rad}(2^i - 1) \text{rad}(c) \leq (2^i - 1) \text{rad}(c) \leq 2^i \text{rad}(c)$$

ja käyttämällä 2-kantaista logaritmia saadaan lopulta arvio

$$L_n = \frac{\log_2 M_{n,i}}{\log_2 m_{n,i}} = \frac{i(2n - 5)}{\log_2 \text{rad}((2^i - 1)c)} \geq \frac{i(2n - 5)}{i + \log_2 \text{rad}(c)} \rightarrow 2n - 5,$$

kun  $i \rightarrow \infty$ . Koska on äärettömästi sellaisia lukuja  $i$ , joille  $2^i - 1$  ovat suhteellisia alkukuja, luvun  $i$  arvoja vastaavia erilaisia osamääriä  $L_n$  on äärettömästi. Näin ollen Lausetta 3.4.8 soveltaen joukolla  $\{L_n\}$  on kasaantumispiste, joka on vähintään  $2n - 5$ .  $\square$

Esitetään vielä lopuksi Hun ja Yangin vuonna 2000 esittämä  $k$ :n termin  $abc$ -konjektuuri, joka on yhteensopiva Nevanlinnan teorian analogian kanssa [30].

**Määritelmä 5.2.7.** Olkoot  $k \in \mathbb{N}$  ja  $a \in \mathbb{Z} \setminus \{0\}$ . Luvun  $a$   $k$ -radikaali määritellään tulona

$$\text{rad}_k(a) = \prod_{v=1}^n p_v^{\min\{i_v, k\}},$$

missä on käytetty kanonista esitystä  $|a| = p_1^{i_1} \cdots p_n^{i_n}$ .

**Konjektuuri 5.2.8.** Olkoot  $a_j \in \mathbb{Z} \setminus \{0\}$  siten, että  $\text{sy}(a_0, a_j) = 1$  kaikilla  $j = 1, \dots, k$  sekä mikään summan

$$a_1 + \cdots + a_k = a_0$$

aito osasumma ei ole yhtä suuri kuin nolla. Tällöin jokaista  $\varepsilon > 0$  kohti on olemassa luku  $C(k, \varepsilon)$  siten, että

$$\max\{|a_0|, |a_1|, \dots, |a_k|\} \leq C(k, \varepsilon) \text{rad}_{k-1}(a_0 a_1 \cdots a_k)^{1+\varepsilon}.$$



### 5.3 Stothers-Masonin lause

Vuonna 1981 Stothers todisti *Abc*-konjektuuria vastaavan tuloksen polynomeille käyttämällä syvällisiä algebrallisen geometrian keinoja. Todistuksen syvällisyyden takia tulos ei kuitenkaan noussut yleiseen tietoisuuteen ennen kuin vasta vuonna 1983, jolloin Mason esitti alkeellisen todistuksen. Yksinkertaisimman tunnetun todistuksen tulokselle antoi Noah Snyder vuonna 2000. [37, s. 165]

Esitetään seuraavaksi Snyderin todistus kirjaan [37, s. 165–170] perustuen sekä selkeyttävää lähdettä [35] apuna käyttäen. Sitä ennen tarvitaan kuitenkin muutama aputuloks.

**Lemma 5.3.1.** *Olkoon  $f$  polynomi suljetussa algebrallisessa kunnassa ja olkoon  $\alpha$  polynomin  $f$  juuri monikertanaan  $m(\alpha)$ . Tällöin polynomin  $f'$  juuren monikerta pisteessä  $\alpha$  on  $m(\alpha) - 1$ .*

*Todistus.* Kirjoitetaan polynomi  $f$  muodossa  $f(x) = (x - \alpha)^m g(x)$ , missä polynomille  $g$  pätee  $g(\alpha) \neq 0$ . Tulon derivoimissäännön nojalla

$$\begin{aligned} f'(t) &= (x - \alpha)^m g'(x) + m(x - \alpha)^{m-1} g(x) \\ &= (x - \alpha)^{m-1} ((x - \alpha)g'(x) + mg(x)) = (x - \alpha)^{m-1} h(x), \end{aligned}$$

missä  $h(x) = ((x - \alpha)g'(x) + mg(x))$  ja arvot  $h(\alpha)$ ,  $mg(\alpha)$  sekä  $g'(\alpha)$  ovat nollasta eroavia. Näin ollen  $(x - \alpha)^{m-1}$  on korkein luvun  $(x - \alpha)$  potenssi, joka jakaa polynomin  $f'$ , joten  $m - 1$  on polynomin  $f'$  juuren  $\alpha$  monikerta.  $\square$

**Merkintä 5.3.2.** Olkoon  $f$  ei-vakio polynomi. Tällöin merkitään

$$\begin{aligned} n_0(f) &= \text{funktion } f \text{ erillisten nollakohtien lukumäärä} \\ (f, f') &= \text{syt}(f, f') = \text{funktioden } f \text{ ja } f' \text{ suurin yhteinen tekijä polynomirenkaassa.} \end{aligned}$$

**Lemma 5.3.3.** *Jos  $f$  on polynomi, niin  $\deg(f, f') = \deg(f) - n_0(f)$ .*

*Todistus.* Olkoon  $\deg(f) = n$  ja olkoot  $\alpha_1, \dots, \alpha_i$  polynomin  $f$  erilliset juuret moninkertoinaan  $k_1, \dots, k_i$ . Tällöin  $n = k_1 + \dots + k_i$ . Lemman 5.3.1 todistuksen mukaan

$$\text{syt}(f, f') = (x - \alpha_1)^{k_1-1} (x - \alpha_2)^{k_2-1} \dots (x - \alpha_i)^{k_i-1}.$$

Näin ollen

$$\begin{aligned} \deg(f, f') &= (k_1 - 1) + (k_2 - 1) + \dots + (k_i - 1) \\ &= (k_1 + k_2 + \dots + k_i) - i \\ &= n - i = \deg(f) - n_0(f), \end{aligned}$$

mistä väite seuraa  $\square$

**Lause 5.3.4** (Stothers-Mason). *Olkoot  $f, g, h \in \mathbb{C}[x]$  keskenään jaottomia polynomeja, joista ainakin yksi ei ole vakio ja jotka toteuttavat yhtälön  $f + g = h$ . Tällöin*

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq n_0(fgh) - 1.$$

*Todistus.* Todetaan ensin, että nyt on voimassa yhtälö

$$f'g - fg' = f'h - fh'. \quad (5.8)$$

Nimittäin yhtälöä  $f + g = h$  derivoimalla saadaan  $f' + g' = h'$ , joten

$$f'g - fg' = f'(h - f) - f(h' - f') = f'h - fh'.$$

Todetaan lisäksi, että nyt ainakin kaksi polynomeista  $f, g$  ja  $h$  eivät ole vakioita. Kahden vakiofunktion tapauksessa nimittäin kolmannenkin funktion täytyy olla vakiofunktio. Näin ollen voidaan olettaa, että polynomit  $f$  ja  $g$  ovat vakiosta eroavia. Tällöin

$$f'g - fg' \neq 0.$$

Jos nimittäin  $f'g = fg' \neq 0$ , niin tällöin saadaan ristiriita  $g \mid g'$ , sillä polynomit  $f$  ja  $g$  ovat keskenään jaottomia.

Tarkastellaan sitten yhtälöä (5.8). Havaitaan, että yhtälön vasen puoli on jaollinen tekijällä  $\text{syt}(f, f')$  sekä  $\text{syt}(g, g')$  ja yhtälön oikea puoli on jaollinen tekijällä  $\text{syt}(h, h')$ . Mutta koska vasen ja oikea puoli ovat yhtäsuuret ja polynomit  $f, g$  ja  $h$  ovat keskenään jaottomia, saadaan

$$\text{syt}(f, f') \text{syt}(g, g') \text{syt}(h, h') \mid (f'g - fg').$$

Näin ollen

$$\deg(f, f') + \deg(g, g') + \deg(h, h') \leq \deg(f'g - fg'),$$

jolloin edelleen

$$\deg(f, f') + \deg(g, g') + \deg(h, h') \leq \deg(f) + \deg(g) - 1. \quad (5.9)$$

Soveltamalla Lemmaa 5.3.3 polynomeihin  $f, g$  ja  $h$  saadaan

$$\deg(f, f') = \deg(f) - n_0(f),$$

$$\deg(g, g') = \deg(g) - n_0(g),$$

$$\deg(h, h') = \deg(h) - n_0(h),$$

jotka sijoittamalla yhtälöön (5.9) saadaan

$$\deg(h) \leq n_0(f) + n_0(g) + n_0(h) - 1 = n_0(fgh) - 1,$$

sillä polynomit  $f, g$  ja  $h$  ovat keskenään jaottomia.

Koska funktiot  $f, g$  ja  $h$  ovat oleellisesti symmetrisiä yhtälön  $f + g = h$  suhteen, voidaan vastaavanlaisella päättelyllä osoittaa sama yläraja asteille  $\deg(f)$  ja  $\deg(g)$ . Väite seuraa.  $\square$

**Huomautus 5.3.5.** Lauseen 5.3.4 ehdot toteuttavien polynomien asteille pätee artikkelin [67] mukaan alaraja

$$\min\{\deg(f), \deg(g), \deg(h)\} \leq n_0(fgh) - 2.$$

Lauseen 5.3.4 välittömänä seurauksena saadaan Fermat'n suuren lauseen polynomiversio [37, s. 169].

**Lause 5.3.6** (Fermat'n suuri lause polynomeille). *Olkoot  $u, v, w \in \mathbb{C}[x]$  keskenään jaottomia vakioista eroavia polynomeja ja olkoon  $n \in \mathbb{N}_{\geq 3}$ . Tällöin yhtälöllä*

$$u^n + v^n = w^n$$

*ei ole ratkaisuja.*

*Todistus.* Lausesta 5.3.4 polynomeihin  $f = u^n, g = v^n$  ja  $h = w^n$  soveltamalla saadaan

$$\deg u^n \leq n_0(u^n v^n w^n) - 1.$$

Koska  $\deg(f) = \deg(u^n) = n \cdot \deg(u)$  ja  $n_0(f) = n_0(u^n) \leq \deg(u)$ , saadaan edelleen

$$n \cdot \deg(u) \leq \deg(u) + \deg(v) + \deg(w) - 1.$$

Analogisella päättelyllä saadaan polynomeille  $v$  ja  $w$  epäyhtälöt

$$n \cdot \deg(v) \leq \deg(u) + \deg(v) + \deg(w) - 1,$$

$$n \cdot \deg(w) \leq \deg(u) + \deg(v) + \deg(w) - 1.$$

Lisäämällä yhtälöt puolittain yhteen saadaan

$$n(\deg(uvw)) \leq 3(\deg(uvw)) - 3 < 3(\deg(uvw)),$$

koska polynomit  $u, v$  ja  $w$  ovat oletuksen mukaan keskenään jaottomia. Jakamalla reunimaiset epäyhtälöt puolittain termillä  $\deg(uvw)$  saadaan  $n < 3$ , mikä on ristiriita.  $\square$

**Huomautus 5.3.7.** Lause 5.3.6 ei ole voimassa arvolla  $n = 2$ . Tämä nähdään asettamalla  $u(x) = 1 - x^2$ ,  $v(x) = 2x$  ja  $w(x) = 1 + x^2$ , jolloin polynomit  $u, v$  ja  $w$  ovat keskenään jaottomia mutta yhtälö

$$(1 - x^2)^2 + (2x)^2 = (1 + x^2)^2$$

toteutuu kaikilla  $x \in \mathbb{C}$ .

**Huomautus 5.3.8.** Lauseessa 5.3.6 tarkasteltiin yksinkertaisuuden vuoksi tilannetta lukukunnassa  $\mathbb{C}$ . Mikäli tarkasteltavan lukukunnan karakteristika  $\text{char } p > 0$ , ei lause ole enää voimassa. Tämä nähdään asettamalla lähteen [71, s. 9] mukaisesti  $f(x) = x + 1, g(x) = x$  ja  $h(x) = 1$ , jolloin yhtälö

$$f(x)^p = g(x)^p + h(x)^p.$$

toteutuu myös arvolla  $p > 3$ .

## 5.4 Yleistys meromorffifunktioille

Tarkastellaan lopuksi vielä Nevanlinnan teorian ja lukuteorian välistä yhteyttä, jonka huomasi C. F. Osgood jo vuonna 1981 ja jota P. Vojta vuonna 1987 julkaisemassaan monografiassa [68, s. 30–45] syvensi rinnastamalla teorioiden käsitteitä ns. sanakirjan avulla [10, s. 151–160]. Lisäksi nähdään, että aiemmin tarkasteltu Stothers-Masonin polynomilause (Lause 5.3.4) voidaan pienellä muokkauksella esittää vielä yleisemmässä, meromorffifunktioiden kontekstissa. Alaluku perustuu pääosin lähteisiin [29] ja [30], perusteellisemmän kuvan Nevanlinnan teoriasta saa lähteestä [10].

Aloitetaan tarkastelu määrittelemällä ei-Arkhimedinen itseisarvo [33, s. 331]:

**Määritelmä 5.4.1.** Kunnan  $\kappa$  *ei-Arkhimedinen itseisarvo* on funktio  $|\cdot| : \kappa \rightarrow \mathbb{R}$ , jolle pätee

- (i)  $|x| \geq 0$  kaikilla  $x \in \kappa$ . Yhtäsuuruus on voimassa, jos ja vain jos  $x = 0_\kappa$ .
- (ii)  $|x + y| \leq \max(|x|, |y|)$  kaikilla  $x, y \in \kappa$ .
- (iii)  $|xy| = |x||y|$  kaikilla  $x, y \in \kappa$ .

**Huomautus 5.4.2.** Arkhimedinen ja ei-Arkhimedinen itseisarvo eroavat kohdassa (ii), jossa arkhimedisellä itseisarvolla on tuttu kolmioepäyhtälö  $|x + y| \leq |x| + |y|$ . Ei-Arkhimediselle itseisarvolla pätee lisäksi

- (iv)  $|x + y| = |x|$ , aina kun alkioilla  $x, y \in \kappa$  pätee  $|y| < |x|$ .

Avataan seuraavaksi jatkossa käytettäviä Nevanlinnan teoriaan liittyviä funktioita  $N$  ja  $T$  lähteeseen [29] perustuen. Tarkastellaan algebrallisesti suljettua kuntaa  $\kappa$ , jonka karakteristika on nolla ja joka on täydellinen ei-triviaalin ei-Arkhimedisin itseisarvon  $|\cdot|$  suhteen. Olkoon  $r > 0$  reaaliluku. Määritellään origo-keskinen kiekko

$$\kappa[0; r] = \{z \in \kappa : |z| \leq r\}.$$

Käytetään lukukunnan  $\kappa$  kokonaisten funktioiden joukosta merkintää  $\mathcal{A}(\kappa)$ . Tällöin jokainen funktio  $f \in \mathcal{A}(\kappa)$  voidaan esittää potenssisarjana

$$f(z) = \sum_{n=0}^{\infty} a_n z^n, \quad (a_n \in \kappa)$$

siten, että kaikilla  $z \in \kappa$  pätee  $|a_n z^n| \rightarrow 0$ , kun  $n \rightarrow \infty$ . Käytetään potenssisarjan maksimitermille merkintää

$$\mu(r, f) = \max_{n \geq 0} |a_n| r^n.$$

Määritellään seuraavaksi edelliseen nojaten lukumääräfunctiot  $n$  ja  $N$ .

**Määritelmä 5.4.3.** Olkoon  $f \in \mathcal{A}(\kappa)$ . Tällöin funktiota  $n$ ,

$$n\left(r, \frac{1}{f}\right) = \max_{n \geq 0} \{n : |a_n| r^n = \mu(r, f)\},$$

kutsutaan *funktio*  $f$  *nollakohtien lukumääräfunctioksi*, joka ilmoittaa funktion  $f$  nollakoh-  
tien määrän (monikertoineen)  $r$ -säteisessä origo-keskisessä kiekossa.

**Huomautus 5.4.4.** Määritelmässä 5.4.3 pidetään tunnettuna, että  $p$ -adisen itseisarvon tapauksessa funktion  $f$  nollakohtien lukumäärä ja potenssisarjan  $|a_n|r^n = \mu(r, f)$  maksimaalinen luku  $n$  ovat yhtä suuret tarkasteltavassa kiekossa, ks. [11, s. 5049–5051].

**Määritelmä 5.4.5.** Olkoot  $\rho, \rho_0 \in \mathbb{R}$ ,  $\rho_0$  kiinnitetty, siten, että  $0 < \rho_0 < \rho$ . Tällöin funktiota  $N$ ,

$$N\left(r, \frac{1}{f-a}\right) = \int_{\rho_0}^r \frac{n\left(t, \frac{1}{f-a}\right)}{t} dt, \quad (\rho_0 < r < \rho)$$

kutsutaan funktion  $f$  *valenssifunktioksi*.

**Huomautus 5.4.6.** Määritelmien 5.4.3 ja 5.4.5 funktioille  $n$  ja  $N$  on voimassa seuraava *Jensenin kaava*:

$$N\left(r, \frac{1}{f}\right) = \log \mu(r, f) - \log \mu(\rho_0, f).$$

**Huomautus 5.4.7.** Määritelmiä 5.4.3 ja 5.4.5 mukailten voidaan määritellä erillisiä nollakohtia laskevat lukumääräfunctiot  $\bar{n}$  ja  $\bar{N}$  kiekossa  $\kappa[0; r]$ . Tällöin funktiolle  $f - a \in \mathcal{A}(\kappa)$  käytetään merkintöjä

$$\bar{n}\left(r, \frac{1}{f-a}\right)$$

sekä

$$\bar{N}\left(r, \frac{1}{f-a}\right) = \int_{\rho_0}^r \frac{\bar{n}\left(t, \frac{1}{f-a}\right)}{t} dt \quad (\rho_0 < r < \rho).$$

Olkoon  $k \in \mathbb{N}$ . Määritelmiä 5.4.3 ja 5.4.5 mukailten voidaan edelleen määritellä lukumääräfunctiot  $n_k$  ja  $N_k$  siten, että nollakohdat lasketaan korkeintaan  $k$ -kertaisena. Toisin sanoen kiekossa  $\kappa[0; r]$  määritellyn funktion  $f - a$   $m$ -kertainen nollakohta lasketaan  $\min\{m, k\}$ -kertaisena funktiossa

$$n_k\left(r, \frac{1}{f-a}\right).$$

Edelleen merkitään

$$N_k\left(r, \frac{1}{f-a}\right) = \int_{\rho_0}^r \frac{n_k\left(t, \frac{1}{f-a}\right)}{t} dt \quad (\rho_0 < r < \rho).$$

Käytetään joukosta  $\mathcal{A}(\kappa)$  muodostettujen osamääräfunctioiden joukkolle merkintää  $\mathcal{M}(\kappa)$ . Joukon  $\mathcal{M}(\kappa)$  alkiota  $f$  kutsutaan *meromorffifunktioksi* kunnassa  $\kappa$ . Olkoon  $f \in \mathcal{M}(\kappa)$ . Koska kahden joukon  $\mathcal{A}(\kappa)$  alkion suurin yhteinen tekijä kuuluu myös joukkoon  $\mathcal{A}(\kappa)$ , voidaan funktio  $f$  esittää muodossa

$$f = \frac{g}{h},$$

missä alkiolla  $g, h \in \mathcal{A}(\kappa)$  ei ole yhteisiä tekijöitä renkaassa  $\mathcal{A}(\kappa)$ . Maksimitermi  $\mu$  määritelmä voidaan yksikäsitteisesti laajentaa meromorffifunktiolle  $f = g/h$  asettamalla

$$\mu(r, f) = \frac{\mu(r, g)}{\mu(r, h)} \quad (0 \leq r \leq \infty).$$

**Määritelmä 5.4.8.** Olkoon  $f \in \mathcal{M}(\kappa)$ . Funktiota  $m$ ,

$$m(r, f) = \max\{0, \log \mu(r, f)\},$$

kutsutaan *kompensaatiofunktioiksi*.

Määritellään vielä karakteristinen funktio.

**Määritelmä 5.4.9.** Olkoon  $f = g/h \in \mathcal{M}(\kappa)$ . Funktiota  $T$ ,

$$T(r, f) = m(r, f) + N(r, f) \quad (\rho_0 < r < \infty),$$

missä

$$N(r, f) = N\left(r, \frac{1}{h}\right),$$

kutsutaan *karakteristiseksi funktioksi*.

Edellä olevilla merkinnöillä Stothers-Masonin lause voidaan esittää seuraavasti [29]:

**Lause 5.4.10** (Stothers-Mason). *Olkoon  $\kappa$  algebrallisesti suljettu kunta, jonka karakteristika on nolla. Olkoot  $a, b, c$  kunnan  $\kappa$  keskenään jaottomia polynomeja, joista ainakin yksi ei ole vakio ja jotka toteuttavat yhtälön  $a + b = c$ . Tällöin*

$$\max\{\deg(a), \deg(b), \deg(c)\} \leq \bar{n} \left( \frac{1}{abc} \right) - 1.$$

Vuonna 2000 Hu ja Yang esittivät Stothers-Masonin lauseen yleistyksen [29]:

**Lause 5.4.11.** *Olkoon  $\kappa$  algebrallisesti suljettu kunta, jonka karakteristika on nolla ja joka on kokonainen epätriviaalin ei-Arkhimedisen itseisarvon suhteen. Olkoot  $a, b, c \in \kappa$  kokonaisia funktioita, joilla ei ole yhteisiä nollakohtia, joista ainakin yksi on ei-vakio ja joille  $a + b = c$ . Tällöin*

$$\max\{T(r, a), T(r, b), T(r, c)\} \leq \bar{N}\left(r, \frac{1}{abc}\right) - \log r + \mathcal{O}(1).$$

**Huomautus 5.4.12.** Jos  $f$  on polynomi, tällöin voidaan osoittaa, että

$$\deg(f) = \lim_{r \rightarrow \infty} \frac{T(r, f)}{\log r}, \quad n_0(f) = \lim_{r \rightarrow \infty} \frac{\bar{N}(r, \frac{1}{f})}{\log r},$$

jolloin Stothers-Masonin lause seuraa Lauseesta 5.4.11 antamalla  $r \rightarrow \infty$  [29]. Näin ollen Lause 5.4.11 voidaan tulkita *Abc*-konjektuurin analogiana ei-Arkhimedisille meromorffifunktiolle.

Vuonna 2002 Hu ja Yang esittivät edelliselle lauseelle vielä seuraavan yleistyksen [30]:

**Lause 5.4.13.** *Olkoon  $\kappa$  algebrallisesti suljettu kunta, jonka karakteristika on nolla ja joka on kokonainen epätriviaalin ei-Arkhimedisen itseisarvon suhteen. Olkoot  $f_j \in \kappa, j = 0, 1, \dots, k$ , kokonaisia lineaarisesti riippumattomia funktioita, joilla ei ole yhteisiä nollakohtia ja joille*

$$f_0 + f_1 + \dots + f_k = 0.$$

*Tällöin*

$$\max_{0 \leq j \leq k} \{T(r, f_j)\} \leq \sum_{i=0}^k N_{k-1}\left(r, \frac{1}{f_i}\right) - \frac{k(k-1)}{2} \log r + \mathcal{O}(1).$$

**Huomautus 5.4.14.** Olkoon  $k \in \mathbb{N}_{\geq 2}$ . Jos polynomilla  $f$  on faktorisointi

$$f(z) = z_0(z - z_1)^{i_1} \cdots (z - z_n)^{i_n},$$

missä  $z_0 \in \kappa \setminus \{0\}$  ja  $z_1, \dots, z_n \in \kappa$  ovat polynomien  $f$  toisistaan eroavia juuria, niin tällöin

$$n_{0,k-1}(f) = \lim_{r \rightarrow \infty} \frac{N_{k-1}(r, \frac{1}{f})}{\log r} = \sum_{v=1}^n \min\{i_v, k\}.$$

Huomautusten 5.4.12 ja 5.4.14 nojalla Lauseesta 5.4.13 saadaan suorana seurauksena seuraava polynomilause [30]:

**Seuraus 5.4.15.** *Olkoon  $\kappa$  algebrallisesti suljettu kunta, jonka karakteristika on nolla ja joka on kokonainen epätriviaalin ei-Arkhimedisen itseisarvon suhteen. Olkoot  $f_j \in \kappa$ ,  $j = 0, 1, \dots, k$ , polynomeja, joilla ei ole yhteisiä nollakohtia ja joille*

$$f_0 + f_1 + \cdots + f_k = 0.$$

*Tällöin*

$$\max_{0 \leq j \leq k} \{ \deg(f_j) \} \leq \sum_{i=0}^k n_{0,k-1}(f_i) - \frac{k(k-1)}{2}.$$

**Huomautus 5.4.16.** Arvolla  $k = 2$  Seuraus 5.4.15 redusoituu Mason-Stothersin lauseeksi.

**Huomautus 5.4.17.** Lausetta 5.4.13 kokonaislukujen tilanteeseen soveltamalla saadaan myös hieman erilainen yleistys *Abc*-konjektuurista (Konjektuuri 5.2.8). Tässäkin tapauksessa arvolla  $k = 2$  konjektuuri redusoituu alkuperäiseen tilanteeseen.

*Abc*-konjektuurin versioissa meromorffifunktiolle on mukana poikkeuksetta logaritmisia termejä. Herääkin kysymys, voidaanko alkuperäiseen *Abc*-konjektuuriin lisätä vastaavanlaisia termejä kokonaislukujen ja meromorffifunktioiden matemaattisten struktuurien yhtenäistämiseksi. Tiedetään ehdon  $\text{rad}(abc) < c$  toteuttavia *abc*-osumia olevan äärettömästi, mutta voidaanko ehtoa vielä tiukentaa logaritminen termi lisäämällä, esimerkiksi

$$\text{rad}(abc) < \frac{c}{\log c},$$

ja saada silti ääretön määrä ehdon toteuttavia *abc*-kolmikoita? Vastaus ainakin kyseiseen esimerkkiin on myönteinen ja sitä on tarkasteltu syvemmin alaluvussa 3.7.

## 6 Yhteenveto

Vuonna 1985 Joseph Oesterlé ja David Masser esittivät  $Abc$ -konjektuurin pohjaten Szpiron elliptisille käyrille esittämään konjektuuriin sekä Masonin ja Stothersin polynomeille todistamaan lauseeseen tarkoituksenaan kehittää uusi työkalu Fermat'n suuren lauseen todistamiseen. Se onkin osoittautunut erittäin käyttökelpoiseksi niin Diophantoksen yhtälöiden ja epäyhtälöiden kuin myös elliptisten käyrien teoriassa. Yleisessä muodossa  $Abc$ -konjektuuri voidaan esittää seuraavasti:

**$Abc$ -konjektuuri.** *Jokaista reaalilukua  $\varepsilon > 0$  kohden on olemassa reaaliluku  $C(\varepsilon) > 0$  siten, että kaikilla kolmikoilla  $(a, b, c) \in \mathbb{Z}^3$ , joilla  $a + b = c$ ,  $abc \neq 0$  ja  $\text{syt}(a, b, c) = 1$ , on voimassa epäyhtälö*

$$\max \{|a|, |b|, |c|\} \leq C(\varepsilon) \text{rad}(abc)^{1+\varepsilon},$$

missä  $\text{rad}(abc)$  tarkoittaa tulon  $abc$  alkutekijöiden tuloa.

$Abc$ -konjektuurin formulaatio on paras mahdollinen tai ainakin hyvin lähellä sitä, sillä se ei ole totta ilman lukua  $\varepsilon > 0$ . Luku  $C(\varepsilon)$  sen sijaan voitaneen jättää pois, mikäli tämä huomioidaan radikaalin eksponentissa  $1 + \varepsilon$ . Lukujen  $\varepsilon$  ja  $C(\varepsilon)$  välillä onkin eräänlainen käänteinen suhde, sillä  $C(\varepsilon) \rightarrow \infty$ , kun  $\varepsilon \rightarrow 0$ . Vakiolta  $C(\varepsilon)$  ei vaadita efektiivistä laskettavuutta, joten sen poisjättäminen mahdollistaisi eksplisiittisten tulosten saamisen. Rajoituttaessa tarkastelemaan asymptoottista "vain äärellisen ratkaisujoukon olemassaoloa" tämä ei kuitenkaan ole ongelma.

Konjektuuria voidaan tarkastella myös keskittymällä pelkästään sen oletukset toteuttaviin positiivisiin  $abc$ -kolmikiin, joilla  $0 < a < b < c$ . Ehdon  $\text{rad}(abc) < c$  toteuttavia  $abc$ -kolmikoita, ns.  $abc$ -osumia, on ääretön määrä kuten myös tiukemman ehdon

$$\text{rad}(abc) < \frac{c}{\log c}$$

toteuttavia ns. *logaritmisia  $abc$ -osumia*, joita ei kirjallisuudessa aiemmin ole esiintynyt. Kasaantumispisteisiin liittyvien menetelmien käytön tarkastelussa mahdollistaa  $abc$ -osumista muodostetut osamäärät eli ns.  $L$ -arvot,

$$L(a, b, c) = \frac{\log c}{\log \text{rad}(abc)}.$$

$Abc$ -konjektuurin monet esitysmuodot perustuvat erilaisiin lähestymistapoihin ymmärtää tai soveltaa otaksumaa. Luonnolliset yleistykset liittyvät konjektuurin väitteen jalostamiseen, tarkasteltavien kokonaislukujen jaollisuuteen tai lukumäärään sekä Stothers-Masonin polynomilauseen pohjalta kehitelyihin  $Abc$ -konjektuurin funktioversioihin.

Tässä tutkielmassa käsitellään  $Abc$ -konjektuuria lähinnä lukuteorian näkökulmasta. Tavoitteena on antaa laaja kuva konjektuurin taustalla olevista matemaattisista rakenteista sekä esittää perusteellinen katsaus kuluneen vajaan 30 vuoden aikana julkaistusta tuloksista.  $Abc$ -osumien etsimiseen liittyviä algoritmeja ei ole aiemmin kirjallisuudessa esiintymättömiä logaritmisia  $abc$ -osumia (liite F) lukuunottamatta tässä yhteydessä käsitelty, vaikka niihin perustuvaa taulukkotietoa onkin esitetty liitteissä A, B, C, D ja E. Kirjoitushetkellä  $Abc$ -konjektuurin todenperäisyys on vieläkin tuntematon.



## Viitteet

- [1] Apostol T. M. *Introduction to Analytic Number Theory*. Springer-Verlag New York Inc., New York, 1976
- [2] Baker A. *Logarithmic forms and the abc-conjecture*. Number Theory: diophantine, computational and algebraic aspects: proceedings of the international conference held in Eger, Hungary, July 29-August 2, s. 37–44, de Gruyter, Berliini, 1998
- [3] Ball P. *Proof claimed for deep connection between primes*. WWW-dokumentti (haettu 16.10.2012). url: <http://www.nature.com/news/proof-claimed-for-deep-connection-between-primes-1.11378>
- [4] Bombieri E., Gubler W. *Heights in Diophantine Geometry*. Cambridge University Press, New York, 2006
- [5] Berndt B. C., Galway W. F. *On the Brocard-Ramanujan Diophantine Equation  $n!+1 = m^2$* . Ramanujan J. 4, No. 1 (2000), s. 41–42
- [6] Browkin J., Brzeziński J. *Some remarks on the abc-conjecture*. Math. Comp. 62, No. 206 (1994), s. 931–939
- [7] Browkin J., Filaseta M., Greaves G., Schinzel A. *Squarefree values of polynomials and the abc conjecture*. Sieve Methods, Exponential Sums, and their Applications in Number Theory, s. 65–85, Cambridge University Press, Cambridge, 1997
- [8] Browkin J. *The abc-conjecture*. Number theory, s. 75–105, Trends Math., Birkhäuser, Basel, 2000
- [9] Cassels J. W. S. *An Introduction to the Geometry of Numbers, reprint of the 1971 edition*. Springer-Verlag, Berliini, 1997
- [10] Cherry W., Ye Z. *Nevanlinna's Theory of Value Distribution*. Springer-Verlag, Berliini, 2001
- [11] Cherry W., Ye Z. *Non-Archimedean Nevanlinna theory in several variables and the non-Archimedean Nevanlinna inverse problem*. Trans. Amer. Math. Soc. 349, No. 12 (1997) s. 5043–5071
- [12] Cochrane T., Dressler R. E. *Gaps between integers with the same prime factors*. Math. Comp. 68, No. 225 (1999), s. 395–401
- [13] Dabrowski A. *On the Diophantine equation  $x! + A = y^2$* . Nieuw Arch. Wisk. (4) 14, No. 3 (1996), s. 321–324
- [14] Dahmen S. R. *Lower bounds for numbers of ABC-hits*. Journal of Number Theory 128 (2008), s. 1864–1873
- [15] Darmon H., Granville A. *On the equations  $z^m = F(x, y)$  and  $Ax^p + By^q = Cz^r$* . Bull. London Math. Soc. 27, No. 6 (1995), s. 513–543

- [16] Edwards H. M. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory*. Springer-Verlag, New York, 1977
- [17] Ellenberg J. S. *Congruence ABC implies ABC*. Indag. Math. (N.S.) 11, No. 2 (2000), s. 197–200
- [18] Filaseta M., Konyagin S. *On a limit point associated with the abc-conjecture*. Colloq. Math. 76 (1998), No. 2, s. 265–268
- [19] Fraleigh J. B. *A first course in abstract algebra*. Addison-Wesley Publishing Company, New York, 2003
- [20] van Frankenhuysen M. *A Lower Bound in the abc Conjecture*. J. Number Theory 82 (2000), No. 1, s. 91–95
- [21] van Frankenhuysen M. *The ABC conjecture implies Roth's Theorem and Mordell's conjecture*. Mat. Contemp. 16 (1999), s. 45–72
- [22] Geuze G., de Smit B. *Reken mee met ABC*. Nieuw Archief voor Wiskunde Part 8, No. 1 (2007), s. 26–30
- [23] Goldfeld D. *Beyond the Last Theorem*. The Sciences, March/April (1996), s. 34–40
- [24] Granville A., Tucker T. *It's as easy as abc*. Notices Amer. Math. Soc. 49, No. 10 (2002), s. 1224–1231
- [25] Granville A., Stark H. *ABC implies no "Siegel zeros" for L-functions of characters with negative discriminant*. Invent. Math. 139, No. 3 (2000), s. 509–523
- [26] Greaves G., Nitaj A. *Some polynomial identities related to the abc-conjecture*. Number theory in progress. Proceedings of the international conference organized by the Stefan Banach International Mathematical Center in honor of the 60th birthday of Andrzej Schinzel, Zakopane, Poland, June 30–July 9, 1997. Volume 1: Diophantine problems and polynomials, s. 229–236. de Gruyter, Berlin, 1999
- [27] Guy R. K. *Unsolved Problems in Number Theory, Second Edition*. Springer Verlag New York Inc., Yhdysvallat, 1994
- [28] Hardy G. H., Wright E. M. *Introduction to the Theory of Numbers, Sixth Edition*. Oxford University Press Inc., Norfolk, 2008
- [29] Hu P.-C., Yang C.-C. *The abc conjecture over function fields*. Proc. Japan Acad. Ser. A Math. Sci 76, No. 7 (2000), s. 118–120
- [30] Hu P.-C., Yang C.-C. *A generalized abc-Conjecture over Function Fields*. Journal of Number Theory, 94 (2002), s. 286–298
- [31] Ingham A. E. *The Distribution of Prime Numbers*. Stechert-Hafner Service Agency Inc., New York, 1964
- [32] Jones G. A., Jones J. M. *Elementary Number Theory*. Springer-Verlag, Lontoo, 2005

- [33] Knapp A. W. *Advanced Algebra*. Birkhäuser Boston ja Springer Science+Business Media LLC, New York, 2007
- [34] Knauer J., Richstein J. *The Continuing Search for Wieferich Primes*. Math. Comp. 74, No. 251 (2005), s. 1559–1563
- [35] Lama V. *Mason-Stothers Theorem and the ABC Conjecture*. WWW-dokumentti (haettu 25.12.2012). url: <http://topologicalmusings.wordpress.com/2008/03/03/mason-stothers-theorem-and-the-abc-conjecture/>
- [36] Lang S. *Old and New Conjectured Diophantine Equations*. Bull. Amer. Math. Soc. 23, No. 1 (1990), s. 37–75
- [37] Lang S. *Undergraduate Algebra, Third Edition*. Springer Science+Business Media Inc., Yhdysvallat, 2005
- [38] Latvala V. *Lukuteoria*. Luentomoniste, Itä-Suomen yliopisto, 2010
- [39] Luca F. *On a conjecture of Erdős and Stewart*. Math. Comp. 70, No. 234 (2001), s. 893–896
- [40] Mathematical Institute of Leiden University. *ABC@Home*. Haettu 5.3.2013 url: <http://abcathome.com/>
- [41] Mihăilescu P. *Primary cyclotomic units and a proof of Catalan’s conjecture*. J. Reine Angew. Math. 572 (2004), s. 167–195
- [42] Mordell L. J. *Diophantine Equations*. Academic Press Inc., Lontoo, 1969
- [43] Nathanson M. B. *Elementary Methods in Number Theory*. Springer-Verlag New York Inc., New York, 2000
- [44] Nitaj A. *Aspects expérimentaux de la conjecture abc*. Séminaire de Théorie des Nombres de Paris, London Math. Soc. Lecture Note Ser. 235 s. 145–156, Cambridge Univ. Press, Cambridge, 1996
- [45] Nitaj A. *On a conjecture of Erdős on 3-powerful numbers*. Bull. London Math. Soc. 27, No. 4 (1995), s. 317–318
- [46] Nitaj A. *Conséquences et aspects expérimentaux des conjectures abc et de Szpiro*. Ph.D. Thesis, University of Caen, 1994
- [47] Nitaj A. *La conjecture abc*. Enseign. Math. (2) 46, No. 1-2 (1996), s. 3–24
- [48] Nitaj A. *The abc conjecture*. WWW-dokumentti (haettu 25.12.2013). url: <http://www.math.unicaen.fr/~nitaj/abc.html>
- [49] Oesterlé J. *Nouvelles approches du “theoreme” de Fermat*. Séminaire N. Bourbaki, Vol. 1987–88. Astérisque No. 161–162 (1988), Exp. No. 694, 4, s. 165–186

- [50] Overholt M. *The Diophantine Equation  $n! + 1 = m^2$* . Bull. Lond. Math. Soc. 25, No. 2 (1993), s. 104
- [51] van der Poorten A. J. *Effectively computable bounds for the solutions of certain diophantine equations*. Acta Arith. 33 (1977), no. 3, s. 195–207
- [52] Ribenboim P. *Remarks on exponential congruences and powerful numbers*. J. Number Theory 29, No. 3 (1988), s. 251–263
- [53] Riesel H. *Prime Numbers and Computer Methods for Factorization, Second Edition*. Birkhäuser, Boston, 1994
- [54] Rosen K. H. *Elementary Number Theory and Its Applications*. Addison-Wesley Publishing Company, Yhdysvallat, 1986
- [55] Ross S. M. *A First Course in Probability*. Prentice-Hall Inc., Yhdysvallat, 1998
- [56] Saari K. *ABC-otaksuma*. Pro gradu -tutkielma, Turun yliopisto, 2003
- [57] Schmidt W. *Diophantine Approximations and Diophantine Equations (Lecture Notes in Mathematics)*. Springer-Verlag Berlin Heidelberg, Saksa, 1991
- [58] Shorey T. N., Tijdeman R. *Exponential Diophantine Equations*. Cambridge University Press, Cambridge, 1986
- [59] Silverman J. H. *The Arithmetic of Elliptic Curves, Second Edition*. Springer Science+Business Media, New York, 2009
- [60] Silverman J. H. *Wieferich's criterion and the abc-conjecture*. J. Number Theory 30, No. 2 (1988), s. 226–237
- [61] de Smit B. *Bart de Smit - ABC triples*. WWW-dokumentti (haettu 25.12.2013).  
url: <http://www.math.leidenuniv.nl/~desmit/abc/index.php?sort=1>
- [62] Stewart C. L., Yu K. *On the abc-conjecture*. Math. Ann. 291, No. 2 (1991), s. 225–230
- [63] Stewart C. L., Yu K. *On the abc-conjecture. II*. Duke Math. J 108, No. 1 (2001), s. 161–181
- [64] Stewart C. L., Tijdeman R. *On the Osterlé-Masser Conjecture*. Monatsh. Math 102, No. 3 (1986), s. 251–257
- [65] Tignol J.-P. *Galois' Theory of Algebraic Equations*. World Scientific Publishing Co. Pte. Ltd, Singapore, 2002
- [66] Trench W. F. *Introduction to real analysis*. Prentice Hall/Pearson Education, 2003
- [67] Vaserstein L. N. *Quantum (abc)-Theorems*. J. Number Theory 81, No. 2 (2000), s. 351–358
- [68] Vojta P. *Diophantine Approximations and Value Distribution Theory*. Springer-Verlag, Berliini, 1987

- [69] Waldschmidt M. *Nombres Transcendants*. Lecture Notes in Mathematics, Springer-Verlag Berlin, Heidelberg, 1974
- [70] Wiles A. *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) 141, No. 3 (1995), s. 443–551
- [71] Wheeler J. P. *The abc conjecture*. Master's Thesis, University of Tennessee, Knoxville, 2002
- [72] Woit P. *Latest on abc*. WWW-dokumentti (haettu 4.3.2014).  
url: <https://www.math.columbia.edu/~woit/wordpress/?p=6514>
- [73] Woods A. L. *Some problems in logic and number theory, and their connections*. Ph.D. thesis, University of Manchester, 1981. WWW-dokumentti (haettu 25.12.2012).  
url: <http://school.maths.uwa.edu.au/~woods/thesis/WoodsPhDThesis.pdf>

## A 50 laadultaan parasta $abc$ -kolmikkaa

$abc$ -kolmikon  $(a, b, c) \in \mathbb{N}^3$  laatu [8, s. 77] määritellään lukuna

$$L = L(a, b, c) = \frac{\log c}{\log \operatorname{rad}(abc)}.$$

$abc$ -kolmikko on laadultaan *hyvä*, mikäli  $L > 1,4$  [47, s. 18]. Nykyään tunnetaan 236 laadultaan hyvää  $abc$ -kolmikkaa, joista 50 parasta on esitetty alla [61].

No.	L	$a$	$b$	$c$	löytäjä	vuosi
1	1.6299	2	$3^{10}109$	$23^5$	ER	1987
2	1.6260	$11^2$	$3^{25}67^3$	$2^{21}23$	BdW	1985
3	1.6235	$19 \cdot 1307$	$7 \cdot 29^2 31^8$	$2^8 3^{22} 5^4$	JB JB	1994
4	1.5808	283	$5^{11}13^2$	$2^8 3^8 17^3$	JB JB AN	1993
5	1.5679	1	$2 \cdot 3^7$	$5^4 7$	BdW	1988
6	1.5471	$7^3$	$3^{10}$	$2^{11}29$	BdW	1988
7	1.5444	$7^2 41^2 311^3$	$11^{16}13^2 79$	$2 \cdot 3^3 5^{23} 953$	AN	1993
8	1.5367	$5^3$	$2^9 3^{17} 13^2$	$11^5 17 \cdot 31^3 137$	HtR PM	
9	1.5270	$13 \cdot 19^6$	$2^{30} 5$	$3^{13} 11^2 31$	AN	1993
10	1.5222	$3^{18} 23 \cdot 2269$	$17^3 29 \cdot 31^8$	$2^{10} 5^2 7^{15}$	AN	1993
11	1.5094	$13^{10} 37^2$	$3^7 19^5 71^4 223$	$2^{26} 5^{12} 1873$	TD	2003
12	1.5033	$2^7 23^8$	$19^9 857^2$	$3^{22} 13 \cdot 47^2 263$	TS MH	
13	1.5028	239	$5^8 17^3$	$2^{10} 37^4$	JB JB AN	1993
14	1.4976	$5^2 7937$	$7^{13}$	$2^{18} 3^7 13^2$	BdW	1988
15	1.4924	$2^{21} 11$	$3^2 13^{10} 17 \cdot 151 \cdot 4423$	$5^9 139^6$	AN	1993
16	1.4916	73	$2^{13} 7^7 941^2$	$3^{16} 103^3 127$	AN	1993
17	1.4892	$2^{24}$	$11^7 19 \cdot 29^2$	$3^{11} 5^3 7^3 41$	AN	1993
18	1.4889	$11^2$	$3^9 13$	$2^{11} 5^3$	BdW	1988
19	1.4829	37	$2^{15}$	$3^8 5$	BdW	1988
20	1.4813	$5^{14} 19$	$2^5 3 \cdot 7^{13}$	$11^7 37^2 353$	AN	1993
21	1.4805	$5^{22} 79 \cdot 45949$	$3^2 13^{18} 61^3$	$2^{23} 17^4 251^2 1733^3$	FR	2010
22	1.4744	1	$3^{16} 7$	$2^3 11 \cdot 23 \cdot 53^3$	AN	1993
23	1.4741	$7^2$	$2^{10} 11 \cdot 53^2$	$3^4 5^8$	JB JB AN	1993
24	1.4713	$3^4 199$	$11^8$	$2^3 5^7 7^3$	JB JB AN	1993
25	1.4657	$17^4 67$	$2^{19} 137^4$	$3^{15} 5^3 13 \cdot 89^2$	HtR PM	
26	1.4655	$7^{12}$	$2^{14} 67^3 461$	$3^{13} 11 \cdot 19^4$	AN	1993
27	1.4646	$5^2 23^{10} 106531$	$7^{11} 11^3 193^4$	$2^4 3^{19} 17^8 29$	FR	2007
28	1.4619	$2^7 5^2$	$7^6 41$	$13^6$	BdW	1988
29	1.4606	$7 \cdot 167 \cdot 811^4 919$	$3^4 13^2 23^{12} 67^4$	$2^3 15^3 11^2 17^5 107^4$	IC	2010
30	1.4594	$5^{11} 31 \cdot 191$	$2^8 7^{13} 89 \cdot 859^2$	$3^{30} 13^4 277$	KV	

No.	L	$a$	$b$	$c$	löytäjä	vuosi
31	1.4578	$5^{12}17^231^21699$	$23^{14}29$	$2^{19}3^{211} \cdot 13^{10}47$	AN	1993
32	1.4578	$3^65^{12}$	$2^{16}13 \cdot 59^4$	$7^{11}47 \cdot 113$	AN	1993
33	1.4575	$3 \cdot 109 \cdot 131^4$	$5^{22}89$	$2^311^219^597^4$	TS	
34	1.4571	$3^25^2$	$2^417^331^4$	$7^{10}257$	AN	1993
35	1.4562	$2^{25}19$	$3 \cdot 5^{15}1033$	$11^713^347^2$	AN	1993
36	1.4557	1	$2^53 \cdot 5^2$	$7^4$	BdW	1988
37	1.4551	$3^211^6$	$2^{35}$	$19^513883$	JB JB	1994
38	1.4550	$23^231^5$	$2^{25}7 \cdot 109^3$	$3^{19}5^219^229$	TS	
39	1.4544	$7^82707$	$2^{10}5^{10}29^3$	$3^{18}11^443$	TS AR	
40	1.4533	$13^6$	$2 \cdot 3^47^411^923$	$5^7103^42399$	AN	1993
41	1.4532	$7^523^2101^4$	$2^{43}359^2$	$3^913 \cdot 19^6307^2$	TS MH	
42	1.4526	$2^{19}13 \cdot 103$	$7^{11}$	$3^{11}5^311^2$	BdW	1988
43	1.4520	$2^{20}233^5$	$37 \cdot 59^84729^2$	$3^{24}5^619 \cdot 23 \cdot 251^2$	FR	2010
44	1.4519	$31^361^5$	$17^{10}83^22719 \cdot 15101$	$2 \cdot 3^35^{17}7^{12}$	FR	2007
45	1.4513	$3^57$	$5^667$	$2^{20}$	JB JB AN	1993
46	1.4509	$3^57^3$	$2^{13}23^359$	$5^319^6$	JB JB	1994
47	1.4502	$23^837^4$	$2^{28}3^711^419^361 \cdot 127 \cdot 173^2$	$5^{18}17^443^24817^2$	IC	2008
48	1.4501	$23^353^63167^2$	$2^83^{29}11399^2$	$5^77^413^{12}523$	FR	2008
49	1.4500	1	$3^35^37^23$	$2^{13}11^413 \cdot 41$	AN	1993
50	1.4497	1	$3 \cdot 5^547^2$	$2^{18}79$	GF	

#### Löytäjien lyhenteet

- AN : Abderrahmane Nitaj  
 AR : Andrej Rosenheinrich  
 BdW : Benne de Weger  
 ER : Eric Reyssat  
 FR : Frank Rubin  
 GF : Gerhard Frey  
 HtR : Herman te Riele  
 IC : Ismael Jiménez Calvo  
 JB JB : Jerzy Browkin, Juliusz Brzezinski  
 KV : Kees Visser  
 MH : Mathias Hegner  
 PM : Peter Montgomery  
 TD : Tim Dokchitser  
 TS : Traugott Schulmeiss

## B 50 laadultaan parasta $abc$ -Szpiro-kolmikka

Szpiiron konjektuurin innoittamana voidaan tarkastella  $abc$ -kolmikon  $(a, b, c) \in \mathbb{N}^3$  Szpiro-laatua [46, s. 8], joka määritellään lukuna

$$\rho = \rho(a, b, c) = \frac{\log |abc|}{\log \text{rad}(abc)}.$$

$Abc$ -kolmikko on Szpiro-laadultaan *hyvä*, mikäli  $\rho > 4$ . Alla on esitetty uudemman tiedon puutteessa 50 parasta vuonna 2003 tunnettua hyvää  $abc$ -Szpiro-kolmikka [48], [44].

No.	$\rho$	$a$	$b$	$c$	löytäjä	vuosi
1	4.41901	$13 \cdot 19^6$	$2^{30}5$	$3^{13}11^231$	AN	1992
2	4.26801	$2^511^219^9$	$5^{15}37^247$	$3^77^{11}743$	AN	1994
3	4.24789	$2^{19}13 \cdot 103$	$7^{11}$	$3^{11}5^311^2$	BdW	1985
4	4.23181	$19^843^4149^2$	$2^{15}5^{23}101$	$3^{13}13 \cdot 29^237^6911$	TD	2003
5	4.23069	$2^{35}7^217^219$	$3^{27}107^2$	$5^{15}37^22311$	AN	1994
6	4.22979	$3^{18}23 \cdot 2269$	$17^329 \cdot 31^8$	$2^{10}5^27^{15}$	AN	1994
7	4.22960	$17^479^3211$	$2^{29}23 \cdot 29^2$	$5^{19}$	AN	1994
8	4.22532	$5^{14}19$	$2^53 \cdot 7^{13}$	$11^737^2353$	AN	1994
9	4.21019	$2^75^47^{22}$	$19^437 \cdot 47^453^6$	$3^{14}11 \cdot 13^9191 \cdot 7829$	TD	2003
10	4.20094	$3^{21}$	$7^211^6199$	$2 \cdot 13^817$	AN	1992
11	4.17428	$3^65^{12}$	$2^{16}13 \cdot 59^4$	$7^{11}47 \cdot 113$	AN	
12	4.17088	$3^{16}23^2$	$2^{13}29^237^3$	$5^911^413$	AN	
13	4.16452	$5^{14}11$	$3^67^513^2 \cdot 251$	$2^{21}23^4$	AN	
14	4.14980	$2^{17}3^{19}11 \cdot 25867$	$7^{12}23^7$	$5 \cdot 37^{10}53 \cdot 71$	TD	2003
15	4.14883	$5^{18}6359$	$3^247^673^3$	$2^719^{10}79$	AN	1994
16	4.13636	$7^813 \cdot 89^3$	$3^{13}5^311^41499$	$2 \cdot 19^{12}$	TD	2003
17	4.13152	$2^723^8$	$19^9857^2$	$3^{22}13 \cdot 47^2263$	MH TS	
18	4.13000	$11^331^5101 \cdot 479$	$107^8$	$2^313^45^67$	AN	1994
19	4.12727	$5^{12}17^231^21699$	$23^{14}29$	$2^{19}3^{211} \cdot 13^{10}47$	AN	
20	4.12465	$13^{10}37^2$	$3^719^571^4223$	$2^{26}5^{12}1873$	TD	2003
21	4.12366	$3 \cdot 5^913^279^3239^291249$	$7^{29}$	$2^{65}37 \cdot 41 \cdot 103$	AN	
22	4.10907	$2^{55}23$	$3^{13}7^913 \cdot 79^2$	$11^443^665353$	TD	2003
23	4.10809	$11^813^953$	$2^45^{16}17 \cdot 547 \cdot 6163$	$7^619^{12}$	TD	2003
24	4.10757	$7 \cdot 11^643$	$3^{11}5^4$	$2^{17}17^343$	GX	1986
25	4.10590	$233^4439$	$2^{15}3^{19}$	$5^817^571$	TD	2003
26	4.10470	$2^{13}71^2337^3$	$7^{13}1117^2$	$3^{21}13^373^2$	TD	2003
27	4.10410	$3 \cdot 5^{14}199$	$7^211^517^441$	$2^{30}13^4$	AN	
28	4.10116	$5^723^71493$	$31^83907^2$	$2^{52}3^2331$	TD	2003
29	4.09700	$3^65^{11}41$	$2^97^9283$	$13^{10}53$	AN	1994
30	4.09655	$2^{16}41 \cdot 71$	$3^{15}7^2$	$19^7$	AN	1993



No.	$\rho$	$a$	$b$	$c$	löytäjä	vuosi
31	4.09647	$3^{12}5^6$	$7^931^2$	$2^911^5571$	AN	1992
32	4.09080	$7^819$	$2^{15}5^237^2$	$3 \cdot 17^7$	AN	1992
33	4.08545	$2^65^27^{13}13^2463$	$3^443^{12}$	$11^{12}389^26841$	AN	
34	4.08362	$2^{13}5^{12}13^429$	$7^{16}19 \cdot 7451$	$3^{20}11^4353^2$	TD	2003
35	4.08331	$79^5677$	$2^{42}$	$3^{12}7 \cdot 13^461$	AN	1994
36	4.08299	$11^{11}73^2991 \cdot 306083$	$2^23 \cdot 5^{11}7^{15}19^2$	$13^{15}31^5$	TD	2003
37	4.08262	$2 \cdot 5^911^441^253^3$	$3^97^{16}37$	$23^{11}40423$	TD	2003
38	4.07920	$31 \cdot 59^6$	$2^{25}3^{11}$	$5^311^713 \cdot 229$	TD	2003
39	4.07709	$5^{18}8837$	$7^919^379 \cdot 191^2$	$2^{22}3^513^8$	AN	
40	4.07457	$3^{13}13 \cdot 23^397^2$	$2^{37}157^2$	$5^531^767$	TD	2003
41	4.07337	$3^273^{10}$	$5^{25}17^223$	$2^{27}11827^2373357$	TD	2003
42	4.07114	$2^{24}3^5$	$5 \cdot 19^559^2$	$7^{10}167$	AN	1992
43	4.07038	$19 \cdot 47 \cdot 71^6$	$5^37^329^{11}$	$3^{35}23^3$	AN	1994
44	4.06886	$3^45^{18}71 \cdot 419 \cdot 876581$	$2^{17}13^219^{15}$	$7^611^{12}977^3$	TD	2003
45	4.06705	$2^{26}11^47639$	$5^623^{11}$	$3^{18}47^47879$	TD	2003
46	4.06668	$5^{16}19^2$	$3^87^389^4$	$2^{28}11^26043$	TD	2003
47	4.06406	$7^329^5151^2$	$2^45^{16}97 \cdot 919$	$3^{27}13^4$	AN	
48	4.06347	$19 \cdot 47 \cdot 71^6$	$3^{21}193^2$	$2^75^{12}127^2$	AN	1994
49	4.06231	$5^77^719^2107$	$2^{14}11^997$	$3^{10}23^731$	TD	2003
50	4.06160	$2^73 \cdot 821^5$	$13^{16}$	$5^{12}101^2324697$	TD	2003

#### Löytäjien lyhenteet

AN : Abderrahmane Nitaj  
 BdW : Benne de Weger  
 GX : Gang Xiao  
 MH TS : Mathias Hegner, Traugott Schulmeiss  
 TD : Tim Dokchitser

## C Abc-osumien lukumäärä

*Abc*-osumien ja alkulukujen lukumäärää kuvataan funktioilla  $N(X)$  ja  $\pi(X)$ ,

$$N(X) = |\{abc\text{-osuma } (a,b,c) \in \mathbb{N}^3 \mid c \leq X\}|$$

$$\pi(X) = |\{p \text{ alkuluku} \mid p \leq X\}|.$$

Alla olevassa taulukossa verrataan *abc*-osumien lukumäärää alkulukujen lukumäärään.<sup>2</sup>

$X$	$N(X)$	$\pi(X)$	$\pi(X)/N(X)$	$N(10X)/N(X)$
10	1	4	4	6
10 <sup>2</sup>	6	25	4,17	5,17
10 <sup>3</sup>	31	168	5,42	3,87
10 <sup>4</sup>	120	1229	10,24	3,48
10 <sup>5</sup>	418	9592	22,95	3,03
10 <sup>6</sup>	1268	78 498	61,91	2,76
10 <sup>7</sup>	3499	664 579	189,93	2,57
10 <sup>8</sup>	8987	5 761 455	641,09	2,48
10 <sup>9</sup>	22 316	50 847 534	2 278,52	2,32
10 <sup>10</sup>	51 677	455 052 512	8 805,71	2,26
10 <sup>11</sup>	116 978	4 118 054 813	35 203,67	2,16
10 <sup>12</sup>	252 856	37 607 912 018	148 732,53	2,09
10 <sup>13</sup>	528 275	346 065 536 839	655 085,96	2,04
10 <sup>14</sup>	1 075 319	3 204 941 750 802	2 980 456,73	1,98
10 <sup>15</sup>	2 131 671	29 844 570 422 669	14 000 551,88	1,93
10 <sup>16</sup>	4 119 410	279 238 341 033 925	67 786 003,59	1,89
10 <sup>17</sup>	7 801 334	2 623 557 157 654 233	336 295 966,52	1,86
10 <sup>18</sup>	14 482 065	24 739 954 287 740 860	1 708 316 755,09	

<sup>2</sup>Arvoilla  $X \leq 10^{12}$  on käytetty lähteitä [22] sekä [54, s. 48] vastaavasti, ja siitä eteenpäin on käytetty 26.12.2012 haettuja internetlähteitä [http://www.rekenmeemetabc.nl/Synthese\\_resultaten](http://www.rekenmeemetabc.nl/Synthese_resultaten) sekä <http://oeis.org/A006880> vastaavasti.

## D 31 ensimmäistä $abc$ -osumaa

Alla taulukoituna kaikki  $abc$ -kolmikot  $(a, b, c) \in \mathbb{N}^3$ , joilla  $\text{rad}(abc) < c \leq 1000$  [22].

No.	$a$	$b$	$c$	$\text{rad}(abc)$
1	1=1	8=2 <sup>3</sup>	9=3 <sup>2</sup>	6
2	5=5	27=3 <sup>3</sup>	32=2 <sup>5</sup>	30
3	1=1	48=2 <sup>4</sup> 3	49=7 <sup>2</sup>	42
4	1=1	63=3 <sup>2</sup> 7	64=2 <sup>6</sup>	42
5	1=1	80=2 <sup>4</sup> 5	81=3 <sup>4</sup>	30
6	32=2 <sup>5</sup>	49=7 <sup>2</sup>	81=3 <sup>4</sup>	42
7	4=2 <sup>2</sup>	121=11 <sup>2</sup>	125=5 <sup>3</sup>	110
8	3=3	125=5 <sup>3</sup>	128=2 <sup>7</sup>	30
9	1=1	224=2 <sup>5</sup> 7	225=3 <sup>2</sup> 5 <sup>2</sup>	210
10	1=1	242=2 · 11 <sup>2</sup>	243=3 <sup>5</sup>	66
11	2=2	243=3 <sup>5</sup>	245=5 · 7 <sup>2</sup>	210
12	7=7	243=3 <sup>5</sup>	250=2 · 5 <sup>3</sup>	210
13	13=13	243=3 <sup>5</sup>	256=2 <sup>8</sup>	78
14	81=3 <sup>4</sup>	175=5 <sup>2</sup> 7	256=2 <sup>8</sup>	210
15	1=1	288=2 <sup>5</sup> 3 <sup>2</sup>	289=17 <sup>2</sup>	102
16	100=2 <sup>2</sup> 5 <sup>2</sup>	243=3 <sup>5</sup>	343=7 <sup>3</sup>	210
17	32=2 <sup>5</sup>	343=7 <sup>3</sup>	375=3 · 5 <sup>3</sup>	210
18	5=5	507=3 · 13 <sup>2</sup>	512=2 <sup>9</sup>	390
19	169=13 <sup>2</sup>	343=7 <sup>3</sup>	512=2 <sup>9</sup>	182
20	1=1	512=2 <sup>9</sup>	513=3 <sup>3</sup> 19	114
21	27=3 <sup>3</sup>	512=2 <sup>9</sup>	539=7 <sup>2</sup> 11	462
22	1=1	624=2 <sup>4</sup> 3 · 13	625=5 <sup>4</sup>	390
23	49=7 <sup>2</sup>	576=2 <sup>6</sup> 3 <sup>2</sup>	625=5 <sup>4</sup>	210
24	81=3 <sup>4</sup>	544=2 <sup>5</sup> 17	625=5 <sup>4</sup>	510
25	1=1	675=3 <sup>3</sup> 5 <sup>2</sup>	676=2 <sup>2</sup> 13 <sup>2</sup>	390
26	1=1	728=2 <sup>3</sup> 7 · 13	729=3 <sup>6</sup>	546
27	25=5 <sup>2</sup>	704=2 <sup>6</sup> 11	729=3 <sup>6</sup>	330
28	104=2 <sup>3</sup> 13	625=5 <sup>4</sup>	729=3 <sup>6</sup>	390
29	200=2 <sup>3</sup> 5 <sup>2</sup>	529=23 <sup>2</sup>	729=3 <sup>6</sup>	690
30	1=1	960=2 <sup>6</sup> 3 · 5	961=31 <sup>2</sup>	930
31	343=7 <sup>3</sup>	625=5 <sup>4</sup>	968=2 <sup>3</sup> 11 <sup>2</sup>	770

## E 31 ensimmäistä logaritmista $abc$ -osumaa

Alla taulukoituna 31 ensimmäistä  $abc$ -kolmikkoa  $(a, b, c) \in \mathbb{N}^3$ , joille  $\text{rad}(abc) < \frac{c}{\log c}$ .

No.	$a$	$b$	$c$	$\text{rad}(abc)$	$\frac{c}{\log c}$
1	1=1	2400=2 <sup>5</sup> 3 · 5 <sup>2</sup>	2401=7 <sup>4</sup>	210	308,47
2	625=5 <sup>4</sup>	2048=2 <sup>11</sup>	2673=3 <sup>5</sup> 11	330	338,74
3	1=1	4374=2 · 3 <sup>7</sup>	4375=5 <sup>4</sup> 7	210	521,85
4	289=17 <sup>2</sup>	6272=2 <sup>7</sup> 7 <sup>2</sup>	6561=3 <sup>8</sup>	714	746,51
5	7=7	32761=181 <sup>2</sup>	32768=2 <sup>15</sup>	2534	3151,62
6	37=37	32768=2 <sup>15</sup>	32805=3 <sup>8</sup> 5	1110	3154,83
7	1=1	59048=2 <sup>3</sup> 11 <sup>2</sup> 61	59049=3 <sup>10</sup>	4026	5374,87
8	343=7 <sup>3</sup>	59049=3 <sup>10</sup>	59392=2 <sup>11</sup> 29	1218	5403,24
9	3=3	65533=13 · 71 <sup>2</sup>	65536=2 <sup>16</sup>	5538	5909,28
10	7168=2 <sup>10</sup> 7	78125=5 <sup>7</sup>	85293=3 <sup>8</sup> 13	2730	7512,26
11	128=2 <sup>7</sup>	109375=5 <sup>6</sup> 7	109503=3 <sup>2</sup> 23 <sup>3</sup>	4830	9436,90
12	81=3 <sup>4</sup>	123823=7 <sup>3</sup> 19 <sup>2</sup>	123904=2 <sup>10</sup> 11 <sup>2</sup>	8778	10565,47
13	12672=2 <sup>7</sup> 3 <sup>2</sup> 11	117649=7 <sup>6</sup>	130321=19 <sup>4</sup>	8778	11065,01
14	18225=3 <sup>6</sup> 5 <sup>2</sup>	112847=7 <sup>4</sup> 47	131072=2 <sup>17</sup>	9870	11123,35
15	81=3 <sup>4</sup>	134375=5 <sup>5</sup> 43	134456=2 <sup>3</sup> 7 <sup>5</sup>	9030	11385,90
16	17=17	140608=2 <sup>6</sup> 13 <sup>3</sup>	140625=3 <sup>2</sup> 5 <sup>6</sup>	6630	11863,23
17	12005=5 · 7 <sup>4</sup>	161051=11 <sup>5</sup>	173056=2 <sup>10</sup> 13 <sup>2</sup>	10010	14347,95
18	5=5	177147=3 <sup>11</sup>	177152=2 <sup>10</sup> 173	5190	14659,12
19	47=47	250000=2 <sup>4</sup> 5 <sup>6</sup>	250047=3 <sup>6</sup> 7 <sup>3</sup>	9870	20117,38
20	121=11 <sup>2</sup>	255879=3 <sup>9</sup> 13	256000=2 <sup>11</sup> 5 <sup>3</sup>	4290	20557,41
21	71875=5 <sup>5</sup> 23	190269=3 <sup>8</sup> 29	262144=2 <sup>18</sup>	20010	21010,77
22	3481=59 <sup>2</sup>	262144=2 <sup>18</sup>	265625=5 <sup>6</sup> 17	10030	21267,28
23	95=5 · 19	279841=23 <sup>4</sup>	279936=2 <sup>7</sup> 3 <sup>7</sup>	13110	22319,32
24	131072=2 <sup>17</sup>	221875=5 <sup>5</sup> 71	352947=3 · 7 <sup>6</sup>	14910	27629,95
25	338=2 · 13 <sup>2</sup>	390625=5 <sup>8</sup>	390963=3 · 19 <sup>4</sup>	7410	30362,83
26	24389=29 <sup>3</sup>	393216=2 <sup>17</sup> · 3	417605=5 · 17 <sup>4</sup>	14790	32266,70
27	1=1	512000=2 <sup>12</sup> 5 <sup>3</sup>	512001=3 <sup>5</sup> 7 <sup>2</sup> 43	9030	38947,04
28	49=7 <sup>2</sup>	531392=2 <sup>6</sup> 19 <sup>2</sup> 23	531441=3 <sup>12</sup>	18354	40311,54
29	533871=3 <sup>5</sup> 13 <sup>3</sup>	9583=7 · 37 <sup>2</sup>	524288=2 <sup>19</sup>	20202	40481,85
30	2197=13 <sup>3</sup>	583443=3 <sup>5</sup> · 7 <sup>4</sup>	585640=2 <sup>3</sup> 5 · 11 <sup>4</sup>	30030	44097,87
31	8192=2 <sup>13</sup>	634933=13 <sup>3</sup> 17 <sup>2</sup>	643125=3 · 5 <sup>4</sup> 7 <sup>3</sup>	46410	48087,37

## F Java-koodi logaritmisten *abc*-osumien etsimiseen

Ohessa ns. brute force -javakoodi, jolla Liitteen E logaritmisten *abc*-osumien taulukko laskettiin. Ohjelmalla luettiin haluttu määrä rivejä tiedostosta *triples\_below\_1018*, joka oli ladattu ABC@Home-projektin kotisivuilta [40]. Tiedostossa oli listattu kaikki *abc*-osumat, joille  $a < b < c < 10^{10}$ , siten, että yksi rivi sisälsi aina yhden osuman muodossa *c a*.

```
1 import java.io.*;
2 import java.io.PrintWriter;
3 import java.util.*;
4 /**
5  * To find abc-triples with rad<c/logc
6  * @author Marko Lamminsalo
7  */
8 public class abclogc {
9     private static Scanner lukija= new Scanner(System.in);
10    private static Scanner input;
11    private static double radical;
12    private static String tiednimi="triples_below_1018";
13    private static String ulostulo="abclogc_triples.txt";
14    private static String text;
15    private static double a;
16    private static double b;
17    private static double c;
18    private static int mones=0;
19    private static String turhake;
20
21    public static void main(String [] args) throws Exception,
22        FileNotFoundException{
23        PrintWriter output=new PrintWriter(ulostulo);
24
25        /* Testing primefactors ();
26        *
27        * System.out.print("Anna luku 1: ");
28        int luku1=Integer.parseInt(lueRivi());
29        int [] taulu=primefactors(luku1);
30        for (int j=0; j<taulu.length; j++){
31            System.out.print(taulu[j] + " ");
32        }
33        */
34
35
36        // Input abc triple
37        /*
38        System.out.print("a: ");
39        float a=Float.parseFloat(lueRivi());
40
41        System.out.print("b: ");
42        float b=Float.parseFloat(lueRivi());
43
44        float c=a+b;
```

```

45     float cee=c;
46     double lokki=c/(java.lang.Math.log(cee));
47
48     radical=rad(a, b, c);
49     System.out.printf("=====" + "\na:%10.0f"+ "\nb:%10.0f" +
50         "\nc:%10.0f"
51         + "\nrad %10.0f"+ "\nc/logc %10.6f", a, b, c,
52         radical, lokki);
53     if (radical < c){
54         System.out.println("\nAbc-hit!");
55     }
56     if (radical < lokki){
57         System.out.println("Mod abc-hit!");
58     }
59     System.out.println ();
60     */
61
62     //Luetaan tiedostosta:
63     if (tiednimi == null) {
64         System.out.println("Tiedoston_nimea_ei_asetettu.");
65     }
66
67     File file = new File(tiednimi);
68     if (file.exists() && file.isFile() && file.canRead() ) {
69         input = new Scanner(file);
70     } else {
71         System.out.println("Tiedostoa_" + tiednimi + "_ei_voi_lukea
72         .");
73     }
74
75     boolean otsikko=false;
76     //1268 on c < 10^6 asti
77     //51677 on c < 10^10 asti
78     //116978 on c < 10^11 asti
79     //14 482 059 kaikki c < 10^18
80     for (int j=0; j < 1000000 ; j++){
81
82         text=lueTiedRivi();
83         text=text.trim();
84         String [] osat = text.split("_");
85         c=Double.parseDouble(osat [0]);
86         a=Double.parseDouble(osat [1]);
87         b=c-a;
88
89         double lokki=c/(java.lang.Math.log(c));
90
91         radical=rad(a, b, c);
92
93         if(radical < lokki){
94             if(otsikko==false){
95                 output.printf("%-10s_" + "%12s="+"%-22s" + "%11s="+"%-19s
96                 " + "%12s="+"%-22s" + "%12s_"
97                 + "_%12s\n", "n(abc-hit)", "c", " fact(c)
98                 ", "a", " fact(a)", "b", " fact(b)", "

```

```

95         radical", "c/logc");
96     }
97     mones+=1;
98     turhake="" + mones + "(" + (j+1) + ")";
99     output.printf("%-10s" + "%12.0f="+"%-22s" + "%11.0f="+"
100         %-19s" + "%12.0f="+"%-22s" + "%12.0f"
101         + "%12.2f\n",turhake,c, printf(c),a,
102         printf(a),b, printf(b),radical,
103         lokki);
104     }
105 }
106 output.close();
107
108 /*
109 int lkm=0;
110 while (input.hasNext()){
111     input.nextLine();
112     lkm++;
113 }
114
115 input.close();
116
117 System.out.println(lkm);
118 */
119 //14 482 059 rivia
120
121
122
123 }
124
125 //tiedostosta luku
126
127
128 public static String lueTiedRivi() {
129     if (input == null) {
130         System.out.println("Avattava_tiedosto_ennen_lukua.");
131         return null;
132     }
133     if (input.hasNext()) {
134         String rivi = input.nextLine();
135         return rivi;
136     } else {
137         return null;
138     }
139 }
140
141
142 //muutakin kuin tiedostosta lukua
143
144 public static String lueRivi(){
145     String teksti = lukija.nextLine();

```

```

146         teksti=teksti.trim();
147         return teksti;
148     }
149
150     public static String printTaulu(double[] taulu, int[] potens){
151         StringBuilder uusi=new StringBuilder();
152         String filler;
153         String[] osat;
154         int k;
155         for (int j=0; j<taulu.length; j++){
156             filler=Double.toString(taulu[j]);
157             filler=filler.trim();
158             osat=filler.split("\\.");
159             uusi.append(osat[0]);
160             if (potens[j] >1){
161                 uusi.append("^");
162                 uusi.append(potens[j]);
163             }
164             uusi.append(".");
165         }
166         uusi.append("I");
167         String palaute=uusi.toString();
168         k = palaute.indexOf("I");
169         palaute=palaute.substring(0,k-1);
170         return palaute;
171     }
172
173
174
175     //rad, primefactors
176
177     public static double rad(double a, double b, double c){
178         double[] ataul=primefactors(a);
179         double[] btaul=primefactors(b);
180         double[] ctaul=primefactors(c);
181         double luku=1;
182
183         for (int j=0; j<ataul.length; j++){
184             luku *= ataul[j];
185         }
186         for (int j=0; j<btaul.length; j++){
187             if (luku % btaul[j] != 0){
188                 luku *= btaul[j];
189             }
190         }
191         for (int j=0; j<ctaul.length; j++){
192             if (luku % ctaul[j] != 0){
193                 luku *= ctaul[j];
194             }
195         }
196         return luku;
197
198
199     }
200

```



```

201     public static double[] primefactors(double n){
202         double[] temp=new double[100];
203         int koko=0;
204         boolean lisattu=false;
205         boolean prime=true;
206         for (double i = 2; i <= n; i++) {
207             while (n % i == 0) {
208                 prime=false;
209                 n/=i;
210                 if (lisattu==false){
211                     temp[koko]=i;
212                     koko++;
213                     lisattu=true;
214                 }
215             }
216             lisattu=false;
217         }
218         if (prime==true){
219             double[] prm={n};
220             return prm;
221         }else{
222             double[] prm= new double[koko];
223             System.arraycopy(temp, 0, prm, 0, koko);
224             return prm;
225         }
226     }
227
228     public static String printpf(double n){
229         double[] temp=new double[100];
230         int koko=0;
231         int potenssi=0;
232         int[] potenssit=new int[100];
233         boolean lisattu=false;
234         boolean prime=true;
235         String texto;
236         for (double i = 2; i <= n; i++) {
237             while (n % i == 0) {
238                 prime=false;
239                 n/=i;
240                 if (lisattu == true){
241                     potenssi++;
242                     potenssit[koko-1]=potenssi;
243                 }
244                 if (lisattu==false){
245                     temp[koko]=i;
246                     potenssi++;
247                     potenssit[koko]=potenssi;
248                     koko++;
249                     lisattu=true;
250                 }
251             }
252             }
253         lisattu=false;
254         potenssi=0;
255     }

```

```
256
257
258     if (prime==true){
259         double [] prm={n};
260         texto=printTaulu(prm, potenssit);
261     }else{
262         double [] prm= new double[koko];
263         System.arraycopy(temp, 0, prm, 0, koko);
264         texto= printTaulu(prm, potenssit);
265     }
266     return texto;
267 }
268 }
```