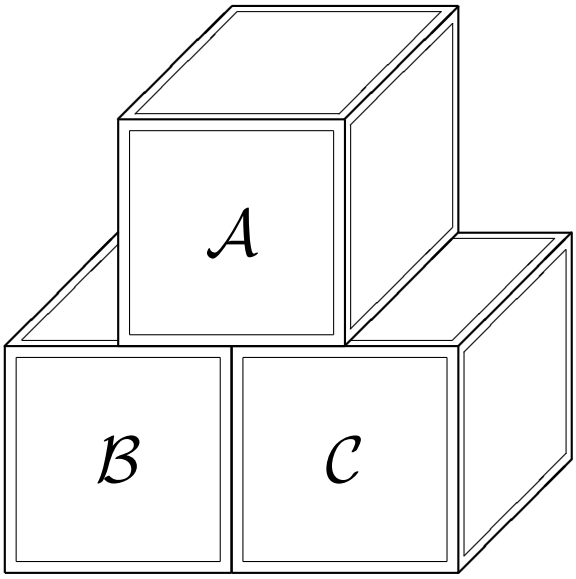
Abc-konjektuuri



Pro gradu -tutkielma
Marko Lamminsalo
180897
Itä-Suomen yliopisto
31. tammikuuta 2012

Sisältö

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 [1]

[1] Fermat'n alkuperäinen huomautus Diophantoksen Aritmetican marginaalissa [54]

1 Johdanto

Lukuteorialle tyypillisiä ovat ongelmat, jotka ovat helposti esittävissä mutta vaikeasti ratkaistavissa. Ongelmista kaikkein kuuluisin lienee edellisellä sivullakin esitetty 1630-luvulta [12, 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 nollasta eroavilla kokonaisluvuilla x, y, z ja $n \geq 3$. Fermat ei kuitenkaan esittänyt todistusta väittämälleen, sillä todistus "ei mahtunut kirjan marginaaliin" [12, s. 2], [54]. Vasta vuonna 1995 Andrew Wiles esitti lopullisen todistuksen väitteelle [54]. Fermat'n suurta lausetta on kuitenkin monta kertaa yritetty todistaa aiemmin, ja *Abc*-konjektuuri onkin eräs seuraus [3, s. 442]

Osoittautuu, että *Abc*-konjektuurin avulla voidaan todistaa monia kokonaislukuja koskevia syvällisiä tuloksia sekä lukuteorian tunnettuja konjektuureja. *Abc*-konjektuurilla on näytetty olevan useita mielenkiintoisia seurauksia erityisesti seuraavilla matematiikan osa-alueilla [7]:

a) Diophantoksen yhtälöt ja epäyhtälöt

b) Elliptiset käyrät

c) Polynomit

Tässä tutkielmassa tarkastellaan *Abc*-konjektuuria erityisesti kokonaislukujen kannalta, mutta myös elliptisiä kyriä ja polynomeja

Vaikka *Abc*-konjektuurin avulla ei voitukaan todistaa itse Ferma'n suurta lausetta, siitä oli suunnatonta hyötyä. Eräs David Hilbertin 1900-luvun alussa esittämistä ongelmista koski yleisen ratkuisun löytämistä mielivaltaiselle Diophantoksen yhtälölle. Vuonna 1970 Yuri Matiyasevich kuitenkin osoitti, ettei menetelmää yleisen ratkaisun löytämiseksi ole. Käytännössä tämä tarkoittaa suurta työmäärää, sillä jokainen yhtälö on ratkaistava erikseen. *Abc*-konjektuurin avulla voidaan kuitenkin esittää lukemattomia Diophantoksen yhtälöitä yhdellä tavalla. [19]

Abc-konjektuurin alkuperäinen formulointi kokonaisluvuille pohjautuu Stothersin (1981) ja Masonin (1983) todistamaan polynomilauseeseen. Lauseessa 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

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq \mathrm{n}_0(fgh) - 1,$$

missä $\mathrm{n}_0(fgh)$ ilmoittaa tulopolynomin fgh eri nollakohtien lukumäärän. Yllä olevan oivalluksen innoittamana Masser ja Oesterle esittivät vuonna 1985 vastaavan tuloksen kokonaisluvuille: Jokaista lukua $\varepsilon > 0$ kohti on olemassa luku $C(\varepsilon) > 0$ siten, että kaikilla nollasta eroavilla suhteellisilla alkuluvuilla a, b ja c, joilla pätee $a + b = c$, on voimassa epäyhtälö

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

missä $\text{rad}(abc)$ on tulon abc alkutekijöiden tulo. [27, ss. 165-171]

Konjektuuri voidaan esittää ekvivalentissa muodossa seuraavasti: Jokaista lukua $\varepsilon > 0$ kohti on olemassa korkeintaan äärellinen määrä suhteellisia alkulukuja a, b ja c, joilla $a + b = c$, siten, että on voimassa epäyhtälö

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

[35]
Tässä tutkielmassa tarkastellaan *Abc*-konjketuuria lukuteorian näkökulmasta. Luvussa 2 käydään läpi tärkeimmät jatkossa tarvittavat aputulokset. Luvussa 3 tarkastellaan *Abc*-konjketuuria ja siihen liittyviä tuloksia. Luvussa 4 osoitetaan monia *Abc*-konjektuurin seurauksia lukuteorian kannalta. Lopuksi luvussa 5 esitellään *Abc*-konjektuurin yleistyksiä. Luvun päätteeksi käydään vielä läpi *Abc*-konjektuurin vastine polynomien kunnassa, joka on vaikuttanut konjektuurin kehittymiseen.

1.1 Merkinnöistä

Tässä tutkielmassa käytetään seuraavia merkintöjä:

$$\begin{aligned}
\mathbb{N} &= \{1, 2, 3, \ldots\} \\
\mathbb{N}_{\geq k} &= \{k, k+1, k+2, \ldots\}, \text{ missä } k \in \mathbb{N} \\
\mathbb{Z} &= \{\ldots, -2, -1, 0, 1, 2, \ldots\} \\
\mathbb{Z}_{\geq 0} &= \mathbb{N} \cup \{0\} = \{0, 1, 2, 3, \ldots\} \\
\mathbb{Q} &= \left\{ \frac{m}{n} : m \in \mathbb{Z}, n \in \mathbb{N} \right\} \\
\mathbb{R}_{>0} &= \mathbb{R} \cap]0, \infty[
\end{aligned}$$

Lisäksi merkintä log tarkoittaa luonnollista (e-kantaista) logaritmia.

2 Peruskäsitteitä

Tässä kappaleessa tarkastellaan jatkossa tarvittavia aputuloksia. Luku on jaettu alalukuihin aihepiirien mukaisesti.

2.1 Jaollisuudesta ja kongruensseista

Tarkastellaan jaollisuuteen ja kongruenssiin liittyviä peruskäsitteitä. Alaluvun sisältö perustuu kirjaan [41].

Aloitetaan lukuteorian tarkastelu jaollisuuden ja suurimman yhteisen tekijän määrittelyillä.

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 $k \in \mathbb{Z}$.

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 $a_1, \ldots, a_n \in \mathbb{Z}$, joista ainakin yksi on nollasta eroava, suurin yhteinen tekijä $\operatorname{syt}(a_1, \ldots, a_n)$ on luku

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

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

$$\operatorname{syt}(a_1, \ldots, a_n) = \min\big(\mathbb{N} \cap \{x_1 a_1 + \cdots + x_n a_n : x_i \in \mathbb{Z}\}\big).$$

Seuraavan esimerkin tuloksia käytetään jatkossa ilman erillistä mainintaa.

Esimerkki 2.1.6. (i) Jos $n \in \mathbb{N}$, niin $\operatorname{syt}(n, n+1) = 1$. 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 $\operatorname{syt}(a, b) = 1$, niin $\operatorname{syt}(a + b, a - b) \leq 2$. Oletuksen $\operatorname{syt}(a, b) = 1$ 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.

Määritelmä 2.1.7. Luku $a > 1$ on alkuluku, mikäli sillä on vain triviaalit tekijät ± 1 ja $\pm a$, muulloin luku a on *yhdistetty*.

Määritelmä 2.1.8. Olkoon $\text{syt}(a_1, ..., a_n) = 1$. Tällöin sanotaan, että luvut $a_1, ..., a_n$ ovat *suhteellisia alkulukuja* (*keskenään jaottomia*).

Lemma 2.1.9. *Olkoot $a_1, \ldots, a_n \in \mathbb{Z}$ siten, että $a_{i_0} \neq 0$ jollekin $i_0 \in \{1, \ldots, n\}$ ja olkoon $d = \text{syt}(a_1, \ldots, a_n)$. Tällöin*

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

Lemma 2.1.10. *Jos $a, b \in \mathbb{N}$ ja $c \in \mathbb{Z}$, niin $\text{syt}(a + cb, b) = \text{syt}(a, b)$.*

Lemma 2.1.11. (Eukleides) *Jos $a \mid bc$ ja $\text{syt}(a, b) = 1$, niin $a \mid c$.*

Lemma 2.1.12. *Luku $p \in \mathbb{N} \setminus \{1\}$ on alkuluku, jos ja vain jos kaikilla $a, b \in \mathbb{N}$ on voimassa implikaatio*

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

Lause 2.1.13. (Aritmetiikan peruslause) *Jokainen luonnollinen luku $n \geq 2$ voidaan esittää järjestystä vaille yksikäsitteisellä tavalla tulona*

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

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

Tuloa (2.1.14) kutsutaan luvun n *kanoniseksi esitykseksi* tai *alkutekijäesitykseksi* ja lukuja p_i luvun n *alkutekijöiksi*.

Huomautus 2.1.14. Aritmetiikan peruslause voidaan yleistää myös negatiivisia kokonaislukuja koskevaksi lisäämällä termi -1 yhtälön (2.1.14) oikealle puolelle. Tällöin kokonaisluku $n \in \mathbb{Z} \setminus \{0, \pm 1\}$ voidaan 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 $a_1, \ldots, a_n \in \mathbb{N}$.

Lemma 2.1.15. *Olkoot $a, b, c \in \mathbb{N}$.*

(i) Jos $\text{syt}(a, c) = \text{syt}(b, c) = 1$, niin $\text{syt}(ab, c) = 1$.

(ii) Jos $a \mid c$ ja $b \mid c$ siten, että $\text{syt}(a, b) = 1$, niin $ab \mid c$.

Lemma 2.1.16. *Jos $a, b \in \mathbb{N}$ ja $\text{syt}(a, b) = 1$, niin $\text{syt}(a^k, b^m)$ kaikilla $k, m \in \mathbb{N}$.*

Määritelmä 2.1.17. Lukujen $a_1, \ldots, a_n \in \mathbb{N}$ *pienin yhteinen monikerta* $\text{pym}(a_1, \ldots, a_n)$ on luku $d \in \mathbb{N}$, jolle on voimassa seuraavat ehdot:

(i) $a_i \mid d$ kaikilla $i = 1, \ldots, n$;

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

Määritellään kongruenssi, joka tuli lukutoeriaan Gaussin julkaisussa Disquisitiones Arithmeticae vuonna 1801.

Määritelmä 2.1.18. 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 2.1.19. *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 2.1.20. *Olkoot $a, b, c, d \in \mathbb{Z}$ ja olkoon $m \in \mathbb{N}$. Tällöin*

(i) $a \equiv a \pmod{m}$ (transitiivisuus)

(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)

Sovelletaan kongruenssia seuraavassa esimerkissä.

Esimerkki 2.1.21. 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 $n = k + 1$

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

jolloin induktio-oletuksen 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 $n \in \mathbb{N}$.

Lause 2.1.22. (Fermat'n pieni lause) *Olkoon p alkuluku ja olkoon $a \in \mathbb{Z}$ siten, että $p \nmid a$. Tällöin*

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

Märitellään seuraavaksi eräs lukuteoriassa oleellinen funktio:

Määritelmä 2.1.23. *Eulerin funktioksi* kutsutaan kuvausta $\phi : \mathbb{N} \to \mathbb{N}$, jonka arvo $\phi(n)$ ilmoittaa niiden lukujen $a \in \{1, \ldots, n\}$ lukumäärän, joille $\text{syt}(a, n) = 1$.

Huomautus 2.1.24. Kaikilla $n \in \mathbb{N}_{\geq 3}$ pätee $2 \leq \phi(n) \leq n - 1$, koska $\text{syt}(n, n) > 1$ ja $\text{syt}(1, n) = \text{syt}(n - 1, n) = 1$.

Lemma 2.1.25. *Olkoon p alkuluku ja $k \in \mathbb{N}$. Tällöin $\phi(p^k) = p^k - p^{k-1}$.*

Lause 2.1.26. *Olkoot $m, n \in \mathbb{N}$ suhteellisia alkulukuja. Tällöin $\phi(mn) = \phi(m)\phi(n)$.*

Huomautus 2.1.27. $\phi(m)$ on parillinen kaikilla $m \in \mathbb{N}_{\geq 3}$ Lemman 2.1.25 ja Lauseen 2.1.26 nojalla.

Lause 2.1.28. (Eulerin lause) *Olkoon $n \in \mathbb{N}$ ja $a \in \mathbb{Z}$ siten, että* $\text{syt}(a, n) = 1$. *Tällöin*

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

Määritelmä 2.1.29. *Luvun a kertaluvuksi modulo m* sanotaa lukua

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

Lemma 2.1.30. *Olkoon $m \in \mathbb{N}$ ja $a \in \mathbb{Z}$ siten, että* $\text{syt}(a, m) = 1$. *Tällöin luvulle $x \in \mathbb{N}$ pätee $a^x \equiv 1 \pmod{m}$ jos ja vain jos* $\text{ord}_m a \mid x$.

Seuraus 2.1.31. *Olkoon $m \in \mathbb{N}$ ja $a \in \mathbb{Z}$ siten, että* $\text{syt}(a, m) = 1$. *Tällöin* $\text{ord}_m a \mid \phi(m)$.

2.2 Kombinatoriikkaa

Tarkastellaan seuraavaksi kirjan [42] pohjalta jatkossa tarvittavia tärkeimpiä kombinatorisia tuloksia.

Määritelmä 2.2.1. Olkoot $n, k \in \mathbb{Z}_{\geq 0}$ siten, että $k \leq n$. Tällöin lukua

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

kutsutaan *binomikertoimeksi*, joka kertoo kuinka monta erilaista k alkioista osajoukkoa voidaan ottaa n alkioisesta joukosta, kun järjestyksellä ei ole merkitystä.

Lemma 2.2.2. *Olkoot $n, k \in \mathbb{N}$ siten, että $k \leq n$. Tällöin*

(i) $\binom{n}{n-k} = \binom{n}{k}$

(ii) $\binom{2n+1}{n} = \binom{2n+1}{n+1}$

Todistus. Seuraavat suoraan määritelmästä. □

Lause 2.2.3. (Binomilause)

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

Lemma 2.2.4. *n-alkioisella joukolla, $n \in \mathbb{N}$, on 2^n erilaista osajoukkoa.*

Todistus. Koska on olemassa $\binom{n}{k}$ erilaista k:n alkion osajoukkoa, $k \leq n$, summaamalla yli kaikkien eri k saadaan binomilauseen nojalla

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

□

Lemma 2.2.5. *Olkoon $n \in \mathbb{N}$. Tällöin $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$.*

Todistus. Soveltamalla binomilausetta 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 oikelta puolelta suorittamalla kertolasku ja soveltamalla Lemmaa 2.2.2

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

mistä väite yhtäsuuruuden nojalla seuraa. □

Lemma 2.2.6. *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

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

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

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

mikä jälleen nähdään kertomalla auki yhtälön oikea puoli. Väite seuraa yhdistämällä edellä olevat yhtälöt. □

Lisäksi seuraavaa aputulosta tarvitaan. [33]

Lemma 2.2.7. *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

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

mistä väite seuraa. □

Lemma 2.2.8. *Olkoon $n \in \mathbb{N}$. Määritellään luvut x_n ja y_n yhtälöllä*

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

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

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

Todistus. (i) Soveltamalla binomilausetta saadaan

$$\left(3 + 2\sqrt{2}\right)^n = \sum_{k=0}^{n} \binom{n}{k} 3^k (2\sqrt{2})^{n-k}$$
$$\left(3 - 2\sqrt{2}\right)^n = \sum_{k=0}^{n} \binom{n}{k} 3^k (-2\sqrt{2})^{n-k}$$

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

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

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 $m \in \mathbb{N}$.

□

2.3 Algebraa

[15] Tarkastellaan seuraavaksi myöhemmin tarvittavia oleellisia käsitteitä. Aloitetaan perusteista.

Määritelmä 2.3.1. Joukossa G määritelty laskutoimitus $\circ$ on funktio $G \times G \to G$. Merkitään näin saatavaa joukon G alkiota $\circ(a, b) = a \circ b$, missä $(a, b) \in G \times G$.

Määritelmä 2.3.2. 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 $x \in G$ $e \circ x = x \circ e = x$ (vasta-alkio)

(iii) jokaista $a \in G$ kohti on olemassa $a' \in G$ siten, että $a \circ a' = a' \circ a = e$ (käänteisalkio).

Määritelmä 2.3.3. Ryhmää $(G, \circ)$ kutsutaan *Abelin ryhmäksi*, jos lisäksi

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

Tarkastellaan sitten joukkoa, jossa on määritelty kaksi laskutoimitusta.

Määritelmä 2.3.4. Kolmikkoa $(R, +, \cdot)$ kutsutaan *renkaaksi*, jos $+$ ja $\cdot$ ovat joukossa R määriteltyjä laskutoimituksia ja seuraavat kolme kohtaa ovat voimassa:

(R1) ryhmä $(R, +)$ on Abelin ryhmä

(R2) laskutoimitus $\cdot$ on liitännäinen

(R3) kaikilla $a, b, c \in R$ on voimassa osittelulait

$$a \cdot (b + c) = (a \cdot b) + (a \cdot c)$$
$$(a + b) \cdot c = (a \cdot c) + (b \cdot c).$$

Huomautus 2.3.5. Ensimmäistä laskutoimitusta kutsutaan *yhteenlaskuksi* ja toista *kertolaskuksi*. Kertolaskun symboli jätetään tavallisesti merkitsemättä. Neutraalialkiota renkaan $(R, +, \cdot)$ yhteenlaskun suhteen kutsutaan *nolla-alkioksi*, merkitään 0_R, ja kertolaskun suhteen *ykkösalkioksi*, merkitään 1_R.

Määritelmä 2.3.6. Rengas $(R, +, \cdot)$ on *ykkösellinen*, jos kertolaskulla $\cdot$ on neutraalialkio, ja vaihdannainen, jos kertolasku $\cdot$ on vaihdannainen.

Määritelmä 2.3.7. Olkoon $(R, +, \cdot)$ rengas. Alkiosta 0_R eroavia alkioita $a, b \in R$ kutsutaan *nollantekijöiksi*, mikäli $ab = 0_R$.

Määritelmä 2.3.8. Kolmikkoa $(R, +, \cdot)$ kutsutaan *kokonaisalueeksi*, mikäli $(R, +, \cdot)$ on ykkösellinen ja vaihdannainen rengas eikä siinä ole nollantekijöitä.

Määritelmä 2.3.9. Kolmikkoa $(R, +, \cdot)$ kutsutaan *kunnaksi*, mikäli $(R, +, \cdot)$ on vaihdannainen ykkösellinen rengas, jolla $1_R \neq 0_R$ ja kaikilla alkiolla $a \in R \setminus \{0_R\}$ on käänteisalkio kertolaskun suhteen.

Tarkastellaan sitten tarkemmin vielä polynomeja.

Määritelmä 2.3.10. Olkoon f, $f(x) = a_0 + a_1 x + \cdots + a_n x^n$, polynomi, jonka *johtava kerroin* $a_n \neq 0$. Tällöin polynomin f aste on luku

$$\deg\big(f(x)\big) = n.$$

2.4 Elliptisistä käyristä

Elliptisiin käyriin liittyvä teoria on hyvin laaja. Tässä alaluvussa käydään läpi vain jatkossa esitettävän Szpiron konjektuurin kannalta oleellisia tuloksia. Tästä johtuen Kerroinkuntana toimii rationaalilukujen joukko $\mathbb{Q}$. Syvällisemmän käsityksen aiheesta saa kirjasta [45], johon tämäkin alaluku pohjautuu.

Määritelmä 2.4.1. Olkoot $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Q}$. Weierstrassin yhtälön

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \tag{2.3}$$

avulla määriteltyä käyrää E kutsutaan *elliptiseksi käyräksi.*

Määritelmä 2.4.2. 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

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

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.

Lause 2.4.3. *Olkoon E elliptinen käyrä. Tällöin*

(i) käyrä E ei leikkaa itseään, jos ja vain jos $\Delta \neq 0$.

(ii) käyrällä E on sulmukohta, jos ja vain jos $\Delta = 0$ ja $c_4 \neq 0$

(iii) kayrällä E on cusp, jos ja vain jos $\Delta = c_4 = 0$.

Seuraavaa aputulosta tarvitaan myöhemmin.

Lemma 2.4.4. *Edellä olevilla merkinnöillä pätee*

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

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

Todistus. (i) Suoralla laskulla saadaan

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

(ii) Suoralla laskulla saadaan

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

mistä väite seuraa kohdan (i) nojalla. □

Otetaan tähän väliin esimerkki.

Esimerkki 2.4.5. Muodostetaan elliptinen käyrä E yhtälöllä

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

Tällöin edellisillä merkinnöillä saadaan

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

diskriminantiksi

$$\begin{aligned} \Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6 = 16(a^2 - 2ab + b^2)a^2b^2 + 64a^3b^3 \\ &= 16(a^4b^2 - 2a^3b^3 + a^2b^4 + 4a^3b^3) = 16(a^4b^2 + 2a^3b^3 + a^2b^4) \\ &= 16\big(ab(a+b)\big)^2 \end{aligned}$$

ja edelleen

$$\begin{aligned} c_4 &= b_2^2 - 24b_4 = 16(a^2 - 2ab + b^2) + 16(3ab) \\ &= 16(a^2 + ab + b^2), \\ c_6 &= -b_2^3 + 36b_2b_4 - 216b_6 = -64(b-a)(a^2 - 2ab + b^2) - 288(b-a)(ab) \\ &= -32(b-a)(2a^2 - 4ab + 2b^2 + 9ab) = -32(b-a)(2a^2 + 5ab + 2b^2) \\ &= -32(b-a)(a+2b)(2a+b) \end{aligned}$$

Huomautus 2.4.6. Esimerkin käyrää E kutsutaan myös *Freyn käyräksi*, ja sen avulla saadaan yhteys Diophantoksen yhtälöiden ja elliptisten käyrien välille. Frey nimittäin huomasi, että jos luvut $a, b, c \in \mathbb{Z}$, $abc \neq 0$, toteuttavat yhtälön

$$a^p + b^p = c^p,$$

missä $p \geq 3$ on alkuluku, niin käyrän

$$y^2 = x(x - a^p)(x - b^p)$$

minimaalidiskriminatti on oleellisesti suuruudeltaan $|abc|^{2p}$ [45, s. 443].

Määritelmä 2.4.7. Elliptisen käyrän E yhtälöä (2.3) kutsutaan *minimaalimalliksi*, mikäli $a_1, a_2, a_3, a_4, a_6 \in \mathbb{Z}$ ja $|\Delta|$ on minimaalinen. Tällöin diskriminanttia kutsutaan käyrän E *minimaalidiskriminantiksi*.

Huomautus 2.4.8. Minimaalimallin tapauksessa $\Delta \in \mathbb{Z}$.

Työssä [35, s. 7] osoitetaan minimaalimallista seuraavaa.

Lemma 2.4.9. *Olkoot a, b, c ehdot*

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

toteuttavia nollasta eroavia kokonaislukuja. Tällöin elliptisen käyrän E_{abc},

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

yhtälö on minimaalimalli.

Hahmotetaan elliptisten käyrien ja *Abc*-konjektuurin välistä yhteyttä tarkemmin seuraavalla aputuloksella.

Lemma 2.4.10. *Olkoot $A, B, C \in \mathbb{Z} \setminus \{0\}$ ehdot*

$$A + B = C \quad ja \quad \operatorname{syt}(A, B, C) = 1$$

toteuttavia lukuja, ja olkoon E muotoa

$$E : y^2 = x(x + A)(x - B)$$

oleva elliptinen käyrä.

(i) Käyrän E minimaalidiskriminantti Δ_E on joko

$$|\Delta_E| = 2^4 |ABC|^2 \quad tai \quad |\Delta_E| = 2^{-8} |ABC|^2.$$

Määritelmä 2.4.11. Elliptisen käyrän *E johtaja* on luku

$$N(E) = \prod_{p \mid \Delta_E} p,$$

missä p on alkuluku ja Δ_E on käyrän E minimaalidiskriminantti.

2.5 Hiloista

Käytetään seuraavaa yleistettyä versiota Minkowskin konveksin kappaleen lauseesta.

Lause 2.5.1. *Olkoon $\Lambda \subset \mathbb{R}^n$ n-asteinen hila ja olkoon $V \subset \mathbb{R}^n$ konveksi ja origon suhteen symmetrinen. Jos*

$$vol_n(V) > m 2^n \det \Lambda$$

jollekin $m \in \mathbb{N}$, niin V sisältää ainakin m erilaista nollasta eroavia hilapistepareja $\pm v_i \in \Lambda$, $i = 1, \ldots, m$.

Edellä olleen lauseen joukko V määritellään (skalaarimonikertaa vaille) yksikäsitteisesti seuraavan lemman avulla.

Lemma 2.5.2. *Olkoon $n \in \mathbb{N}$ ja määritellään joukko $V \subset \mathbb{R}^n$ siten, että*

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

Tällöin $vol_n(V) = \frac{(2n)!}{n!^3}$

Todistus. Olkoon $p \in \mathbb{Z}$ siten, että $0 \leq p \leq n$. Määritellään

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

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

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

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

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

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

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

Kappaleen V tilavuus saadaan nyt summaamalla yli kaikkien 2^n mahdollisen joukon I, joilla K_I sisältää joukon V pisteitä. Tässä on huomattava, että $K_p = K_{\{1,2,\ldots,p\}}$. Jos I sisältää p alkiota, niin symmetrian nojalla

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

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

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

Lemman 2.2.5 nojalla $\sum_{k=0}^{n} \binom{n}{k}^2 = \binom{2n}{n}$, joten saadaan

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

□

2.6 Analyysin perustuloksia

Käydään seuraavaksi läpi muutamia Analyysi I-kurssilta tuttuja tuloksia. L'Hospital [51, ss. 88–89]

Lause 2.6.1 (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*

$$\lim_{x \to b-} f(x) = \lim_{x \to b-} g(x) = 0$$

tai

$$\lim_{x \to b-} f(x) = \pm\infty \quad ja \quad \lim_{x \to b-} g(x) = \pm\infty,$$

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

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

Tällöin

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

Huomautus 2.6.2. L'Hospitalin lause on voimassa myös raja-arvoilla $x \to a+$, $x \to \pm\infty$ ja $x \to c$ jollekin $c \in (a, b)$, mikäli lauseen oletukset vain muuten ovat voimassa.

Palautetaan vielä mieleen raja-arvoon liittyviä käsitteitä. [51, s. 47]

Määritelmä 2.6.3. Olkoon $x_0 \in \mathbb{R} \cup \{\infty\}$ ja olkoon funktio f välillä $[a, x_0[$ rajoitettu funktio. Määritellään luku $S_f(x; x_0)$ siten, että

$$S_f(x; x_0) = \sup_{x \leq t < x_0} f(t).$$

Tällöin funktion f *limes superior pisteessä* x_0 määritellään raja-arvona

$$\lim_{x \to x_0-} S_f(x; x_0) = \lim_{x \to x_0-} \big(\sup_{x \leq t < x_0} f(t) \big).$$

Palautetaan mieleen Taylorin polynomit, joilla voidaan approksimoida monimutkaisempia funktioita annetun pisteen ympäristössä [51, s. 99]

Määritelmä 2.6.4. Olkoon $x_0 \in \mathbb{R}$ ja olkoon funktio f n kertaa derivoituva jossakin pisteen x_0 ympäristössä. 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 $n \to \infty$ saadaan päättymätön Taylorin sarja [51, s. 265].

Määritelmä 2.6.5. 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*.

Ohitetaan Taylorin sarjaan liittyvät suppenemis- ja yksikäsitteisyystarkastelut, ks. [51]. Käsitellään Taylorin sarjaa seuraavan jatkossa tarvittavan esimerkin avulla.

Esimerkki 2.6.6. (a) Lasketaan Taylorin sarja funktiolle $f(t) = \log t$ pisteessä $x_0 = 1$. Välillä $(0, 2)$ funktio f on äärettömästi derivoituva, joten Määritelmän 2.6.5 mukaan saadaan

$$\log t = (t-1) - \frac{1}{2}(t-1)^2 + \frac{1}{3}(x-1)^3 - \cdots = -\sum_{k=1}^{\infty} \frac{(-1)^k(-1+t)^k}{k}.$$

(b) Lasketaan (a)-kohdan avulla Taylorin sarja funktiolle $g(x) = \log(1 - \frac{1}{\log x})$ pisteessä $x_0 = 1$. Sijoittamalla nyt $t = 1 - \frac{1}{\log x}$ saadaan

$$\log(1 - \frac{1}{\log x}) = -\frac{1}{\log x} - \frac{1}{2\log^2 x} - \frac{1}{3\log^3 x} - \cdots = -\sum_{k=1}^{\infty} \frac{1}{k(\log x)^k}$$

Otetaan käyttöön seuraava asymptoottinen merkintä [1, s. 53].

Merkintä 2.6.7. Olkoon $a \in \mathbb{R}$. Jos on olemassa vakio $C > 0$ siten, että funktioille f ja $g > 0$ pätee epäyhtälö

$$|f(x)| \leq Cg(x) \tag{2.4}$$

kaikilla $x \geq a$, niin tällöin

$$f(x) = \mathcal{O}\big(g(x)\big).$$

Huomautus 2.6.8. Vakiolle $b \in \mathbb{R}$ pätee $b = \mathcal{O}\big(g(x)\big)$ aina, kun

$$\lim_{x\to\infty} g(x) = \infty.$$

Raja-arvon määritelmän nojalla nimittäin kaikilla $M > 0$ on olemassa luku $a > 0$ siten, että $f(x) > M$ aina, kun $x \geq a$. Valitsemalla esimerkiksi $M = |b|$ epäyhtälö (2.4) toteutuu arvolla $C = 1$.

Havainnollistetaan määritelmää esimerkillä.

Esimerkki 2.6.9. Tähän jotain

2.7 Alkulukuihin liittyviä tuloksia

Tarkastellaan seuraavaksi alkulukuihin liittyviä tuloksia. Todistetaan ensin jatkossa hyvin oleellinen lemma mukaillen lähdettä [33, ss. 269-270].

Lemma 2.7.1. *Kaikilla $n \in \mathbb{N} \setminus \{1\}$ ja alkuluvuilla p pätee*

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

Todistus. Osoitetaan väite induktiolla.
1°) Tapauksessa $n = 2$ saadaan $2 < 4^2$ ja väite on voimassa.
2°) Oletetaan, että väite pätee arvolla $n = k \geq 2$. Jos k on pariton, niin arvolla $n = k + 1$

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

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

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

Tarkastellaan binomikerrointa $M = \binom{2m+1}{m} = \frac{(2m+1)2m(2m-1)\cdots(m+2)}{m!}$. Binomikertoimena M on kokonaisluku. Edelleen Lemman 2.2.2 ja Binomilauseen nojalla

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

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 $m < p$. Näin ollen $p \mid M$ ja siten myös $(\prod_{m+2 \leq p \leq 2m+1} p) \mid M$. Näin ollen pätee

$$\prod_{m+2 \leq p \leq 2m+1} p \leq M \leq 4^m \tag{2.5}$$

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

$$\prod_{p \leq m+1} < 4^{m+1}, \tag{2.6}$$

jolloin epäyhtälöistä (2.5) ja (2.6) 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. □

Alaluvun viimeisen aputuloksen osoittamisessa tarvitaan seuraavaa Abelin summakaavaa, jonka todistus löytyy kirjasta [1, s.77].

Lause 2.7.2 (Abel)**.** *Olkoon $n \in \mathbb{N}$ ja olkoon funktio $A : \mathbb{R} \to \mathbb{R}$ määritelty funktion $a : \mathbb{N} \to \mathbb{R}$ 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

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

Määritelmä 2.7.3. Funktiota $\pi : \mathbb{R}_{>0} \to \mathbb{Z}_{\geq 0}$,

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

kutsutaan *alkulukujen lukumääräfunktioksi.*

Todetaan sitten kuuluisa alkulukukulause, jonka Gauss (1792) ja Legendre (1798) alkulukutaulukoiden perusteella otaksuivat mutta jonka varsinaisen todistuksen esittivät Hadamard ja de la Vallee-Poussin vasta vuonna 1896 [1, s. 74].

Lause 2.7.4 (Alkulukulause)**.** *Olkoon π alkulukujen lukumääräfunktio. Tällöin*

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

Alkulukulauseen mukaan funktio π käyttäytyy asymptoottisesti samalla tavalla kuin funktio $\frac{x}{\log x}$, mikä ei kuitenkaan tarkoita niiden erotusten olevan lähellä nollaa. Lukumääräfunktio virhetermeineen voidaan esittää muodossa (ks. [23, s. 65])

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

Arvolla $k = 3$ saadaan

$$\pi(x) = x \left(\frac{1}{\log x} + \frac{1}{\log^2 x} + \frac{2}{\log^3 x} + \mathcal{O}\left(\frac{1}{\log^4 x} \right) \right), \tag{2.7}$$

mikä on tarvittava tarkkuus seuraavaan luvun viimeiseen aputulokseen [10].

Lemma 2.7.5. *Olkoon $x \in \mathbb{R}_{>0}$ ja merkitään lukua x pienempien tai yhtäsuurten parittomien alkulukujen lukumäärää luvulla $n = \pi(x) - 1$ ja $p_1, \ldots, p_n$ n ensimmäistä paritonta alkulukua. Tällöin*

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

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

Todistus. Määritellään funktio $a : \mathbb{N} \to \mathbb{R}$ 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 2.7.2 arvolla $y = 2$ sovellettaessa saadaan

$$\sum_{i=1}^{n} f(p_i) = f(x)\pi(x) - f(2) - \int_2^x f'(y)\pi(y)dy. \tag{2.8}$$

Tarkastellaan tilanteita, missä $f(y) = \log y$ ja $f(y) = \log\log y$.

Olkoon ensin $f(y) = \log y$. Yhtälön (2.7) nojalla voidaan kirjoittaa

$$f(x)\pi(x) = x\left(1 + \frac{1}{\log x} + \frac{2}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right)\right) \tag{2.9}$$

ja

$$\int_2^x f'(y)\pi(y)dy = \int_2^x \left(\frac{1}{\log y} + \frac{1}{\log^2 y} + \mathcal{O}\left(\frac{1}{\log^3 y}\right)\right) dy. \tag{2.10}$$

Osittaisintegroimalla saadaan kaikille $m \in \mathbb{N}$, $a, b \in \mathbb{R}, a, b > 1$

$$\int_a^b \frac{1}{\log^m y} dy = \int_a^b \frac{y}{\log^m y} + m \int_a^b \frac{1}{\log^{m+1} y} dy. \tag{2.11}$$

Yhtälöstä (2.10) saadaan siten

$$\begin{aligned}
\int_2^x f'(y)\pi(y)dy &= \int_2^x \frac{1}{\log y} dy + \int_2^x \frac{1}{\log^2 y} dy + \int_2^x \mathcal{O}\left(\frac{1}{\log^3 y}\right) dy \\
&= \int_2^x \frac{y}{\log y} + \int_2^x \frac{1}{\log^2 y} dy + \int_2^x \frac{y}{\log^2 y} + 2\int_2^x \frac{1}{\log^3 y} dy + \mathcal{O}\left(\frac{x}{\log^3 x}\right) \\
&= \int_2^x \frac{y}{\log y} + \int_2^x \frac{y}{\log^2 y} + \int_2^x \frac{1}{\log^3 y} dy + \int_2^x \frac{y}{\log^2 y} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) \\
&= \frac{x}{\log x} + \frac{2x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right)
\end{aligned}$$

Sijoittamalla nyt tämä ja yhtälö (2.9) yhtälöön (2.8) saadaan

$$\sum_{i=1}^{n} \log p_i = x + \mathcal{O}\left(\frac{x}{\log^3 x}\right) \tag{2.12}$$

Oletuksen mukaan $n = \pi(x) - 1$. Kirjoittamalla (2.7) uudelleen käyttämällä geometrista sarjaa saadaan

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

Kertomalla puolittain luvulla $\log x - 1$ saadaan

$$n(\log x - 1) = x + \frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right), \tag{2.13}$$

josta edelleen

$$x = n\log\left(\frac{x}{e}\right) - \frac{x}{\log^2 x} - \mathcal{O}\left(\frac{x}{\log^3 x}\right), \tag{2.14}$$

sillä $\log x - 1 = \log x - \log e = \log \frac{x}{e}$. Lemman ensimmäinen osa seuraa yhdistämällä yhtälöt (2.14) ja (2.12).

Tarkastellaan sitten tapausta $f(y) = \log\log y$. Yhtälön (2.7) mukaan

$$f(x)\pi(x) = (\log\log x)(n+1) = n\log\log x + \mathcal{O}(\log\log x) \tag{2.15}$$

ja vastaavasti osittaisintegroinnista (2.11) seuraa

$$\begin{aligned} \int_2^x f'(y)\pi(y)dy &= \int_2^x \frac{1}{y\log y}\cdot y\left(\frac{1}{\log y} + \frac{1}{\log^2 y} + \frac{2}{\log^3 y} + \mathcal{O}\left(\frac{1}{\log^4 y}\right)\right)dy \\ &= \int_2^x \left(\frac{1}{\log^2 y} + \mathcal{O}\left(\frac{1}{\log^3 y}\right)\right)dy \\ &= \frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right). \end{aligned} \tag{2.16}$$

Sijoittamalla tulokset (2.15) ja (2.16) yhtälöön (2.8) saadaan

$$\sum_{i=1}^{n}\log\log p_i = n\log\log x - \frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right). \tag{2.17}$$

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

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

missä toinen yhtäsuuruus seuraa ensimmäisen asteen Taylorin sarjakehitelmästä ja kolmas yhtälöstä (2.7). Näin ollen yhtälö (2.17) voidaan kirjoittaa muodossa

$$\sum_{i=1}^{n} \log\log p_i = n\log(\log x - 1) + \mathcal{O}\left(\frac{x}{\log^3 x}\right), \tag{2.18}$$

josta edelleen

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

missä toinen yhtäsuuruus seuraa yhtälöstä (2.13) ja neljäs yhtälöstä (2.7) sekä ensimmäisen asteen Taylorin sarjakehitelmästä. □

3 Abc-konjektuuri ja siihen liittyviä tuloksia

3.1 Abc-summa ja radikaali

Merkintöjen yksinkertaistamiseksi määritellään *abc*-summa.

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 $0 < a < b < c$. Kyseinen tilanne saadaan nimittäin aina aikaan *abc*-summan termejä siirtämällä ja valitsemalla uudelleen luvut a, b ja c.
(ii) Oletuksesta $\text{syt}(a, b) = 1$ seuraa $\text{syt}(a, b, c) = 1$. Soveltamalla Lemmaa 2.1.10 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 [35, ss. 2-3]. Tällaisia ovat muun muassa

(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 $m, n \in \mathbb{N}$, $m > n$, ovat suhteellisia alkukuja, joista toinen on pariton ja toinen parillinen [41, ss. 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 ϕ 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 $\operatorname{syt}(n, b) = 1$.

Määritellään seuraavaksi nollasta eroavan luvun radikaali.

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

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

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

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

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 2.1.13 ja Huomautus 2.1.14)

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

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

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

Seuraavaan aputulokseen on kerätty jatkon kannalta oleelliset radikaalin ominaisuudet.

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

(i) $\operatorname{rad}(a) \leq a$.

(ii) $\operatorname{rad}(ab) \leq \operatorname{rad}(a) \operatorname{rad}(b)$, *missä pätee yhtäsuuruus jos vain jos* $\operatorname{syt}(a, b) = 1$.

(iii) $\operatorname{rad}(a^m b^n) \leq \operatorname{rad}(a) \operatorname{rad}(b)$.

Todistus. Oletetaan, että $a, b, m, n \geq 2$, sillä muuten väitteet pätevät triviaalisti. Luvuilla on Aritmetiikan peruslauseen (Lause 2.1.13) nojalla kanoniset esitykset $a = p_1^{t_1} p_2^{t_2} \cdots p_n^{t_r}$ ja $b = q_1^{s_1} q_2^{s_2} \cdots q_m^{s_v}$, missä p_i ja q_j ovat eri alkulukuja ja $t_i, s_j \in \mathbb{N}$. Tällöin

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

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

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

missä epäyhtälö mikä osoittaa väitteen (ii). Väite (iii) saadaan soveltamalla väitettä (ii) ja radikaalin määritelmää. □

Huomautus 3.1.8. Kohdan (ii) nojalla radikaalifunktio on multiplikatiivinen.

Osoitetaan vielä työhön [43, ss. 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 $0 < p_1 < p_2 < \cdots < p_s \leq P$, missä $p_1, \ldots, p_s$ ovat alkulukuja. Käytetään merkintää S_P joukolle

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

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

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

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 [44, Corollary 1.2, ss. 41–45] □

Lemman suorana seurauksena saadaan

Lemma 3.1.11. *Olkoot $x, y, z \in S$ siten, että $\operatorname{syt}(x,y) = 1$, $|x| < |y|$, $|y| \geq 3$ 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

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

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. □

Huomautus 3.1.12. Lemma 3.1.11 osoittaa itse asiassa, että joukko

$$\left\{(x,y,z) \in S_P^3 : \operatorname{syt}(x,y) = 1, |x| < |y|, x + y = z\right\}$$

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 $\operatorname{rad}(abc) \in S_P$.*

Todistus. Jos $\operatorname{rad}(abc) \in S_P$, 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. □

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*

$$\lim_{n\to\infty} \operatorname{rad}(a_n b_n c_n) = \infty.$$

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

3.2 Abc-konjektuuri

Oesterlé ja Masser esittivät *Abc*-konjektuurin vuonna 1985 yrityksenä ymmärtää paremmin Fermat'n suurta lausetta [36, ss. 3-4], [38]. 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.

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

$$c \leq C(\varepsilon)\,\mathrm{rad}(abc)^{1+\varepsilon}. \tag{3.1}$$

Konjektuuri voidaan esittää yleisemmässä muodossa hieman oletuksia muuttamalla.

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

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

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 kiinnitetylle luvulle $\varepsilon > 0$, esimerkiksi arvolle $\varepsilon = 1$. [3, s. 403]

Konjektuuri voidaan esittää myös hieman eri tavalla:

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

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

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

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

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

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

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

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

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

Esitetään vielä yksi edellisten kanssa samantapainen *Abc*-konjektuurin muoto [35, s. 9].

Konjektuuri 3.2.6. *Jokaista reaalilukua $\varepsilon > 0$ 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*

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

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. □

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 [26, s. 40]. Tulkintaa tukee seuraava taulukko, jossa tarkastellaan *abc*-kolmikon

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

kanonisia esityksiä arvoilla $n = 2, 3, 4, 5, 6$.

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	$(7^{32} - 1) \cdot 2 \cdot 7699649 \cdot 134818753 \cdot 531968664833$	7^{64}

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

Myös kirjan [40, ss. 399–428] taulukot suhteellisten alkulukujen $a^n \pm b^m$ kanonisista esityksistä tukevat yllä esitettyä tulkintaa.

Tarkastellaan sitten lähemmin *Abc*-konjektuuria. Seuraava lause osoittaa, että on *abc*-summan muodostavien lukujen täytyy olla suhteellisia alkulukuja.

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

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 $a_n + b_b = c_n$, ja edelleen

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

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

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 määritteleminen. Artikkelissa [2] A. Baker ehdottaakin ongelman kiertämistä modifioimalla *Abc*-konjektuuria yhdenmukaisemmaksi logaritmisten muotojen kanssa seuraavasti.

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

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

missä ω on tulon abc eri alkutukijöiden lukumäärä.

Hän ehdottaa myös seuraavaa muotoa.

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

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

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

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

Konjektuuri 3.2.11 (Abc, Granville)**.** *Olkoon $\lambda > 0$ absoluuttinen vakio. Tällöin olemassa vakio $C > 0$ site, että kaikille abc-summille (a,b,c) pätee epäyhtälö*

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

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

Ongelmista huolimatta voidaan osoittaa, että luvun $C(\varepsilon)$ suuruus riippuu jossain määrin käänteisesti luvun ε valinnasta. Tämän osoittamiseksi määritellään luku $C(\varepsilon)$ tutkielman [43] mukaisesti yhtälöllä

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

missä supremum otetaan yli kaikkien (a,b,c)-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 $C(\varepsilon)$ tällöin on äärellinen (Huomautus 3.2.14). Seuraava tulos [35, s. 10] osoittaa luvun $C(\varepsilon)$ kasvavan rajatta, kun luku ε lähenee nollaa.

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

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

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

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

Lemman 2.2.8 nojalla luvut x_n ja y_n toteuttavat tällöin myös yhtälön $x_n - y_n\sqrt{2} = \left(3 - 2\sqrt{2}\right)^n$, jolloin yhtälöt puolittain kertomalla saadaan

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

Kun valitaan $n = 2^m$, pätee Lemman 2.2.8 nojalla $2^{m+1} \mid y_n$ kaikilla $m \in \mathbb{N}$. Oletetaan nyt, että Konjektuuri 3.2.1 on totta ja sovelletaan sitä *abc*-summaan $x_n^2 = 1 + 2y_n^2$. Ylöspäin arvioimalla saadaan

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

josta edelleen

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

Antamalla nyt $\varepsilon \to 0$ saadaan

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

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

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 [26, ss. 40–41] antamaa vastaesimerkkiä käyttämällä, että luvun ε olemassaolo on perusteltua.

Lause 3.2.13. *Konjektuuri 3.2.1 ei pidä paikkaansa ilman lukua $\varepsilon > 0$.*

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

$$c \leq K\,\mathrm{rad}(abc). \tag{3.3}$$

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

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

Esimerkin 2.1.21 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

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

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. □

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

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

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

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

ei saada, vaikka käydään läpi kaikki *abc*-kolmikot [19]. Erityisesti tämä tarkoittaa sitä, että luku $C(\varepsilon)$ on äärellinen.

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

$$c = \text{rad}(a, b, c)^{L(a,b,c)}. \tag{3.4}$$

Yhtälöstä (3.4) saadaan L-arvolle seuraava muoto [7, 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* [16].

No.	L(a,b,c)	a	b	c	löytövuosi
1	1.6299	2	$3^{10}109$	23^5	1987
2	1.6260	11^2	$3^2 5^6 7^3$	$2^{21}23$	1985
3	1.6235	$19 \cdot 1307$	$7 \cdot 29^2 31^8$	$2^8 3^{22} 5^4$	1994
4	1.5808	283	$5^{11}13^2$	$2^8 3^8 17^3$	1993
5	1.5679	1	$2 \cdot 3^7$	$5^4 7$	1988

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

Tyypillisesti L-arvo on välillä $[\frac{1}{3}, 1]$. *Abc*-konjektuurin kannalta mielenkiintoisia ovat kuitenkin L-arvot, jotka ovat suurempia kuin yksi. *Abc*-kolmikko on laadultaan *hyvä*, mikäli sen L-arvo on suurempi kuin $1,4$. Tällaisia kolmikoita tunnetaan tällä hetkellä 234 ja ne on esitetty laadun mukaan laskevassa järjestyksessä lähteessä [47]. Alla on taulukoitu kaikki tunnetut abc-kolmikot, joilla $L > 1,55$. Laajempi esitys hyvistä abc-kolmikoista löytyy liitteestä A.

Oesterlén esitti kysymyksen, onko L-arvojen joukko rajoitettu [5]. Tätä kysymystä tarkastellaan lähemmin luvussa 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 reaalilukua $\varepsilon > 0$ kohden on olemassa luku $C(\varepsilon) > 0$ siten, että että kaikilla abc-kolmikoilla $(a, b, c) \in \mathbb{N}^3$ on voimassa epäyhtälö*

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

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

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

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 $\operatorname{rad}(abc) \geq 2$ kaikilla abc-kolmikoilla $(a, b, c) \in \mathbb{N}^3$.

3.3 Abc-konjektuuriin liittyviä tuloksia

Vuonna 1986 Stewart ja Tijdeman julkaisivat ensimmäisen tuloksen kohti rajoituksia [50] :

Lause 3.3.1. *Jokaista $\delta > 0$ kohti on olemassa äärettömästi abc-summia, joille pätee*

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

Lisäksi he osoittivat seuraavan:

Lause 3.3.2. *Kaikilla abc-summilla pätee epäyhtälö*

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

missä D on efektiivisesti laskettavissa oleva vakio.

Myöhemmin vuonna 1991 Stewart ja Yu osoittivat logaritmin lineaarimuotojen p-adisten arvoiden avulla seuraavan tuloksen [48].

Lause 3.3.3. *On olemassa efektiivisesti laskettavissa oleva vakio K siten, että kaikille abc-summille (a, b, c) on voimassa*

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

Erityisesti jokaista $\varepsilon > 0$ kohti on olemassa efektiivisesti laskettavissa oleva vakio $K(\varepsilon)$ siten, että kaikille abc-summille (a, b, c) pätee

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

Vuonna 2001 samat tekijät paransivat tulostaan [49] vielä muotoon

Lause 3.3.4. *On olemassa efektiivisesti laskettavissa oleva vakio K siten, että kaikille abc-summille (a, b, c) on voimassa*

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

Lauseen 3.3.1 avulla voidaan osoittaa seuraava tulos.

Lause 3.3.5. *([36]) Kaikilla $k > 0$ ja $k_1 > 0$ on olemassa abc-summa (a, b, c), jolle*

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

Todistus. Olkoot $k, k_1 > 0$ ja olkoon (a, b, c) *abc*-summa siten, että $0 < a < b < c$ ja luvut toteuttavat yhtälön

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

Olettamalla kolmikon (a, b, c) toteuttavan myös Lauseen 3.3.1 epäyhtälön saadaan

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

Tarkastellaan nyt reunimmaisia epäyhtälöitä. Jakamalla puolittain luvulla $\operatorname{rad}(abc)$ ja ottamalla logaritmi saadaan

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

josta edelleen

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

Näin ollen luku $\operatorname{rad}(abc)$ on rajoitettu mikä johtaa ristiriitaan. □

Tuloksen avulla saadaan viimein vastaus kysymykseen, voidaanko *Abc*-konjektuurissa vakio $C(\varepsilon)$ valita käänteisesti verrattuna lukuun ε.

Lause 3.3.6. *Kaikilla $k > 0$ on olemassa luku $\varepsilon > 0$ ja abc-summa (a, b, c) siten, että*

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

Todistus. Olkoon $k > 0$. Oletetaan vastoin väitettä, että jollekin $\varepsilon > 0$ ja jollekin *abc*-summalle (a, b, c) pätee epäyhtälö

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

Oikeanpuoleisen termin minimi saavutetaan arvolla $\varepsilon = \frac{k}{\log \operatorname{rad}(abc)}$, jolloin epäyhtälö saa muodon

$$c \leq \left(\frac{e}{k}\right)^k \operatorname{rad}(abc)(\log \operatorname{rad}(abc))^k.$$

Tämä on ristiriita Lauseen 3.3.5 kanssa. □

3.4 *L*-arvojen joukosta ja sen kasautumispisteistä

Abc-kolmikon $(a, b, c) \in \mathbb{N}^3$ *L*-arvo määriteltiin osamääränä

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

Käytetään kaikkien *L*-arvojen joukolle merkintää $\mathcal{L}$, toisin sanoen

$$\mathcal{L} = \big\{L(a, b, c) : (a, b, c) \in \mathbb{N}^3,\ \operatorname{syt}(a, b) = 1,\ a + b = c\big\}.$$

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 totettava *abc*-kolmikko, jolle

$$L(a, b, c) = \frac{\log c}{\log \operatorname{rad}(abc)} = \frac{m}{n}, \tag{3.5}$$

missä $m, n \in \mathbb{N}$. Yhtälö (3.5) voidaan esittää ekvivalentissa muodossa

$$c^n = \operatorname{rad}(abc)^m, \tag{3.6}$$

josta nähdään, että luvulla c ja tulolla abc täytyy olla samat alkutekijät. Huomautauksen 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. □

Osoitetaan sitten, että on korkeintaan äärellinen määrä tietyn L-arvon antavia *abc*-kolmikoita [34]. Sitä varten tarvitsemme kuitenkin seuraavaa aputulosta [53, 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 λ. Merkitään kunkin kolmikon radikaalia $r_i = \operatorname{rad}(a_i b_i c_i)$ 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 $\operatorname{syt}(k_1, k_2, k_3) = 1$, 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 $\operatorname{syt}(r_1, r_2) = 1$, niin tällöin $k_1 = k_2 = k_3 = 1$ ja $r_3 = r_1 r_2$.
- Jos $\operatorname{syt}(r_1, r_2) \neq 1$, 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 $\operatorname{rad}(abc)$, joita vastaavien *abc*-kolmikoiden L-arvo on λ. Lauseen 3.1.13 nojalla on vain äärellisen monta sellaista *abc*-kolmikkoa, joilla on sama radikaali. Väite seuraa. □

Määritellään sitten kasaantumispiste [51, s. 197] mutta sallitaan myös tilanne, missä kasaantumispiste on ääretön.

Määritelmä 3.4.5. Piste $\lambda \in \mathbb{R}_{>0} \cup \{\infty\}$ on joukon $\mathcal{L}$ *kasautumispiste*, jos on olemassa sellainen L-arvojen jono $(L_n)_{n\in\mathbb{N}}$, jolla $L_n \neq \lambda$ kaikilla $n \in \mathbb{N}$ ja

$$\lim_{n\to\infty} L_n = \lambda. \tag{3.7}$$

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. Tämä osoitetaan kirjassa [51, s. 196].

Edellistä tulosta hyväksikäyttämällä voidaan osoittaa edelleen seuraavat tulokset [43].

Lause 3.4.7. *Olkoon $\lambda \in \mathbb{R}_{>0}$. Luku λ on joukon $\mathcal{L}$ kasautumispiste, jos ja vain jos on olemassa eri abc-kolmikoista muodostuva jono $\big((a_n, b_n, c_n)\big)_{n\in\mathbb{N}}$, jolle*

$$\lim_{n\to\infty} L(a_n, b_n, c_n) = \lambda.$$

Todistus. Oletetaan ensin, että luku λ 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

$$\lim_{n\to\infty} L_n = \lambda.$$

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 $\big((a_n, b_n, c_n)\big)_{n\in\mathbb{N}}$, jolle pätee

$$\lim_{n\to\infty} L(a_n, b_n, c_n) = \lambda.$$

Lauseen 3.4.4 nojalla voidaan nyt muodostaa sellainen L-arvojen osajono $\big(L(a_k, b_k, c_k)\big)_{k\in\mathbb{N}}$, 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 λ on siis joukon $\mathcal{L}$ kasaantumispiste. □

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 kasautumispiste, joka on vähintään α.

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 $\big(L(a_k, b_k, c_k)\big)_{k\in\mathbb{N}}$, 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. □

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 kasautumispiste. Joukon $\mathcal{L}$ kasautumispisteiden joukko on siis epätyhjä.

Pienimmälle kasautumispisteelle saadaan itse asiassa seuraava arvio.

Lause 3.4.10. *Joukon $\mathcal{L}$ jokainen kasautumispiste on vähintään $\frac{1}{3}$.*

Todistus. Koska jokaisen *abc*-kolmikon $(a, b, c) \in \mathbb{N}^3$ radikaalille pätee epäyhtälö

$$\operatorname{rad}(abc) \leq abc < c^3,$$

saadaan L-arvolle alaraja

$$L(a, b, c) = \frac{\log c}{\log \operatorname{rad}(abc)} > \frac{\log c}{\log c^3} = \frac{1}{3}.$$

Väite seuraa Lauseesta 3.4.8. □

Otetaan käyttöön seuraava merkintä.

Merkintä 3.4.11. Käytetään joukon $\mathcal{L}$ kasautumispisteille merkintää $\mathcal{L}'$.

Lauseen 3.4.10 tulos voidaan nyt tulkita siten, että $\mathcal{L}' \subset [\frac{1}{3}, \infty]$. Tarkastellaan seuraavaksi joukkoon $\mathcal{L}'$ liittyviä tuloksia. Artikkelissa [7, ss. 97–98] osoitetaan, että

$$\left[\frac{1}{3}, \frac{1}{2}\right] \subset \mathcal{L}'.$$

Tätä parempi tulos on artikkelissa [6].

Lause 3.4.12.

$$\left[\frac{1}{3}, \frac{15}{16}\right] \subset \mathcal{L}'$$

Edellistä tulosta voidaan vielä oleellisesti samoilla menetelmillä parantaa [20].

Lause 3.4.13.

$$\left[\frac{1}{3}, \frac{36}{37}\right] \subset \mathcal{L}'$$

Hieman erilainen tulos joukon $\mathcal{L}'$ suuruudesta esitetään artikkelissa [14].

Lause 3.4.14.

$$\mathcal{L}' \cap \left[1, \frac{3}{2}\right) \neq \emptyset.$$

Huomautus 3.4.15. Lauseen 3.4.14 tulos voidaan esittää vielä yleisemmässä muodossa. Todistusta hieman muuttamalla nimittäin saadaan, että

$$\mathcal{L}' \cap \left[\frac{3}{3+\varepsilon}, \frac{3}{2+\varepsilon}\right] \neq \emptyset$$

kaikilla $\varepsilon \in (0, 1)$ [14].

Aiemmat tulokset saatiin olettamatta mitään *Abc*-konjektuurin todenperäisyydestä. Osoitetaan sitten, että jos *Abc*-konjektuuri on voimassa, niin $\mathcal{L}' \subset [\frac{1}{3}, 1]$ [6]. Tätä varten tarvitaan seuraavaa määritelmää.

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. Määritelmän 3.4.16 selkiyttämiseksi huomautetaan, että

(i) $x \leq \sup \mathcal{L}'$ kaikilla $x \in \mathcal{L}'$ [51, 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 [51, ss. 187–188].

Seuraava esitys perustuu pääosin lähteisiin [6] ja [55].

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

$$\begin{aligned} L(a_n, b_n, c_n) &= \frac{\log c_n}{\log \operatorname{rad}(a_n b_n c_n)^{1+\varepsilon}} \\ &\leq \frac{\log\big(C(\varepsilon)\operatorname{rad}(a_n b_n c_n)^{1+\varepsilon}\big)}{\log \operatorname{rad}(a_n b_n c_n)^{1+\varepsilon}} \\ &= \frac{\log C(\varepsilon)}{\log \operatorname{rad}(a_n b_n c_n)^{1+\varepsilon}} + 1 + \varepsilon. \end{aligned}$$

Lauseen 3.1.14 nojalla $\operatorname{rad}(a_n b_n c_n)$ kasvaa rajatta, kun $n \to \infty$. Näin ollen epäyhtälön oikeasta puolesta saadaan tarpeeksi suurilla muuttujan n arvoilla pienempää kuin $1 + \varepsilon$, jolloin 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

$$\operatorname{rad}\big(2^n(2^n-1)\big) = 2\operatorname{rad}(2^n - 1) \leq 2 \cdot 2^n = 2^{n+1},$$

jota edelleen L-arvoon soveltamalla saadaan

$$L(a_n, b_n, c_n) = \frac{\log 2^n}{\log \operatorname{rad}\big(2^n(2^n-1)\big)} \geq \frac{n \log 2}{(n+1)\log 2} = \frac{n}{n+1} \to 1,$$

kun $n \to \infty$. Lauseen 3.4.8 nojalla joukolla $\mathcal{L}$ on kasautumispiste, 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 $n \geq k$, $k \in \mathbb{N}$. Toisin sanoen, kaikilla $n \geq k$ pätee

$$c_n \leq \operatorname{rad}(a_n b_n c_n)^{1+\varepsilon}.$$

Valitaan sitten vakiot $C_1(\varepsilon), C_2(\varepsilon), \ldots, C_{k-1}(\varepsilon)$ siten, että epäyhtälö

$$c_i \leq C_i(\varepsilon)\operatorname{rad}(a_i b_i c_i)^{1+\varepsilon}$$

toteutuu kaikilla $i = 1, 2, \ldots, k-1$. Määritellään

$$C(\varepsilon) = \max_{1\leq i\leq k-1} \big\{C_i(\varepsilon)\big\},$$

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 seuraava [6].

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-osumien lukumäärästä

Abc-konjektuuri voidaan esittää muodossa, jonka mukaan jokaisella $\varepsilon > 0$ on olemassa korkeintaan äärellisen monta epäyhtälön

$$c > \operatorname{rad}(a,b,c)^{1+\varepsilon}. \tag{3.8}$$

toteuttavaa *abc*-kolmikkoa $(a,b,c) \in \mathbb{N}^3$. Tässä alaluvussa tarkastellaan sellaisia *abc*-kolmikoita, jotka toteuttavat yhtälön (3.8) arvolla $\varepsilon = 0$.

Määritelmä 3.5.1. *Abc*-kolmikkoa $(a,b,c) \in \mathbb{N}^3$ kutsutaan *abc-osumaksi*, jos $\operatorname{rad}(abc) < c$.

Lauseen 3.2.13 nojalla tiedetään, että *Abc*-konjektuuri ei ole voimassa ilman lukua $\varepsilon > 0$. Seuraava tulos antaa tälle vielä vahvistuksen.

Lause 3.5.2. *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 $\operatorname{rad}(b_n) \leq 2j$ jollekin $j \in \mathbb{N}$. Koska tulolla $a_n c_n$ on vain alkutekijä 3, saadaan

$$\operatorname{rad}(a_n b_n c_n) \leq 2j \cdot 3 = 6j < 8j + 1 = c_n,$$

Näin ollen kolmikko (a_n, b_n, c_n) on *abc*-osuma kaikilla $n \in \mathbb{N}$. □

Lauseen 3.5.2 todistuksessa käytetty ääretön *abc*-osumien jono on eritystapaus seuraavasta S. Dahmenin [10] esittämästä tuloksesta.

Lemma 3.5.3. *Olkoot $s \in \mathbb{N} \setminus \{1\}$ ja p alkuluku siten, että $p \nmid s$. Tällöin kolmikot*

$$(a_n, b_n, c_n) = \left(1, s^{(p-1)p^n} - 1, s^{(p-1)p^n}\right)$$

ovat abc-osumia tarpeeksi suurilla luvun $n \in \mathbb{N}$ arvoilla.

Todistus. Lemman 2.1.25 ja Eulerin lauseen (Lause 2.1.28) 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 $p^{n+1} \mid a_n$. Näin ollen tulon $a_n b_n c_n$ radikaalille saadaan arvio

$$\operatorname{rad}(a_n b_n c_n) \leq \frac{b_n}{p^n} \cdot 1 \cdot s \leq \frac{s}{p^n} c_n < c_n,$$

missä viimeinen epäyhtälö on voimassa kaikilla $n > \frac{\log s}{\log p}$. Siten tarpeeksi suurilla luvun n arvoilla kaikki edellä olevan muotoiset *abc*-summat ovat *abc*-osumia. □

Vastaavanlaista konstruktiota ei voida esittää *abc*-osumalle, jonka termistä yksikään ei ole yksi.

Huomautus 3.5.4. Lauseen 3.5.2 tulos voidaan esittää myös muodossa, että on äärettömästi *abc*-kolmikoita, joiden L-arvo on suurempi kuin yksi. Kaikkien *abc*-osumien L-arvolle nimittäin pätee

$$L(a,b,c) = \frac{\log c}{\log \operatorname{rad}(abc)} > 1.$$

Edellinen tulos voidaan esittää

Merkintä 3.5.5. Merkitään *abc*-osumien lukumäärää funktiolla $N : \mathbb{R}_{\geq 0} \to \mathbb{Z}_{\geq 0}$,

$$N(X) = \#\{Abc\text{-osuma (a,b,c)} \mid c \leq X\}.$$

Voidaan osoittaa Abc-osumien lukumäärällä olevan seuraava alaraja:

Lause 3.5.6. *Jokaista $\varepsilon > 0$ kohti on olemassa $X_0 > 0$ siten, että kaikilla $X \geq X_0$ pätee*

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

Todistus. Olkoon $q = \frac{b}{c} \in \mathbb{Q}^*$ siten, että $b, c \in \mathbb{Z} \setminus \{0\}$ ja $\operatorname{syt}(b,c) = 1$. Määritellään luvun q korkeus funktiolla $h : \mathbb{Q} \to \mathbb{R}$,

$$h(q) := \log(\max(|b|, |c|)),$$

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 $p_1, \ldots, p_n$ n ensimmäistä paritonta alkulukua. Tarkastellaan näiden 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 $B(x) : \mathbb{R}_+ \to \mathbb{R}_+$ on jokin muuttujan x funktio. Määritellään injektiivinen joukkohomomorfismi $\varphi_n : (Q)_n \to \mathbb{R}^n$,

$$p_1^{a_1} p_1^{a_2} \cdots p_n^{a_n} \mapsto (a_1 \log p_1, a_2 \log p_2, \ldots, a_n \log p_n).$$

Tällöin

$$\Lambda_n := \varphi_n(\mathcal{Q}_n) = \left\{(a_1 \log p_1, \ldots, a_n \log p_n) \in \mathbb{R}^n \mid a_i \in \mathbb{Z}\right\}$$

on n-asteinen hila. Määritellään lisäksi

$$L_x := \varphi_n(\mathcal{B}_x) = \left\{ y \in \Lambda_n \;\middle|\; \sum_{\substack{i=1 \\ y_i>0}}^{n} y_i \leq B(x) \text{ ja } \sum_{\substack{i=1 \\ y_i<0}}^{n} |y_i| \leq B(x) \right\},$$

jolloin

$$L_x \subset V_x := \left\{ y \in \mathbb{R}^n \;\middle|\; \sum_{\substack{i=1 \\ y_i>0}}^{n} y_i \leq B(x) \text{ ja } \sum_{\substack{i=1 \\ y_i<0}}^{n} |y_i| \leq B(x) \right\}.$$

Käytämme todistuksessa oleellisesti hyväksi tietoa, että järjestämättömien parien $\pm y \in \Lambda_n \setminus \{0\}$ ja Abc-summien (a,b,c), joille $\mathrm{rad}(bc) \mid \prod_{i=1}^{n} p_i$ välillä on bijektio siten, että

$$(a,b,c) \mapsto \{\varphi_n\Big(\frac{b}{c}\Big), \varphi_n\Big(\frac{b}{c}\Big)\}.$$

Saman bijektiivisen kuvauksen nojalla parit $\pm y \in L_x \setminus \{0\}$ vastaavat abc-summia (a,b,c), joille $\mathrm{rad}(bc) \mid \prod_{i=1}^{n} p_i$ ja $\log c \leq B(x)$.

Määritellään joukko

$$\mathcal{Q}_{n,m} := \left\{ \frac{b}{c} \in \mathcal{Q}_n \;\middle|\; b \equiv c \pmod{2^m};\, b,c \in \mathbb{N} \text{ ja } \mathrm{syt}(b,c) = 1 \right\}$$

ja vastaavasti $\Lambda_{n,m} := \varphi_n(\mathcal{Q}_{n,m})$. Koska alkiot 3 ja 5 virittävät ryhmän $(\mathbb{Z}/2^m\mathbb{Z})^*$, on olemassa surjektiivinen homomorfismi $\mathcal{Q}_n \to (\mathbb{Z}/2^m\mathbb{Z})^*$, jonka ydin on joukko $\mathcal{Q}_{n,m}$. Näin ollen on joukot $\mathcal{Q}_n/\mathcal{Q}_{n,m}$ ja $(\mathbb{Z}/2^m\mathbb{Z})^*$ ovat isomorfiset. Tällöin koska $|\mathcal{Q}_n/\mathcal{Q}_{n,m}| = 2^{m-1}$, myös

$$|\Lambda_n/\Lambda_{n,m}| = 2^{m-1} \tag{3.9}$$

Olkoon sitten $\alpha \in \mathbb{Q} \cap (0,1)$ ja olkoon $\beta := 1-\alpha$ sekä merkitään luvun α nimittäjää luvulla $d \in \mathbb{N}$. Valitaan luku $m \in \mathbb{Z}$ siten, että $d \mid m$ ja

$$2^{m-d} < \frac{\mathrm{vol}_n V_x}{2^n \det \Lambda_n} \leq 2^m. \tag{3.10}$$

Lemman 2.5.2 ja tiedon $\det \Lambda_n = \prod_{i=1}^{n} \log p_i$ nojalla

$$\begin{aligned} 2^m \geq \frac{\mathrm{vol}_n V_x}{2^n \det \Lambda_n} &= \frac{(2n)!B(x)^n}{(n!)^3 2^n \prod_{i=1}^{n} \log p_i} \\ &= \exp\left(\log\left(\left(\frac{(2n)!B(x)^n}{(n!)^3 2^n} \right) \Big(\prod_{i=1}^{n} \log p_i \Big)^{-1} \right) \right) \\ &= \exp\left(\log\left(\frac{(2n)!B(x)^n}{(n!)^3 2^n} \right) - \sum_{i=1}^{n} \log\log p_i \right) \end{aligned} \tag{3.11}$$

Käyttämällä Stirlingin kaavaa, $\log n! = n\log n - n + \mathcal{O}(\log n)$, saadaan edelleen

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

Käyttämällä tätä tietoa ja Lemmaa 2.7.5 saadaan epäyhtälöstä (3.11)

$$\begin{aligned} 2^m &\geq \exp\left(\log\left(\frac{(2n)!}{(n!)^3 2^n} B(x)^n\right) - \sum_{i=1}^{n} \log\log p_i\right) \\ &= \exp\left(n\log\left(\frac{2e}{n}\right) + \mathcal{O}(\log n) + n\log B(x) - n\log\left(\frac{x}{n}\right) + \mathcal{O}\left(\frac{x}{\log^3 x}\right)\right) \\ &= \exp\left(n\log\left(\frac{2eB(x)}{x}\right) + \mathcal{O}\left(\frac{x}{\log^3 x}\right)\right). \end{aligned} \tag{3.12}$$

Tarkastellaan sitten epäyhtälön (3.10) alarajaa. Koska $m = kd$ jollekin $k \in \mathbb{Z} \setminus \{0\}$, $\alpha m, \beta m \in \mathbb{Z}$ ja yhtälöistä (3.9) ja (3.10) saadaan

$$\mathrm{vol}_n(V_x) > 2^{m-d} 2^n \det \Lambda_n = 2^{\beta m+1-d} 2^n 2^{\alpha m-1} \det \Lambda_n = 2^{\beta m+1-d} 2^n \det \Lambda_{n,\alpha m},$$

sillä $m - \alpha m + 1 - d + n + \alpha m - 1 = m - d - n$. Myöhemmin todistuksessa nähdään, että $2^m \to \infty$, kun $x \to \infty$, joten riittävän suurella muuttujan x arvolla $2^{\beta m+1-d} \in \mathbb{N}$. Lauseen 2.5.1 nojalla 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 bijektion mukaan nämä pisteparit vastaavat $2^{\beta m+1-d}$ eri abc-summaa (a, b, c), joille $\log c \leq B(x)$ ja

$$\mathrm{rad}(bc) \,\Big|\, \prod_{i=1}^{n} p_i, \quad \text{ja} \quad 2^{\alpha m} \mid c - b = a. \tag{3.13}$$

Osoitetaan, että tarpeeksi suurilla muuttujan x arvoilla nämä abc-summat ovat itse asiassa abc-osumia. Kaavoista (3.12) ja (3.13) sekä Lemmasta 2.7.5 saadaan

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

Määritellään sitten rajoitefunktio B siten, että

$$\frac{x}{e}\left(\frac{x}{2eB(x)}\right)^{\alpha} = 1, \tag{3.14}$$

toisin sanoen

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

Näin ollen riittävän suurilla muuttujan x arvoilla pätee

$$\operatorname{rad}(abc) \leq c \exp\left(-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right)\right) < c,$$

siis kyseessä olevat *abc*-summat ovat *abc*-osumia. Tarpeeksi suurilla muuttujan x arvoilla siten *abc*-osumien lukumäärälle pätee

$$N\big(\exp\big(B(x)\big)\big) \geq 2^{\beta m+1-d}. \tag{3.15}$$

Epäyhtälöstä (3.12) saadaan yhtälöstä (3.14) $\frac{2eB(x)}{x} = \left(\frac{x}{e}\right)^{\frac{1}{\alpha}}$ ja $n = \pi(x) - 1$ (2.7) soveltamalla arvio

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

Soveltamalla yllä olevaa epäyhtälöön (3.15) saadaan tarpeeksi suurille muuttujan x arvoille edelleen arvio

$$\begin{aligned}
N\big(\exp\big(B(x)\big)\big) &\geq \exp\big(\log 2^{m\beta+1-d}\big) = \exp\left(\beta\log 2^m + (1-d)\log 2\right) \\
&\geq \exp\left(\beta\log\left[\exp\left(\frac{x}{\alpha}\left(1 + \frac{1}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right)\right)\right)\right] + (1-d)\log 2\right) \\
&= \exp\left(\frac{\beta}{\alpha}x\left(1 + \frac{1}{\log^2 x} + \mathcal{O}\left(\frac{1}{\log^3 x}\right) + \frac{\alpha}{\beta x}[(1-d)\log 2]\right)\right) \\
&\geq \exp\left(\frac{\beta}{\alpha}x\right) = \exp\left(\frac{1-\alpha}{\alpha}\Big(e\big(2eB(x)\big)^{\alpha}\Big)^{\frac{1}{\alpha+1}}\right) \\
&= \exp\left(\big[\frac{1}{\alpha} - 1\big]e^{\frac{1}{\alpha+1}}e^{\frac{\alpha}{\alpha+1}}2^{\frac{\alpha}{\alpha+1}}B(x)^{\frac{\alpha}{\alpha+1}}\right) \\
&= \exp\big(C'_\alpha B(x)^{\frac{\alpha}{1+\alpha}}\big),
\end{aligned}$$

missä $C'_\alpha := e(\frac{1}{\alpha} - 1)2^{\frac{\alpha}{\alpha+1}} > 0$. Koska kuvaus $x \mapsto \exp\big(B(x)\big) :]0,\infty[\to]1,\infty[$ on surjektio ja monotonisesti kasvava, tarpeeksi suurelle muuttujalle X pätee

$$N(X) \geq \exp\big(C'_\alpha(\log X)^{\frac{\alpha}{1+\alpha}}\big). \tag{3.16}$$

Koska lisäksi $\frac{\alpha}{1+\alpha} > \frac{1}{2}$ aina, kun $\alpha > 1$, jokaista $\varepsilon > 0$ kohden on olemassa luku $C_\varepsilon > 0$ siten, että tarpeeksi suurilla muuttujan X arvoilla

$$N(X) \geq \exp\big(C'_\alpha(\log X)^{\frac{1}{2}-\varepsilon}\big).$$

Lopuksi nähdään, että jokaisella $\varepsilon > 0$ ja riittävän suurella muuttujan X arvolla

$$\log N(X) \geq C_{\frac{\varepsilon}{2}}(\log X)^{\frac{1}{2}-\frac{\varepsilon}{2}} = C_{\frac{\varepsilon}{2}}(\log X)^{\frac{1}{2}}(\log X)^{\frac{1}{2}-\varepsilon} \geq (\log X)^{\frac{1}{2}-\varepsilon}.$$

□

3.6 Logaritmisten Abc-osumien lukumäärästä

Määritellään sitten *abc*-summille tiukempi ehto.

Määritelmä 3.6.1. *Abc*-summaa (a, b, c) kutsutaan *logaritmiseksi abc-osumaksi*, mikäli $\mathrm{rad}(abc) < \frac{c}{\log c}$.

Huomautus 3.6.2. Kaikki logaritmiset *abc*-osumat ovat myös "tavallisia" *abc*-osumia, sillä kaikilla $c > e$ logaritmisille *abc*-osumille pätee epäyhtälöketju $\mathrm{rad}(abc) < \frac{c}{\log c} < c$.

Lause 3.6.3. *Logaritmisia abc-osumia on äärettömästi.*

Todistus. Osoitetaan väite konstruoimalla jono *abc*-kolmikoita, joille ehto on voimassa. Asetetaan

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

jolloin kolmikko (a_n, b_n, c_n) muodostaa *abc*-summan kaikilla $n \in \mathbb{N}$. Osoitetaan, että arvosta $n = 2$ lähtien *abc*-summat toteuttavat ehdon $\mathrm{rad}(a_n b_n c_n) < \frac{c_n}{\log c_n}$.

Näytetään ensin induktiolla, että $2^{n+3} \mid a_n$ kaikilla $n \in \mathbb{N}$.
1°) Tapaus $n = 1$: $a_1 = 7^2 - 1 = 48 = 2^4 \cdot 3$.
2°) Oletetaan, että väite pätee arvolla $n = k \geq 1$. Tällöin arvolla $n = k + 1$

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

jolloin induktio-oletuksesta ja kongruenssista $7^{2^k} \equiv 1^{2^k} \equiv 1 \equiv -1 \pmod 2$ seuraa, että $2^{(k+1)+3} \mid a_{k+1}$. Näin ollen väite pätee kohtien 1°) ja 2°) sekä induktioperiaatteen nojalla.

Osoitetaan lisäksi, että $25 \mid a_n$ kaikilla $n \in \mathbb{N} \setminus \{1\}$. Kongruenssin transitiivisuuden nojalla kaikilla luonnollisilla luvuilla $n \geq 2$

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

mistä väite seuraa.

Soveltamalla yllä olevia tuloksia saadaan

$$rad(a_n b_n c_n) \leq \frac{a_n}{2^{n+2}5} \cdot 1 \cdot 7 \leq \frac{7}{2^{n+2}5} c_n \leq \frac{7}{2^{n+2}4} c_n = \frac{7}{2^{n+4}} c_n.$$

Lauseen väitteen todistamiseksi riittää näyttää, että

$$\frac{7}{2^{n+4}} < \frac{1}{\log c_n} = \frac{1}{\log 7^{2^n}}.$$

Ristiinkertomalla ja termejä järjestelemällä saadaan epäyhtälö

$$2^{n+4} - 7 \cdot 2^n \log 7 = 2^n (2^4 - 7 \log 7) > 0.$$

Koska $2^n > 0$ kaikilla $n \in \mathbb{N} \setminus \{1\}$ ja $2^4 - 7 \log 7 \approx 2,38 > 0$, epäyhtälön vasen puoli positiivinen kaikilla $n \in \mathbb{N} \setminus \{1\}$. □

Huomautus 3.6.4. Todistuksen *abc*-summalle ehto

$$\frac{7}{2^{n+4}} < \frac{1}{\log c_n}$$

on paras mahdollinen tai ainakin 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 $n \in \mathbb{N} \setminus \{1\}$ arvoilla.

Merkitään logaritmisten *abc*-osumien lukumäärää funktiolla $N_{log} : \mathbb{R}_{\geq 0} \to \mathbb{Z}_{\geq 0}$,

$$N_{\log}(X) = \#\{\text{Logaritminen } abc\text{-osuma (a,b,c)} \mid c \leq X\}.$$

Vastaavalla tavalla kuin *abc*-osumien lukumäärälle voidaan myös logaritmisten *abc*-osumien lukumäärälle asettaa samanlainen alaraja:

Lause 3.6.5. *Jokaista $\varepsilon > 0$ kohti on olemassa $X_0 > 0$ siten, että kaikilla $X \geq X_0$ pätee*

$$N_{\log}(X) \geq \exp\left((\log X)^{\frac{1}{2}-\varepsilon}\right).$$

Todistus. Lauseen 3.5.6 todistuksessa määriteltiin rajoitefunktio B siten, että

$$B(x) = \frac{1}{2}\left(\frac{x}{e}\right)^{1+\frac{1}{\alpha}}, \tag{3.17}$$

jolloin riittävän suurilla muuttujan x arvoilla pätee

$$\operatorname{rad}(abc) \leq c \exp\left(-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right)\right) < c.$$

Osoitetaan, että riittävän suurilla muuttujan x arvoilla pätee tiukempi ehto

$$\exp\left(-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right)\right) < \frac{1}{\log c}, \tag{3.18}$$

jolloin tarkasteltavat *abc*-summat ovat logaritmisia *abc*-osumia. Koska epäyhtälön (3.18) molemmat puolet ovat positiivisia, voidaan ottaa puolittain logaritmi:

$$-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) < \log\left(\frac{1}{\log c}\right).$$

Osoitetaan lauseen väite näyttämällä, että riittävän suurilla muuttujan x arvoilla

$$-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) < \log\left(\frac{1}{B(x)}\right), \tag{3.19}$$

jolloin *abc*-summille asetetun ehdon $\log c \leq B(x)$ nojalla myös

$$-\frac{x}{\log^2 x} + \mathcal{O}\left(\frac{x}{\log^3 x}\right) < \log\left(\frac{1}{B(x)}\right) \leq \log\left(\frac{1}{\log c}\right).$$

Sijoittamalla nyt rajoitefunktio (3.17) epäyhtälöön (3.19) 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

$$\frac{x}{\log^2 x}+\mathcal{O}\left(\frac{x}{\log^3 x}\right)-\left(1+\frac{1}{\alpha}\right)\log x-\log C''_\alpha>0, \tag{3.20}$$

missä $C''_\alpha=(2e^{1+\frac{1}{\alpha}})^{-1}$ on vakio. Jaetaan epäyhtälön (3.20) tarkastelu kahteen osaan riippuen termin $\mathcal{O}\left(\frac{x}{\log^3 x}\right)=K\frac{x}{\log^3 x}$ kertoimesta $K\in\mathbb{R}$.

Jos $K\geq 0$, riittää tarkastella epäyhtälön (3.20) alaspäin arvioitua muotoa

$$\frac{x}{\log^2 x}-\left(1+\frac{1}{\alpha}\right)\log x-\log C''_\alpha>0.$$

Tällöin L'Hospitalin lausetta kolme kertaa soveltamalla saadaan

$$\begin{aligned}
\lim_{x\to\infty}\frac{\frac{x}{\log^2 x}}{-(1+\frac{1}{\alpha})\log x-\log C''_\alpha}&=\lim_{x\to\infty}\frac{x}{-(1+\frac{1}{\alpha})\log^3 x-\log C''_\alpha\log^2 x}\\
&=\lim_{x\to\infty}\frac{x}{-3(1+\frac{1}{\alpha})\log^2 x-2\log C''_\alpha\log x}\\
&=\lim_{x\to\infty}\frac{x}{-6(1+\frac{1}{\alpha})\log x-2\log C''_\alpha}\\
&=\lim_{x\to\infty}\frac{x}{-6(1+\frac{1}{\alpha})}=-\infty.
\end{aligned}$$

Näin ollen murtoluvun osoittaja kasvaa nimittäjää nopeammin. Raja-arvon määritelmän nojalla on olemassa luku $x_0>0$ siten, että epäyhtälö (3.20) on voimassa kaikilla $x>x_0$. Tällöin myös epäyhtälö (3.18) on voimassa.

Jos taas $K<0$, niin neljä kertaa L'Hospitalin lausetta soveltamalla saadaan

$$\begin{aligned}
\lim_{x\to\infty}\frac{\frac{x}{\log^2 x}}{K\frac{x}{\log^3 x}-(1+\frac{1}{\alpha})\log x-\log C''_\alpha}&=\lim_{x\to\infty}\frac{x\log x}{Kx-(1+\frac{1}{\alpha})\log^4 x-\log C''_\alpha\log^3 x}\\
&=\lim_{x\to\infty}\frac{x\log x+x}{Kx-4(1+\frac{1}{\alpha})\log^3 x-3\log C''_\alpha\log^2 x}\\
&=\lim_{x\to\infty}\frac{x\log x+2x}{Kx-12(1+\frac{1}{\alpha})\log^2 x-6\log C''_\alpha\log x}\\
&=\lim_{x\to\infty}\frac{x\log x+3x}{Kx-24(1+\frac{1}{\alpha})\log x-6\log C''_\alpha}\\
&=\lim_{x\to\infty}\frac{\log x+4}{K-4!(1+\frac{1}{\alpha})\frac{1}{x}}=-\infty.
\end{aligned}$$

Tässäkin tapauksessa murtoluvun osoittaja kasvaa nimittäjää nopeammin, joten raja-arvon määritelmän nojalla on olemassa luku $x_0>0$ siten, että kun $x>x_0$, epäyhtälö (3.20) toteutuu.

Tapausten tulokset yhdistämällä nähdään, että epäyhtälö (3.20) ja siten myös epäyhtälöt (3.19) ja (3.18) ovat voimassa tarpeeksi suurilla muuttujan x arvoilla. Väite seuraa analogisesti Lauseen 3.5.6 todistuksesta. □

3.7 Szpiron konjektuureista

Tässä alaluvussa tarkastellaan Szpiron elliptisille käyrille esittämiä konjektuureja, jotka ovat vaikuttaneet Abc-konjektuurin syntyyn. Lisäksi tarkastellaan Szpiron konjektuurien yhteyttä *Abc*-konjektuuriin. Tässä alaluvussa *Abc*-konjektuurilla tarkoitetaan ilman erillistä mainintaa yleistettyä muotoa, jossa sallitaan *abc*-summan termeille myös negatiiviset arvot.

Aloitetaan L. Szpiron vuonna 1983 esittämällä alkuperäisellä konjektuurilla [38].

Konjektuuri 3.7.1 (Szpiro, heikko muoto)**.** *On olemassa luvut $\alpha > 0$ ja $\beta > 0$ siten, että jokaiselle puolivakaalle elliptiselle käyrälle E pätee epäyhtälö*

$$|\Delta_E| \leq \alpha N_E^{\beta}.$$

Kokonaisluvuille saadaan analoginen tulos:

Konjektuuri 3.7.2. *On olemassa luvut $\alpha' > 0$ ja $\beta' > 0$ siten, että kaikille abc-summille $(a, b, c) \in \mathbb{Z}^3$, $abc \neq 0$, pätee epäyhtälö*

$$|abc| \leq \alpha' \operatorname{rad}(abc)^{\beta'}.$$

Huomautus 3.7.3. Konjektuuri 3.7.2 voidaan esittää myös pelkän radikaalin avulla [39]: On olemassa luku $s > 0$ siten, että kaikille *abc*-summille $(a, b, c) \in \mathbb{Z}^3$, $abc \neq 0$, pätee epäyhtälö

$$|abc| \leq \operatorname{rad}(abc)^s.$$

Tämä nähdään soveltamalla työn [43, s. 26] ajatusta seuraavasti: valitaan luku $r > 0$ siten, että $2^r \geq \alpha'$. Koska kaikilla *abc*-summilla $\operatorname{rad}(abc) \geq 2$, saadaan tällöin $\alpha' \leq \operatorname{rad}(abc)^r$. Väite seuraa valitsemalla $s = \beta' + r$.

Nähdään, että yllä oleva konjektuuri seuraa helposti *Abc*-konjektuurista.

Lause 3.7.4. *Konjektuurista 3.2.2 seuraa Konjektuuri 3.7.2.*

Todistus. Oletetaan, että Konjektuuri 3.2.2 on voimassa. Tällöin Huomautuksen 3.2.14 nojalla luku $C(\varepsilon)$,

$$C(\varepsilon) = \sup\left\{ \frac{\max\{|a|, |b|, |c|\}}{\operatorname{rad}(abc)^{1+\varepsilon}} : \operatorname{syt}(a, b) = 1,\ a + b = c \right\},$$

on äärellinen jokaisella $\varepsilon > 0$. Näin ollen Konjektuuria 3.2.2 soveltamalla saadaan

$$|abc| \leq \left(\max\{|a|, |b|, |c|\}\right)^3 \leq \left(C(\varepsilon) \operatorname{rad}(abc)^{1+\varepsilon}\right)^3,$$

mistä väite seuraa valitsemalla $\alpha' = C(\varepsilon)^3$ ja $\beta' = 3(1 + \varepsilon)$. □

Konjektuurissa 3.7.1 ei aseteta tarkemmin rajaa luvulle β. Seuraava konjektuuri tunnetaan *vahvana Szpiron konjektuurina.*

Konjektuuri 3.7.5 (Szpiro, vahva muoto)**.** *Kaikilla $\varepsilon > 0$ on olemassa vakio $C(\varepsilon) > 0$ siten, että kaikille rationaalisille elliptisille käyrille pätee epäyhtälö*

$$|\Delta_E| \leq C(\varepsilon) N_E^{6+\varepsilon}.$$

Osoitetaan lähteisiin [38, s. 168] ja [35, ss. 4–5] perustuen, että konjektuurin väite on paras mahdollinen.

Szpiron konjektuurin vahvan muodon avulla voidaan osoittaa seuraava *abc*-summiin liittyvä konjektuuri [35, ss. 7–8].

Konjektuuri 3.7.6. *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*

$$|abc| \leq C(\varepsilon) \operatorname{rad}(abc)^{3+\varepsilon}.$$

Lause 3.7.7. *Konjektuurista 3.7.5 seuraa Konjektuuri 3.7.6.*

Huomautus 3.7.8. Konjektuurin 3.7.6 mukaan osamäärä

$$\rho = \rho(a, b, c) = \frac{\log |abc|}{\log \operatorname{rad}(abc)} \tag{3.21}$$

on rajoitettu. Osamäärää (3.21) kutsutaan *abc*-kolmikon *Szpiron osamääräksi* (engl. Szpiro ratio). Taulukko parhaista Spiron osamääristä on liitteessä ???.

Osoitetaan, että edellä oleva konjektuuri on seuraus Szpiron konjektuurin vahvasta muodosta [35, ss. 7–8].

Lause 3.7.9. *Konjektuuri 3.7.5 implikoi Konjektuurin 3.7.6*

Todistus. Oletetaan, että nollasta eroaville luvuille a, b ja c pätee ehdot

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

Lemman 2.4.9 nojalla tällöin käyrä

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

on minimaalimalli, jolloin Konjektuuria 3.7.5 soveltamalla 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

$$|abc| \leq 16 C_1(\varepsilon)^{\frac{1}{2}} \operatorname{rad}(abc)^{3+\frac{\varepsilon}{2}},$$

mistä väite seuraa merkitsemällä $\varepsilon' = \frac{\varepsilon}{2}$ ja $C(\varepsilon') = 16 C_1(\varepsilon)^{\frac{1}{2}}$. □

Seuraavaa konjektuuria kutsutaan myös Lang-Szpiron konjektuuri [36].

Konjektuuri 3.7.10. *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*

$$\operatorname{syt}(Au, Bv) = 1 \quad ja \quad k = Au^3 + Bv^2, \tag{3.22}$$

niin tällöin

$$|u| \leq c(\varepsilon, A, B) \operatorname{rad}(k)^{2+\varepsilon} \quad ja \quad |v| \leq c(\varepsilon, A, B) \operatorname{rad}(k)^{3+\varepsilon}$$

Osoitetaan, että yllä oleva konjektuuri on yhtäpitävä yleistetyn *Abc*-konjektuurin kanssa.

Lause 3.7.11. *Konjektuuri on 3.2.2 ja Konjektuuri 3.7.10 ovat ekvivalentteja.*

Todistus. Oletetaan ensin, että Konjektuuri 3.2.1 on voimassa. Olkoot $A, B \in \mathbb{Z}$ suhteellisia alkulukuja ja $u, v, k \in \mathbb{Z}$ ehdot (3.22) toteuttavia lukuja. Konjektuurin 3.2.2 nojalla saadaan

$$|Bv^2| \leq \max\left\{|Au^3|, |Bv^2|, |k|\right\} \leq C_1(\varepsilon) \operatorname{rad}(ABuvk)^{1+\varepsilon} \leq C_1(\varepsilon)|ABuv|^{1+\varepsilon} \operatorname{rad}(k)^{1+\varepsilon},$$

josta edelleen

$$|v|^2 \leq \frac{C_1(\varepsilon)|AB|^{1+\varepsilon}}{|B|}|uv|^{1+\varepsilon} \operatorname{rad}(k)^{1+\varepsilon} = C_2(\varepsilon, A, B)|uv|^{1+\varepsilon} \operatorname{rad}(k)^{1+\varepsilon}, \tag{3.23}$$

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 (3.23) saadaan

$$|v|^2 \leq C_2(\varepsilon, A, B) C_3(A, B)^{1+\varepsilon} |u|^{\frac{5}{3}(1+\varepsilon)} \operatorname{rad}(k)^{1+\varepsilon},$$

josta edelleen puolittain termillä $|u|^{\frac{5}{3}(1+\varepsilon)}$ jakamalla

$$|v|^{\frac{1-5\varepsilon}{3}} \leq C_4(\varepsilon, A, B) \operatorname{rad}(k)^{1+\varepsilon}, \tag{3.24}$$

missä $C_4(\varepsilon, A, B) = C_2(\varepsilon, A, B) C_3(A, B)^{1+\varepsilon}$. Valitaan nyt ε väliltä $\left(0, \frac{1}{5}\right)$, jolloin $1 - 5\varepsilon > 0$, ja määritellään $\varepsilon' = \frac{18\varepsilon}{1-\varepsilon}$, jolloin $3 + \varepsilon' = \frac{3(1+\varepsilon)}{1-5\varepsilon}$. Tällöin $\varepsilon' > 0$ ja epäyhtälöstä (3.24) saadaan

$$|v| \leq \left(C_4(\varepsilon, A, B)\right)^{\frac{3}{1-5\varepsilon}} \operatorname{rad}(k)^{\frac{3}{1-5\varepsilon}(1+\varepsilon)} = C_5(\varepsilon', A, B) \operatorname{rad}(k)^{3+\varepsilon'},$$

missä $C_5(\varepsilon', A, B) = \left(C_4(\varepsilon, A, B)\right)^{\frac{3}{1-5\varepsilon}}$. Epäyhtälöstä $|u| \leq C_3(A, B)|v|^{\frac{2}{3}}$ saadaan edelleen

$$|u| \leq C_3(A, B)\left(C_5(\varepsilon', A, B) \operatorname{rad}(k)^{3+\varepsilon'}\right)^{\frac{2}{3}} \leq C_6(\varepsilon', A, B) \operatorname{rad}(k)^{2+\varepsilon},$$

missä $C_6(\varepsilon', A, B) = C_3(A, B)\left(C_5(\varepsilon', A, B)\right)^{\frac{2}{3}}$. Näin ollen Konjektuuri 3.7.10 on voimassa. Tapauksessa $|Au^3| \geq |Bv^2|$ päättely on oleellisesti samanlainen.

Oletetaan kääntäen, että Konjektuuri 3.7.10 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 2.4.5 nojalla luvut c_4 ja c_6 sekä käyrän diskriminantti ovat tällöin

$$\begin{aligned} c_4 &= 16(a^2+ab+b^2) \\ c_6 &= -32(b-a)(a+2b)(2a+b) \\ \Delta &= 16\big(ab(a+b)\big)^2 \end{aligned}$$

Lemman 2.4.4 mukaan $1728\Delta = c_4^3 - c_6^2$, joten sijoittamalla yllä olevat luvut ja jakamalla luvulla 4096 saadaan yhtälö

$$(a^2+ab+b^2)^3 - \big(\tfrac{1}{2}(b-a)(a+2b)(2a+b)\big)^2 = 3^3\big(\tfrac{1}{2}ab(a+b)\big)^2.$$

Koska $\operatorname{syt}(a,b)=1$, niin Lemmaa 2.1.10 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 $k = \big(\frac{1}{2}ab(a+b)\big)^2$. Mikäli taas suurin yhteinen tekijä on yksi, valitaan $k = 3^3\big(\frac{1}{2}ab(a+b)\big)^2$. Tällöin yhtälö toteuttaa ehdot (3.22) arvoilla $A=1$ ja $B=-1$, jolloin Konjektuuria 3.7.10 soveltamalla saadaan

$$a^2 \le a^2+ab+b^2 \le C_1(\varepsilon,1,-1)\operatorname{rad}(k)^{2+\varepsilon} \le 3C_1(\varepsilon,1,-1)\operatorname{rad}(abc)^{2+\varepsilon}, \tag{3.25}$$

josta edelleen

$$a \le C_2(\varepsilon)\operatorname{rad}(abc)^{1+\frac{\varepsilon}{2}}, \tag{3.26}$$

missä $C_2(\varepsilon) = \big(3C_1(\varepsilon,1,-1)\big)^{\frac{1}{2}}$. 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

$$c = a+b \le C(\varepsilon')\operatorname{rad}(abc)^{1+\varepsilon'}.$$

Näin ollen Konjektuuri 3.2.2 on voimassa. □

Osoitetaan seuraavaksi kirjaan [46, ss. 259–260] perustuen, että yleistetty *Abc*-konjektuuri implikoi Szpiron konjektuurin vahvan muodon.

Lause 3.7.12. *Konjektuurista 3.2.2 seuraa Konjektuuri 3.7.5.*

Todistus. □

3.8 *Abc*-konjektuurin vahvasta 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 ([47], 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 ehdollinen tulos [36].

Lause 3.8.1. *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 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*-kolmikoista 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

$$L(a_n, b_n, c_n) \leq 1 + \varepsilon + \frac{\log C(\varepsilon)}{\log \operatorname{rad}(a_n b_n c_n)}.$$

toteutuu kaikilla $n \in \mathbb{N}$. Valitaan luku ε siten, että $1 + \varepsilon < L(a_0, b_0, c_0)$. Lauseen 3.1.14 nojalla radikaali $\operatorname{rad}(a_n b_n c_n)$ kasvaa rajatta, kun $n \to \infty$. Näin ollen saadaan

$$\lim_{n\to\infty} L(a_n, b_n, c_n) \leq 1 + \varepsilon < L(a_0, b_0, c_0),$$

mikä on ristiriita. □

Monien mielestä seuraava heikko konjektuuri pitää paikkansa [3]

Konjektuuri 3.8.2. *Kaikilla abc-kolmikoilla* $(a, b, c) \in \mathbb{N}^3$ *pätee epäyhtälö*

$$c < \operatorname{rad}(abc)^2.$$

Taulukoiden perusteella voidaankin asettaa *Abc*-konjektuurille efektiivinen muoto.

Konjektuuri 3.8.3. *Kaikilla abc-kolmikoilla* $(a, b, c) \in \mathbb{N}^3$ *pätee epäyhtälö*

$$c < \operatorname{rad}(abc)^{1.63}.$$

3.9 Fermat'n suuri lause

Abc-konjektuurin syntyä on vahvasti innoittanut Fermat'n suuri lause, joten käsitellään sitä vielä tässä luvussa tarkemmin.

Lause 3.9.1 (Fermat'n suuri lause)**.** *Yhtälöllä*

$$x^n + y^n = z^n, \tag{3.27}$$

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 positiivinen kokonaislukukolmikko (x, y, z) toteuttaa yhtälön (3.27) ja 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.

Abc-konjektuurin avulla voidaan todistaa Fermat'n suuren lauseen asymptoottinen muoto:

Lause 3.9.3. *Abc-konjektuurin nojalla on olemassa positiivinen kokonaisluku n_0 siten, että yhtälöllä (3.27) ei ole suhteellisia alkulukuratkaisuja millään eksponentilla $n \geq n_0$.*

Todistus. Olkoot x, y ja z positiivisia suhteellisia alkulukuja siten, että

$$x^n + y^n = z^n.$$

Tällöin

$$\mathrm{rad}(x^n y^n z^n) = \mathrm{rad}(xyz) \leq xyz \leq z^3.$$

Jos nyt $n \geq 2$, niin $z \geq 3$. Soveltamalla abc-konjektuuria arvoilla $\varepsilon = 1$ ja $K_1 = \max\{1, K(1)\}$ saadaan

$$z^n = \max\{x^n, y^n, z^n\} \leq K_1 \mathrm{rad}(x^n y^n z^n)^2 < K_1 z^6,$$

josta edelleen

$$n < 6 + \frac{\log K_1}{\log z} \leq 6 + \frac{\log K_1}{\log 3}.$$

Väite seuraa. □

Mikäli *Abc*-konjektuurista saadaan saadaan osoitettua efektiivinen muoto, saadaan tuloksia parannettua seuraavasti.

Lause 3.9.4. *Konjektuurin 3.8.2 nojalla yhtälöllä (3.27) ei ole suhteellisia alkulukuratkaisuja millään $n \geq 6$.*

Todistus. Olkoot x, y ja z positiivisia suhteellisia alkulukuja siten, että

$$x^n + y^n = z^n.$$

Tällöin

$$\mathrm{rad}(x^n y^n z^n) = \mathrm{rad}(xyz) \leq xyz \leq z^3.$$

Konjektuurin 3.8.2 nojalla

$$z^n = \max\{x^n, y^n, z^n\} \leq \mathrm{rad}(x^n y^n z^n)^2 < z^6,$$

josta edelleen $n < 6$. Väite seuraa. □

Lausetta voidaan vielä tiukentaa.

Lause 3.9.5. *Konjektuurin 3.8.3 nojalla yhtälöllä (3.27) ei ole suhteellisia alkulukuratkaisuja millään $n \geq 5$.*

Testi

4 *Abc*-konjektuurin seurauksia

Tässä kappaleessa tarkastellaan *Abc*-konjektuurin seurauksia lähinnä lukuteorian kannalta, mutta viimeisessä kohdassa laajennetaan tarkstelua täydellisyyden vuoksi myös muihin yhteyksiin. On huomattavaa, että vaikka *Abc*-konjketuurin avulla ei usein voida suoraan todistaa monia konjektuureja, pystytään kuitenkin osoittamaan vain äärellisen monen ratkaisun olemassaolo. Mikäli *Abc*-konjektuurissa luvusta $\varepsilon > 0$ riippuva vakio $C(\varepsilon)$ voitaisiin määrittää efektiivisesti, saataisiin ratkaisujen lukumäärälle numeerinen yläraja nykyisen "äärellisen määrän" sijaan.

[33]

4.1 *Abc*-kolmikoihin liittyviä tuloksia

Soveltamalla *Abc*-konjektuuria sen oletukset toteuttaaviin kolmikoihin saadaan muutamia mielenkiintoisia tuloksia.

Lause 4.1.1. *Abc-konjektuurin nojalla kaikilla $\varepsilon > 0$ on olemassa vakio $C(\varepsilon)$ siten, että kaikille abc-summille $(x_1, x_2, x_3) \in \mathbb{N}^3$ pätee*

$$x_i \leq C(\varepsilon)\,\mathrm{rad}(x_i)^{3+\varepsilon}$$

kaikilla $i = 1, 2, 3$.

Todistus. *Abc*-konjektuurin nojalla kaikilla $i = 1, 2, 3$ pätee

$$x_i \leq C(\varepsilon)\,\mathrm{rad}(x_1x_2x_3)^{1+\varepsilon},$$

joten kertomalla puolittain yhtälöt saadaan

$$x_1x_2x_3 \leq C(\varepsilon)^3\,\mathrm{rad}(x_1x_2x_3)^{3+\varepsilon}.$$

Oletetaan vastoin väitettä, että kaikilla $i = 1, 2, 3$ pätee

$$x_i > C(\varepsilon)\,\mathrm{rad}(x_i)^{1+\varepsilon}, \tag{4.1}$$

jolloin kertomalla puolittain yhtälöt (4.1) saadaan

$$x_1x_2x_3 > C(\varepsilon)^3\,\mathrm{rad}(x_1x_2x_3)^{3+\varepsilon}.$$

Tämä on ristiriita *Abc*-konjektuurin kanssa. □

Abc-konjektuurin avulla saadaan myös seuraava tulos.

Lause 4.1.2. *Abc-konjektuurin nojalla kaikilla $\varepsilon > 0$ on olemassa vakio $K(\varepsilon) > 0$ siten, että kaikilla $x, n \in \mathbb{N}_{\geq 2}$*

$$x^{n-1} \leq K(\varepsilon)\,\mathrm{rad}(x^n - 1)^{1+\varepsilon}.$$

Todistus. Valitaan luku ε siten, että $0 < \varepsilon < \frac{1}{2}$. Soveltamalla nyt *Abc*-konjektuuria summaan $(x^n - 1) + 1 = x^n$ saadaan

$$x^n \leq C(\varepsilon) \operatorname{rad}\big((x^n - 1)x^n\big)^{1+\varepsilon} \leq \operatorname{rad}(x^n - 1)^{1+\varepsilon} x^{1+\varepsilon},$$

josta jakamalla puolittain luvulla $x^{1+\varepsilon}$ 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 on seuraa suoraan epäyhtälöstä $n - 1 - 2\varepsilon > 0$ sekä oletuksista $0 < \varepsilon < \frac{1}{2}$ ja $n \geq 2$, ja

$$\frac{(n-1)(1+\varepsilon)}{n-1-\varepsilon} \leq \frac{(n-1-\varepsilon)(1+\varepsilon)}{n-1-\varepsilon} = 1 + \varepsilon \leq \frac{1+\varepsilon}{1-\varepsilon} = \frac{1-\varepsilon+2\varepsilon}{1-\varepsilon} = 1 + \varepsilon',$$

missä $\varepsilon' = \frac{2\varepsilon}{1-\varepsilon}$. Näin ollen väite seuraa, kun valitaan $K(\varepsilon) = C(\varepsilon)^2$. □

Osoitetaan vielä yksi tulos.

Lause 4.1.3. *Olkoon kolmikko $(x_1, x_2, x_3) \in \mathbb{N}$ 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 nyt *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 kertomalla yllä olevan epäyhtälö puolittain luvulla d ja käyttämällä arviota $d \leq d^{1+\varepsilon}$. □

4.2 Hallin konjektuuri

Vuonna 1971 M. Hall esitti täydellisten neliöiden ja täydellisten kuutioiden erotuksella olevan seuraavanlaisen alarajan [35]:

Konjektuuri 4.2.1. (Hall, alkuperäinen) *Olkoot u ja v nollasta eroavia suhteellisia alkulukuja siten, että $u^3 - v^2 \neq 0$. Tällöin on olemassa vakio $C > 0$ siten, että*

$$C|u^3 - v^2| > |u|^{\frac{1}{2}-\varepsilon}.$$

Osoiteteen seuraava väite kirjaan [27] pohjautuen.

Lause 4.2.2. *Abc-konjektuurin nojalla Hallin alkuperäinen konjektuuri on voimassa.*

Todistus. Osoitetaan ensin yleisempi tapaus, jonka erityistapauksena saadaan lauseen väite. Olkoot $A, B \in \mathbb{Z} \setminus \{0\}$ ja olkoot $m, n \in \mathbb{N}$ siten, että $mn > m + n$. Tarkastellaan yhtälöä

$$Au^m + Bv^n = k. \tag{4.2}$$

Tällöin kolmikko (Au^m, Bv^n, k) muodostaa *abc*-summan. Olkoon $\varepsilon > 0$. Soveltamalla *Abc*-konjektuuria ja Lemmaa 3.1.7 saadaan

$$|u|^m \leq |k| \leq C(\varepsilon) \operatorname{rad}(|Au^m||Bv^n||k|)^{1+\varepsilon} \leq C_1(\varepsilon)\big(|uv| \operatorname{rad}(|k|)\big)^{1+\varepsilon},$$

missä $C_1(\varepsilon) = C(\varepsilon) \operatorname{rad}(|A|)^{1+\varepsilon} \operatorname{rad}(|B|)^{1+\varepsilon}$. Vastaavanlainen päättely osoittaa, että sama yläraja pätee myös luvulle $|v|^n$. Oletetaan sitten, että $|Au^m| \leq |Bv^n|$, jolloin

$$|u| \leq \left|\frac{B}{A}\right| |v|^{\frac{n}{m}}. \tag{4.3}$$

Sijoittamalla tämä tieto yllä olevaan epäyhtälöön saadaan uudeksi ylärajaksi

$$|v|^n \leq C_2(\varepsilon)\big(|v|^{1+\frac{n}{m}} \operatorname{rad}(k)\big)^{1+\varepsilon} = C_2(\varepsilon)|v|^{(1+\frac{n}{m})(1+\varepsilon)} \operatorname{rad}(|k|)^{1+\varepsilon},$$

missä $C_2(\varepsilon) = C_1(\varepsilon)\left|\frac{B}{A}\right|^{1+\varepsilon}$. Näin ollen

$$|v|^{n-(\frac{m+n}{m})(1+\varepsilon)} = |v|^{\frac{nm-(m+n)(1+\varepsilon)}{m}} \leq C_2(\varepsilon) \operatorname{rad}(|k|)^{1+\varepsilon},$$

josta edelleen

$$|v| \leq C_2(\varepsilon) \operatorname{rad}(k)^{\frac{m(1+\varepsilon)}{nm-(m+n)(1+\varepsilon)}}. \tag{4.4}$$

Muuttujalle u saadaan tällöin ylärajaksi yhtälöiden (4.3) ja (4.4) nojalla

$$|u| \leq \left|\frac{B}{A}\right| C_2(\varepsilon)^{\frac{n}{m}} \operatorname{rad}(|k|)^{\frac{m(1+\varepsilon)}{nm-(m+n)(1+\varepsilon)} \cdot \frac{n}{m}} = C_3(\varepsilon) \operatorname{rad}(|k|)^{\frac{n(1+\varepsilon)}{nm-(m+n)(1+\varepsilon)}}, \tag{4.5}$$

missä $C_3(\varepsilon) = \left|\frac{B}{A}\right| C_2(\varepsilon)^{\frac{n}{m}}$. Näin ollen yhdistämällä yhtälöt (4.2) sekä (4.4) ja (4.5) saadaan

Osoitetaan sitten lauseen väite. Asettamalla $A = B = 1$ sekä $m = 3$ ja $n = 2$ saadaan

$$|k| \leq$$

$$|u| \leq C_3(\varepsilon) k^{\frac{2+2\varepsilon}{6-5(1+ve)}} = C_3(\varepsilon) k^{\frac{2-10\varepsilon+10\varepsilon+2\varepsilon}{1-5\varepsilon}} = C_3(\varepsilon) k^{2+\frac{12\varepsilon}{1-5\varepsilon}},$$

josta edelleen

$$|u|^{\frac{1}{2}-\frac{12\varepsilon}{1-5\varepsilon}} \leq C_3(\varepsilon) k^{(2+\frac{12\varepsilon}{1-5\varepsilon})(\frac{1}{2}-\frac{12\varepsilon}{1-5\varepsilon})} = C_3 k^{1-\frac{3}{2}\cdot\frac{12\varepsilon}{1-5\varepsilon}-(\frac{12\varepsilon}{1-5\varepsilon})^2}.$$

Sijoittamalla nyt $\varepsilon' = \frac{12\varepsilon}{1-5\varepsilon}$ saadaan

$$|u|^{\frac{1}{2}-\varepsilon'} \leq C_3 k^{1-\frac{3}{2}\varepsilon'-\varepsilon'^2} < C_3 k,$$

mistä väite seuraa. □

4.3 Luvuista, joilla on samat alkutekijät

Tarkastellaan seuraavan konjektuurin yhteyttä *Abc*-konjektuuriin artikkelin [8] mukaisesti.

Konjektuuri 4.3.1. (Dressler) *Olkoot $a, c \in \mathbb{N}$ siten, että luvuilla a ja c on samat alkutekijät ja $a < c$. Tällöin on olemassa alkuluku p, jolle pätee*

$$a \leq p < c.$$

Konjektuuri 4.3.2. *Olkoot $a, c \in \mathbb{N}$ siten, että luvuilla a ja c on samat alkutekijät sekä $a < c$. Tällöin jokaista $\varepsilon > 0$ kohti on olemassa luku $C(\varepsilon)$ siten, että*

$$c - a \geq C(\varepsilon) a^{\frac{1}{2}-\varepsilon}.$$

Osoitetaan seuraava.

Lause 4.3.3. *Abc-konjektuurin nojalla Konjektuuri 4.3.2 on voimassa.*

Todistus. Oletetaan, että luvut a ja c ovat Konjektuurin 4.3.2 oletukset täyttäviä lukuja ja asetetaan $b = c - a$. Määritellään luvut P ja d siten, että $P = \operatorname{rad}(a) = \operatorname{rad}(c)$ ja $d = \operatorname{syt}(a, b) = \operatorname{syt}(a, c) = \operatorname{syt}(b, c)$. Tällöin kolmikko $(\frac{a}{d}, \frac{b}{d}, \frac{c}{d})$ muodostaa *abc*-summan. Radikaalille saadaan arvio

$$\operatorname{rad}\left(\frac{a}{d}\frac{b}{d}\frac{c}{d}\right) \leq \operatorname{rad}(ac) \operatorname{rad}\left(\frac{b}{d}\right) \leq P \cdot \frac{b}{d} \leq \frac{b^2}{d},$$

missä viimeinen epäyhtälö seuraa tiedosta $P \mid b$. Soveltamalla nyt *Abc*-konjektuuria edellä mainittuun *abc*-summaan 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

$$b \geq C(\varepsilon)^{-\frac{1}{2(1+\varepsilon)}} c^{\frac{1}{2(1+\varepsilon)}} = C'(\varepsilon) c^{\frac{1}{2}-\frac{\varepsilon}{2(1+\varepsilon)}} \geq C'(\varepsilon) c^{\frac{1}{2}-\varepsilon}$$

missä $C'(\varepsilon) = C(\varepsilon)^{-\frac{1}{2(1+\varepsilon)}}$. Koska $b = c - a$, väite seuraa. □

Itse asiassa seuraava Konjektruurin 4.3.2 mukainen tulos on voimassa .

Lause 4.3.4. *Olkoot $a, c \in \mathbb{N}$ siten, että luvuilla a ja c on samat alkutekijät sekä $a < c$. Tällöin jokaista $\varepsilon > 0$ kohti on olemassa luku $C(\varepsilon)$ siten, että*

$$c - a \geq C(\varepsilon) a^{\frac{1}{2}-\varepsilon}.$$

4.4 Catalanin ja Pillain konjektuuri

Vuonna 1844 E. C. Catalan esitti konjektuurin, jonka mukaan 8 ja 9 ovat ainoat peräkkäiset kokonaislukupotenssit [44, s. 201]. Formaalimmin konjektuuri voidaan esittää muodossa

Konjektuuri 4.4.1. (Catalan) *Olkoot $x, y, m, n \in \mathbb{N} \setminus \{1\}$. Tällöin yhtälöllä*

$$x^m - y^n = 1 \tag{4.6}$$

on vain ratkaisu $(x, y, m, n) = (3, 2, 2, 3)$.

Aiemmin on pystytty osoittamaan muun muassa, että yhtälöllä (4.10) 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) [44, ss. 216-217]. Läpimurto saatiin viimein vuonna 2002, kun P. Mihăilescu osoitti konjektuurin todeksi käyttämällä hyväksi syklotomisten kuntien teoriaa [31]. Näytetään seuraavaksi kirjaan [33, ss. 186-187] perustuen, että myös *Abc*-konjektuurilla on yhteys Mihăilescun todistamaan tulokseen.

Lause 4.4.2. *Abc-konjektuurin nojalla yhtälöllä (4.10) on vain äärellisen monta ratkaisua.*

Todistus. Olkoon (x, y, m, n) yhtälön (4.10) ratkaisu. Edellä olleen huomautuksen nojalla riittää tarkastella tilannetta $\min\{m, n\} \geq 3$. Tällöin x ja y ovat suhteellisia alkulukuja. Soveltamalla *abc*-konjektuuria arvolla $\varepsilon = \frac{1}{4}$ ja vakiolla $K_2 = C(\frac{1}{4})$ saadaan

$$y^n < x^m \leq K_2 \mathrm{rad}(x^m y^n) = K_2 \mathrm{rad}(xy)^{\frac{5}{4}} \leq K_2 (xy)^{\frac{5}{4}},$$

josta seuraa yhtälöt

$$m \log x \leq \log K_2 + \frac{5}{4}(\log x + \log y) \tag{4.7}$$

$$n \log y < \log K_2 + \frac{5}{4}(\log x + \log y). \tag{4.8}$$

Laskemalla yhtälöt (4.7) ja (4.8) puolittain yhteen saadaan

$$m \log x + n \log y < 2 \log K_2 + \frac{5}{2}(\log x + \log y),$$

josta edelleen termejä järjestelemällä

$$\left(m - \frac{5}{2}\right) \log x + \left(n - \frac{5}{2}\right) \log y < 2 \log K_2. \tag{4.9}$$

Koska oletuksen nojalla $x \geq 2$ ja $y \geq 2$, saadaan

$$(m + n - 5) \log 2 = \left(m - \frac{5}{2}\right) \log 2 + \left(n - \frac{5}{2}\right) \log 2 \leq \left(m - \frac{5}{2}\right) \log x + \left(n - \frac{5}{2}\right) \log y,$$

jolloin sijoittamalla yhtälöön (4.9) saadaan

$$m + n < \frac{2 \log K_2}{\log 2} + 5.$$

Koska epäyhtälön oikea puoli on vakio, yhtälöllä (4.10) on vain äärellinen määrä ratkaisuja eksponenttiparilla (m, n). Näin ollen kiinnitetyillä eksponenteilla $m \geq 3$ ja $n \geq 3$ yhtälöllä (4.9) on vain äärellisen monta positiivista kokonaislukuratkaisua x ja y, mistä väite seuraa. □

Catalanin konjektuurin yleisti Pillai vuonna 1945 [44, s. 201].

Konjektuuri 4.4.3. (Pillai) *Olkoon $k \in \mathbb{Z}$ sekä olkoot $A, B \in \mathbb{N}$ ja $x, y, m, n \in \mathbb{N} \setminus \{1\}$ siten, että $mn > 4$. Tällöin yhtälöllä*

$$Ax^m - By^n = k \tag{4.10}$$

on vain äärellinen määrä ratkaisuja.

Osoitetaan konjektuuri *Abc*-konjektuurin avulla [35].

Lause 4.4.4. *Abc-konjektuurin nojalla Pillain konjektuurin on voimassa.*

Todistus. Todetaan aluksi, että kaiki todistuksessa esiintyvät luvut ovat luonnollisia lukuja. Olkoon $d = \operatorname{syt}(Ax^m, By^n, k)$. Soveltamalla *Abc*-konjektuuria *abc*-summaan $(\frac{Ax^m}{d}, \frac{By^n}{d}, \frac{k}{d})$ saadaan luvuille $\frac{Ax^m}{d}$ ja $\frac{By^n}{d}$ yläraja

$$\frac{Ax^m}{d}, \frac{By^n}{d} \leq \frac{k}{d} \leq C(\varepsilon) \operatorname{rad}\left(\frac{Ax^m By^m k}{d^3}\right)^{1+\varepsilon},$$

josta edelleen

$$Ax^m, By^n \leq C(\varepsilon)\left(d \operatorname{rad}\left(\frac{Ax^m By^m k}{d^3}\right)\right)^{1+\varepsilon} \leq C_1(\varepsilon, A, B, k)(xy)^{1+\varepsilon},$$

missä $C_1(\varepsilon, A, B, k) = C(\varepsilon) d^{1+\varepsilon} \operatorname{rad}\left(\frac{ABk}{d^3}\right)^{1+\varepsilon}$. Näin ollen saadaan yhtälöt

$$x^m \leq C_2(\varepsilon, A, B, k)(xy)^{1+\varepsilon}, \tag{4.11}$$
$$y^n \leq C_3(\varepsilon, A, B, k)(xy)^{1+\varepsilon}, \tag{4.12}$$

missä $C_2(\varepsilon, A, B, k) = \frac{C_1(\varepsilon, A, B, k)}{A}$ ja $C_3 = \frac{C_1(\varepsilon, A, B, k)}{B}$. Jos nyt esimerkiksi $x^m \leq y^n$, niin yhtälöstä (4.12) saadaan

$$y^n \leq C_3(\varepsilon, A, B, k) y^{(1+\frac{n}{m})(1+\varepsilon)},$$

jolloin edelleen

$$y^{n-(1+\frac{n}{m})(1+\varepsilon)} = (y^n)^{1-(\frac{1}{n}+\frac{1}{m})(1+\varepsilon)} \leq C_3(\varepsilon, A, B, k). \tag{4.13}$$

Koska oletuksen mukaan $m \geq 2$ ja $n \geq 2$ siten, että $mn > 4$, täytyy olla $mn \geq 6$, jolloin

$$\frac{1}{n} + \frac{1}{m} \leq \frac{1}{2} + \frac{1}{3} = \frac{5}{6}$$

Näin ollen voidaan valisemalla $0 < \varepsilon < \frac{1}{5}$ epäyhtälö

$$(\frac{1}{n} + \frac{1}{m})(1 + \varepsilon) < 1$$

toteutuu. Yhtälön (4.13) nojalla siten y ja n ovat rajoitettuja, jolloin myös x ja m ovat rajoitettuja. □

Tarkastellaan vielä tilannetta $m = n = 2$, joka jäi Pillain konjektuurin ulkipuolelle. Olkoon $A \in \mathbb{N}$ ja $B, k \in \mathbb{Z}$ suhteellisia alkulukuja. Olkoot $x, y \in \mathbb{N}$ ja tarkastellaan yhtälöä

$$Ax^2 - By^2 = k. \tag{4.14}$$

Voidaan todistaa seuraava [35]:

Lause 4.4.5. *Abc-konjektuurin nojalla yhtälöllä (4.14) on vain äärellinen määrä ratkaisuja, kun* $\operatorname{rad}(y)$ *on rajoitettu.*

Todistus. Olkoon $d = \operatorname{syt}(Ax^2, By^2)$. Soveltamalla *Abc*-konjektuuria kolmikkoon $(\frac{Ax^2}{d}, \frac{By^2}{d}, \frac{k}{d})$ saadaan

$$\frac{Ax^2}{d} \leq C(\varepsilon) \operatorname{rad}\left(\frac{ABkx^2y^2}{d^3}\right)^{1+\varepsilon},$$

josta edelleen

$$Ax^2 \leq C(\varepsilon)\left(d \cdot \frac{k}{d} \operatorname{rad}\left(\frac{ABkx^2y^2}{d^3}\right)\right)^{1+\varepsilon} \leq C(\varepsilon)\left(kAB \operatorname{rad}(xy)\right)^{1+\varepsilon}.$$

Jakamalla puolittain luvulla A saadaan siten

$$x^2 \leq C_1(\varepsilon, A, B, k)|x|^{1+\varepsilon} \operatorname{rad}(y)^{1+\varepsilon},$$

josta edelleen

$$|x|^{1-\varepsilon} \leq C_1(\varepsilon, A, B, k) \operatorname{rad}(y)^{1+\varepsilon},$$

missä $C_1(\varepsilon, A, B, k) = \frac{1}{A} \cdot C(\varepsilon)(kAB)^{1+\varepsilon}$. Koska $\operatorname{rad}(y)$ on rajoitettu oletuksen nojalla, $|x|$ on myös rajoitettu. Näin ollen yhtälöllä (4.14) on vain äärellinen määrä ratkaisuja. □

4.5 Yleistetty Fermat'n yhtälö

Yhdistämällä Fermat'n suuren lauseen ja Catalanin konjektuurin ideat saadaan

Konjektuuri 4.5.1. (Fermat-Catalan) *Olkoot* $x, y, z, p, q, r \in \mathbb{N}$ *siten, että* $\operatorname{syt}(x, y, z) = 1$ *ja* $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. *Tällöin yhtälöllä*

$$x^p + y^q = z^r$$

on vain äärellinen määrä ratkaisuja.

Tällä hetkellä tunnetaan ratkaisut

$$1^p + 2^3 = 3^2 \qquad 2^5 + 7^2 = 3^4$$
$$7^3 + 13^2 = 2^9 \qquad 2^7 + 17^3 = 71^2$$
$$3^5 + 11^4 = 122^2 \qquad 17^7 + 76271^3 = 21063928^2$$
$$1414^3 + 2213459^2 = 65^7 \qquad 9262^3 + 15312283^2 = 113^7$$
$$43^8 + 96222^3 = 30042907^2 \qquad 33^8 + 1549034^2 = 15613^3.$$

Ensimmäisessä yhtälössä valitsemalla $p \geq 6$ saadaan äärettömästi ratkaisuja, mutta konjektuurin valossa tarkastellaan sitä kuitenkin vain yhtenä ratkaisuna. [11]

Abc-konjektuurin avulla voidaan osoittaa hieman yleisempi tulos [35].

Lause 4.5.2. *Olkoot* $A, B, C, x, y, z, p, q, r \in \mathbb{N}$ *siten, että* $\operatorname{syt}(x, y, z) = 1$ *ja* $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} < 1$. *Tällöin Abc-konjektuurin nojalla yhtälöllä*

$$Ax^p + By^q = Cz^r$$

on vain äärellinen määrä ratkaisuja.

Todistus. Oletuksen mukaan $\operatorname{syt}(x, y, z) = 1$. Jos $z = 1$, väite seuraa Pillain konjektuurista (Konjektuuri 4.4.3). Voidaan olettaa $z \geq 2$. Olkoon $d = \operatorname{syt}(Ax^p, By^q, Cz^r)$. Soveltamalla *Abc*-konjektuuria kolmikkoon $\frac{1}{d}(Ax^p, By^q, Cz^r)$ saadaan

$$\frac{Cz^r}{d} \leq C(\varepsilon) \operatorname{rad}\left(\frac{ABCx^p y^q z^r}{d^3}\right)^{1+\varepsilon},$$

josta edelleen

$$z^r \leq \frac{1}{C} \cdot C(\varepsilon)\left(d \operatorname{rad}\left(\frac{ABCx^p y^q z^r}{d^3}\right)\right)^{1+\varepsilon} \leq C_1(\varepsilon, A, B, C)(xyz)^{1+\varepsilon},$$

missä $C_1(\varepsilon, A, B, C) = \frac{1}{C} \cdot C(\varepsilon)(dABC)^{1+\varepsilon}$. Koska $Ax^p < Cz^r$ ja $By^q \leq Cz^r$, niin

$$z^r \leq C_2(\varepsilon, A, B, C)(z^r)^{(1+\varepsilon)(\frac{1}{r}+\frac{1}{p}+\frac{1}{q})},$$

missä $C_2(\varepsilon, A, B, C) = C_1(\varepsilon, A, B, C)\left(\frac{C^2}{AB}\right)^{1+\varepsilon}$. Tästä saadaan

$$(z^r)^{1-(1+\varepsilon)(\frac{1}{r}+\frac{1}{p}+\frac{1}{q})} \leq C_2(\varepsilon, A, B, C).$$

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. □

4.6 Shorey-Tijdemanin konjektuuri

Vuonna 1986 T. N. Shorey ja R. Tijdeman esittivät seuraavan konjektuurin [44, s. 202]:

Konjektuuri 4.6.1. (Shorey-Tijdeman) *Olkoot* $x, y, v, w \in \mathbb{N}$ *ja* $m, n \in \mathbb{N} \setminus \{1\}$ *siten, että* $\operatorname{syt}(x, v) = \operatorname{syt}(y, w) = 1$ *ja* $mn > 4$. *Tällöin yhtälöllä*

$$\left(\frac{x}{v}\right)^m - \left(\frac{y}{w}\right)^n = 1$$

on vain äärellinen määrä ratkaisuja.

Teoksen [44] samassa yhteydessä osoitetaan, että konjektuuri pitää paikkansa, mikäli jokin luvuista v, w, x, y on kiinnitettyjen alkulukujen tulo. *Abc*-konjektuurin avulla voidaan konjektuuri todeksi asettamalla lisäoletus eksponenteille m ja n [35].

Lause 4.6.2. *Abc-konjketuurin nojalla Shorey-Tijdemanin konjektuuri on voimassa.*

Todistus. Olkoon $\text{syt}(x, v) = \text{syt}(y, w) = 1$. Jos $v = 1$, niin $w = 1$ ja väite seuraa Catalanin yhtälöstä ???. Oletetaan siten $v, w > 1$. Konjektuurin yhtälö saadaan muotoon

$$w^n x^m - v^m y^n = v^m w^n, \tag{4.15}$$

josta edelleen saadaan yhtälöt

$$w^n x^m = v^m \left(y^n + w^n\right), \tag{4.16}$$
$$v^m y^n = w^n \left(x^m - v^m\right). \tag{4.17}$$

Tällöin yhtälön (4.16) nojalla $v^m \mid w^n$ ja yhtälön (4.17) nojalla $w^n \mid v^n$. Siis $v^m = w^n$, jolloin on olemassa luonnollinen luku $z > 1$ siten, että

$$v^m = w^n = z^{pym(n,m)}.$$

Näin ollen yhtälö (4.15) saadaan muotoon

$$x^m - y^n = z^{pym(m,n)},$$

jolla on lauseen 9 ???? mukaan äärellinen määrä ratkaisuja aina kun on voimassa

$$\frac{1}{m} + \frac{1}{n} + \frac{1}{pym(m,n)} < 1. \tag{4.18}$$

Yhtälö (4.18) 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. Tapaus $(m, n) = (2, 3)$: Yhtälöllä $x^2 - y^4 = z^4$ ei ole ei-triviaaleja ratkaisuja
2. Tapaus $(m, n) = (3, 2)$: Yhtälöllä $x^2 - y^4 = z^4$ ei ole ei-triviaaleja ratkaisuja
3. Tapaus $(m, n) = (3, 3)$: Yhtälöllä $x^3 - y^3 = z^3$ ei ole ei-triviaaleja ratkaisuja
4. Tapaus $(m, n) = (2, 4)$: Yhtälöllä $x^2 - y^4 = z^4$ ei ole ei-triviaaleja ratkaisuja [32, s.16]
5. Tapaus $(m, n) = (4, 2)$: Yhtälöllä $x^4 - y^2 = z^4$ ei ole ei-triviaaleja ratkaisuja [32, s.17]

□

4.7 Brocard-Ramanujan yhtälö $n! + 1 = m^2$

Toisistaan tietämättä sekä H. Brocard (1876 ja 1885) että S. Ramanujan (1913) esittivät ongelman kaikkien kokonaislukuratkaisujen löytämiseksi yhtälölle

$$n! + 1 = m^2. \tag{4.19}$$

Ongelma on edelleenkin avoin. Tällä hetkellä tunnettuja ratkaisuja (n, m) arvoon $n = 10^9$ asti ovat ainoastaan $(4, 5)$, $(5, 11)$, $(7, 71)$ [4]. Vuonna 1993 M. Overholt todisti, että *Abc*-konjektuurin nojalla yhtälöllä (4.19) on vain äärellinen määrä ratkaisuja [39]. Todistuksen kiteyttämiseksi hän käytti seuraavaa Szpiron konjektuurin heikkoa muotoa.

Lause 4.7.1. *Szpiron konjektuurin heikon muodon nojalla yhtälöllä*

$$n! + 1 = m^2$$

on vain äärellinen määrä positiivisia kokonaislukuratkaisuja.

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 $m = 2k + 1$ jollekin $k \in \mathbb{N}$, saadaan tarkasteltava yhtälö muotoon

$$n! = (2k + 1)^2 - 1 = 4k(k + 1). \tag{4.20}$$

Kolmikko $(1, k, k + 1)$ muodostaa *abc*-summan. Näin ollen soveltamalla Lemmoja 2.2.7 ja 2.7.1 sekä Konjektuuria 3.7.1 yhtälöön (4.20) saadaan

$$\frac{1}{4}\left(\frac{n}{e}\right)^n < \frac{1}{4}n! = k(k+1) \leq \operatorname{rad}(k(k+1))^s \leq \operatorname{rad}\left(\frac{n!}{4}\right)^s = \left(\prod_{p \leq n} p\right)^s < 4^{sn}.$$

Kertomalla puolittain luvulla $4e^n$ saadaan

$$n^n < 4^{sn+1}e^n \leq 4^{sn+n}e^n = \left(4^{s+1}e\right)^n,$$

jolloin $n < 4^{s+1}e$ eli luku n on ylhäältä rajoitettu. Koska s on vakio, yläraja $4^{s+1}e$ on kiinteä eikä luku n voi kasvaa mielivaltaisen suureksi. □

Vuonna 1996 A. Dabrowski yleisti tuloksen osoittamalla, että yhtälöllä

$$n! + A = m^2, \tag{4.21}$$

on vain äärellinen määrä positiivisia kokonaislukuratkaisuja, kun $A \in \mathbb{N}$ ei ole minkään luonnollisen luvun neliö. Mikäli A on neliö, Dabrowski osoitti yhtälöllä (4.21) olevan vain äärellinen määrä positiivisia kokonaislukuratkaisuja Szpiron konjektuurin heikon muodon nojalla. [9]

4.8 Simmonsin yhtälö $n! = m(m^2 - 1)$

Kirjassa [21, Problem D25, s. 193] Simmons tarkastelee yhtälöä

$$n! = (m-1)m(m+1) = m(m^2 - 1)$$

ja kysyy onko ratkaisujen $(n, m) = (3, 2), (4, 3), (5, 5), (6, 9)$ lisäksi muita positiivisia kokonaislukuratkaisuja. Osoitetaan *Abc*-konjektuurin avulla yleisempi tapaus [35].

Lause 4.8.1. *Olkoot $n, m, k \in \mathbb{N} \setminus \{1\}$. Abc-konjektuurin nojalla yhtälöllä*

$$n! = m\left(m^k \pm 1\right) \tag{4.22}$$

on vain äärellinen määrä ratkaisuja.

Todistus. Kirjoitetaan yhtälö (4.22) muodossa

$$m^k \pm 1 = \frac{n!}{m}, \tag{4.23}$$

jolloin $\text{syt}(m^k, \frac{n!}{m}) = 1$. Soveltamalla arviota $m^{k-1} \leq n!$ ja *Abc*-konjektuuria saadaan

$$\frac{n!}{m} \leq C(\varepsilon) \operatorname{rad}\left(1 \cdot m^k \cdot \frac{n!}{m}\right)^{1+\varepsilon} \leq C(\varepsilon) \operatorname{rad}(n!)^{1+\varepsilon}. \tag{4.24}$$

Yhtälöstä (4.23) saadaan ylöspäin arvioimalla $m^k \leq \frac{2n!}{m}$, josta edelleen

$$m \leq (2n!)^{\frac{1}{k+1}}. \tag{4.25}$$

Soveltamalla epäyhtälöön (4.24) arvioita (4.25) ja $\prod_{p \leq n} p < 4^n$ (Lemma 2.7.1) 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 2.2.7) 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

$$\left(\frac{n}{e}\right)^{\frac{k}{k+1}} \leq C(\varepsilon)^{\frac{1}{n}} 2^{\frac{1}{n(k+1)}} 4^{(1+\varepsilon)} \leq C(\varepsilon) 2^{\frac{1}{3}} 4^{(1+\varepsilon)},$$

mistä nähdään, että luku n on rajoitettu. Näin ollen myös luvut m ja k ovat rajoitettuja. □

4.9 Erdös-Stewartin konjektuuri

Olkoon p_k k:s alkuluku, missä $k \in \mathbb{N}$. P. Erdös ja C.L. Stewart asettivat seuraavan konjektuurin [21, Problem A2, s. 7]:

Konjektuuri 4.9.1. (Erdös-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*

$$n! + 1 = p_k^a p_{k+1}^b \tag{4.26}$$

on ratkaisu ainoastaan arvoilla $n \leq 5$.

F. Luca todisti konjektuurin vuonna 2001 osoittamalla luvun n olevan ylhäältä rajoitettu ja tarkistamalla loput tapaukset tietokoneavusteisesti [29]. Osoitetaan kuitenkin vielä *Abc*-konjektuuri avulla, että yhtälölle (4.30) on olemassa ainoastaan äärellinen määrä positiivisia kokonaislukuratkaisuja. Todistus perustuu työhön [35] ja siinä tarvitaan seuraavaa kirjassa [22, ss. 455-457] osoitettavaa tulosta.

Lause 4.9.2. (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 4.9.3. *Abc-konjektuurin nojalla yhtälöllä (4.26) on vain äärellisen monta ratkaisua.*

Todistus. Olkoon $\varepsilon > 0$. Lauseen 2.1.5 nojalla $\operatorname{syt}(n!, p_k^a p_{k+1}^b) = 1$. Näin ollen voidaan soveltaa *Abc*-konjektuuria *abc*-summaan $(1, n!, p_k^a p_{k+1}^b)$, jolloin saadaan

$$n! \leq p_k^a p_{k+1}^b \leq C(\varepsilon) \operatorname{rad}(n! p_k p_{k+1})^{1+\varepsilon} = C(\varepsilon) \left(\prod_{p \leq p_{k+1}} p \right)^{1+\varepsilon}. \tag{4.27}$$

Käyttämällä epäyhtälöitä $\frac{n^n}{e^n} \leq n!$ ja $\prod_{p \leq n} p < 4^n$ sekä oletusta $p_{k-1} \leq n$ ja Bertrandin postulaattia $p_{k+1} < 2p_k < 4p_{k-1}$ saadaan epäyhtälö (4.27) muotoon

$$\left(\frac{n}{e}\right)^n \leq C(\varepsilon) 4^{p_{k+1}(1+\varepsilon)} \leq C(\varepsilon) 4^{4(1+\varepsilon)n} \leq \left(C(\varepsilon) 4^{4(1+\varepsilon)}\right)^n,$$

josta edelleen $\frac{n}{e} \leq C(\varepsilon) 4^{4(1+\varepsilon)}$. Tästä nähdään, että luku n on rajoitettu. □

4.10 Voimakkaista luvuista

Määritelmä 4.10.1. Luvun $n \in \mathbb{N}$ sanotaan olevan *voimakas* (engl. powerful), jos

$$\operatorname{rad}(n)^2 \mid n.$$

Konjektuuri 4.10.2. (Erdös-Mollin-Walsh) *Ei ole olemassa kolmea peräkkäistä voimakasta lukua.*

Konjektuuri ei selvästikään ole voimassa kahdelle peräkkäiselle luvulle, vastaesimerkkinä toimii Catalanin konjektuurista tuttu pari $(8, 9) = (2^3, 3^2)$. *Abc*-konjektuurin avulla saadaan osoitettua konjektuurin suuntainen tulos [35].

Lause 4.10.3. *Abc-konjektuurin nojalla on olemassa vain äärellinen määrä kolmen peräkkäisen voimakkaan luvun joukkoja.*

Todistus. Jos $1 < a < b < c$ ovat kolme peräkkäistä lukua, niille on voimassa yhtälö

$$b^2 = ac + 1.$$

Oletetaan, että luvut a, b ja c ovat voimakkaita. Soveltamalla *Abc*-konjektuuria kolmikkoon $(ac, 1, b^2)$ saadaan

$$b^2 \leq C(\varepsilon) \operatorname{rad}(abc)^{1+\varepsilon} \leq C(\varepsilon)(abc)^{\frac{1+\varepsilon}{2}} \leq C(\varepsilon) b^{\frac{3(1+\varepsilon)}{2}}, \tag{4.28}$$

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. □

Seuraava konjektuuri yleistää Fermat'n ja Mersennen lukujen tuloksen

Konjektuuri 4.10.4. *Jokaista lukua $k \in \mathbb{Z}_{\geq 2}$ kohti on olemassa luku n_k, joka on lähinnä lukua 2^k oleva luku mutta $n_k \neq 2^k$. Tällöin*

$$\lim_{k\to\infty} |2^k - n_k| = +\infty.$$

Osoitetaan seuraava tulos [35].

Lause 4.10.5. *Abc-konjektuurin nojalla konjektuuri 4.10.4 on voimassa.*

Todistus. Olkoon $k \geq 2$. Tällöin lähinnä lukua 2^k oleva voimakas luku on muotoa

$$n_k = 2^s n_k', \quad \text{missä } s = 0 \text{ tai } 1 < s < k$$

ja n_k' on pariton voimakas luku. Sovelletaan sitten *Abc*-konjektuuria summaan

$$2^{k-s} - \frac{n_k}{2^s} = z,$$

jolloin saadaan

$$\frac{n_k}{2^s} \leq C(\varepsilon)\,\mathrm{rad}\left(\frac{n_k z}{2^s}\right)^{1+\varepsilon}.$$

Näin ollen

$$n_k \leq C(\varepsilon)\left(2^s z\,\mathrm{rad}\left(\frac{n_k}{2^s}\right)\right)^{1+\varepsilon} \leq C(\varepsilon)|2^k - n_k|^{1+\varepsilon} n_k^{\frac{1+\varepsilon}{2}},$$

josta saadaan

$$n_k^{\frac{1-\varepsilon}{2}} \leq C(\varepsilon)|2^k - n_k|^{1+\varepsilon}$$

Koska $\lim_{k\to\infty} n_k = \infty$, väite seuraa valitsemalla $0 < \varepsilon < 1$. □

Seuraava väite koskee suoraan Fermat'n ja Mersennen lukuja.

Konjektuuri 4.10.6. *On olemassa äärettömästi Fermat'n ja Mersennen lukuja, jotka eivät ole voimakkaita.*

Lause 4.10.7. *Abc-konjektuurin nojalla konjektuuri 4.10.6 on voimassa.*

Todistus. Riittää näyttää, että *Abc*-konjektuurin nojalla on olemassa äärellinen määrä vastaavia voimakkaita lukuja. Tarkastellaan Diophantoksen yhtälöä

$$2^k \pm 1 = z,$$

missä $k \in \mathbb{N}$ ja z on voimakas. Nyt kuitenkin Lauseen 4.10.5 nojalla yhtälöllä on vain äärellinen määrä ratkaisuja. Koska Fermat'n ja Mersennen lukuja on äärettömästi, väite seuraa. □

Tarkastellaan vielä lopuksi erästä Erdösin konjektuuria. Sitä varten tarvitsemme seuraavan yleistyksen. [21, s.70]

Määritelmä 4.10.8. Olkoon $k \in \mathbb{N}_{\geq 2}$. Luvun $n \in \mathbb{N}$ sanotaan olevan *k-voimakas* (engl. k-ful), jos

$$\mathrm{rad}(n)^k \mid n.$$

Konjektuuri 4.10.9. (Erdös) *Yhtälöllä*

$$x + y = z$$

on vain äärellinen määrä ratkaisuja 4-voimakkailla suhteellisilla alkuluvuilla x, y ja z.

Osoitetaan jälleen *Abc*-konjektuurin voima [35].

Lause 4.10.10. *Abc-konjektuurin nojalla Erdösin konjektuuri on voimassa.*

Todistus. Olkoot $x, y, z \in \mathbb{N}$ 4-voimakkaita lukuja siten, että $\mathrm{syt}(x, y, z) = 1$ ja $x + y = z$. Tällöin *Abc*-konjektuurin nojalla

$$z \leq C(\varepsilon)\,\mathrm{rad}\,(xyz)^{1+\varepsilon} \leq C(\varepsilon)(xyz)^{\frac{1+\varepsilon}{4}} \leq C(\varepsilon)z^{\frac{3(1+\varepsilon)}{4}},$$

josta edelleen

$$z^{\frac{1-3\varepsilon}{4}} \leq C(\varepsilon).$$

Valitsemalla $0 < \varepsilon < \frac{1}{3}$ nähdään, että z on rajoitettu. □

4.11 Wieferichin alkuluvuista

Yrittäessään todistaa Fermat'n suurta lausetta 1900-luvun alussa A. Wieferich osoitti seuraavan tuloksen [24]:

Lause 4.11.1. *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 konguenssin $2^{p-1} \equiv 1 \pmod{p^2}$.

Kongruenssin toteuttavia alkulukuja alettiinkin kutsua esittäjänsä mukaisesti.

Määritelmä 4.11.2. Paritonta alkulukua p sanotaan *Wieferichin alkuluvuksi*, jos se toteuttaa kongruenssin

$$2^{p-1} \equiv 1 \pmod{p^2}. \tag{4.29}$$

Wieferichin alkulukuja uskotaan olevan äärettömästi, vaikka tällä hetkellä ainoat tunnetut lukua $1,25 \cdot 10^{15}$ pienemmät Wieferichin alkuluvut ovat 1093 ja 3511 [24]. Suurimmalle osalle alkuluvuista kongruenssi (4.29) ei siis toteudu. Tätä havaintoa tukee myös Lang-Trotterin konjektuuri, jonka nojalla suuruudeltaan korkeintaan lukua x olevien Wieferichin alkulukujen lukumäärää rajoittaa ylhäältä hitaasti kasvava funktio $C \log\log x$, missä $C > 0$ on vakio [27, s.175].

Osoitetaan seuraavaksi kirjaan [33] perustuen, että *Abc*-konjektuurin nojalla on äärettömästi sellaisia alkulukuja, jotka eivät toteuta kongruenssia 4.29. Sitä varten tarvitsemme seuraavaa aputulosta.

Lemma 4.11.3. *Olkoon p pariton alkuluku. Jos jollekin $n \in \mathbb{N}$ pätee*

$$2^n \equiv 1 \pmod{p} \quad \textit{ja} \quad 2^n \not\equiv 1 \pmod{p^2},$$

niin luku p ei ole Wieferichin alkuluku.

Todistus. Oletuksen mukaan $\text{syt}(p, 2) = 1$. Olkoon $d = \text{ord}_p 2$. Tällöin $d \mid n$ Lemman 2.1.30 nojalla ja yhtälöstä $2^n \not\equiv 1 \pmod{p^2}$ 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 2.1.28) nojalla $2^{p-1} \equiv 1 \pmod{p}$ ja Seurauksen 2.1.31 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

$$2^{p-1} = (2^d)^e = (1 + kp)^e \equiv 1 + ekp \not\equiv 1 \pmod{p^2},$$

joten p ei ole Wieferichin alkuluku. □

Määritelmä 4.11.4. Positiivisen kokonaisluvun v sanotaan olevan *voimakas*, mikäli jokin alkuluku p jakaa sen seuraa että myös p^2 jakaa sen.

Esimerkiksi 72 on voimakas mutta 192 ei ole. Jos v on voimakas, niin $\text{rad(v)} \leq v^{\frac{1}{2}}$.

Lause 4.11.5. *Abc-konjektuurin nojalla on olemassa äärettömästi alkulukuja, jotka eivät toteuta kongruenssia (4.29).*

Todistus. Merkitään $W = \{p \text{ alkuluku} : \ 2^{p-1} \not\equiv 1 \pmod{p^2}\}$. Jokaisella $n \in \mathbb{N}$ voidaan kirjoittaa erotus $2^n - 1$ muodossa

$$2^n - 1 = u_n v_n,$$

missä luvun v_n alkutekijät eivät kuulu joukkoon W ja luvun u_n kuuluvat.

$$u_n = \prod_{\substack{p \mid n \\ v_p(n)=1}} p, \qquad v_n = \prod_{\substack{p \ \mid \ n \\ v_p(n) \geq 2}} p^{v_p(n)}.$$

Mikäli p jakaa luvun u_n, niin on voimassa $2^n \equiv 1 \pmod{p}$ muttei $2^n \not\equiv 1 \pmod{p^2}$. Tällöin Lemman 4.11.3 nojalla $p \in W$, ja u_n on neliövapaa kokonaisluku, joka on jaollinen vain Wieferichin alkuluvuilla.

Jos joukko W on äärellinen, on olemassa vain äärellisen monta neliövapaata kokonaislukua, joiden kaikki alkutekijät kuuluvat joukkoon W. Näin ollen joukko

$$\{u_n : n = 1, 2, 3, \ldots\}$$

on äärellinen. Siitä seuraa, että joukko $\{v_n : n = 1, 2, 3, \ldots\}$ on ääretön ja, vastaavasti, rajoittamaton. Koska v_n on voimakas, on voimassa arvio

$$\text{rad}(v_n) \leq v_n^{\frac{1}{2}}.$$

Olkoon $0 < \varepsilon < 1$. Soveltamalla *Abc*-konjektuuria *abc*-summaan $(1, u_n v_n, 2^n)$ saadaan

$$\begin{aligned} v_n &< 2^n \\ &\leq K(\varepsilon)\mathrm{rad}(2^n \cdot 1 \cdot (2^n - 1))^{1+\varepsilon} \\ &\leq K(\varepsilon)\mathrm{rad}(2u_n v_n)^{1+\varepsilon} \\ &\leq K(\varepsilon)\mathrm{rad}(2u_n)^{1+\varepsilon}\mathrm{rad}(v_n)^{1+\varepsilon} \\ &\leq K'(\varepsilon) v_n^{\frac{1+\varepsilon}{2}}, \end{aligned}$$

missä $K'(\varepsilon) = K(\varepsilon)\max\{(2u_n)^{1+\varepsilon}\}$ on vakio. Näin ollen luvut v_n ovat rajoitettuja, mikä on mieletöntä. Väite seuraa. □

J. H. Silverman todisti vuonna 1988 edellistä voimakkaamman tuloksen [46]:

Lause 4.11.6. *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

$$\#\{p \leq X : a^{p-1} \not\equiv 1 \pmod{p^2}\} > C(a)\log X,$$

missä $C(a) > 0$ on vakio.

4.12 Erdös-Woodsin konjektuuri arvolla $k = 3$

Konjektuuri 4.12.1. (Erdös-Woods) *On olemassa vakio $k \in \mathbb{N}$ siten, että jos luvuille $x, y \in \mathbb{N}$ pätee*

$$\mathrm{rad}(x + i) = \mathrm{rad}(y + 1) \tag{4.30}$$

kaikilla $i = 1, \ldots, k$, niin tällöin $x = y$.

Huomautus 4.12.2. Erdös-Woodsin konjektuuri ei toteutu luvulla $k = 2$. Tämä nähdään esimerkiksi valitsemalla $x = 74$ ja $y = 1214$, jolloin

$$\begin{aligned} x + 1 &= 75 = 3 \cdot 5^2 \\ y + 1 &= 1215 = 3^5 5, \\ x + 2 &= 76 = 2^2 19, \\ y + 2 &= 1216 = 2^6 19 \end{aligned}$$

Vastaesimerkkejä voidaan itse asiassa konstruoida äärettömästi asettamalla

$$x_n = 2^n - 3 \qquad \text{ja} \qquad y_n = 2^{2n} - 2^{n+1} - 1.$$

Tällöin nimittäin

$$\begin{aligned} x_n + 1 &= 2(2^{n-1} - 1), \\ y_n + 1 &= 2^{2^n} - 2^{n+1} = 2^{n+1}\left(2^{n-1} - 1\right), \\ x_n + 2 &= 2^n - 1, \\ y_n + 2 &= 2^{2n} - 2^{n+1} + 1 = (2^n - 1)^2 \end{aligned}$$

Vastaavanlaisia esimerkkejä ei tunneta luvulle $k \geq 3$. [35]

Vuonna 1993 M. Langevin osoitti todeksi lukua $k = 3$ koskevan konjektuurin [28].

Lause 4.12.3. *Abc-konjektuurin nojalla Erdös-Woodsin konjektuuri on voimassa arvolla $k = 3$ lukuunottamatta äärellistä määrää vastaesimerkkejä.*

Todistus. Olkoot $x, y \in \mathbb{N}$ siten, että $x < y$ ja yhtälö (4.30) toteutuu arvoilla $i = 1, 2, 3$. Tällöin

$$\operatorname{rad}(y+i) = \operatorname{rad}(x+i) \mid (x+i)$$

ja edelleen

$$\operatorname{rad}(y+i) \mid (y-x)$$

kaikilla $i = 1, 2, 3$, sillä $y - x = (y + i) - (x + i)$. Näin ollen

$$\operatorname{rad}\big((y+1)(y+2)(y+3)\big) \mid (y-x).$$

Soveltamalla sitten *Abc*-konjektuuria *abc*-summaan $(1, (y+1)(y+3), (y+2)^2)$ saadaan

$$y^2 < (y+2)^2 \leq C(\varepsilon) \operatorname{rad}\big((y+1)(y+2)(y+3)\big)^{1+\varepsilon} \leq C(\varepsilon)(y-x)^{1+\varepsilon} < C(\varepsilon) y^{1+\varepsilon},$$

jolloin siis

$$y^{1-\varepsilon} < C(\varepsilon).$$

Valitsemalla $0 < \varepsilon < 1$ nähdään, että epäyhtälön oikea puoli antaa luvulle y vain luvusta ε riippuvan ylärajan. Siis yhtälön (4.30) toteuttavia lukupareja (x, y), $x < y$ on vain äärellisen monta. Tapaus $x > y$ käsitellään vastaavasti. □

Konjektuurin yleiseen tapaukseen päästään käsiksi kuitenkin seuraavan lauseen avulla [35].

Lause 4.12.4. *Olkoon $k \in \mathbb{N} \setminus \{1\}$. Jokaista lukua $x \in \mathbb{N}$ kohti on olemassa korkeintaan äärellinen määrä lukuja $y \in \mathbb{N}$, joille on voimassa yhtäsuuruus*

$$\operatorname{rad}(x+i) = \operatorname{rad}(y+i)$$

kaikilla $i = 1, \ldots, k$.

Todistus. □

4.13 Diofantoksen yhtälöstä $x^n + y^n = n!z^n$

Kirjassa [21, Problem D 2, s. 145] J. M. Gandhi esittää avoimen kysymyksen ratkaisuista yhtälölle

$$x^n + y^n = n!z^n, \tag{4.31}$$

kun $x, y, z \in \mathbb{Z}$ ja $n \in \mathbb{N}_{\geq 3}$. Osoitetaan työhön [35] pohjautuen, että yhtälöllä on äärellinen määrä ratkaisuja *Abc*-konjektuurin nojalla arvoilla $n \geq 4$.

Tapauksessa $n = 2$ saadaan äärettömästi ratkaisuja. Valitsemalla nimittäin luvut x_k ja y_k siten, että

$$x_k + y_k\sqrt{2} = \left(1 + \sqrt{2}\right)^k,$$

toteutuu myös yhtälö $x_k^2 - 2y_k^2 = (-1)^k$. Erityisesti parittomille muuttujan k arvoilla saadaan yhtälön (4.31) muotoinen yhtälö

$$1 + x_k^2 = 2y_k^2,$$

mikä osoittaa yhtälöllä olevan ratkaisuja ainakin arvolla $n = 2$.

Tapauksessa $n = 3$ saadaan myös äärettömästi ratkaisuja asettamalla

$$x_0 = 37, \qquad y_0 = 17 \qquad \text{ja} \qquad z_0 = 21,$$

jolloin kaikilla $k \in \mathbb{N}$ saadaan yhtälön (4.31) toteuttavat kolmikot

$$\begin{aligned} x_{k+1} &= x_k \left(x_k^3 + 2y_k^3\right) \\ y_{k+1} &= -y_k \left(2x_k^3 + y_k^3\right) \\ z_{k+1} &= z_k \left(x_k^3 - y_k^3\right) \end{aligned}$$

Lause 4.13.1. *Abc-konjektuurin nojalla yhtälöllä (4.31) on vain äärellinen määrä ratkaisuja, kun $x, y, z, n \in \mathbb{N}$ ja $n \geq 4$.*

Todistus. Olkoot x, y, z, n yhtälön (4.31) toteuttavat luvut. Voidaan olettaa $\operatorname{syt}(x, y) = 1$. Nyt lisäksi $\operatorname{syt}(x^n, n!) = 1$, sillä jos $\operatorname{syt}(x^n, n!) = d > 1$, niin $d^n \mid n!$, mikä on mahdotonta. Näin ollen $\operatorname{syt}(x^n, n!z^n)$, joten soveltamalla *Abc*-konjektuuria *abc*-summaan (4.31) saadaan

$$n!z^n \leq C(\varepsilon) \operatorname{rad}(x^n y^n n! z^n)^{1+\varepsilon} \leq C(\varepsilon)(xyz)^{1+\varepsilon} \operatorname{rad}(n!)^{1+\varepsilon}.$$

Oletuksien $x, y, z \in \mathbb{N}$ ja $n \geq 4$ nojalla $x, y, z \leq (n!z^n)^{\frac{1}{n}}$ saadaan nyt

$$n!z^n \leq C(\varepsilon)(n!z^n)^{\frac{3(1+\varepsilon)}{n}} \operatorname{rad}(n!)^{1+\varepsilon},$$

josta jakamalla puolittain termillä $(n!z^n)^{\frac{3(1+\varepsilon)}{n}}$ sekä tuloksia $\left(\frac{n}{e}\right)^n < n!$ (Lemma 2.2.7) ja $\prod_{p \leq n} p < 4^n$ (Lemma 2.7.1) käyttämällä edelleen

$$\left(\frac{nz}{e}\right)^{n\left(1 - \frac{3(1+\varepsilon)}{n}\right)} \leq (n!z^n)^{1 - \frac{3(1+\varepsilon)}{n}} \leq C(\varepsilon) 4^{n(1+\varepsilon)}.$$

Ottamalla puolittain n:s juuri saadaan viimein

$$\left(\frac{nz}{e}\right)^{1 - \frac{3(1+\varepsilon)}{n}} \leq C(\varepsilon)^{\frac{1}{n}} 4^{1+\varepsilon},$$

mistä nähdään lukujen n ja z olevan rajoitettuja, jolloin yhtälöllä (4.31) on vain äärellinen määrä ratkaisuja. □

4.14 Edgarin ja Shorey-Tijdemanin probleema

Kirjassa [21, Problem D 10, s. 157] Hugh Edgar kysyy onko yhtälöllä

$$1 + q + q^2 + \cdots + q^{x-1} = \frac{q^x - q}{q - 1} = p^y$$

ratkaisun $1+3+3^2+3^3+3^4+3^5=11^2$ lisäksi muita ratkaisuja parittomilla alkuluvuilla p ja q ja luonnollisilla luvuilla x ja y, kun $x \geq 5$ ja $y \geq 2$. Muita tunnettuja ratkaisuja ovat kuitenkin $(q,x,p,y)=(7,4,20,2)$ ja $(18,3,7,3)$, ja tietyillä lisehdoilla voidaankin osoittaa yhtälöllä olevan vain äärellinen määrä ratkaisuja. Shorey ja Tijdeman asettivat yleiselle tapaukselle konjektuurin, jonka mukaan yhtälöllä on vain äärellinen määrä ratkaisuja. [44, ss. 202-203]

Osoitetaan *Abc*-konjektuuriin nojautuen, että yleisemmässä tapauksessa yhtälöllä

$$x^{n-1}+x^{n-2}y+\cdots+xy^{n-2}+y^{n-1}=\frac{x^n-y^n}{x-y}=az^m, \tag{4.32}$$

missä $x,y,z,n,m \in \mathbb{N}$ siten, että $x>y$ ja $n>3$, on vain äärellinen määrä ratkaisuja [35].

Lause 4.14.1. *Abc-konjektuurin nojalla yhtälöllä (4.32) on vain äärellinen määrä ratkaisuja, kun $x,y,z,n,m \in \mathbb{N}$ siten, että $\operatorname{syt}(x,y)=1$, $x>y$, $n>3$ ja $\frac{3}{n}+\frac{1}{m}<1$.*

Todistus. Yhtälöstä (4.32) saadaan puolittain termillä $x-y$ kertomalla summa

$$y^n+az^m(x-y)=x^n.$$

Nyt ehdosta $\operatorname{syt}(x,y)=\operatorname{syt}(x^n,y^n)=1$ saadaan $\operatorname{syt}(x^n,y^n,az^m(x-y))=1$ Lemman 2.1.10 nojalla. Arvioita $x-y<x$ ja $z \leq x^{\frac{n}{m}}$ sekä *Abc*-konjketuuria soveltamalla saadaan

$$x^n \leq C(\varepsilon)\operatorname{rad}(y^n az^m(x-y)x^n)^{1+\varepsilon} \leq C(\varepsilon)(ayz(x-y)x)^{1+\varepsilon} \leq C'(\varepsilon,a)x^{(3+\frac{n}{m})(1+\varepsilon)},$$

missä $C'(\varepsilon,a)=C(\varepsilon)a^{1+\varepsilon}$. Edelleen

$$(x^n)^{1-(\frac{3}{n}+\frac{1}{m})(1+\varepsilon)} \leq C'(\varepsilon,a).$$

Valitsemalla siis $0<\varepsilon<\left(\frac{3}{n}+\frac{1}{m}\right)^{-1}-1$ nähdään, että luvut x,n ja siten myös luvut y,z ja m ovat rajoitettuja. □

4.15 Goormaghtighin ongelma

Goormaghtigh esitti ongelman olemassaolosta luvuille, joilla on on samoista numeroista koostuvat esitykset eri lukujärjestelmissä [44, s. 203]. Toisin sanoen, onko olemassa alkulukuja, jotka voidaan esittää kahdella eri tavalla muodossa

$$\frac{x^m-1}{x-1}=\frac{y^n-1}{y-1}, \tag{4.33}$$

missä $x,m,y,n \in \mathbb{N}$ siten, että $m>n>2$ ja $y>x>1$. Ongelmaan tunnetaan ainakin ratkaisut

$$31=\frac{2^5-1}{2-1}=\frac{5^3-1}{5-1} \qquad \text{ja} \qquad 8191=\frac{2^{13}-1}{2-1}=\frac{90^3-1}{90-1},$$

joista ensimmäinen toteuttaa myös ns. Batemanin ongelman, jossa x ja y ovat alkulukuja ja $m,n \geq 3$. Batemanin ongelmalle ei ole muita ratkaisuja suuruudeltaan korkeintaan 10^{10} olevien alkulukujen joukossa. [21, Problem B25, s. 81]

Lause 4.15.1. *Abc-konjketuurin nojalla yhtälöllä (4.33) on olemassa vain äärellinen määrä ratkaisuja luvuilla $x, m, y, n \in \mathbb{N}$, joille $m > n > 3$ ja $y > x > 1$.*

Todistus. Kertomalla nimittäjillä ja termejä siirtämällä saadaan yhtälö (4.33) muotoon

$$x^m(y-1) = y^n(x-1) + (y-x).$$

Merkitään $d = \operatorname{syt}\big(x^m(y-1), y^n(x-1)\big)$. Nyt $(\frac{y^n(x-1)}{d}, \frac{y-x}{d}, \frac{x^m(y-1)}{d})$ muodostaa *abc*-summan, joten *Abc*-konjektuuria soveltamalla saadaan

$$\frac{x^m(y-1)}{d} \leq C(\varepsilon) \operatorname{rad}\left(\frac{y^n(x-1)(y-x)x^m(y-1)}{d^3}\right)^{1+\varepsilon},$$

josta edelleen

$$\begin{aligned} yx^m &\leq C'(\varepsilon)\left((y-x)\operatorname{rad}(\frac{x^m y^n(x-1)(y-1)}{d^2})\right)^{1+\varepsilon} \\ &\leq C'(\varepsilon)\left((y-x)\operatorname{rad}(x^m y^n(x-1)(y-1))\right)^{1+\varepsilon} \\ &\leq C'(\varepsilon)\left((y-x)xy(x-1)(y-1)\right)^{1+\varepsilon}. \end{aligned}$$

Yhtälön (4.33) nojalla luvut y ja $x^{\frac{m-1}{n-1}}$ ovat saman suuruisia, joten

$$x^m + \frac{m-1}{n-1} \leq C''(\varepsilon)\left(x^{2+\frac{3(m-1)}{n-1}}\right)^{1+\varepsilon}.$$

Tästä saadaan viimein

$$x^{\frac{mn-1-(2n+3m-5)(1+\varepsilon)}{n-1}} \leq C''(\varepsilon).$$

Nyt pienellä ε arvolla mennessä yhtälö yllä antaa ylärajan, sillä $mn - 1 > 2n + 3m - 5$ oletuksella $m > n > 3$. □

4.16 Aritmeettisista lukujonoista

Olkoot $m, d, k \in \mathbb{N}$ siten, että $\operatorname{syt}(m, d) = 1$. Tarkstellaan tuloa

$$\Pi = m(m+d)\cdots(m+(k-1)d),$$

joka on k:n peräkkäisen termin tulo aritmeettisesta lukujonosta m, $m+d$, …, $m+(k-1)d$. Vuonna 1975 P. Erdös ja J. L. Selfridge osoittivat, että jos $d = 1$, niin π ei voi olla muotoa y^n, missä $y, n \geq 2$. 1985 R. Marzsalek osoitti kuinka k voi olla d:n funktiona rajoitettu kun $n \geq 2$. ???

Tarvitaan seuraavaa aputulosta [35].

Lemma 4.16.1. *Olkoot $i, j \in \mathbb{N}$ site, että $0 < i < j \leq k-1$. Tällöin $\operatorname{syt}(m+id, m+jd) < k$.*

Todistus. Olkoot i ja j oletukset toteuttavat luvut ja olkoon $g = (m+id, m+jd)$. Tällöin $g \mid (j-i)d$. Jos p on luvun g alkutekijä ja $p \mid d$, niin silloin joko $p \mid m$ tai $p = 1$. Näin ollen $p \mid (j-i)$, joten $g < k$. Tämä osoittaa, että termeillä $m+id$ ja $m+jd$ ei ole alkutekijöitä p, joille $p \geq k$. □

Huomautus 4.16.2. Jos $i \in \mathbb{N}$, niin edellisen Lemman mukaan
(i) jos $0 \leq i \leq k-2$, niin $\operatorname{syt}(m+id, m+(i+1)d) = 1$.
(ii) jos $0 \leq i \leq k-3$, niin $\operatorname{syt}(m+id, m+(i+2)d) \leq 2$.

Lause 4.16.3. *Abc-konjektuurin nojalla kaikilla $d \in \mathbb{N}$ yhtälöllä*

$$m(m+d)\cdots(m+(k-1)d) = y^n$$

on äärellinen määrä ratkaisuja, kun $m, k, y, n \in \mathbb{N}$ siten, että $k \geq 3$ ja $n \geq 2$.

Todistus. Osoitetaan väite arvolla $k = 3$. Lemman 4.16.1 nojalla kaikilla $i \in \mathbb{N}$, $0 \leq i \leq 2$ pätee

$$m + id = a_i y_i^n,$$

missä luku a_i koostuu lukua 3 pienemmistä alkutekijöistä ja luku y_i koostuu suuruudeltaan vähintään lukua 3 olevista alkutekijöistä tai $y_i = 1$. Koska oletuksen mukaan $\operatorname{syt}(m+d, m(m+2d)) = 1$, jolloin $a_1 = 1$ ja $y_1 \geq 2$. Yhtälöstä $(m+d)^2 = d^2 + m(m+2d)$ saadaan siten

$$a_1 y_1^{2n} = d^2 + a_0 a_2 y_0^n y_2^n.$$

Soveltamalla nyt *Abc*-konjektuuria saadaan

$$y_1^{2n} \leq C(\varepsilon) \operatorname{rad}(y_0 y_1 y_2)^{1+\varepsilon} \leq C(\varepsilon) y_1^{3(1+\varepsilon)},$$

josta edelleen

$$y_1^{2n-3(1+\varepsilon)} \leq C(\varepsilon).$$

Yllä olevasta epäyhtälöstä nähdään, että n on rajoitettu ja kaikilla $n \geq 2$ myös luvut y_1, y_2 ja y_3 ovat rajoitettuja. □

4.17 Richardin konjektuuri

Artikkelissa Richard esitti seuraavan konjektuurin

Konjektuuri 4.17.1. (Richard) *Jos kaikilla $n \in \mathbb{Z}_{\geq 0}$ luvuille $x, y \in \mathbb{Z}$ on voimassa yhtälö*

$$\operatorname{rad}\left(x^{2^n} - 1\right) = \operatorname{rad}\left(y^{2^n} - 1\right),$$

niin tällöin $x = y$.

Tarvitaan seuraavaa lemmaa.

Lemma 4.17.2. *Abc-konjektuurin nojalla kaikilla $\varepsilon > 0$ on olemassa vakio $C(\varepsilon) > 0$ siten, että kaikilla $x \in \mathbb{N}_{\geq 2}$ ja $n \in \mathbb{N}$ on voimassa*

$$\operatorname{rad}\left(x^n - 1\right) \geq C(\varepsilon) x^{n(1-\varepsilon)-1}.$$

Todistus. Soveltamalla *abc*-summaan $(x^n - 1) + 1 = x^n$ Konjektuuria 3.2.6 saadaan

$$C(\varepsilon)(x^n)^{1-\varepsilon} \leq \operatorname{rad}((x^n - 1)x^n) \leq x \operatorname{rad}(x^n - 1),$$

mistä väite seuraa jakamalla puolittain luvulla x. □

Lause 4.17.3. *Abc-konjektuurin nojalla Richardin konjektuuri on totta.*

Todistus. Oletetaan, että luvuille $x, y \in \mathbb{Z}$ pätee kaikilla $n \in \mathbb{Z}_{\geq 0}$ yhtälö

$$\operatorname{rad}(x^n - 1) \geq C(\varepsilon) x^{n(1-\varepsilon)-1}.$$

Valitaan luku $\varepsilon > 0$ siten, että $x^{1-\varepsilon} = \sqrt{x(x-1)}$ ja luku n siten, että $(x-1)^{2^{n-1}} < C(\varepsilon) x^{2^{n-1}}$. Oletetaan vielä $x > y$, jolloin saadaan

$$y^{2^n} - 1 < (x-1)^{2^n} < C(\varepsilon) x^{2^{n-1}-1} (x-1)^{2^{n-1}} = C(\varepsilon) x^{2^n(1-\varepsilon)-1} \leq \operatorname{rad}\left(x^{2^n} - 1\right).$$

Siten saadaan epäyhtälö

$$y^{2^n} - 1 < \operatorname{rad}\left(x^{2^n} - 1\right),$$

joka ei ole voimassa luvuilla $y > 1$. □

4.18 Croftin ongelma

Kirjassa [21, Problem F23, s. 261] Croft kysyy Littlewoodin innoittamana kuinka pieni erotus $|n! - 2^m|$ voi olla suhteessa lukuun 2^m. Nitaj'n mukaan [35] *Abc*-konjektuurilla saadaan seuraava arvio.

Lause 4.18.1. *Abc-konjektuurin nojalla jokaista $\varepsilon > 0$ kohti on olemassa vakio $C(\varepsilon) > 0$ siten, että luvuilla $m, n \in \mathbb{N}$, $(m,n) \neq (0,0), (1,0), (2,1)$ on voimassa*

$$n \leq C(\varepsilon) \operatorname{rad}(n! - 2^m)^{\frac{1+\varepsilon}{n}}$$

Todistus. Kirjoitetaan $n!$ muodossa $n! = 2^s n'$, missä n' on pariton. Nyt selvästi $s < n$. Jaetaan tarkastelu kahteen osaan riippuen luvun s suuruudesta.

Jos $s \geq m$, niin soveltamalla *Abc*-konjketuuria summaan

$$\frac{n!}{2^m} - 1 = k$$

saadaan

$$\frac{n!}{2^n} \leq \frac{n!}{2^m} \leq C(\varepsilon) \operatorname{rad}(n!k)^{1+\varepsilon} \leq C(\varepsilon) \operatorname{rad}(n! 2^m k)^{1+\varepsilon},$$

jolloin Lemmoja käyttämällä saadaan

$$\left(\frac{n}{2e}\right)^n \leq C(\varepsilon) 4^{n(1+\varepsilon)} \operatorname{rad}(2^m k)^{1+\varepsilon}.$$

Tästä edelleen

$$n \leq C'(\varepsilon) \operatorname{rad}(n! - 2^m)^{1+\varepsilon},$$

missä

Jos taas $s < m$, niin soveltamalla *Abc*-konjektuuria summaan

$$\frac{n!}{2^s} - 2^{m-s} = k$$

saadaan

$$\frac{n!}{2^n} \leq \frac{n!}{2^s} \leq C(\varepsilon) \operatorname{rad}(n! 2^s k)^{1+\varepsilon}.$$

Väite seuraa. □

Huomautus 4.18.2. Työssä [35] asetetaan kokeellisten tulosten perusteella voimakkaampi konjektuuri, jonka mukaan lauseen vakio $C(\varepsilon)$ voidaan korvata absoluuttisella vakiolla C ja termi $1 + \varepsilon$ termillä 1.

5 *Abc*-konjektuurin yleistyksiä

5.1 *Abc*-konjektuuri kongruensseille

Vuonna 2000 J. S. Ellenberg esitti todistuksen sille, että kongruenssi *Abc*-konjektuurista seuraa itse *Abc*-konjektuuri [13]. Seuraavassa osoitetaan sama seuraten kirjan [33] esitystapaa.

Konjektuuri 5.1.1. (Abc kongruensseille) *Kaikilla $m \in \mathbb{N} \setminus \{1\}$ ja $\varepsilon > 0$ on olemassa luku $C(m, \varepsilon)$ siten, että kaikille nollasta eroaville suhteellisille alkuluvuille $a, b, c \in \mathbb{Z}$, joille*

$$abc \equiv 0 \pmod{m} \qquad ja \qquad a + b = c,$$

pätee epäyhtälö

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

Kongruenssiehdosta johtuen tämä on normaalia *abc*-konjektuuria heikompi väittämä, mutta osoitetaan, että jos Konjektuuri 5.1.1 on totta jollekin m, niin tavallinen *abc*-konjektuuri on myös totta.

Lemma 5.1.2. *Olkoon (a, b, c) abc-summa siten, että $0 < a < b < c$.*

(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.

Tapauksessa (ii) pätee lisäksi joko $4 \mid c$ tai $4 \mid (b - a)$.

Todistus. Olkoon (a, b, c) *abc*-summa. 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 $\operatorname{syt}(a, b, c) > 1$. Nyt $c = 2(m + k + 1)$. ja $b - a = 2(k - m)$ eli (ii) on 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. *Abc*-konjektuuri kongruensseille arvolla $m = 2$ on sama kuin alkuperäinen *Abc*-konjektuuri. Nimittäin ainakin yksi *abc*-summan $a + b = c$ luvuista a, b ja c on parillinen, joten $abc \equiv 0 \pmod{2}$.

Lemma 5.1.4. *Olkoon $n \in \mathbb{N}$ ja olkoot (a, b, c) abc-summa siten, että $0 < a < b < c$. Jos luku c on pariton, asetetaan*

$$A_n = (b-a)^n, \qquad B_n = c^n - (b-a)^n, \qquad C_n = c^n.$$

Jos luku c on parillinen, asetetaan

$$A_n = \left(\frac{b-a}{2}\right)^n, \qquad B_n = \left(\frac{c}{2}\right)^n - \left(\frac{b-a}{2}\right)^n, \qquad C_n = \left(\frac{c}{2}\right)^n.$$

Tällöin (A_n, B_n, C_n) muodostaa abc-summan.

Todistus. Selvästi $A_n + B_n = C_n$ molemmissa tapauksissa. Oletuksen nojalla $0 < b - a < c$, jolloin edelleen Lemman 5.1.2 nojalla luvut A_n, B_n ja C_n ovat luonnollisia lukuja kaikilla $n \in \mathbb{N}$. Riittää siis osoittaa, että $\operatorname{syt}(A_n, B_n, C_n) = 1$.

Olkoon c ensin pariton. Esimerkin 2.1.6 nojalla $\operatorname{syt}(c, b-a) \leq 2$. Koska luvut c ja $b-a$ ovat parittomia (Lemma 5.1.2), täytyy olla $\operatorname{syt}(c, b-a) = 1$. Lemmojen 2.1.16 ja 2.1.10 nojalla edelleen

$$1 = \operatorname{syt}(c^n, (b-a)^n) = \operatorname{syt}(c^n - (b-a)^n, (b-a)^n) = \operatorname{syt}(c^n - (b-a)^n, c^n).$$

Olkoon sitten luku c parillinen. Tällöin myös $b-a$ on parillinen (Lemma 5.1.2), joten Esimerkin 2.1.6 nojalla $\operatorname{syt}(c, b-a) = 2$. Lemman 2.1.9 nojalla $\operatorname{syt}\left(\frac{c}{2}, \frac{b-a}{2}\right) = 1$, jolloin päättely on analoginen yllä olevan kanssa. □

Tarvitaan vielä seuraava aputulos.

Lemma 5.1.5. *Valitaan kolmikko (A_n, B_n, C_n) kuten Lemmassa 5.1.4. Jos $m \geq 3$ ja $n = \phi(m)$, niin*

$$A_n B_n C_n \equiv 0 \pmod{m}. \tag{5.1}$$

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 seuraa soveltamalla tulosta luvun m kanoniseen esitykseen. 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 2.1.25 ja Lause 2.1.26) 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 2.1.25 sekä Eulerin lauseen (Lause 2.1.28) nojalla

$$c^{(p-1)p^{r-1}} \equiv 1 \pmod{p^r}$$

ja

$$(b-a)^{(p-1)p^{r-q}} \equiv 1 \pmod{p^r}.$$

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 2. □

Osoitetaan viimein yhteys *Abc*-konjektuurien kongruenssiversion ja tavallisen version välillä.

Lause 5.1.6. *Olkoon $m \geq 3$. Jos Abc-konjektuuri kongruensseille on voimassa luvulle m, niin myös Abc-konjektuuri on voimassa.*

Todistus. Olkoon $0 < \varepsilon < 1$. Määritellään *abc*-summille (a,b,c) funktio Φ_ε siten, että

$$\Phi_\varepsilon(a,b,c) = \log c - (1+\varepsilon) \log \operatorname{rad}(abc). \tag{5.2}$$

Kirjoittamalla $\log c = (1+\varepsilon)(\log c) - \varepsilon \log c$ saadaan siten

$$\log \operatorname{rad}(abc) = \log c - \frac{\varepsilon \log c}{1+\varepsilon} - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon}. \tag{5.3}$$

Olkoon sitten (a,b,c) *abc*-summa siten, että $a < b < c$ jas $abc \equiv 0 \pmod{m}$. Osoitetaan, että on olemassa vakio $K(m,\varepsilon) > 0$ siten, että

$$\Phi_\varepsilon(a,b,c) \leq \log K(m,\varepsilon) = K^*(m,\varepsilon),$$

mistä *Abc*-konjektuuri seuraa.

Olkoon $m \geq 3$, jolloin $n = \phi(m)$ on parillinen Huomautuksen 2.1.27 nojalla. Määritellään luvut A_n, B_n ja C_n kuten Lemmassa 5.1.4. Nyt Lemman 5.1.5 nojalla pätee $A_n B_n C_n \equiv 0 \pmod{m}$ ja lisäksi oletuksen mukaan on olemassa vakio $K(m,\varepsilon) > 0$ siten, että

$$\Phi_\varepsilon(A_n, B_n, C_n) \leq K^*(m,\varepsilon). \tag{5.4}$$

Nyt luvun n parillisuuden nojalla saadaan Lemmaa 2.2.6 käyttämällä arvio

$$\begin{aligned} B_n &= c^n - (b-a)^n = (b+a)^n - (b-a)^n \\ &= 4ab\big((b+a)^{n-2} + (b+a)^{n-2}(b-a)^2 + \cdots + (b-a)^{n-2}\big) \\ &\leq 4ab\left(\frac{n}{2}\right)(b+a)^{n-2} = 2abnc^{n-2}. \end{aligned}$$

Koska

$$A_nB_nC_n = (b-a)^n\left(\frac{B_n}{ab}\right)abc^n,$$

saadaan

$$\begin{aligned}
\operatorname{rad}(A_nB_nC_n) &\le \operatorname{rad}\left((b-a)^n\left(\frac{B_n}{ab}\right)abc^n\right) = \operatorname{rad}\left((b-a)\left(\frac{B_n}{ab}\right)abc\right)\\
&\le \operatorname{rad}(b-a)\operatorname{rad}\left(\frac{B_n}{ab}\right)\operatorname{rad}(abc) \le (b-a)\left(\frac{B_n}{ab}\right)\operatorname{rad}(abc)\\
&\le (b-a)\left(2nc^{n-2}\right)\operatorname{rad}(abc)\\
&\le 2nc^{n-1}\operatorname{rad}(abc).
\end{aligned}$$

Ottamalla logaritmi ja sijoittamalla yhtälö (5.3) saadaan

$$\begin{aligned}
\log\operatorname{rad}(A_nB_nC_n) &\le (n-1)\log c + \log\operatorname{rad}(abc) + \log 2n\\
&= n\log c - \frac{\varepsilon\log c}{1+\varepsilon} - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + \log 2n\\
&= \left(1-\frac{\varepsilon}{(1+\varepsilon)n}\right)\log c^n - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + \log 2n\\
&\le \left(1-\frac{\varepsilon}{(1+\varepsilon)n}\right)(\log C_n + n\log 2) - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + \log 2n\\
&\le \left(\frac{n+(n-1)\varepsilon}{(1+\varepsilon)n}\right)\log C_n - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + 3n\log n,
\end{aligned}$$

kun käytetään arviota

$$\left(\frac{n+(n-1)\varepsilon}{(1+\varepsilon)n}\right)n\log 2 + \log 2n \le (2n-1)\log 2 + \log 2^n \le 3n\log 2.$$

Ratkaisemalla $\Phi_\varepsilon(a,b,c)$ saadaan

$$\begin{aligned}
\Phi_\varepsilon(a,b,c) &\le \left(\frac{n+(n-1)\varepsilon}{n}\right)\left(\log C_n - \left(\frac{(1+\varepsilon)n}{n+(n-1)\varepsilon}\right)\log\operatorname{rad}(A_nB_nC_n)\right)\\
&\quad + 3(1+\varepsilon)n\log 2\\
&< 2\left(\log C_n - \left(\frac{(1+\varepsilon)n}{n+(n-1)\varepsilon}\right)\log\operatorname{rad}(A_nB_nC_n)\right) + 6n\log 2\\
&= 2\big(\log C_n - (1-\varepsilon')\log\operatorname{rad}(A_nB_nC_n)\big) + 6n\log 2,
\end{aligned}$$

missä

$$\varepsilon' = \frac{(1+\varepsilon)n}{n+(n-1)\varepsilon} - 1 = \frac{\varepsilon}{\phi(m)+(\phi(m)-1)\varepsilon}.$$

Soveltamalla *abc*-summaan (A_n, B_n, C_n) yhtälöä (5.2) ja oletusta (5.4) saadaan

$$\log C_n - (1+\varepsilon')\log\operatorname{rad}(A_nB_nC_n) = \Phi_{\varepsilon'}(A_n,B_n,C_n) \le K^*(\varepsilon', m),$$

jolloin edelleen

$$\Phi_\varepsilon(a,b,c) < 2K^*(\varepsilon', m) + 6\phi(m)\log 2.$$

Näin ollen jokaisella $\varepsilon > 0$ funktio $\Phi_\varepsilon(a,b,c)$ on ylhäältä rajoitettu, mikä on yhtäpitävää *Abc*-konjektuurin kanssa.

□

5.2 n-konjektuuri

J. Brownkin ja J. Brzeziński esittivät vuonna 1994 *Abc*-konjektuurin ilmeisen yleistyksen $n \geq 3$ kokonaisluvun tapaukseen seuraavasti [5].

Määritelmä 5.2.1. Vektoria $(a_1, a_2, \ldots, a_n) \in \mathbb{Z}^n$, missä $n \geq 3$, kutsutaan *n-summaksi*, mikäli seuraavat kolme ehtoa toteutuvat:

(i) $\operatorname{syt}(a_1, a_2, \ldots, a_n) = 1$,

(ii) $a_1 + a_2 + \cdots + a_n = 0$,

(iii) mikään kohdan (ii) summan aito osasumma ei ole yhtä suuri kuin nolla.

Tällöin merkitään $M_n = M = \max_{1 \leq j \leq n}(|a_j|)$, $m_n = m = \operatorname{rad}(a_1 \cdots a_n)$ ja

$$L_n = L(a, \ldots, a_n) = \frac{\log M_n}{\log m_n}.$$

n-konjektuuri voidaan esittää silloin muodossa:

Konjektuuri 5.2.2. *Olkoon $n \in \mathbb{N}_{\geq 3}$ ja $\varepsilon > 0$ ja. Tällöin on olemassa vakio $C(n, \varepsilon) > 0$ siten, että kaikille n-summille $(a_1, \ldots, a_n)$ pätee*

$$\max\{|a_1|, \ldots, |a_n|\} \leq C(n, \varepsilon) \operatorname{rad}(a_1 \cdots a_n)^{2n-5+\varepsilon}.$$

Käytetään konjektuurista todistuksen helpottamiseksi muotoa $\limsup L_n = 2n - 5$. Ensin tarvitaan kuitenkin seuraava aputulos.

Lemma 5.2.3. *Jokaista lukua $k \in \mathbb{Z}_{>0}$ kohti on olemassa k-asteinen positiivikertoiminen polynomi $f_k \in \mathbb{Z}[x]$ siten, että*

$$\frac{x^{2k+1} - 1}{x - 1} = x^k f_k\left(\frac{(x-1)^2}{x}\right). \tag{5.5}$$

Todistus. Määrittelemällä $\alpha_j = \frac{2\pi j}{2k+1}$, $j = 1, 2, \ldots, k$, saadaan

$$\begin{aligned}\frac{x^{2k+1} - 1}{x - 1} &= \prod_{j=1}^{k}(x^2 - 2x\cos\alpha_j + 1) \\ &= x^k \prod_{j=1}^{k}\left(\frac{(x-1)^2}{x} + 2(1 - \cos\alpha_j)\right)\end{aligned}$$

Ny riittää valita

$$f_k(z) = \prod_{j=1}^{k}\big(z + 2(1 - \cos\alpha_j)\big).$$

Väitteen yhtälöstä seuraa nyt, että f_k on kokonaislukukertoimet ja koska sen kaikki juuret ovat negatiivisia, kaikki kertoimet ovat positiivisia. □

Huomautus 5.2.4. 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

$$\begin{aligned} f_2(z) &= z^2 + 5z + 5, \\ f_3(z) &= z^3 + 7z^2 + 14z + 7, \\ f_4(z) &= z^4 + 9z^3 + 27z^2 + 30z + 9 \\ f_5(z) &= z^5 + 11z^4 + 44z^3 + 77z^2 + 55z + 11. \end{aligned}$$

Lause 5.2.5. *Jokaisella $n \geq 3$ on voimassa*

$$\limsup\{L_n\} \geq 2n - 5.$$

Todistus. Olkoon Lemman 5.2.3 mukaisesti f_k polynomi siten, että

$$f_k(z) = \sum_{j=0}^{k} s_j z^j,$$

missä luvut s_j ovat positiivisia kokonaislukuja kaikilla $j \in \{0, 1, \ldots, k\}$. Asetetaan yhtälössä (5.5) $k = n-3$ ja $x = -\frac{a_1}{a_2}$, jolloin saadaan

$$\begin{aligned} &\frac{\left(-\frac{a_1}{a_2}\right)^{2(n-3)+1} - 1}{\left(-\frac{a_1}{a_2}\right) - 1} - \left(-\frac{a_1}{a_2}\right)^{n-3} \cdot \sum_{j=0}^{n-3} s_j \left(\frac{(\left(-\frac{a_1}{a_2}\right) - 1)^2}{\left(-\frac{a_1}{a_2}\right)} \right)^j \\ &= \frac{\left(\frac{a_1}{a_2}\right)^{2n-5} + 1}{\frac{a_1}{a_2} + 1} - \left(-\frac{a_1}{a_2}\right)^{n-3} \cdot \sum_{j=0}^{n-3} s_j \left(\frac{(\frac{a_1}{a_2} + 1)^2}{-\frac{a_1}{a_2}} \right)^j \\ &= \frac{a_1^{2n-5} + a_2^{2n-5}}{a_2^{2n-6}(a_1+a_2)} - \left(-\frac{a_1}{a_2}\right)^{n-3} \cdot \sum_{j=0}^{n-3} s_j \left(\frac{(a_1+a_2)^2}{-a_1 a_2} \right)^j = 0. \end{aligned}$$

Kertomalla nyt yhtälö puolittain luvulla $a_2^{2n-6}(a_1+a_2)$ saadaan

$$\begin{aligned} &a_1^{2n-5} + a_2^{2n-5} - a_2^{2n-6}(a_1+a_2) \left(-\frac{a_1}{a_2}\right)^{n-3} \cdot \sum_{j=0}^{n-3} s_j \left(\frac{(a_1+a_2)^2}{-a_1 a_2} \right)^j \\ &= a_1^{2n-5} + a_2^{2n-5} - (a_1+a_2)\,(-a_1 a_2)^{n-3} \sum_{j=0}^{n-3} s_j \frac{(a_1+a_2)^{2j}}{(-a_1 a_2)^j} \\ &= a_1^{2n-5} + a_2^{2n-5} - \sum_{j=0}^{n-3} s_j (a_1+a_2)^{2j+1} (-a_1 a_2)^{n-j-3} = 0. \end{aligned}$$

Valitaan $a_1 = 2^i$, $i > 1$, ja $a_2 = -1$, jolloin edellä olevasta yhtälöstä saadaan n:n kokonaisluvun summa

$$2^{i(2n-5)} - 1 - \sum_{j=0}^{n-3} s_j (2^i - 1)^{2j+1} 2^{i(n-j-3)} = 0. \tag{5.6}$$

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. Näin ollen määritelmän 5.2.1 ehdot ovat voimassa. Tällä lukujen a_1 ja a_2 valinnalla saadaan edellä olevasta yhtälöstä

$$M_n = 2^{i(2n-5)}.$$

Merkitsemällä $c = 2s_0 s_1 \cdots s_{n-3}$ saadaan summan (5.6) luvuille $m_n = \operatorname{rad}((2^i - 1)c)$. Soveltamalla arviota

$$\operatorname{rad}\big((2^i - 1)c\big) \leq \operatorname{rad}(2^i - 1)\operatorname{rad}(c) \leq (2^i - 1)\operatorname{rad}(c) \leq 2^i \operatorname{rad}(c)$$

ja käyttämällä 2-kantaista logaritmia saadaan lopulta

$$L_n = \frac{\log_2 M_n}{\log_2 m_n} = \frac{i(2n-5)}{\log_2 \operatorname{rad}((2^i - 1)c)} \geq \frac{i(2n-5)}{i + \log_2 \operatorname{rad}(c)} \to 2n - 5,$$

kun $i \to \infty$. Koska on äärettömästi sellaisia lukuja i, joille $2^i - 1$ ovat suhteellisia alkukuja, nähdään helposti, että niitä luvun i arvoja vastaavat osamäärät L_n ovat eri lukuja. Näin ollen joukolla $\{L_n\}$ on kasaantumispiste, joka on ainakin $2n - 5$. □

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. [27, s. 165]

Esitetään seuraavaksi Snyderin todistus kirjaan [27] perustuen sekä selkeyttävää lähdettä [25] avuksi käyttäen.

Lemma 5.3.1. *Olkoon f polynomi suljetussa algebrallisessa kunnassa ja olkoon α polynomin f juuri moninkertanaan $m(\alpha)$. Tällöin polynomin f' moninkerta pisteessä α on $m(\alpha) - 1$.*

Todistus. Kirjoitetaan polynomi f muodossa $f(t) = (t-\alpha)^m g(t)$, missä polynomille g pätee $g(\alpha) \neq 0$. Tulon derivoimissäännön nojalla

$$\begin{aligned} f'(t) &= (t-\alpha)^m g'(t) + m(t-\alpha)^{m-1} g(t) \\ &= (t-\alpha)^{m-1}\big((t-\alpha)g'(t) + mg(t)\big) = (t-\alpha)^{m-1} h(t), \end{aligned}$$

missä $h(t) = \big((t-\alpha)g'(t) + mg(t)\big)$ ja arvot $h(\alpha)$, $mg(\alpha)$ sekä $g(\alpha)$ ovat nollasta eroavia. Näin ollen $(t-\alpha)^{m-1}$ on korkein luvun $(t-\alpha)$ potenssi, joka jakaa polynomin f', joten $m-1$ on polynomin f' juuren α monikerta. □

Määritelmä 5.3.2. Olkoon f ei-vakio polynomi. Tällöin merkitään

$$\mathrm{n}_0(f) = \text{funktion } f \text{ erillisten nollakohtien lukumäärä.}$$

Lemma 5.3.3. *Jos f on polynomi, niin* $\deg(f, f') = \deg(f) - \mathrm{n}_0(f)$.

Todistus. Olkoon $\deg(f) = n$ ja olkoot $\alpha_1, \ldots, \alpha_i$ polynomin f erilliset juuret moninkertoinaan $k_1, \ldots, k_i$. Tällöin $n = k_1 + \cdots + k_i$. Lemman 5.3.1 todistuksen mukaan

$$\mathrm{syt}(f, f') = (t - \alpha_1)^{k_1 - 1}(t - \alpha_2)^{k_2 - 1} \cdots (t - \alpha_n)^{k_n - 1}.$$

Näin ollen

$$\begin{aligned} \deg(f, f') &= (k_1 - 1) + (k_2 - 1) + \cdots + (k_i - 1) \\ &= (k_1 + k_2 + \cdots + k_i) - i \\ &= n - i = \deg(f) - \mathrm{n}_0(f), \end{aligned}$$

mistä väite seuraa □

Lause 5.3.4 (Stothers-Mason)**.** *Olkoot $f, g, h \in \mathbb{C}[t]$ keskenään jaottomia polynomeja, joista ainakin yksi ei ole vakio ja jotka toteuttavat yhtälön $f + g = h$. Tällöin*

$$\max\{\deg(f), \deg(g), \deg(h)\} \leq \mathrm{n}_0(fgh) - 1.$$

Todistus. Todetaan ensin, että nyt on voimassa yhtälö

$$f'g - fg' = f'h - fh'. \tag{5.7}$$

Derivoimalla yhtälöä $f + g = h$ saadaan $f' + g' = h'$, joten

$$f'g - fg' = f'(h - f) - f(h' - f') = f'h - fh'.$$

Huomioidaan tässä, että nyt ainakin kaksi polynomeista f, g, h ei 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 (5.7). Havaitaan, että yhtälön vasen puoli on jaollinen tekijöillä $\mathrm{syt}(f, f')$ sekä $\mathrm{syt}(g, g')$ ja yhtälön oikeapuoli on jaollinen tekijällä $\mathrm{syt}(h, h')$. Mutta koska vasen ja oikea puoli ovat yhtäsuuret ja polynomit f, g ja h ovat keskenään jaottomia, saadaan

$$\mathrm{syt}(f, f')\,\mathrm{syt}(g, g')\,\mathrm{syt}(h, h') \mid (f'g - fg').$$

Näin ollen

$$\deg(f, f') + \deg(g, g') + \deg(h, h') \leq \deg(f'g - fg'),$$

jolloin edelleen

$$\deg(f, f') + \deg(g, g') + \deg(h, h') \leq \deg(f) + \deg(g) - 1. \tag{5.8}$$

Soveltamalla Lemmaa 5.3.3 polynomeihin f, g ja h saadaan

$$\begin{aligned} \deg(f, f') &= \deg(f) - \mathrm{n}_0(f), \\ \deg(g, g') &= \deg(g) - \mathrm{n}_0(g), \\ \deg(h, h') &= \deg(h) - \mathrm{n}_0(h), \end{aligned}$$

jotka sijoittamalla yhtälöön (5.8) saadaan

$$\deg(h) \leq \mathrm{n}_0(f) + \mathrm{n}_0(g) + \mathrm{n}_0(h) - 1 = \mathrm{n}_0(fgh) - 1,$$

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. □

Huomautus 5.3.5. Mason-Stothersin lauseen ehdot toteuttavien polynomien asteille saadaan artikkelin [52] mukaan alaraja

$$\min\{\deg(f), \deg(g), \deg(h)\} \leq \mathrm{n}_0(fgh) - 2.$$

Lauseen seurauksena saadaan välittömästi Fermat'n suuren lauseen polynomiversio [27].

Lause 5.3.6. (Fermat'n suuri lause polynomeille) *Olkoot $u, v, w \in \mathbb{C}[t]$ keskenään jaottomia vakiosta eroavia polynomeja ja olkoon $n \in \mathbb{N}_{\geq 3}$. Tällöin yhtälöllä*

$$u^n + v^n = w^n$$

ei ole ratkaisuja.

Todistus. Soveltamalla Mason-Stothersin lausetta funktioihin $f = u^n, g = v^n$ ja $h = w^n$ saadaan

$$\deg u^n \leq \mathrm{n}_0(u^n v^n w^n) - 1.$$

Koska $\deg(u^n) = n \cdot \deg(u)$ ja $\mathrm{n}_0(f) = \mathrm{n}^{\mathrm{n}} \leq \deg(u)$, saadaan edelleen

$$n \cdot \deg(u) \leq \deg(u) + \deg(v) + \deg(w) - 1.$$

Samanlaisella päättelyllä saadaan polynomeille v ja w epäyhtälöt

$$\begin{aligned} n \cdot \deg(v) &\leq \deg(u) + \deg(v) + \deg(w) - 1, \\ n \cdot \deg(w) &\leq \deg(u) + \deg(v) + \deg(w) - 1. \end{aligned}$$

Lisäämällä yhtälöt puolittain yhteen saadaan

$$n\big(\deg(uvw)\big) \leq 3\big(\deg(uvw)\big) - 3 < 3\big(\deg(uvw)\big).$$

Jakamalla puolittain termillä $\deg(uvw)$ saadaan epäyhtälö $n < 3$, mikä on ristiriita. □

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, ss. 37-44, de Gruyter, Berliini, 1998.

[3] Bombieri, E., Gubler, W. *Heights in Diophantine Geometry.* Cambridge University Press, New York, 2006.

[4] Berndt, B. C., Galway, W. F. *On the Brocard-Ramanujan Diophantine Equation* $n! + 1 = m^2$. Ramanujan J. 4, No. 1 (2000), ss. 41-42.

[5] Browkin, J., Brzeziński, J. *Some remarks on the abc-conjecture.* Math. Comp. 62, No. 206 (1994), ss. 931-939.

[6] 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, Cambridge University Press ss. 65–85, Cambridge, 1997.

[7] Browkin, J. *The abc-conjecture.* Number theory, ss. 75–105, Trends Math., Birkhäuser, Basel, 2000.

[8] Cochrane, T., Dressler, R. E. *Gaps between integers with the same prime factors.* Math. Comp. 68, No. 225 (1999), ss. 395-401.

[9] Dabrowski, A. *On the Diophantine equation* $x! + A = y^2$. Nieuw Arch. Wisk. (4) 14, No. 3 (1996), ss. 321-324.

[10] Dahmen, S. R. *Lower bounds for numbers of ABC-hits.* Journal of Number Theory 128 (2008), ss. 1864-1873.

[11] 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), ss. 513-543.

[12] Edwards, H. M. *Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory.* Springer-Verlag, New York, 1977.

[13] Ellenberg, J. S. *Congruence ABC implies ABC.* Indag. Math. (N.S.) 11, No. 2 (2000), ss. 197-200.

[14] Filaseta, M., Konyagin, S. *On a limit point associated with the abc-conjecture.* Colloq. Math. 76 (1998), No. 2, ss. 265–268.

[15] Fraleigh, J. B. *A first course in abstract algebra.* Addison-Wesley Publishing Company, New York, 2003.

[16] van Frankenhuysen, M. *A Lower Bound in the abc Conjecture.* J. Number Theory 82 (2000), No. 1, ss. 91–95.

[17] van Frankenhuysen, M. *The ABC conjecture implies Roth's Theorem and Mordell's conjecture*. Mat. Contemp. 16 (1999), ss. 45-72.

[18] Geuze, G., de Smit, B. *Reken mee met ABC.* Nieuw Archief voor Wiskunde Part 8, No. 1 (2007), ss. 26-30.

[19] Goldfeld, D. *Beyond the Last Theorem*. The Sciences, March/April (1996), ss. 34-40.

[20] 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, ss. 229–236. de Gruyter, Berlin, 1999.

[21] Guy, R. K. *Unsolved Problems in Number Theory, Second Edition*. Springer Verlag New York Inc., Yhdysvallat, 1994.

[22] Hardy, G. H., Wright, E. M. *Introduction to the Theory of Numbers, Sixth Edition.* Oxford University Press Inc., Norfolk , 2008.

[23] Ingham, A. E. *The Distribution of Prime Numbers*. Stechert-Hafner Service Agency Inc., New York, 1964.

[24] Knauer, J., Richstein, J. *The Continuing Search for Wieferich Primes*. Math. Comp. 74, No. 251 (2005), ss. 1559-1563.

[25] Lama, V. *Mason-Stothers Theorem and the ABC Conjecture*. WWW-dokumentti (luettu 26.7.2011). url: `http://topologicalmusings.wordpress.com/2008/03/03/mason-stothers-theorem-and-the-abc-conjecture/`

[26] Lang, S. *Old and New Conjectured Diophantine Equations*. Bull. Amer. Math. Soc. 23, No. 1 (1990), ss. 37-75.

[27] Lang, S. *Undergraduate Algebra, Third Edition*. Springer Science+Business Media Inc., Yhdysvallat, 2005.

[28] Langevin, M. *Cas d'égalité pour le théorème de Mason et applications de la conjecture (abc)*. C. R. Acad. Sci. Paris Sér. I Math. 317, No. 5 (1993), ss. 441-444.

[29] Luca, F. *On a conjecture of Erdös and Stewart*. Math. Comp. 70, No. 234 (2001), ss. 893–896.

[30] Luca, F. *On the diophantine equation* $p^{x1} - p^{x2} = q^{y1} - q^{y2}$. Indag. Math. (N.S.) 14, No. 2 (2003), ss. 207-222.

[31] Mihăilescu, P. *Primary cyclotomic units and a proof of Catalan's conjecture*. J. Reine Angew. Math. 572 (2004), ss. 167-195.

[32] Mordell, L. J. *Diophantine Equations*. Academic Press Inc., Lontoo, 1969.

[33] Nathanson, M. B. *Elementary Methods in Number Theory*. Springer-Verlag New York Inc., New York, 2000.

[34] Nitaj, A. *Aspects expérimentaux de la conjecture abc*. Séminaire de Théorie des Nombres de Paris, London Math. Soc. Lecture Note Ser. 235 ss. 145–156, Cambridge Univ. Press, Cambridge, 1996.

[35] Nitaj, A. *Conséquences et aspects expérimentaux des conjectures abc et de Szpiro*. Ph.D. Thesis, University of Caen, 1994.

[36] Nitaj, A. *La conjecture abc*. Enseign. Math. (2) 46, No. 1-2 (1996), ss. 3-24.

[37] Nitaj, A. *The abc conjecture*. WWW-dokumentti (luettu 17.12.2011).
url: `http://www.math.unicaen.fr/~nitaj/abc.html`

[38] Oesterlé, J. *Nouvelles approches du "theoreme" de Fermat*. Séminaire N. Bourbaki, Vol. 1987-88. Astérisque No. 161-162 (1988), Exp. No. 694, 4, ss. 165–186.

[39] Overholt, M. *The Diophantine Equation* $n! + 1 = m^2$. Bull. Lond. Math. Soc. 25, No. 2 (1993), s.104.

[40] Riesel, H. *Prime Numbers and Computer Methods for Factorization, Second Edition*. Birkhäuser, Boston, 1994.

[41] Rosen, K. H. *Elementary Number Theory and Its Applications*. Addison-Wesley Publishing Company, Yhdysvallat, 1986.

[42] Ross, S. M. *A First Course in Probability*. Prentice-Hall Inc., Yhdysvallat, 1998.

[43] Saari, K. *ABC-otaksuma*. Pro gradu –tutkielma, Turun yliopisto, 2003.

[44] Shorey, T. N., Tijdeman, R. *Exponential Diophantine Equations*. Cambridge University Press, Cambridge, 1986.

[45] Silverman, J. H. *The Arithmetic of Elliptic Curves, Second Edition*. Springer Science+Business Media, New York, 2009.

[46] Silverman, J. S. *Wieferich's criterion and the abc-conjecture*. J. Number Theory 30, No. 2 (1988), ss. 226-237.

[47] de Smit, B. *Bart de Smit - ABC triples*. WWW-dokumentti (luettu 23.12.2011).
url: `http://www.math.leidenuniv.nl/~desmit/abc/index.php?sort=1`

[48] Stewart, C. L., Yu, Kun Rui. *On the abc-conjecture*. Math. Ann. 291, No. 2 (1991), ss. 225-230.

[49] Stewart, C. L., Yu, Kun Rui. *On the abc-conjecture. II*. Duke Math. J 108, No. 1 (2001), ss. 161-181.

[50] Stewart, C. L., Tijdeman, R. *On the Osterlé-Masser Conjecture*. Monatsh. Math 102, No. 3 (1986), ss. 251-257.

[51] Trench, W. F. *Introduction to real analysis*. Prentice Hall/Pearson Education, 2003.

[52] Vaserstein, L. N. *Quantum (abc)-Theorems*. J. Number Theory 81, No. 2 (2000), ss. 351– 358.

[53] Waldschmidt, M. *Nombres Transcendants*. Lecture Notes in Mathematics, Springer-Verlag Berlin, Heidelberg, 1974.

[54] Wiles, A. *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. (2) 141, No. 3 (1995), ss. 443–551.

[55] Wheeler, J. P. *The abc conjecture*. Master's Thesis, University of Tennessee, Knoxville, 2002.

A 50 laadultaan parasta *abc*-kolmikkoa

Abc-kolmikon $(a, b, c) \in \mathbb{N}^3$ laatu [7, s. 77] määritellään lukuna

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

Abc-kolmikko on laadultaan *hyvä*, mikäli $L > 1,4$. Nykyään tunnetaan 234 laadultaan hyvää *abc*-kolmikkoa, joista 50 parasta on esitetty alla [47].

No.	L	a	b	c	löytäjä	vuosi
1	1.6299	2	$3^{10}109$	23^5	ER	1987
2	1.6260	11^2	$3^2 5^6 7^3$	$2^{21}23$	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	$2^2 11$	$3^2 13^{10} 17 \cdot 151 \cdot 4423$	$5^9 139^6$	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	$7 \cdot 167 \cdot 811^4 919$	$3^4 13^2 23^{12} 67^4$	$2^{31}5^3 11^2 17^5 107^4$	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	$5^{12}17^2 31^2 1699$	$23^{14}29$	$2^{19}3^2 11 \cdot 13^{10}47$	AN	1993
32	1.4578	$3^6 5^{12}$	$2^{16}13 \cdot 59^4$	$7^{11}47 \cdot 113$	AN	1993
33	1.4575	$3 \cdot 109 \cdot 131^4$	$5^{22}89$	$2^3 11^2 19^5 97^4$	TS	
34	1.4571	$3^2 5^2$	$2^4 17^3 31^4$	$7^{10}257$	AN	1993
35	1.4562	$2^{25}19$	$3 \cdot 5^{15}1033$	$11^7 13^3 47^2$	AN	1993
36	1.4557	1	$2^5 3 \cdot 5^2$	7^4	BdW	1988
37	1.4551	$3^2 11^6$	2^{35}	$19^5 13883$	JB JB	1994
38	1.4550	$23^2 31^5$	$2^{25}7 \cdot 109^3$	$3^{19}5^2 19^2 29$	TS	
39	1.4544	$7^8 2707$	$2^{10}5^{10}29^3$	$3^{18}11^4 43$	TS AR	
40	1.4533	13^6	$2 \cdot 3^4 7^4 11^9 23$	$5^7 103^4 2399$	AN	1993
41	1.4532	$7^5 23^2 101^4$	$2^{43}359^2$	$3^9 13 \cdot 19^6 307^2$	TS MH	
42	1.4526	$2^{19}13 \cdot 103$	7^{11}	$3^{11}5^3 11^2$	BdW	1988
43	1.4520	$2^{20}233^5$	$37 \cdot 59^8 4729^2$	$3^{24}5^6 19 \cdot 23 \cdot 251^2$	FR	2010
44	1.4519	$31^3 61^5$	$17^{10}83^2 2719 \cdot 15101$	$2 \cdot 3^3 5^{17}7^{12}$	FR	2007
45	1.4513	$3^5 7$	$5^6 67$	2^{20}	JB JB AN	1993
46	1.4509	$3^5 7^3$	$2^{13}23^3 59$	$5^3 19^6$	JB JB	1994
47	1.4502	$23^8 37^4$	$2^{28}3^7 11^4 19^3 61 \cdot 127 \cdot 173^2$	$5^{18}17^4 43^2 4817^2$	IC	2008
48	1.4501	$23^3 53^6 3167^2$	$2^8 3^{29}11399^2$	$5^7 7^4 13^{12}523$	FR	2008
49	1.4500	1	$3^3 5^3 7^7 23$	$2^{13}11^4 13 \cdot 41$	AN	1993
50	1.4497	1	$3 \cdot 5^5 47^2$	$2^{18}79$	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-kolmikkoa

Szpiron konjektuurin innoittamana voidaan tarkastella *abc*-kolmikon $(a, b, c) \in \mathbb{N}^3$ Szpiro-laatua [35, s. 8], joka määritellään lukuna

$$\rho = \rho(a, b, c) = \frac{\log |abc|}{\log \operatorname{rad}(abc)}.$$

Abc-kolmikko on Szpiro-laadultaan *hyvä*, mikäli $\rho > 4$. Alla on esitetty uudemman tiedon puutteessa 50 parasta vuonna 2003 tunnettua hyvää *abc*-Szpiro-kolmikkoa [37], [34].

No.	ρ	a	b	c	löytäjä	vuosi
1	4.41901	$13 \cdot 19^6$	$2^{30}5$	$3^{13}11^231$	AN	1992
2	4.26801	$2^5 11^2 19^9$	$5^{15}37^247$	$3^7 7^{11}743$	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	$2^{31}3^45^67$	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.	ρ	a	b	c	löytäjä	vuosi
31	4.09647	$3^{12}5^6$	$7^9 31^2$	$2^9 11^5 571$	AN	1992
32	4.09080	$7^8 19$	$2^{15}5^2 37^2$	$3 \cdot 17^7$	AN	1992
33	4.08545	$2^6 5^2 7^{13} 13^2 463$	$3^4 43^{12}$	$11^{12} 389^2 6841$	AN	
34	4.08362	$2^{13}5^{12}13^4 29$	$7^{16}19 \cdot 7451$	$3^{20}11^4 353^2$	TD	2003
35	4.08331	$79^5 677$	2^{42}	$3^{12}7 \cdot 13^4 61$	AN	1994
36	4.08299	$11^{11}73^2 991 \cdot 306083$	$2^2 3 \cdot 5^{11}7^{15}19^2$	$13^{15}31^5$	TD	2003
37	4.08262	$2 \cdot 5^9 11^4 41^2 53^3$	$3^9 7^{16}37$	$23^{11}40423$	TD	2003
38	4.07920	$31 \cdot 59^6$	$2^{25}3^1 1$	$5^3 11^7 13 \cdot 229$	TD	2003
39	4.07709	$5^{18}8837$	$7^9 19^3 79 \cdot 191^2$	$2^{22}3^5 13^8$	AN	
40	4.07457	$3^{13}13 \cdot 23^3 97^2$	$2^{37}157^2$	$5^5 31^7 67$	TD	2003
41	4.07337	$3^2 73^{10}$	$5^{25}17^2 23$	$2^2 7^1 1827^2 373357$	TD	2003
42	4.07114	$2^{24}3^5$	$5 \cdot 19^5 59^2$	$7^{10}167$	AN	1992
43	4.07038	$19 \cdot 47 \cdot 71^6$	$5^3 7^3 29^{11}$	$3^{35}23^3$	AN	1994
44	4.06886	$3^4 5^{18}71 \cdot 419 \cdot 876581$	$2^{17}13^2 19^{15}$	$7^6 11^{12} 977^3$	TD	2003
45	4.06705	$2^{26}11^4 7639$	$5^6 23^{11}$	$3^{18}47^4 7879$	TD	2003
46	4.06668	$5^{16}19^2$	$3^8 7^3 89^4$	$2^{28}11^2 6043$	TD	2003
47	4.06406	$7^3 29^5 151^2$	$2^4 5^{16}97 \cdot 919$	$3^{27}13^4$	AN	
48	4.06347	$19 \cdot 47 \cdot 71^6$	$3^{21}193^2$	$2^7 5^{12}127^2$	AN	1994
49	4.06231	$5^7 7^7 19^2 107$	$2^{14}11^9 97$	$3^{10}23^7 31$	TD	2003
50	4.06160	$2^7 3 \cdot 821^5$	13^{16}	$5^{12}101^2 324697$	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

X	$N(X)$	$\pi(X)$
10	1	4
10^2	6	25
10^3	31	168
10^4	120	1229
10^5	418	9592
10^6	1268	78 498
10^7	3499	664 579
10^8	8987	5 761 455
10^9	22 316	50 847 534
10^{10}	51 677	455 052 512
10^{11}	116 978	4 118 054 813
10^{12}	252 856	37 607 912 018

Taulukko 3: Abc-osumien ja alkulukujen lukumäärä (lähde: [41, s. 48].)

D 31 ensimmäistä *abc*-osumaa

Alla taulukoituna kaikki *abc*-summat $a + b = c$, joilla $\mathrm{rad}(abc) < c \leq 1000$ [18].

No.	a	b	c	$\mathrm{rad}(abc)$
1	$1=1$	$8=2^3$	$9=3^2$	6
2	$5=5$	$27=3^3$	$32=2^5$	30
3	$1=1$	$48=2^43$	$49=7^2$	42
4	$1=1$	$63=3^27$	$64=2^6$	42
5	$1=1$	$80=2^45$	$81=3^4$	30
6	$32=2^5$	$49=7^2$	$81=3^4$	42
7	$4=2^2$	$121=11^2$	$125=5^3$	110
8	$3=3$	$125=5^3$	$128=2^7$	30
9	$1=1$	$224=2^57$	$225=3^25^2$	210
10	$1=1$	$242=2\cdot 11^2$	$243=3^5$	66
11	$2=2$	$243=3^5$	$245=5\cdot 7^2$	210
12	$7=7$	$243=3^5$	$250=2\cdot 5^3$	210
13	$13=13$	$243=3^5$	$256=2^8$	78
14	$81=3^4$	$175=5^27$	$256=2^8$	210
15	$1=1$	$288=2^53^2$	$289=17^2$	102
16	$100=2^25^2$	$243=3^5$	$343=7^3$	210
17	$32=2^5$	$343=7^3$	$375=3\cdot 5^3$	210
18	$5=5$	$507=3\cdot 13^2$	$512=2^9$	390
19	$169=13^2$	$343=7^3$	$512=2^9$	182
20	$1=1$	$512=2^9$	$513=3^319$	114
21	$27=3^3$	$512=2^9$	$539=7^211$	462
22	$1=1$	$624=2^43\cdot 13$	$625=5^4$	390
23	$49=7^2$	$576=2^63^2$	$625=5^4$	210
24	$81=3^4$	$544=2^517$	$625=5^4$	510
25	$1=1$	$675=3^35^2$	$676=2^213^2$	390
26	$1=1$	$728=2^37\cdot 13$	$729=3^6$	546
27	$25=5^2$	$704=2^611$	$729=3^6$	330
28	$104=2^313$	$625=5^4$	$729=3^6$	390
29	$200=2^35^2$	$529=23^2$	$729=3^6$	690
30	$1=1$	$960=2^63\cdot 5$	$961=31^2$	930
31	$343=7^3$	$625=5^4$	$968=2^311^2$	770

E 31 ensimmäistä logaritmista *abc*-osumaa

Alla taulukoituna 31 ensimmäistä *abc*-kolmikko $(a, b, c) \in \mathbb{N}^3$, joille $\operatorname{rad}(abc) < \frac{c}{\log c}$.

No.	a	b	c	$\operatorname{rad}(abc)$	$\frac{c}{\log c}$
1	$1=1$	$2400=2^5 3 \cdot 5^2$	$2401=7^4$	210	$308,47$
2	$625=5^4$	$2048=2^{11}$	$2673=3^5 11$	330	$338,74$
3	$1=1$	$4374=2 \cdot 3^7$	$4375=5^4 7$	210	$521,85$
4	$289=17^2$	$6272=2^7 7^2$	$6561=3^8$	714	$746,51$
5	$7=7$	$32761=181^2$	$32768=2^{15}$	2534	$3151,62$
6	$37=37$	$32768=2^{15}$	$32805=3^8 5$	1110	$3154,83$
7	$1=1$	$59048=2^3 11^2 61$	$59049=3^{10}$	4026	$5374,87$
8	$343=7^3$	$59049=3^{10}$	$59392=2^{11}29$	1218	$5403,24$
9	$3=3$	$65533=13 \cdot 71^2$	$65536=2^{16}$	5538	$5909,28$
10	$7168=2^1 07$	$78125=5^7$	$85293=3^8 13$	2730	$7512,26$
11	$128=2^7$	$109375=5^6 7$	$109503=3^2 23^3$	4830	$9436,90$
12	$81=3^4$	$123823=7^3 19^2$	$123904=2^{10} 11^2$	8778	$10565,47$
13	$12672=2^7 3^2 11$	$117649=7^6$	$130321=19^4$	8778	$11065,01$
14	$18225=3^6 5^2$	$112847=7^4 47$	$131072=2^{17}$	9870	$11123,35$
15	$81=3^4$	$134375=5^5 43$	$134456=2^3 7^5$	9030	$11385,90$
16	$17=17$	$140608=2^6 13^3$	$140625=3^2 5^6$	6630	$11863,23$
17	$12005=5 \cdot 7^4$	$161051=11^5$	$173056=2^{10} 13^2$	10010	$14347,95$
18	$5=5$	$177147=3^{11}$	$177152=2^{10} 173$	5190	$14659,12$
19	$47=47$	$250000=2^4 5^6$	$250047=3^6 7^3$	9870	$20117,38$
20	$121=11^2$	$255879=3^9 13$	$256000=2^{11} 5^3$	4290	$20557,41$
21	$71875=5^5 23$	$190269=3^8 29$	$262144=2^{18}$	20010	$21010,77$
22	$3481=59^2$	$262144=2^{18}$	$265625=5^6 17$	10030	$21267,28$
23	$95=5 \cdot 19$	$279841=23^4$	$279936=2^7 3^7$	13110	$22319,32$
24	$131072=2^{17}$	$221875=5^5 71$	$352947=3 \cdot 7^6$	14910	$27629,95$
25	$338=2 \cdot 13^2$	$390625=5^8$	$390963=3 \cdot 19^4$	7410	$30362,83$
26	$24389=29^3$	$393216=2^{17} \cdot 3$	$417605=5 \cdot 17^4$	14790	$32266,70$
27	$1=1$	$512000=2^{12} 5^3$	$512001=3^5 7^2 43$	9030	$38947,04$
28	$49=7^2$	$531392=2^6 19^2 23$	$531441=3^1 2$	18354	$40311,54$
29	$533871=3^5 13^3$	$9583=7 \cdot 37^2$	$524288=2^{19}$	20202	$40481,85$
30	$2197=13^3$	$583443=3^5 \cdot 7^4$	$585640=2^3 5 \cdot 11^4$	30030	$44097,87$
31	$8192=2^{13}$	$634933=13^3 17^2$	$643125=3 \cdot 5^4 7^3$	46410	$48087,37$

F Java-koodi logaritmisten *abc*-osumien etsimiseen

Ohessa "brute force-javakoodi, jolla edellä ollut logaritmisten abc-osumien taulukko oli laskettu.

```
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,
               FileNotFoundException{
22                 PrintWriter output=new PrintWriter(ulostulo);
23
24                 /*Testing primefactors();
25                  *
26                  * System.out.print("Anna luku 1: ");
27                 int luku1=Integer.parseInt(lueRivi());
28                 int[] taulu=primefactors(luku1);
29                 for (int j=0; j<taulu.length; j++){
30                         System.out.print(taulu[j] + " ");
31                 }
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" +
                    "\nc:%10.0f"
50                              + "\nrad %10.0f"+ "\nc/logc %10.6f", a, b, c,
                                    radical, lokki);
51              if (radical < c){
52                      System.out.println("\nAbc-hit!");
53              }
54              if (radical < lokki){
55                      System.out.println("Mod abc-hit!");
56              }
57              System.out.println();
58              */
59
60
61              //Luetaan tiedostosta:
62              if (tiednimi == null) {
63                  System.out.println("Tiedoston nimea ei asetettu. ");
64               }
65
66          File file = new File(tiednimi);
67          if (file.exists() && file.isFile() && file.canRead() ) {
68              input = new Scanner(file);
69          } else {
70              System.out.println("Tiedostoa " + tiednimi + " ei voi lukea
                    . ");
71          }
72
73          boolean otsikko=false;
74          //1268 on c < 10^6 asti
75          //51677 on c < 10^10 asti
76          //116978 on c < 10^11 asti
77          //14 482 059 kaikki c < 10^18
78          for (int j=0; j < 1000000 ; j++){
79
80              text=lueTiedRivi();
81              text=text.trim();
82              String[] osat = text.split(" ");
83              c=Double.parseDouble(osat[0]);
84              a=Double.parseDouble(osat[1]);
85              b=c-a;
86
87              double lokki=c/(java.lang.Math.log(c));
88
89              radical=rad(a, b, c);
90
91              if(radical < lokki){
92              if(otsikko==false){
93                output.printf("%-10s " + "%12s="+"%-22s" + "%11s="+"%-19s
                      " + "%12s="+"%-22s" + "%12s "
94                                  + "  %12s\n","n(abc-hit)","c", "fact(c)
                                        ","a", "fact(a)","b", "fact(b)","
                                        radical","c/logc");
95                 otsikko=true;
96                }
97               mones+=1;
```

```
98                      turhake="" + mones + "(" + (j+1) + ")";
99                     output.printf("%-10s " + "%12.0f="+"%-22s" + "%11.0f="+"
                          %-19s" + "%12.0f="+"%-22s" + "%12.0f "
100                                        + "  %12.2f\n",turhake,c, printpf(c),a,
                                             printpf(a),b, printpf(b),radical,
                                           lokki);
101                     }
102
103                }
104                output.close();
105
106                /*
107                int lkm=0;
108                  while (input.hasNext()){
109                          input.nextLine();
110                          lkm++;
111                  }
112
113                  input.close();
114
115                  System.out.println(lkm);
116                  */
117
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 }
```