Tartu Ülikool

Loodus- ja täppisteaduste valdkond

Matemaatika ja statistika instituut

Jon Hendrik Aruväli

abc-hüpoteesist ja selle järeldustest

Matemaatika

Bakalaureusetöö (9 EAP)

Juhendaja: PhD Lauri Tart

Tartu 2022

ABC-HÜPOTEESIST JA SELLE JÄRELDUSTEST

Bakalaureusetöö

Jon Hendrik Aruväli

Lühikokkuvõte.

Bakalaureusetöös antakse ülevaade *abc*-hüpoteesist ning sellega seotud järeldustest, mis sisaldavad mitmeid teisi tuntuid tulemusi ja lahtiseid küsimusi. Lisaks *abc*-hüpoteesi sõnastamisele, tuuakse välja *abc*-hüpoteesi kirjeldav mõttekäik, tähtsus ja ajalugu, milles sisaldub ka väidetava tõestuse kujunemislugu. Lihtsamad järeldused tõestatakse. Käsitletakse ka *abc*-hüpoteesi kongruentsvarianti ja näidatakse, et sellest järeldub *abc*-hüpotees.

CERCS teaduseriala: P120 Arvuteooria, väljateooria, algebraline geomeetria, algebra, rühmateooria.

Märksõnad: arvuteooria, diofantilised võrrandid, Fermat' teoreem, algebraline geomeetria.

ABC CONJECTURE AND ITS RESULTS

Bachelor's thesis

Jon Hendrik Aruväli

Abstract.

The bachelor's thesis gives an overview of the *abc* conjecture and its results, many of which include various well-known results. In addition to defining the *abc* conjecture, we describe its importance, a way to understand it and its history, which contains the story of its alleged proof. We prove some results related to the *abc* conjecture. We also describe the congruence *abc* conjecture and prove how the *abc* conjecture follows from it.

CERCS research specialisation: P120 Number theory, field theory, algebraic geometry, algebra, group theory.

Key Words: number theory, diophantine equations, Fermat' theorem, algebraic geometry.

Sisukord

Sissejuhatus

abc-hüpotees on kuulus lahtine küsimus, mida on proovitud üle kolmekümne aasta tõestada, aga millel puudub tänapäevani arvuteoorikute poolt üldiselt aksepteeritav tõestus. *abc*-hüpotees uurib täisarvude aditiivsete ja multiplikatiivsete omaduste suhet, täpsemalt, et võrduse $a + b = c$ korral pole üldiselt arvu abc erinevate algtegurite korrutis palju väiksem kui arv c. Kui aksepteeritav tõestus eksisteeriks, järelduksid *abc*-hüpoteesist paljud teised arvuteooria või arvuteooriaga seotud hüpoteesid ning mitmeid tuntuid teoreeme saaks tõestada märgatavalt lihtsamini. Ameerika matemaatik Dorian M. Goldfeld on öelnud *abc*-hüpoteesi kohta lause: „See on kõige tähtsam lahendamata probleem diofantilises analüüsis" (Goldfeld, 1996).

Antud bakalaureusetöö eesmärk on anda ülevaade *abc*-hüpoteesist ja sellega seostuvatest järeldustest. Töö on referatiivne ja toetub mitmetele allikatele, selle matemaatiline osa põhineb suuresti ameerika matemaatiku Melvyn B. Nathansoni raamatul „Elementary Methods in Number Theory" (Nathanson, 2000). Osa sealseid tõestusi sisaldavad lugejale endale mõtlemiseks jäetud lünki, mis bakalaureusetöös on täidetud. Bakalaureusetöö on jaotatud kuueks peatükiks.

Esimeses peatükis sõnastatakse põhimõisted, mis on seotud *abc*-hüpoteesiga või on vajalikud eelmainitud lünkade lahendamiseks. Lisaks tutvustatakse radikaali mõistet ning illustreeritakse seda paari näitega.

Teine peatükk sisaldab mõttekäiku, mille abil kergemini mõista *abc*-hüpoteesi ideed ning formuleeringut. Mõttekäik ja hüpoteesi nõrga versiooni formuleering põhineb raamatu „Trolling Euclid: An Irreverent Guide to Nine of Mathematics' Most Important Problems" (Wright, 2016) *abc*-hüpoteesi käsitlusel.

Kolmandas peatükis antakse lühiülevaade *abc*-hüpoteesi ajaloost, eriti jaapani matemaatiku Shinichi Mochizuki välja pakutud tõestusega seotust. Kolmas peatükk põhineb mitmetel erinevatel allikatel, millele viidatakse vastavate lausete või lõi-

kude juures.

Neljandas peatükis tuuakse välja olulisemad *abc*-hüpoteesist järelduvad tulemused ja hüpoteesid. Osa neist on juba teiste meetoditega tõestatud, teised on tänaseni lahtised. Lihtsamalt formuleeritavad järeldused sõnastatakse täielikult, kaasates vajadusel uusi mõisteid. Peatükk põhineb mitmetel erinevatel allikatel, millele viidatakse vastavate lausete või lõikude juures.

Viiendas peatükis tõestatakse, et *abc*-hüpoteesist järelduvad järgmised neli tulemust: Fermat' suur teoreem, Catalani hüpotees, mitte-Wieferichi algarvude lõpmatus ja järjestikuste astmeliste arvude lõplikus. Tõestused järgivad raamatut „Elementary Methods in Number Theory" (Nathanson, 2000).

Kuuendas peatükis sõnastatakse ja tõestatakse *abc*-hüpoteesi kongruentsvariant. Kuues peatükk põhineb samuti raamatul „Elementary Methods in Number Theory" (Nathanson, 2000).

1 Põhimõisted

Enne *abc*-hüpoteesi sõnastamist tutvustatakse mõisteid ja tulemusi, mida bakalaureusetöös kasutatakse. Mõisted järgivad aine „Arvuteooria" loengukonspekti (Laan, V. ja Tart, L., 2020), kui pole märgitud teisiti. *Algarvuks* nimetatakse naturaalarvu $p > 1$, mille ainsad naturaalarvulised jagajad on arvud 1 ja p. Kõigi algarvude hulka tähistatakse edaspidi sümboliga $\mathbb{P}$ ning algarve üldiselt tähisega p.

Bakalaureusetöös on naturaalarvude hulk defineeritud kui $\mathbb{N} = \{1, 2, 3, \ldots\}$ ehk arv 0 ei kuulu siinses töös naturaalarvude hulka. Arvude x ja y suurimat ühistegurit tähistame kui $\text{SÜT}(x, y)$. Seejuures kaks arvu x ja y on ühistegurita, kui $\text{SÜT}(x, y) = 1$.

Teades algarvude mõistet ja tähistust, saab sõnastada aritmeetika põhiteoreemi.

Teoreem 1 (Aritmeetika põhiteoreem)**.** *Iga naturaalarvu $n > 1$ saab esitada algarvude korrutisena ehk leiduvad $k \in \mathbb{N}$ ja algarvud $p_1, \ldots, p_k$ nii, et*

$$n = p_1 \cdot \ldots \cdot p_k,$$

ja see esitus on ühene tegurite järjekorra täpsuseni.

Teoreemist 1 saadakse järgnev järeldus.

Järeldus 1. *Iga naturaalarvu $n > 1$ saab üheselt esitada kujul*

$$n = p_1^{k_1} p_2^{k_2} \ldots p_s^{k_s}, \tag{1}$$

kus $k_i \in \mathbb{N}$, p_i on algarv iga i = 1,2,. . . ,s korral ning $p_1 < p_2 < \ldots < p_s$.

Naturaalarvu n esitust kujul (1) nimetatakse selle arvu *kanooniliseks kujuks.*

Lemma 1. *Olgu a täisarv ja olgu naturaalarv $n = p_1^{k_1} \cdot \ldots \cdot p_s^{k_s} > 1$ antud kanoonilisel kujul. Siis $n \mid a$ parajasti siis, kui $p_i^{k_i} \mid a$ iga $i \in \{1, \ldots, s\}$ korral.*

Lemma 2 (Eukleidese lemma)**.** *Mistahes a, b, $c \in \mathbb{Z}$ korral, kui $a \mid bc$ ja* $\text{SÜT}(a, b) = 1$*, siis $a \mid c$.*

Järeldus 2. *Mistahes $b, c \in \mathbb{Z}$ ja algarvu p korral, kui $p \mid bc$, siis kas $p \mid b$ või $p \mid c$.*

Järgmist lemmat aine „Arvuteooria" loengukonspektis pole, seetõttu on see siin tõestatud.

Lemma 3. *Mistahes kaks järjestikust positiivset täisarvu on ühistegurita.*

Tõestus. Olgu täisarvud n ja $n+1$ kaks suvaliselt valitud järjestikust positiivset täisarvu. Olgu nende suurim ühistegur $\text{SÜT}(n, n+1) = d$. Jaguvuse definitsiooni järgi $d|n$ ja $d|n+1$. Jaguvusseose omaduste tõttu kehtib, et $d|n+1-n$ ehk $d|1$. Jaguvusseose omaduste tõttu on $d = 1$ ainuke positiivne täisarv, mille korral saab kehtida $d|1$. Seega arvude n ja $n+1$ suurim ühistegur on 1 ehk nad on ühistegurita. □

Definitsioon 1. *Euleri funktsioon $\varphi : \mathbb{N} \longrightarrow \mathbb{N}$ defineeritakse võrdusega*

$$\varphi(n) = |\{x \in \mathbb{N} \mid 1 \leq x \leq n,\ \text{SÜT}(x, n) = 1\}|.$$

Teoreem 2. *Kui $n > 1$ ja $n = p_1^{k_1} \cdot \ldots \cdot p_k^{k_s}$ on naturaalarvu n kanooniline kuju, siis*

$$\varphi(n) = p_1^{k_1-1} \cdot \ldots \cdot p_s^{k_s-1}(p_1 - 1) \cdot \ldots \cdot (p_s - 1).$$

Lemma 4. *Iga naturaalarvu $n > 2$ korral on $\varphi(n)$ paarisarv.*

Teoreem 3 (Euleri teoreem)**.** *Kui $a \in \mathbb{Z}$, $n \in \mathbb{N}$ ja* $\text{SÜT}(a, n) = 1$*, siis*

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

Teoreem 4 (Fermat' väike teoreem)**.** *Kui p on algarv ja a on täisarv, mis ei jagu arvuga p, siis*

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

Definitsioon 2. *Vähimat naturaalarvu m, mille korral $a^m \equiv 1 \pmod{n}$, nimetatakse täisarvu a järguks mooduli n järgi.*

See definitsioon on korrektne ehk järk leidub iga täisarvu a korral teoreemi 3 tõttu.

Lemma 5. *Olgu elemendi a järk m mooduli n järgi ning olgu $l \in \mathbb{N}$. Siis $a^l \equiv 1 \pmod{n}$ parajasti siis, kui $m \mid l$.*

Definitsioon 3. Astmeliseks *nimetatakse naturaalarvu v, mille korral kehtib*

$$\forall p \in \mathbb{P}\,[\,p \mid v \Rightarrow p^2 \mid v\,].$$

Naturaalarvu n *radikaaliks* nimetatakse arvu n erinevate algtegurite korrutist. Kergesti saab seda mõista kui kanoonilist kuju, kus algarvude astmed on võetud võrdseks arvuga 1. Radikaali täpne definitsioon on välja toodud järgnevalt:

Definitsioon 4. *Olgu naturaalarv n kanoonilisel kujul (1). Siis naturaalarvu $n > 1$ radikaal defineeritakse järgnevalt:*

$$\mathrm{rad}(n) = \prod_{i=1}^{s} p_i.$$

Vaatame paari näidet, et radikaali mõistest paremini aru saada. Kuigi tihti on arvu radikaal väiksem, siis järgmisest näitest on näha, et see pole alati nii.

Näide 1.

1. $\mathrm{rad}(900) = \mathrm{rad}(2^2 \cdot 3^2 \cdot 5^2) = 2 \cdot 3 \cdot 5 = 30.$
2. $\mathrm{rad}(42) = \mathrm{rad}(2 \cdot 3 \cdot 7) = 2 \cdot 3 \cdot 7 = 42.$

abc-hüpotees ongi suuresti küsimus, kui palju on arvu radikaal üldjuhul väiksem kui arv ise.

2 *abc*-hüpotees

Selles peatükis tutvustatakse ühte mõttekäiku, kuidas *abc*-hüpoteesini jõuda. Lisaks sõnastatakse *abc*-hüpoteesi teine, samaväärne kuju ja tõestatakse nende kahe kuju samaväärsus. Samuti näidatakse, et *abc*-hüpoteesi eeldused on tarvilikud.

Eelmises peatükis jõudsime küsimuseni, kui palju on üldjuhul arvu radikaal väiksem kui arv ise. Vaatleme võrrandit kujul

$$a + b = c, \tag{2}$$

kus a, b ja c on positiivsed paarikaupa ühistegurita täisarvud. Saame uue ja täiendatud küsimuse: kuidas võrrelda arve a, b ja c arvuga $\mathrm{rad}(abc)$.

Kui arvud a, b ja c poleks paarikaupa ühistegurita, siis selgub, et võrduse (2) tõttu saab kõik kolm arvu nende suurima ühisteguriga d läbi jagada ning vaadelda võrdust (2) uute saadud arvude $\frac{a}{d}$, $\frac{b}{d}$ ja $\frac{c}{d}$ korral. Seega saame üldisust kitsendamata eeldada, et arvud a, b ja c on paarikaupa ühistegurita. Võib tekkida küsimus, et miks just kolme arvu korraga võrrelda. Ühe arvu võrdlemise korral peaks väide katma väga erinevaid arvu ja tema radikaali vahekordi, näiteks 42 ja 2^{1000}. Kahte arvu võrdlemine oleks parem, aga siis ei oleks nende arvude vahel aditiivset seost. Kolme arvu korral on olemas nii aditiivne seos kui ka väiksem tõenäosus, et nende kõigi radikaalid suurel määral vähenevad, mis annab meile üldisema väite.

Järgmiseks võib tekkida küsimus, et miks kolme arvu asemel ei või kasutada veel rohkem arve. Seda saab teha, kuid juba kolme arvu korral tuleb välja hüpoteesi põhiolemus. Kuigi hüpoteesi on võimalik üldistada suurema arvu muutujate jaoks, on kolme arvu variant piisavalt sisukas, et seda oleks huvitav uurida. Tuleb välja, et isegi kolme arvu variandi korral saab *abc*-hüpoteesi abil tõestada või lahendada terve rea arvuteooria ja teistegi matemaatika valdkondade rohkem või vähem tuntud tulemusi ning lahtiseid küsimusi.

Järgmiste näidete abil uurime, kui palju erinevad korrutis abc ja $\mathrm{rad}(abc)$. See

oleneb kindlasti a, b ja c valikust.

Näide 2. *Valime täisarvud järgnevalt:* $a = 6$, $b = 11$, $c = 17$. *Kehtib*

$$6 + 11 = 17.$$

Vaatame täisarvu abc radikaali:

$$\mathrm{rad}(6 \cdot 11 \cdot 17) = 2 \cdot 3 \cdot 11 \cdot 17 = 6 \cdot 11 \cdot 17.$$

Nagu näha, siis sellise kolmiku korral radikaal arvude korrutist ei muuda ehk $\mathrm{rad}(abc) = abc$.

Näide 3. *Valime täisarvud järgnevalt:* $a = 27$, $b = 49$, $c = 76$. *Kehtib*

$$27 + 49 = 76.$$

Vaatame täisarvu abc radikaali:

$$\mathrm{rad}(27 \cdot 49 \cdot 76) = \mathrm{rad}(3^3 \cdot 7^2 \cdot (2^2 \cdot 19)) = 3 \cdot 7 \cdot 2 \cdot 19 = 798.$$

Kuna $27 \cdot 49 \cdot 76 = 100\ 548$, siis seekord on arvukolmiku radikaali ja arvukolmiku korrutise vahe palju suurem. Arve c ja $\mathrm{rad}(abc)$ võrreldes on jõutud järgmise väiteni.

Kui $a + b = c$ ning a, b ja c on positiivsed paarikaupa ühistegurita täisarvud, siis võrratus

$$c < \mathrm{rad}(abc) \tag{3}$$

on suurem osa ajast tõene.

Järgmisena tuuakse näide arvukolmikust, kus võrratus (3) ei kehti.

Näide 4. *Valime täisarvud järgnevalt:* $a = 9$, $b = 2048$, $c = 2057$. *Kehtib*

$$9 + 2048 = 2057.$$

Vaatame täisarvu abc radikaali:

$$\mathrm{rad}(9 \cdot 2048 \cdot 2057) = \mathrm{rad}(3^2 \cdot 2^{11} \cdot (11^2 \cdot 17)) = 3 \cdot 2 \cdot 11 \cdot 17 = 1122.$$

Kuna $2057 > 1122$, siis näeme, et võrratus (3) ei kehti. Matemaatikas pole eriti kasulikud tulemused, mis kehtivad vaid suurem osa ajast. Eriti siis, kui me ei suuda täpsustada, mida „suurem osa ajast" täpselt tähendab. Seega vaatleme, kuidas saaks seda lauset muuta nii, et see oleks alati tõene.

Lihtne viis seda saavutada oleks võrratuses (3) parem pool astmesse võtta. Kui valida liiga väike aste, siis võib endiselt leiduda arvukolmikuid, mille korral võrratus (3) ei kehti. Samas mida suurem aste valida, seda nõrgem on hüpotees. Seega tahame leida võimalikult väikest astet, mille korral võrratus (3) kehtib. Proovime alguses valida astmeks arvu 2, saades järgmise hüpoteesi.

Hüpotees 1 (*abc*-hüpoteesi nõrk versioon)**.** *Olgu $a, b, c \in \mathbb{N}$ paarikaupa ühistegurita ja kehtigu $a + b = c$. Siis kehtib võrratus*

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

Vaatame, mis juhtub eelmise näitega, kui sellele rakendada hüpoteesi 1. Eelnevas näites olid arvud $c = 2057$ ja $\mathrm{rad}(abc) = 1122$. Kuna $1122^2 = 1\ 258\ 884$, siis arvukolmiku (9, 2048, 2057) korral kehtib *abc*-hüpoteesi nõrk versioon, sest $2057 < 1\ 258\ 884$.

Eelneva näite põhjal on näha, et saaksime valida ka väiksema astme. Projekti ABC@Home, mida tutvustatakse lähemalt peatükis 3, abil on arvutuslike meetodite kaudu leitud arvukolmikuid, mille korral ei kehti võrratus (3). Projekti poolt leitud suurim astendaja q, mille korral $c = \mathrm{rad}(abc)^q$, on ligikaudu $1,6299$. Seega kui tahame, et võrratus $c < \mathrm{rad}(abc)^r$ kehtiks iga arvukolmiku korral, peab olema radikaali astendaja $r > 1,6299$. Järelikult arvutusandmed toetavad hüpoteesi 1.

Prantsuse matemaatik Joseph Oesterlé avaldas artiklis „Nouvelles approches du «théorème» de Fermat" (Oesterlé, 1988) hüpoteesi 1 mõnevõrra täpsema ja üldisema variandi, mida tänapäeval tuntakse *abc*-hüpoteesina. Bakalaureusetöös käsitleme *abc*-hüpoteesina just seda väidet, aga lihtsuse mõttes kujul, kus vaadeldavad arvukolmikud kuuluvad naturaalarvude hulka.

Hüpotees 2 (*abc*-hüpotees)**.** *Iga reaalarvu $\varepsilon > 0$ jaoks leidub $K_\varepsilon \in \mathbb{R}$ nii, et iga arvukolmiku (a, b, c), kus $a, b, c \in \mathbb{N}$ on paarikaupa ühistegurita ja $a + b = c$, korral kehtib*

$$c < K_\varepsilon \cdot \operatorname{rad}(abc)^{1+\varepsilon}.$$

Eelnevat hüpoteesi sisuliselt eitades saame järgmise, *abc*-hüpoteesiga samaväärse formuleeringu.

Hüpotees 3. *Iga reaalarvu $\varepsilon > 0$ jaoks leidub vaid lõplik arv arvukolmikuid (a, b, c), kus $a, b, c \in \mathbb{N}$ on paarikaupa ühistegurita ja $a + b = c$, nii et*

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

Lause 1. *Hüpotees 2 ja hüpotees 3 on samaväärsed.*

Tõestus. Olgu $\varepsilon \in \mathbb{R}$, $a, b, c \in \mathbb{N}$ paarikaupa ühistegurita ning kehtigu võrdus $a + b = c$.

Näitame esimesena, et hüpoteesist 2 järeldub hüpotees 3.

Kehtigu hüpotees 2. Fikseerime $\varepsilon > 0$. Siis leidub $K_\varepsilon \in \mathbb{R}$ nii, et iga arvukolmiku (a, b, c) korral kehtib

$$c < K_\varepsilon \cdot \operatorname{rad}(abc)^{1+\varepsilon}.$$

Näitame, et kehtib hüpoteesi 3 väide arvu ε jaoks.

Kui $K_\varepsilon \leq 1$, siis kehtib iga arvukolmiku (a, b, c) korral

$$c < K_\varepsilon \cdot \operatorname{rad}(abc)^{1+\varepsilon} \leq \operatorname{rad}(abc)^{1+\varepsilon}.$$

Seega $c > \mathrm{rad}(abc)^{1+\varepsilon}$ ei ole täidetud ühegi arvukolmiku (a, b, c) korral ehk kehtib hüpotees 3.

Vaatame nüüd juhtu, kus $K_\varepsilon > 1$. Defineerime $\varepsilon' = \frac{\varepsilon}{2}$. Siis leidub $K_{\varepsilon'} \in \mathbb{R}$ nii, et iga arvukolmiku (a, b, c) korral on

$$\frac{c}{K_{\varepsilon'}} < \mathrm{rad}(abc)^{1+\varepsilon'} \quad \text{ehk} \quad \frac{c^{\frac{1}{1+\varepsilon'}}}{K_{\varepsilon'}^{\frac{1}{1+\varepsilon'}}} < \mathrm{rad}(abc).$$

Paneme tähele, et kehtib

$$\begin{aligned}\frac{1}{1+\varepsilon'} &= \frac{1}{1+\frac{\varepsilon}{2}} = \frac{2}{2+\varepsilon} = \frac{2(1+\varepsilon)}{(2+\varepsilon)(1+\varepsilon)} \\ &= \frac{2+\varepsilon}{(2+\varepsilon)(1+\varepsilon)} + \frac{\varepsilon}{(2+\varepsilon)(1+\varepsilon)} \\ &= \frac{1}{1+\varepsilon} + \frac{\varepsilon}{(2+\varepsilon)(1+\varepsilon)}.\end{aligned}$$

Seega saame kirjutada

$$\frac{c^{\frac{1}{1+\varepsilon'}}}{K_{\varepsilon'}^{\frac{1}{1+\varepsilon'}}} = c^{\frac{1}{1+\varepsilon}} \frac{c^{\frac{\varepsilon}{(2+\varepsilon)(1+\varepsilon)}}}{K_{\varepsilon'}^{\frac{1}{1+\varepsilon'}}} = c^{\frac{1}{1+\varepsilon}} \frac{c^{\frac{\varepsilon}{2(1+\varepsilon)} \cdot \frac{2}{2+\varepsilon}}}{K_{\varepsilon'}^{\frac{1}{1+\varepsilon'}}} = c^{\frac{1}{1+\varepsilon}} \left(\frac{c^{\frac{\varepsilon}{2(1+\varepsilon)}}}{K_{\varepsilon'}} \right)^{\frac{1}{1+\varepsilon'}}.$$

Kui arv c rahuldab järgmist tingimust:

$$\frac{c^{\frac{\varepsilon}{2(1+\varepsilon)}}}{K_{\varepsilon'}} \geq 1 \quad \text{ehk} \quad c \geq K_{\varepsilon'}^{\frac{2(1+\varepsilon)}{\varepsilon}} = \text{const},$$

siis saame

$$c^{\frac{1}{1+\varepsilon}} \left(\frac{c^{\frac{\varepsilon}{2(1+\varepsilon)}}}{K_{\varepsilon'}} \right)^{\frac{1}{1+\varepsilon'}} \geq c^{\frac{1}{1+\varepsilon}}.$$

Sellega oleme näidanud, et kehtib

$$\mathrm{rad}(abc) > \frac{c^{\frac{1}{1+\varepsilon'}}}{K_{\varepsilon'}^{\frac{1}{1+\varepsilon'}}} = c^{\frac{1}{1+\varepsilon}} \left(\frac{c^{\frac{\varepsilon}{2(1+\varepsilon)}}}{K_{\varepsilon'}} \right)^{\frac{1}{1+\varepsilon'}} \geq c^{\frac{1}{1+\varepsilon}}.$$

Järelikult

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

Seega võrratust $c > \mathrm{rad}(abc)^{1+\varepsilon}$ saab rahuldada vaid lõplik hulk naturaalarve c, sest tingimust

$$c < K_{\varepsilon'}^{\frac{2(1+\varepsilon)}{\varepsilon}} = \text{const}$$

saab täita lõplik arv naturaalarve c. Kuna $a + b = c$, siis $a, b < c$, mille tõttu on ka arve a ja b lõplik arv. Järelikult on lõplik arv ka arvukolmikuid (a, b, c), mis rahuldavad võrratust $c > \mathrm{rad}(abc)^{1+\varepsilon}$, st kehtib hüpotees 3.

Näitame järgmiseks, et hüpoteesist 3 järeldub hüpotees 2.

Kehtigu hüpotees 3, st iga $\varepsilon > 0$ korral leidub ainult lõplik arv arvukolmikuid (a, b, c) nii, et kehtib

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

Fikseerime $\varepsilon > 0$. Juhul kui ei leidu arvukolmikuid (a, b, c), et kehtiks võrratus $c > \mathrm{rad}(abc)^{1+\varepsilon}$, siis iga arvukolmiku (a, b, c) korral

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

kus $K_\varepsilon > 1$. Järelikult kehtib sel juhul hüpotees 2. Vaatleme nüüd juhte, kus võrratust $c > \mathrm{rad}(abc)^{1+\varepsilon}$ rahuldavaid arvukolmikud on vähemalt üks ning tähistame neid kui $(a_{i_\varepsilon}, b_{i_\varepsilon}, c_{i_\varepsilon})$, kus $i \in \{1, \ldots, n_\varepsilon\}$, $n_\varepsilon \in \mathbb{N}$ ja nende arvukolmikute hulka tähisega A. Näitame, et ka sellisel juhul kehtib hüpotees 2.

Võtame

$$K_\varepsilon = \max_{i \in \{1,\ldots,n_\varepsilon\}} \frac{c_{i_\varepsilon}}{\mathrm{rad}(a_{i_\varepsilon} b_{i_\varepsilon} c_{i_\varepsilon})^{1+\varepsilon}} + 1 \in \mathbb{R}.$$

Seega iga i $\in \{1, \ldots, n_\varepsilon\}$ korral kehtib

$$\frac{c_{i_\varepsilon}}{\mathrm{rad}(a_{i_\varepsilon} b_{i_\varepsilon} c_{i_\varepsilon})^{1+\varepsilon}} < K_\varepsilon$$

ehk

$$c_{i_\varepsilon} < K_\varepsilon \cdot \mathrm{rad}(a_{i_\varepsilon} b_{i_\varepsilon} c_{i_\varepsilon})^{1+\varepsilon}.$$

Kuna arvukolmikute $(a, b, c) \notin A$ korral $c \leq \mathrm{rad}(abc)^{1+\varepsilon} < K_\varepsilon \cdot \mathrm{rad}(abc)^{1+\varepsilon}$, kus $K_\varepsilon > 1$, siis oleme näidanud, et leidub K_ε nii, et iga arvukolmiku (a, b, c) korral kehtib $c < K_\varepsilon \cdot \mathrm{rad}(abc)^{1+\varepsilon}$. Seega oleme näidanud, et kehtib hüpotees 2. Sellega on näidatud hüpoteeside samaväärsus. □

Järgmisena veendume, et eeldus ühistegurita olekust on tarvilik, samuti see, et astendaja on rangelt suurem ühest (ehk $\varepsilon > 0$).

Lause 2. *abc-hüpotees ei kehti, kui jätta välja tingimus SÜT(a, b) = SÜT(a, c) = SÜT(b, c) = 1.*

Tõestus. Vaatame arve kujul $a = 3^k$, $b = 2 \cdot 3^k$ ja $c = 3^{k+1}$, kus $k \in \mathbb{N}$. Paneme tähele, et nende arvude korral $\mathrm{SÜT}(a, b) = \mathrm{SÜT}(a, c) = \mathrm{SÜT}(b, c) = 3^k \neq 1$ ning

$$a + b = 3^k + 2 \cdot 3^k = 3 \cdot 3^k = 3^{k+1} = c \quad \forall k \in \mathbb{N}.$$

Fikseerime $\varepsilon > 0$. Eeldame, et *abc*-hüpoteesis ei ole nõutud tingimust $\mathrm{SÜT}(a, b) = \mathrm{SÜT}(a, c) = \mathrm{SÜT}(b, c) = 1$. Seega peaks leiduma $K_\varepsilon \in \mathbb{R}$ nii, et kehtib

$$3^{k+1} < K_\varepsilon \cdot \mathrm{rad}(3^k \cdot 2 \cdot 3^k \cdot 3^{k+1})^{1+\varepsilon} \quad \forall k \in \mathbb{N}.$$

Radikaali definitsiooni 4 põhjal võime kirjutada

$$\begin{aligned} 3^{k+1} &< K_\varepsilon \cdot \mathrm{rad}(2 \cdot 3)^{1+\varepsilon} = K_\varepsilon \cdot (2 \cdot 3)^{1+\varepsilon} \\ &= K_\varepsilon \cdot 2^{1+\varepsilon} \cdot 3^{1+\varepsilon} \quad \forall k \in \mathbb{N}. \end{aligned}$$

Edasi saame

$$\frac{3^{k+1-1-\varepsilon}}{2^{1+\varepsilon}} < K_\varepsilon \quad \text{ehk} \quad \frac{3^{k-\varepsilon}}{2^{1+\varepsilon}} < K_\varepsilon \quad \text{ehk}$$

$$3^k \frac{1}{3^\varepsilon \cdot 2^{1+\varepsilon}} < K_\varepsilon \quad \text{ehk} \quad 3^k < K_\varepsilon \cdot 3^\varepsilon \cdot 2^{1+\varepsilon} \quad \forall k \in \mathbb{N}.$$

Paneme tähele, et viimases võrratuses on paremal poolel konstant ehk võrratus $3^k <$ const peaks kehtima iga $k \in \mathbb{N}$ korral. See pole aga võimalik. Sellega oleme näidanud, et *abc*-hüpotees ei kehti, kui pole täidetud tingimus $\text{SÜT}(a, b) = \text{SÜT}(a, c) = \text{SÜT}(b, c) = 1$. □

Lause 3. *abc-hüpotees ei kehti, kui asendada astendaja* $1 + \varepsilon$ *astendajaga* 1.

Tõestus. Oletame vastuväiteliselt, et *abc*-hüpotees kehtib ka $\varepsilon = 0$ korral ehk leidub $K_0 \in \mathbb{R}$ nii, et

$$c < K_0 \cdot \text{rad}(abc)$$

kehtib kõigi selliste arvude a, b ja $c \in \mathbb{N}$ korral, mis on paarikaupa ühistegurita ning rahuldavad võrdust $a + b = c$.

Tõestame esmalt, et iga positiivse täisarvu n korral leidub positiivne täisarv u_n nii, et

$$2^n u_n + 1 = 3^{2^{n-1}}.$$

Olgu $a = 3$ ja $m = 2^n$. Paneme tähele, et need kaks arvu on ühistegurita. Siis Euleri teoreemi 3 põhjal kehtib $a^{\varphi(m)} \equiv 1 \pmod{m}$. Teoreemi 2 põhjal avaldub $\varphi(m) = 2^{n-1}$. Seega saame, et

$$3^{2^{n-1}} \equiv 1 \pmod{2^n}$$

ehk $2^n \mid 3^{2^{n-1}} - 1$. Seega leidub positiivne täisarv u_n nii, et $3^{2^{n-1}} - 1 = 2^n \cdot u_n$. Sellega oleme näidanud, et iga positiivse täisarvu n korral leidub positiivne täisarv u_n nii, et $2^n u_n + 1 = 3^{2^{n-1}}$.

Nüüd olgu $a_n = 2^n u_n$, $b_n = 1$ ja $c_n = 3^{2^{n-1}}$. Eelnevalt näitasime, et $a_n + b_n = c_n$. Paneme tähele, et arvud a_n, b_n ja c_n on paarikaupa ühistegurita, sest a_n ja c_n on

kaks järjestikust täisarvu. Saame arvu $\mathrm{rad}(a_n b_n c_n)$ hinnata ülevalt järgmiselt:

$$\begin{aligned}\mathrm{rad}(a_n b_n c_n) &= \mathrm{rad}(2^n u_n \cdot 1 \cdot 3^{2^{n-1}}) = \mathrm{rad}(2 \cdot 3 \cdot u_n) \\ &= \mathrm{rad}(6u_n) \leq 6u_n = 6\frac{3^{2^{n-1}} - 1}{2^n} < 6\frac{3^{2^{n-1}}}{2^n}.\end{aligned}$$

Saame eelnevat tulemust kasutades kirjutada

$$\mathrm{rad}(a_n b_n c_n) \cdot K_0 < 6 \cdot \frac{3^{2^{n-1}}}{2^n} \cdot K_0 = \frac{6K_0}{2^n} \cdot c_n.$$

Paneme tähele, et $6K_0$ on konstant, mistõttu leidub $N = \frac{\log(6K_0)}{\log 2}$ nii, et $n > N$ korral

$$\frac{6K_0}{2^n} < 1.$$

Korrutades eelmise võrratuse mõlemad pooled läbi arvuga 2^n ja seejärel võttes mõlemalt poolt logaritmi, saame

$$\log(6K_0) < n \log 2 \quad \text{ehk} \quad n > \frac{\log(6K_0)}{\log 2}.$$

Seega kui $n > N = \frac{\log(6K_0)}{\log 2}$, siis kehtib

$$\frac{6K_0}{2^n} \cdot c_n < c_n.$$

Ehk piisavalt suure n korral

$$\mathrm{rad}(a_n b_n c_n) \cdot K_0 < c_n,$$

mis on vastuolus *abc*-hüpoteesiga, sest *abc*-hüpoteesi korral peab antud arvukolmiku (a_n, b_n, c_n) jaoks kehtima võrratus $c_n < K_0 \cdot \mathrm{rad}(a_n b_n c_n)$. Sellega oleme näidanud, et *abc*-hüpotees ei saa kehtida, kui asendada astendaja $1 + \varepsilon$ astendajaga 1. □

3 Ajalugu

Paljud matemaatikas tuntud ja olulised hüpoteesid on sajandi või mitme sajandi vanused. Vastupidiselt on *abc*-hüpotees väga noor. See formuleeriti 1985. aastal inglise matemaatiku David Masseri (Masser, 1985) ja prantsuse matemaatiku Joseph Oesterlé (Oesterlé, 1988) poolt, kes mõlemad avaldasid selle eri aegadel. Masser ja Oesterlé proovisid mõista Szpiro hüpoteesi, mis sõnastatakse alapeatükis 4.2.2. Selle käigus nad formuleerisid *abc*-hüpoteesi, mis on samaväärne modifitseeritud Szpiro hüpoteesiga.

abc-hüpotees on saanud väga oluliseks, sest sellest järelduvad mitmed erinevad arvuteooria, algebralise geomeetria ning muude matemaatikaharude hüpoteesid ja teoreemid. Prantsuse matemaatik Lucien Szpiro pakkus 2007. aasta mais Columbia Ülikoolis toimunud konverentsil välja tõestuse mis lähemal uurimisel osutus vigaseks (Szpiro, 2007). Kõige kuulsam on Shinichi Mochizuki poolt välja pakutud tõestus, millest kirjutatakse täpsemalt alapeatükis 3.1.

On näidatud, et *abc*-hüpoteesist järeldub, et arvu c saab ülevalt hinnata kasutades peaaegu lineaarset funktsiooni, mis sõltub arvu abc radikaalist. Teadaolevad tõkked on eksponentsiaalsed ning bakalaureusetöö kirjutamise ajaks on neid teada vähemalt kolm. Need tõkked kehtivad iga täisarvukolmiku (a, b, c) korral, kus $c > 2$.

Esimene tõke avaldub kujul

$$c < e^{(K_1 \cdot \mathrm{rad}(abc)^{15})}.$$

Võrratus tõestati aastal 1986 (Stewart, C. L. ja Tijdeman, R., 1986) ja selle korral ei sõltu konstant K_1 arvukolmiku valikust.

Teine tõke avaldub kujul

$$c < e^{\left(K_2 \cdot \mathrm{rad}(abc)^{\frac{2}{3}+\varepsilon}\right)}$$

ja see tõestati aastal 1991 (Stewart, C. L. ja Yu, K., 1991). Selle tõkke korral sõltub konstant K_2 muutujast ε, kuid ei sõltu arvukolmiku valikust.

Kolmas tõke avaldub kujul

$$c < e^{\left(K_3 \cdot \mathrm{rad}(abc)^{\frac{1}{3}} (\log(\mathrm{rad}(abc)))^3\right)}.$$

See tõke tõestati aastal 2001 (Stewart, C. L. ja Yu, K., 2001) ning ka selle korral ei sõltu konstant K_3 arvukolmiku valikust.

Eelmises peatükis mainiti, et *abc*-hüpoteesi saab uurida kolme täisarvu asemel ka n arvu korral. Aastal 1994 püstitatigi n-hüpotees (Browkin, J. ja Brzeziński, J., 1994). Inglise matemaatik Alan Baker sõnastas *abc*-hüpoteesi tugevama formuleeringu aastal 1998 (Baker, 1998). Ta väitis samas teoses, et inglise matemaatiku Andrew Granville'i hüpoteesidest saab järeldada, et *abc*-hüpoteesis saab leida arvule c ülemisi tõkkeid. Granville ise märkas Bakeri *abc*-hüpoteesi sõnastuse omadust, mille abil Baker sõnastas teise *abc*-hüpoteesi tugevama formuleeringu (Baker, 2004).

Aastal 2006 algatas Hollandis asuva Leideni Ülikooli matemaatika teaduskond projekti nimega „ABC@Home", mille eesmärgiks oli avastada täisarvukolmikuid (a, b, c), mille korral kehtib võrratus $\mathrm{rad}(abc) < c$. Selle käigus loodeti paremini mõista *abc*-hüpoteesi ning arvuteooria valdkonda üldiselt. Aastaks 2015 oli projekti abil leitud 23,8 miljonit sellist täisarvukolmikut ja projekt lõpetati (de Smit, 2019).

3.1 Shinichi Mochizuki tõestus

Aastal 2012 avaldas jaapani matemaatik Shinichi Mochizuki neli artiklit, mille kogupikkus oli üle 500 lehekülje (Ball, 2012). Artiklid kirjeldavad Mochizuki enda loodud ja sõnastatud teooriat, mis kannab inglise keeles nime „Inter-universal Teichmüller theory" (edaspidi IUT). Esimese artikli lühikokkuvõttes selgitab Moc-

hizuki, et tegemist on „aritmeetilise versiooniga Teichmülleri teooriast elliptilise joonega arvukorpuste jaoks" (Mochizuki, 2021). Lisaks on artiklites väidetud, et teooriat rakendades on võimalik tõestada modifitseeritud Szpiro hüpotees ehk järelikult ka *abc*-hüpotees.

Ameerika matemaatik Dorian Goldfeld väitis: „Kui Mochizuki tõestus on korrektne, siis see on üks hämmastavamaid 21. sajandi matemaatika valdkonna saavutusi" (Ball, 2012). Kuigi paljud matemaatikud lootsid, et IUT on korrektne ning *abc*-hüpotees on lõpuks tõestatud, siis tegelikult tekitasid Mochizuki teoorias mõisted ning nende kasutusviis nende seas segadust (Chen, 2013). Artiklid kasutasid autori isikupärast terminoloogiat ja seetõttu oli isegi spetsialistidel keeruline IUT-d mõista. Teooria mõistmine on aga *abc*-hüpoteesi tõestuse korrektsuse hindamiseks vajalik ja seetõttu jäi küsimus, kas *abc*-hüpotees sai ikka tõestatud, lahtiseks.

2015. aastal peeti Oxfordi Ülikoolis nädala pikkune konverents, kuhu kogunes kokku palju matemaatikuid üle maailma, et paremini mõista IUT-d. Konverentsi üks tähtsamaid osasi oli kui ameerika matemaatik Kiran Kedlaya seletas lahti, mis meetodite abil Mochizuki *abc*-hüpoteesi kavatses tõestada. Samas kui Mochizuki kolleegid, jaapani matemaatikud Yuichiro Hoshi ja Go Yamashita, konverentsi viimastel päevadel IUT-ga seotud nelja artiklit lahti seletasid, valitses kuulajate seas segadus. Kuigi konverentsi tulemusena veel IUT-d ei mõistetud, siis vähemalt hakati aru saama, mis meetodite abil Mochizuki *abc*-hüpoteesi tõestada üritab. (Hartnett, 2015)

Aastal 2017 avaldas jaapani ajaleht The Asahi Shimbun, et tõestus võidakse avaldada jaapani ajakirjas Publications of the Research Institute for Mathematical Sciences (edaspidi PRIMS). PRIMS on lugupeetud ajakiri, kuid kuna Mochizuki ise on ajakirja peatoimetaja, siis teadlaste nagu brasiilia matemaatiku Felipe Volochi ja ameerika füüsiku Peter Woiti sõnul ei kinnita artiklite avaldamine ajakirjas PRIMS tõestuse korrektsust, vaid suurendab lõhet IUT toetajate ja vastaste vahel. (Revell, 2017)

2018. aasta märtsis olid saksa matemaatikud Peter Scholze ja Jakob Stix nädal aega Mochizukil ning tema kolleegil Yuichiro Hoshil külas Kyoto Ülikoolis. Kuigi visiidi abil erimeelsusi lahendada ei suudetud, siis Scholze sõnul aitas see saksa matemaatikute vastuväiteid täpsemini väljendada. Nad jõudsid järelduseni, et Mochizuki *abc*-hüpoteesi tõestus on vigane ja seda ei saa parandada väikeste muudatuste abil (Scholze, P. ja Stix, J., 2018). Samas Mochizuki väitis, et Scholzel ja Stixil on IUT mõistmisega teatud fundamentaalsed arusaamatused (Mochizuki, 2019) ning nende poolt leitud lüngad tulenevad saksa matemaatikute liigsest IUT lihtsustamisest (Mochizuki, 2018b; Mochizuki, 2018a). (Klarreich, 2018)

2020. aasta aprillis kinnitasid pressikonverentsil Kyotos kaks Kyoto Ülikooli matemaatikut Masaki Kashiwara ja Akio Tamagawa, et Mochizuki neli artiklit avaldatakse ajakirjas PRIMS. Peter Scholze lausus uudise peale, et tema arvamus tõestuse korrektsuse osas pole vahepeal muutunud. Tamagawa kinnitas, et artiklites olevaid lahendusi pole Scholze ja Jakob Stixi arvustusest hoolimata muudetud, kuid väljaanne sisaldab kommentaare kriitika kohta. Euroopas avaldab ajakirja PRIMS Euroopa Matemaatika Selts (edaspidi EMS). EMS-i president, saksa matemaatik Volker Mehrmann, väitis, et kui ajakirja toimetajad ei kontrollinud üle Mochizuki artiklite sisu vastavalt Scholze ja Stixi arvustusele, siis see alandab nii ajakirja PRIMS kui ka Mochizuki enda mainet. Kashiwara väitis, et Mochizuki polnud publikatsiooni arvustusega seotud ning ühtegi reeglit artiklite avaldamisega ei rikutud. Mehrmann kinnitas, et sellisel juhul EMS-i juhiseid ei rikuta. (Castelvecchi, 2020)

Vene matemaatik Vladimir Vojevodski ütles 2012. aasta intervjuus, et matemaatika valdkond on „kriisi piiril". Ta selgitas, et puhta matemaatika keerukuse tõttu on osa avaldatud artiklite korrektsust raske täielikult kontrollida, mistõttu tekib märkamatuks jäänud vigu. Kuna matemaatikas kasutatakse tihti eelnevalt avaldatud tulemusi, siis need vead võivad kiiresti kuhjuda. (Bordg, 2021)

Sama probleem tuli esile 2021. aasta märtsis, kui Mochizuki avaldas oma töö seoses IUT-ga ja *abc*-hüpoteesi tõestuse nelja artiklina ajakirjas PRIMS. Kokku olid ar-

tiklid üle 700 lehekülge pikad. Peter Scholze kirjutas referentsajakirjale zbMATH arvustuse, milles ta rõhutas, et tema eelnevalt välja toodud murekohtadele pole artiklites lahendust leitud (Scholze, 2021). Selle tõttu kritiseeriti ajakirja PRIMS artiklite sisu korrektsuse hindamise protsessi. Jaapani matemaatikuid see ei heidutanud ja nad käsitlevad *abc*-hüpoteesi kui teoreemi. Bakalaureusetöö kirjutamise ajaks ei aksepteeri Mochizuki *abc*-hüpoteesi tõestust suurem osa matemaatikuid väljaspoolt Kyoto Ülikooli instituuti Research Institute for Mathematical Science. (Bordg, 2021)

4 *abc*-hüpoteesi järeldusi

Selles peatükis tutvustame rida *abc*-hüpoteesi järeldusi, alustades kuulsamatest ja lihtsamini sõnastatavatest. Seejärel kirjeldame põgusalt keerukamaid, peamiselt algebralise geomeetria valda kuuluvaid tulemusi ilma detailidesse laskumata. See järelduste loetelu ei ole ammendav.

4.1 Arvuteoreetilisi järeldusi

4.1.1 Fermat' suur teoreem

Fermat' suur teoreem sõnastati prantsuse matemaatiku Pierre de Fermat poolt 1637. aastal. Teoreem on kuulus, sest seda ei suudetud tõestada rohkem kui kolme sajandi jooksul. Korrektne tõestus ilmus alles inglise matemaatiku Andrew Wiles poolt ajakirja „Annals of Mathematics" 1995. aasta mainumbris. (Wiles, 1995)

Teoreem 5 (Fermat' suur teoreem)**.** *Olgu $n \geq 3$ naturaalarv ja $a, b, c \in \mathbb{N}$. Siis ei leidu võrrandil*

$$a^n + b^n = c^n \tag{4}$$

ühtegi lahendit.

Wilesi tõestus on kokku üle 100 lehekülge pikk. Algsest tõestusest leiti viga ja pärast aastast koostööd inglise matemaatikuga Richard Taylor avaldasid nad koos tõestuse paranduse (Taylor, R. ja Wiles, A., 1995). Fermat' suur teoreem tõestatakse ära järgmises peatükis eeldusega, et hüpotees 1 kehtib. Lisaks näidatakse, et *abc*-hüpoteesist endast järeldub, et Fermat' suur teoreem võib mitte kehtida vaid lõpliku arvu astendajate n korral.

4.1.2 Catalani hüpotees

Catalani hüpotees väidab, et naturaalarvud 8 ja 9 on ainukesed järjestikused naturaalarvud, mille kanooniline kuju on p^k, kus p on algarv ja $k > 1$. Hüpotees tõestati ära 2002. aastal rumeenia matemaatiku Preda Mihăilescu poolt (Mihăilescu, 2004) ja kannab ka nime Mihăilescu teoreem. Hüpoteesi täpne sõnastus on järgmine:

Teoreem 6 (Catalani hüpotees)**.** *Olgu $x, y \in \mathbb{N}$ ja $m, n \in \mathbb{N} \setminus \{1\}$. Siis võrrandil*

$$x^m - y^n = 1 \tag{5}$$

leidub ainult üks lahend ja see on $x = 3, y = 2, m = 2, n = 3$.

Järgmises peatükis tõestatakse, et *abc*-hüpoteesi kehtides saab võrrandil (5) olla vaid lõplik arv lahendeid.

4.1.3 Fermat-Catalani hüpotees

Fermat-Catalani hüpotees on Fermat' suure teoreemi ja Catalani hüpoteesi üldistus.

Hüpotees 4 (Fermat-Catalani hüpotees)**.** *Olgu $a, b, c \in \mathbb{N}$ paarikaupa ühistegurita ning $m, n, k \in \mathbb{N}$ sellised, et kehtib võrratus*

$$\frac{1}{m} + \frac{1}{n} + \frac{1}{k} < 1.$$

Siis on võrrandil

$$a^m + b^n = c^k$$

lõplik arv lahendeid selliseid lahendeid (a, b, c, m, n, k), kus arvud a^m, b^n ja c^k on kõik erinevad.

4.1.4 Mitte-Wieferichi algarvude hulga lõpmatus

Esimesena kirjeldas Wieferichi algarve saksa matemaatik Arthur Wieferich (Wieferich, 1909), uurides Fermat' suurt teoreemi.

Definitsioon 5. *Wieferichi algarvuks nimetatakse algarvu p, kui kehtib*

$$p^2 \mid 2^{p-1} - 1.$$

Bakalaureusetöö kirjutamise ajaks on leitud ainult kaks Wieferichi algarvu: 1093 ja 3511 (Sloane, 2021).

Nathansoni raamatus on Wieferichi algarvude mõiste vastupidine kui laiemalt levinud definitsioonis. Bakalaureusetöös nimetame neid mitte-Wieferichi algarvudeks.

Definitsioon 6. *Mitte-Wieferichi algarvuks nimetatakse paaritut algarvu p, kui kehtib*

$$2^{p-1} \not\equiv 1 \pmod{p^2}.$$

Mitte-Wieferichi algarvude hulga lõpmatus tõestatakse ära järgmises peatükis eeldusega, et *abc*-hüpotees kehtib. Esimesena näitas seda ameerika matemaatik Joseph Silverman (Silverman, 1988).

4.1.5 Erdősi hüpotees järjestikuste astmeliste arvude kohta

Ungari matemaatik Paul Erdős (Erdős, P. ja Szekeres, G., 1934) ning kanada matemaatikud Richard Mollin ja Gary Walsh (Mollin, R. A. ja Walsh, P. G., 1986) on püstitanud järgmise hüpoteesi.

Hüpotees 5 (Erdősi hüpotees järjestikuste astmeliste arvude kohta)**.** *Ei leidu kolme järjestikust astmelist arvu.*

Järgmises peatükis tõestatakse, et *abc*-hüpoteesi järeldusena leidub vaid lõplik arv täisarvukolmikuid, mis koosnevad kolmest järjestikusest astmelisest arvust.

4.1.6 Erdős-Woodsi hüpotees

Inglise matemaatik Alan Woods uuris seda Paul Erdősi poolt püstitatud hüpoteesi oma doktoritöös. Hüpoteesiga on seotud Erdős-Woodsi arvud (Lygeros, 2021).

Hüpotees 6. *Leidub naturaalarv $k > 2$ nii, et kui arvud x ja y on positiivsed täisarvud, mis rahuldavad iga $i = 1, \ldots, k$ korral võrrandit*

$$\mathrm{rad}(x + i) = \mathrm{rad}(y + i),$$

siis kehtib võrdus $x = y$.

Prantsuse matemaatik Michel Langevin tõestas, et *abc*-hüpoteesist järeldub, et $k = 3$ korral leidub hüpoteesile ülimalt lõplik arv kontranäiteid (Langevin, 1992), (Langevin, 1993).

4.1.7 Rothi teoreem

Alljärgnev teoreem avaldati artiklis „Rational approximations to algebraic numbers" (Roth, 1955). See väidab, et algebraliste arvudel pole „head" ratsionaalarvulist lähendust. Tuletame meelde, et algebraline arv on nullist erineva ratsionaalarvuliste kordajatega polünoomi juur.

Teoreem 7 (Rothi teoreem)**.** *Olgu α algebraline irratsionaalarv. Siis iga reaalarvulise $\varepsilon > 0$ korral leidub võrratusel*

$$\left|\alpha - \frac{p}{q}\right| < \frac{1}{q^{2+\varepsilon}}$$

ülimalt lõplik arv ühistegurita lahendipaare $(p, q) \in \mathbb{Z}^2$.

4.1.8 Halli hüpotees

Halli hüpotees sõnastati ameerika matemaatiku Marshall Hall, Jr. poolt (Hall Jr., 1971). See väljendab täisruutude ja täiskuupide vahet. Hüpotees väidab, et kui täisruut y^2 ja täiskuup x^3 pole võrdsed, siis nende vahe on märgatavalt suur.

Hüpotees 7. *Kui x ja y on sellised täisarvud, et $y^2 \neq x^3$, siis leidub positiivne konstant C nii, et*

$$|y^2 - x^3| > C\sqrt{|x|}$$

abc-hüpoteesist järeldub järgnev „nõrk" Halli hüpotees (Schmidt, 2006).

Hüpotees 8. *Iga reaalarvulise $\varepsilon > 0$ korral leidub konstant $C_\varepsilon > 0$ nii, et iga positiivse täisarvu x ja y, mille korral $x^3 - y^2 \neq 0$, kehtib võrratus*

$$|y^2 - x^3| > C_\varepsilon \cdot \max(x^3, y^2)^{\frac{1}{2}-\varepsilon}.$$

4.1.9 Beali hüpotees

Beali hüpotees sõnastati 1993. aastal ameerika pankuri Andrew Beali poolt (American Mathematical Society, i.a).

Hüpotees 9. *Kui arvud A, B, C, x, y ja z on sellised positiivsed täisarvud, et kehtib võrrand*

$$A^x + B^y = C^z,$$

ning $x, y, z \geq 3$, siis arvudel A, B ja C on ühine algtegur.

abc-hüpoteesist järeldub, et Beali hüpoteesile leidub ülimalt lõplik arv kontranäiteid.

4.1.10 Brocardi probleem

Olgu meil võrrand $n! + 1 = m^2$. Brocardi probleem on küsimus selle võrrandi lahenduvusest täisarvude seas. Lahendipaare (n, m) nimetatakse Browni arvudeks

(Pickover, 1995). Bakalaureusetöö kirjutamise ajaks on leitud kolm Browni arvude paari: $(4, 5)$, $(5, 11)$ ja $(7, 71)$ (Matson, 2017). Matemaatik Marius Overholt on tõestanud, et Brocardi probleemile leidub vaid lõplik arv lahendeid eeldusel, et *abc*-hüpotees kehtib (Overholt, 1993). Lisaks on matemaatik Andrzej Dabrowski tõestanud, et *abc*-hüpoteesi kehtides on võrrandil $n! + A = k^2$ iga $A \in \mathbb{Z}$ korral lõplik arv lahendeid (Dabrowski, 1996).

4.1.11 Dressleri hüpotees

Alljärgnev hüpotees (Cochrane, T. ja Dressler, R., 1999) käsitleb algarvude paiknemist.

Hüpotees 10 (Dressleri hüpotees)**.** *Olgu meil kaks erinevat positiivset täisarvu, mille algtegurid on samad. Siis nende vahel on vähemalt üks algarv.*

On tõestatud, et *abc*-hüpoteesist järeldub, et iga $\varepsilon > 0$ korral leidub konstant C_ε nii, et kui $a < b$ on positiivsed täisarvud, millel on võrdsed algtegurid, siis

$$b - a > C_\varepsilon \cdot a^{\frac{1}{2}-\varepsilon}.$$

abc-hüpoteesi ja mõnda lisatulemust kasutades saab eelmisest väitest järeldada Dressleri hüpoteesi kehtivuse.

4.1.12 Diofantiline võrrand $p^v - p^w = q^x - q^y$

Aastal 2003 tõestas rumeenia matemaatik Florian Luca, et kui *abc*-hüpotees kehtib, siis diofantilisel võrrandil

$$p^v - p^w = q^x - q^y$$

leidub vaid lõplik arv positiivseid täisarvulisi lahendeid p, q, v, w, x, y, kus arvud p ja q on erinevad algarvud (Luca, 2003).

4.1.13 Erdős-Ulami probleem

Erdős-Ulami probleem on järgmine: kas on võimalik, et tasand sisaldab kõikjal tihedat punktide hulka, mille iga kahe punkti vaheline (eukleidiline) kaugus on ratsionaalarv. Tasandi punktide hulga kõikjal tihedus tähendab, et ükskõik millises tasandile joonistatud ringis leidub vähemalt üks selle hulga punkt.

Matemaatik Hector Pasten tõestas 2017. aastal artiklis „Definability of Frobenius orbits and a result on rational distance sets", et *abc*-hüpoteesist järeldub, et Erdős-Ulami probleemi väide ei kehti (Pasten, 2017).

4.1.14 Schinzel-Tijdemani hüpotees

Schinzel-Tijdemani hüpotees käsitleb teatud diofantiliste võrrandite lahenduvust.

Hüpotees 11. *Kui ratsionaalarvuliste kordajaga polünoomil $P(x)$ on vähemalt kolm ühekordset juurt, siis diofantilisel võrrandil*

$$P(x) = y^2 z^3$$

leidub täisarvude x, y, z seas lõplik arv mittetriviaalseid (st $yz \neq 0$) lahendeid.

Matemaatik Peter Walsh tõestas, et eelnev hüpotees järeldub *abc*-hüpoteesist (Walsh, 2012).

4.2 Teisi seotud tulemusi

Selles alapeatükis tutvustame põgusalt teisi tuntumaid *abc*-hüpoteesiga seotud tulemusi.

4.2.1 Mordelli hüpotees

Inglise matemaatik Louis Mordell sõnastas hüpoteesi aastal 1922 (Mordell, 1922).

Hüpotees 12. *Algebralisel kõveral geenusega vähemalt kaks üle korpuse* $\mathbb{Q}$ *eksisteerib ainult lõplik arv* $\mathbb{Q}$*-ratsionaalseid punkte.*

Saksa matemaatik Gerd Faltings tõestas hüpoteesi järgmise, üldisema variandi 1983. aastal (Faltings, 1983).

Teoreem 8 (Faltingsi teoreem)**.** *Algebralisel kõveral geenusega vähemalt kaks üle arvukorpuse* K *eksisteerib ainult lõplik arv* K*-ratsionaalseid punkte.*

Aastal 1991 tõestas ameerika matemaatik Noam Elkies, et Faltingsi teoreem järeldub *abc*-hüpoteesist (Elkies, 1991).

4.2.2 Szpiro hüpotees

1980ndatel sõnastas prantsuse matemaatik Lucien Szpiro järgmise hüpoteesi.

Hüpotees 13 (Szpiro hüpotees)**.** *Olgu* $\varepsilon > 0$*. Siis leidub konstant* $C(\varepsilon)$ *nii, et iga minimaalse diskriminandiga* $\triangle$ *ja konduktoriga* f *elliptilise kõvera* E *üle korpuse* $\mathbb{Q}$ *korral kehtib võrratus*

$$|\triangle| \leq C(\varepsilon) \cdot f^{6+\varepsilon}.$$

Kui hüpoteesi kuju veidi muuta, saame uue hüpoteesi, mis on samaväärne *abc*-hüpoteesiga (Oesterlé, 1988).

Hüpotees 14 (Modifitseeritud Szpiro hüpotees)**.** *Olgu* $\varepsilon > 0$*. Siis leidub konstant* C_ε *nii, et iga elliptiline kõver* E *üle korpuse* $\mathbb{Q}$ *rahuldab võrratust*

$$\max\{|c_4|^3, |c_6|^2\} \leq C_\varepsilon \cdot f^{6+\varepsilon},$$

kus f on E konduktor ning invariandid c_4 ja c_6 on pärit Tate'i algoritmist.

abc-hüpotees tekkiski matemaatikute Joseph Oesterlé ja David Masseri soovist mõista Szpiro hüpoteesi (Fesenko, 2015). Eelmainitud *abc*-hüpoteesi väidetav tõestus jaapani matemaatiku Shinichi Mochizuki poolt ongi täpsemalt Szpiro hüpoteesi tõestus.

4.2.3 Polünoomide ruuduvabad väärtused

Ei ole teada, et leiduks ühtegi taandumatut (vähemalt viienda astme) ühemuutuja polünoomi F üle $\mathbb{Q}$, mille korral $F(n)$ oleks ruuduvaba täisarv lõpmata paljude n väärtuste korral. On tõestatud, et *abc*-hüpoteesist järeldub, et kõikide arvu n väärtuste korral on ringpolünoomidel $\Phi_n(X)$ ja $(X^n - 1)/(X - 1)$ selline omadus (Browkin, J. *et al.*, 1997).

4.2.4 Ruutjuurte pöördväärtuste ümardamine

Olgu $\alpha = x^{-\frac{1}{2}}$, kus x on positiivne reaalarv (seda tehet on teadusarvutustes palju vaja). Olemasolevad tulemused näitavad, et arvu α ümardamiseks ujukoma-arvude süsteemis p olulise bitini, tuleb arvutada võib-olla kuni $3p+1$ arvu α esimest bitti. Aastal 2004 tõestati, et *abc*-hüpoteesist järeldub, et arvutatavate esimeste bittide arvu saab vähendada arvuni $2p$. (Croot, E., Li, R.-C. ja Zhu, H. J., 2004)

4.2.5 Teisi järeldusi

abc-hüpoteesil on veel teisigi järeldusi. Tuntumad neis on näiteks Vojta hüpotees, Dirichet' L-funktsiooni Siegeli juurte puudumine, Greenbergi hüpotees, Langi hüpotees, Hilbert-Waringi teoreem ja tõkked Tate-Šafarevitši rühma suurusele. Paljud neist on huvilistele kättesaadavad A. Nitaj *abc*-hüpoteesi kodulehel (Nitaj, 2021).

5 Valitud järelduste tõestusi

Käesolevas peatükis esitame mõned lihtsamini tõestatavad *abc*-hüpoteesi järeldused koos vastavate tõestustega.

5.1 Fermat' suure teoreem

Tuletame meelde, et Fermat' suur teoreem väidab, et kui $n \geq 3$, siis võrrandil

$$a^n + b^n = c^n \tag{6}$$

ei leidu ühtegi naturaalarvulist lahendit.

Teoreem 9. *Hüpoteesist 1 järeldub Fermat' suur teoreem.*

Tõestus. Olgu $n \geq 3$ naturaalarv ja kehtigu hüpotees 1. Oletame vastuväiteliselt, et leiduvad $a, b, c \in \mathbb{N}$, mis on võrrandi (6) lahendid. Märkame, et kui naturaalarvud a, b ja c on võrrandi (6) lahendid ja mingi algarv p jagab arve a ja b, siis algarv p jagab ka arvu c. See tähendab, et naturaalarvud $\frac{a}{p}$, $\frac{b}{p}$ ja $\frac{c}{p}$ on võrrandi (6) lahendid. Järelikult kui võrrandil (6) leidub lahend naturaalarvude seas, siis leidub tal ka lahend paarikaupa ühistegurita naturaalarvude seas. On ilmne, et kui arvud a, b ja c on paarikaupa ühistegurita, siis ka arvud a^n, b^n ja c^n on paarikaupa ühistegurita. Radikaali definitsioonist (vt definitsiooni 4) saame, et

$$\operatorname{rad}(a^n b^n c^n) = \operatorname{rad}(abc) \leq abc < c^3.$$

Tõepoolest, võrdus kehtib radikaali definitsiooni tõttu ning esimene võrratus kehtib, sest naturaalarvu radikaal „eemaldab" naturaalarvu kanoonilise kuju liikmete astmed. Nimelt kui kõik kanoonilise kuju liikmete astmed on 1, siis $\operatorname{rad}(abc) = abc$. Kui aga vähemalt ühe kanoonilise kuju liikme aste $k_i > 1$, siis $\operatorname{rad}(abc) < abc$. Teine võrratus kehtib, sest $a^n, b^n < c^n$, millest saame $a, b < c$ ja seega $abc < c^3$.

Hüpoteesi 1 saab vaadata kui *abc*-hüpoteesi juhtu, kus $\varepsilon = 1$ ning $K_1 = 1$. Nüüd saame võrratuse

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

Rakendame seda Fermat' suurele teoreemile.

$$c^n < \mathrm{rad}(a^n b^n c^n)^2 < (c^3)^2 = c^6$$

Nüüd saime tulemuseks, et $c^n < c^6$ ehk $n < 6$. Fermat' suure teoreemi eelduse järgi $n \geq 3$. Järelikult peame veel vaatama juhte, kus $n = \{3, 4, 5\}$. Nende erijuhtude jaoks on tõestused juba ammu olemas (Euler, 1770), (Barlow, 1811), (Lebesgue, 1843) ning neid käesolevas töös lähemalt ei käsitleta. □

abc-hüpoteesist järeldub otse asümptootiline Fermat' suur teoreem. Täpsemalt:

Teoreem 10. *abc-hüpoteesist järeldub, et leidub positiivne täisarv n_0 nii, et võrrandil (6) ei leidu lahendeid paarikaupa ühistegurita positiivsete täisarvude seas ühegi astendaja $n \geq n_0$ korral.*

Tõestus. Kehtigu *abc*-hüpotees (vt hüpoteesi 2). Olgu a, b ja c paarikaupa ühistegurita positiivsed täisarvud nii, et kehtib

$$a^n + b^n = c^n. \tag{7}$$

Saame, et

$$\mathrm{rad}(a^n b^n c^n) = \mathrm{rad}(abc) \leq abc < c^3.$$

Oleme eelmises tõestuses näidanud, miks antud võrdus ja võrratused kehtivad.

Kui $n = 1$, siis võrrandis (7) saab arvu c kõige väiksem väärtus olla 3 juhul kui $a = 1$ ja $b = 2$. Järelikult $c \geq 3$. Rakendame eelmisele võrratusele *abc*-hüpoteesi

nii, et $\varepsilon = 1$ ja $K = \max(1, K_1)$ ja saame, et

$$c^n < K \cdot \mathrm{rad}(a^n b^n c^n)^2 < K \cdot c^6.$$

Võttes mõlemalt poolt logaritmi, saame

$$n < 6 + \frac{\log K}{\log c} \leq 6 + \frac{\log K}{\log 3} = \text{const}.$$

Võttes $n_0 = 6 + \frac{\log K}{\log 3}$ oleme tõestanud asümptootilise Fermat' suure teoreemi. □

Järgmine lause näitab, et *abc*-hüpoteesi kehtivusel ei saa Fermat' suur teoreem kehtida vaid ülimalt lõplikul arvul juhtudel.

Lause 4. *abc-hüpoteesist järeldub, et fikseeritud astendaja $n \geq 4$ korral leidub Fermat' võrrandil $a^n + b^n = c^n$ positiivsete täisarvude seas ülimalt lõplik arv lahendeid.*

Tõestus. Eeldame, et *abc*-hüpotees kehtib. Olgu $n \geq 4$ ja a, b, c sellised positiivsed täisarvud, et kehtib

$$a^n + b^n = c^n. \tag{8}$$

Põhjendus, miks saab arvudele a^n, b^n, c^n rakendada *abc*-hüpoteesi, seletati lahti Fermat' suure teoreemi tõestuse esimeses lõigus (vt teoreemi 5).

Fikseerime $\varepsilon = \frac{1}{6}$. Siis *abc*-hüpoteesi põhjal leidub $K_{\frac{1}{6}} \in \mathbb{R}$ nii, et kehtib

$$\begin{aligned} c^n &< K_{\frac{1}{6}} \cdot \mathrm{rad}(a^n b^n c^n)^{1+\frac{1}{6}} \\ &= K_{\frac{1}{6}} \cdot \mathrm{rad}(abc)^{\frac{7}{6}} \\ &\leq K_{\frac{1}{6}} \cdot (abc)^{\frac{7}{6}} \\ &< K_{\frac{1}{6}} \cdot (c^3)^{\frac{7}{6}} \\ &= K_{\frac{1}{6}} \cdot c^{\frac{7}{2}}. \end{aligned}$$

Seega saime, et

$$c^{n-\frac{7}{2}} < K_{\frac{1}{6}}. \tag{9}$$

Paneme tähele, et kuna $n \geq 4$, siis astendaja $n - \frac{7}{2}$ on positiivne. Mistõttu saame kirjutada

$$c < \left(K_{\frac{1}{6}}\right)^{\frac{1}{n-\frac{7}{2}}}.$$

Näeme, et viimase võrratuse paremal poolel on konstant ehk sobivaid positiivseid täisarve c on ülimalt lõplik arv. Teame, et $a < c$ ja $b < c$, järelikult leidub ülimalt lõplik arv positiivseid täisarve a ja b. Järelikult leidub ka ülimalt lõplik arv arvukolmikuid (a,b,c). See tähendab, et võrrandil (8) leidub ülimalt lõplik arv lahendeid positiivsete täisarvude seas. □

Paneme tähele, et see tõestus ei sobi astendaja $n = 3$ korral. Fikseerime $\varepsilon > 0$. Siis eelnevat lahenduskäiku korrates saame võrratuse (9) kirjutada üldkujul

$$c^{n-3-3\varepsilon} < K_\varepsilon,$$

mis $n = 3$ korral on kujul

$$c^{-3\varepsilon} < K_\varepsilon$$

ehk

$$c^{3\varepsilon} > \frac{1}{K_\varepsilon}.$$

Kuna $\varepsilon > 0$, siis saame kirjutada

$$c > \left(\frac{1}{K_\varepsilon}\right)^{\frac{1}{3\varepsilon}}.$$

Näeme, et viimase võrratuse paremal poolel on konstant ehk sobivaid positiivseid

täisarve c on potentsiaalselt lõpmatu arv. Järelikult eelmine tõestusstrateegia juhul $n = 3$ ei tööta.

5.2 Asümptootiline Catalani hüpotees

On teada, et diofantilisel võrrandil $x^m - y^2 = 1$ pole positiivsete täisarvude seas ühtegi lahendit (Lebesgue, 1850). Lisaks on teada, et diofantilise võrrandi $x^2 - y^n = 1$ ainuke lahend positiivsete täisarvude seas on $x = n = 3$ ja $y = 2$. Kokkuvõttes on tarvis uurida Catalani hüpoteesi vaid neil juhtudel, kus $\min(m, n) \geq 3$. Oletades, et *abc*-hüpotees kehtib, saame tõestada asümptootilise Catalani teoreemi.

Teoreem 11 (Asümptootiline Catalani teoreem)**.** *abc-hüpoteesist järeldub, et võrrandil (5) on vaid lõplik arv lahendeid positiivsete täisarvude seas.*

Tõestus. Eeldame, et *abc*-hüpotees kehtib. Olgu täisarvude nelik (x, y, m, n) võrrandi (5) lahend, mille korral $\min(m, n) \geq 3$. Kuna arvud x^m ja y^n on järjestikused täisarvud, siis lemma 3 järgi on nad ühistegurita.

Näitame, et ka arvud x ja y on ühistegurita. Oletame vastuväiteliselt, et $\text{SÜT}(x, y) = d > 1$. See tähendab, et $d \mid x$ ja $d \mid y$. Seega jaguvusseose omaduste põhjal $d \mid xx^{m-1} = x^m$ ja $d \mid yy^{n-1} = y^n$, mis on vastuolus sellega, et arvud x^m ja y^n on ühistegurita. Oleme näidanud, et täisarvud x ja y on ühistegurita.

Fikseerime $\varepsilon = \frac{1}{4}$. Siis *abc*-hüpoteesist järeldub, et leidub konstant $K_{\frac{1}{4}}$ nii, et

$$y^n < x^m < K_{\frac{1}{4}} \text{rad}(x^m y^n)^{\frac{5}{4}} = K_{\frac{1}{4}} \text{rad}(xy)^{\frac{5}{4}} \leq K_{\frac{1}{4}} (xy)^{\frac{5}{4}}$$

ehk

$$m \log x < \log K_{\frac{1}{4}} + \frac{5}{4}(\log x + \log y)$$

ja

$$n \log y < \log K_{\frac{1}{4}} + \frac{5}{4}(\log x + \log y).$$

Järelikult saame, et

$$m \log x + n \log y < 2 \log K_{\frac{1}{4}} + \frac{5}{2}(\log x + \log y)$$

ehk

$$\left(m - \frac{5}{2}\right) \log x + \left(n - \frac{5}{2}\right) \log y < 2 \log K_{\frac{1}{4}}. \tag{10}$$

Paneme tähele, et $x = y = 1$ korral $x^m - y^n = 1 - 1 = 0 \neq 1$. Samuti kui $x = 1$ ja $y > 1$, siis $x^m - y^n = 1 - y^n \neq 1$. Viimaks, kuna $m \geq 3$, siis $x > 1$ ja $y = 1$ korral $x^m - 1 \geq 2^3 - 1 = 7$. Oleme näidanud, et sellised arvude x ja y valikud ei saa rahuldada võrrandit (5). Järelikult $x \geq 2$ ja $y \geq 2$.

Märkame, et kuna $m \geq 3$ ja $n \geq 3$, siis

$$m - \frac{5}{2} \geq 3 - \frac{5}{2} > 0 \quad \text{ja} \quad n - \frac{5}{2} \geq 3 - \frac{5}{2} > 0.$$

Seega vastavad tegurid on võrratuses (10) positiivsed. Kasutades seda teadmist ja fakti, et $x \geq 2$ ja $y \geq 2$, saame võrratuse (10) vasakut poolt hinnata alt järgmiselt:

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

Järelikult saime, et kehtib

$$\left(m - \frac{5}{2}\right) \log 2 + \left(n - \frac{5}{2}\right) \log 2 < 2 \log K_{\frac{1}{4}}.$$

Jagame mõlema poole läbi arvuga $\log 2$ ja saame

$$m - \frac{5}{2} + n - \frac{5}{2} < \frac{2 \log K_{\frac{1}{4}}}{\log 2}$$

ehk

$$m + n < \frac{2 \log K_{\frac{1}{4}}}{\log 2} + 5.$$

Kuna $K_{\frac{1}{4}}$ on konstant, siis on eelneva võrratuse parem pool konstant ja järelikult

on summa $m+n$ erinevaid väärtusi ülimalt lõplik arv. See tähendab, et nii arve m kui ka n on ülimalt lõplik arv. Sellest järeldub, et on ülimalt lõplik arv astmepaare (m, n), mille korral on võrrand (5) lahenduv. Fikseerides $m \geq 3$ ja $n \geq 3$ kehtib võrratuse (10) põhjal

$$c_1 \log x + c_2 \log y < c_3,$$

kus c_1, c_2 ja c_3 on positiivsed konstandid. Seda võrratust rahuldab ülimalt lõplik arv positiivseid täisarve x ja y ehk fikseeritud m ja n korral on võrrandil (5) ülimalt lõplik arv lahendeid positiivsete täisarvude x ja y seas.

Kuna arvude m ja n valikuid on ülimalt lõplik arv, siis saame sellist fikseerimist teha ülimalt lõplik arv kordi. Järelikult on võrrandil (5) ülimalt lõplik arv lahendeid positiivsete täisarvude seas. □

5.3 Mitte-Wieferichi algarvude lõpmatus

Näitame, et *abc*-hüpoteesist saab järeldada, et mitte-Wieferichi algarvude hulk on lõpmatu. Mitte-Wieferichi algarvude hulka tähistame tähega W. Enne väite tõestamist tõestame abitulemuse.

Lemma 6. *Olgu p paaritu algarv. Kui leidub $n \in \mathbb{N}$ nii, et kehtib*

$$2^n \equiv 1 \pmod{p} \quad \wedge \quad 2^n \not\equiv 1 \pmod{p^2},$$

siis p on mitte-Wieferichi algarv.

Tõestus. Kehtigu lemma eeldused. Olgu $d \in \mathbb{N}$ arvu 2 järk mooduli p järgi (vt definitsiooni 2). Lemma 5 kaudu saame, et $d \mid n$. Eelduste põhjal kehtib $2^n \not\equiv 1 \pmod{p^2}$. Näitame, et $2^d \not\equiv 1 \pmod{p^2}$. Oletame vastuväiteliselt, et $2^d \equiv 1 \pmod{p^2}$. Kasutades kongruentsusseose multiplikatiivsust ja fakti, et leidub

täisarv l nii, et $n = ld$, saame

$$2^n = 2^{ld} = (2^d)^l \equiv 1^l = 1 \pmod{p^2},$$

mis on vastuolus eeldusega. Järelikult $2^d \not\equiv 1 \pmod{p^2}$.

Kuna arv d on arvu 2 järk mooduli p järgi, siis leidub $k \in \mathbb{Z}$ nii, et $2^d = 1 + kp$. Paneme tähele, et arvud k ja p on ühistegurita. Kui neil oleks ühistegur, siis selle tõttu, et arv p on algarv, saame, et $\text{SÜT}(k, p) = p$. Seega leidub täisarv k_1 nii, et $k = k_1 p$, mille tõttu saame $2^d = 1 + kp = 1 + k_1 p^2$. See on vastuolus sellega, et $2^d \not\equiv 1 \pmod{p^2}$ ehk arvud k ja p peavad olema ühistegurita.

Fermat' väikese teoreemi (vt teoreemi 4) põhjal kehtib $2^{p-1} \equiv 1 \pmod{p}$, millest järeldub lemma 5 põhjal, et $d \mid (p-1)$. Saame, et leidub $e \in \mathbb{Z}$, kus $1 \leq e \leq p-1$ nii, et $p - 1 = de$. Kuna $e < p$ ja arv p on algarv, siis järelikult $\text{SÜT}(e, p) = 1$. Eelnevalt teame ka, et $\text{SÜT}(k, p) = 1$. Näitame, et $p \nmid ek$. Oletame vastuväiteliselt, et $p \mid ek$, siis järelduse 2 põhjal $p \mid e$ või $p \mid k$. See on vastuolus sellega, et $\text{SÜT}(e, p) = 1$ ja $\text{SÜT}(k, p) = 1$. Järelikult kehtib $p \nmid ek$ ja täisarvud ek ja p on ühistegurita.

Edasi saame binoomvalemit kasutades, et

$$\begin{aligned} 2^{p-1} &= 2^{de} = (2^d)^e = (1 + kp)^e \\ &= C_e^0 (kp)^0 + C_e^1 (kp)^1 + C_e^2 (kp)^2 + \ldots + C_e^e (kp)^e \\ &= 1 + ekp + C_e^2 k^2 p^2 + \ldots + C_e^e k^e p^{e-2} p^2 \\ &\equiv 1 + ekp \not\equiv 1 \pmod{p^2}. \end{aligned}$$

Viimane kongruentsus ei kehti, sest arvud ek ja p on ühistegurita. Kokkuvõttes oleme näidanud, et p on mitte-Wieferichi algarv. □

Esimese saja naturaalarvu seas on astmelised arvud 1, 4, 8, 9, 16, 25, 27, 32, 36,

49, 64, 72, 81, 100. Kui v on astmeline arv, siis kehtib

$$\mathrm{rad}(v) \leq \sqrt{v}. \tag{11}$$

Teoreem 12. *abc-hüpoteesist järeldub, et eksisteerib lõpmata palju mitte-Wieferichi algarve.*

Tõestus. Eeldame, et *abc*-hüpotees kehtib. Olgu W mitte-Wieferichi algarvude hulk. Iga positiivse täisarvu n korral kirjutame

$$2^n - 1 = p_{1,n}^{k_{1,n}} \cdot \ldots \cdot p_{s,n}^{k_{s,n}} = u_n v_n,$$

kus arvud u_n ja v_n avalduvad järgmiselt:

$$u_n = \prod_{k_{i,n}=1} p_{i,n}^{k_{i,n}}$$

ja

$$v_n = \prod_{k_{i,n}\geq 2} p_{i,n}^{k_{i,n}}.$$

Kui $p \mid u_n$, siis

$$2^n \equiv 1 \pmod{p},$$

aga

$$2^n \not\equiv 1 \pmod{p^2}.$$

Lemma 6 põhjal saame, et $p \in W$ ja seega on arv u_n ruuduvaba täisarv, mis jagub ainult mitte-Wieferichi algarvudega. Oletame vastuväiteliselt, et hulk W on lõplik, siis eksisteerib vaid lõplik arv täisarve kujul u_n, sest hulga W elementidest moodustatud kõikvõimalikke erinevatest teguritest koosnevaid korrutisi on lõplik arv. Järelikult hulk $\{u_n : n \in \mathbb{N}\}$ on lõplik.

Teame, et hulk $\{2^n - 1 : n \in \mathbb{N}\} = \{u_n v_n : n \in \mathbb{N}\}$ on lõpmatu. Kuna hulk

$\{u_n : n \in \mathbb{N}\}$ on lõplik, siis peab olema hulk $\{v_n : n \in \mathbb{N}\}$ lõpmatu ja järelikult ka tõkestamata. Kuna v_n on astmeline arv, siis võrratuse (11) tõttu kehtib, et

$$\mathrm{rad}(v_n) \leq \sqrt{v_n}.$$

Olgu $0 < \varepsilon < 1$. Rakendame *abc*-hüpoteesi võrrandile

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

ja saame, et

$$\begin{aligned} v_n &< 2^n \\ &< K(\varepsilon)\mathrm{rad}(2^n(2^n-1))^{1+\varepsilon} \\ &= K(\varepsilon)\mathrm{rad}(2u_nv_n)^{1+\varepsilon} \\ &\leq K(\varepsilon)(2u_n)^{1+\varepsilon}\mathrm{rad}(v_n)^{1+\varepsilon} \\ &\leq K(\varepsilon)(2\max_n(u_n))^{1+\varepsilon}\mathrm{rad}(v_n)^{1+\varepsilon} \\ &\leq \mathrm{const} \cdot v_n^{(1+\varepsilon)/2}. \end{aligned}$$

Esimene võrdus kehtib radikaali definitsiooni ja võrduse $2^n - 1 = u_nv_n$ tõttu. Viimane võrratus kehtib võrratuse (11) tõttu.

Kuna $\varepsilon < 1$, siis $\frac{1-\varepsilon}{2} > 0$ ja saame kirjutada

$$\frac{v_n}{(v_n)^{\frac{1+\varepsilon}{2}}} < \mathrm{const}$$

ehk

$$(v_n)^{\frac{1-\varepsilon}{2}} < \mathrm{const}$$

ehk

$$v_n < \text{const}'.$$

Siit järeldub, et arvud v_n on tõkestatud, mis on vastuolus eelneva informatsiooniga. Järelikult on mitte-Wieferichi algarve lõpmata palju. □

5.4 Järjestikuste astmeliste arvude lõplikus

Astmelisi arve on käsitlenud ungari matemaatikud Paul Erdős ja George Szekeres (Erdős, P. ja Szekeres, G., 1934), ameerika matemaatik Solomon Golomb (Golomb, 1970) ning kanada matemaatikud Richard Mollin ja Gary Walsh (Mollin, R. A. ja Walsh, P. G., 1986). Aastal 1976 sõnastas Erdős hüpoteesi, et ei saa olla kolme järjestikust astmelist naturaalarvu (Erdős, 1976). See on tuntud ka kui Erdős-Mollin-Walshi hüpotees.

Teoreem 13. *abc-hüpoteesist järeldub, et leidub vaid lõplik arv täisarvukolmikuid, mis koosnevad kolmest järjestikusest astmelisest arvust.*

Tõestus. Eeldame, et *abc*-hüpotees kehtib. Olgu $n-1$, n, $n+1$ kolm järjestikust astmelist arvu (vt definitsiooni 3). Oletame vastuväiteliselt, et eksisteerib lõpmatu arv täisarvukolmikuid, mis koosnevad kolmest järjestikusest astmelisest arvust. St kõigi astmeliste arvukolmikute hulk $A = \{(n-1, n, n+1) : n-1, n, n+1 \text{ on astmelised arvud}\}$ on lõpmatu.

Paneme tähele, et kehtib

$$(n^2 - 1) + 1 = n^2. \tag{12}$$

Ühisteguri omaduste järgi on arv 1 ühistegurita iga täisarvuga. Lemma 3 põhjal teame, et mistahes kaks järjestikust täisarvu on ühistegurita. Seega on arvud $n^2 - 1$, 1 ja n^2 paarikaupa ühistegurita ning saame rakendada võrrandile (12) *abc-*

hüpoteesi. Olgu $\varepsilon > 0$, siis *abc*-hüpoteesi põhjal leidub $K_\varepsilon \in \mathbb{R}$ nii, et kehtib

$$n^2 < K_\varepsilon \cdot \mathrm{rad}((n^2-1)\cdot 1 \cdot n^2)^{1+\varepsilon} = K_\varepsilon \cdot \mathrm{rad}((n^2-1)\cdot n^2)^{1+\varepsilon} \quad \forall n \in A.$$

Märkame, et

$$\begin{aligned} \mathrm{rad}((n^2-1)\cdot n^2) &= \mathrm{rad}((n^2-1)\cdot n) \\ &= \mathrm{rad}((n-1)\cdot(n+1)\cdot n) \\ &= \mathrm{rad}((n-1)\cdot n\cdot(n+1)). \end{aligned}$$

Näitame, et kahe astmelise arvu m ja n korrutis mn on ka astmeline arv. Olgu $p \in \mathbb{P}$ selline, et $p \mid mn$. Siis järelduse 2 põhjal $p \mid m$ või $p \mid n$. Vaatame esmalt juhtu $p \mid m$. Kuna arv m on astmeline arv, siis $p^2 \mid m$ ja sellest järeldub, et $p^2 \mid nm$. Analoogiliselt saame $p \mid n$ korral, et $p^2 \mid nm$. Järelikult on kahe astmelise arvu korrutis mn samuti astmeline arv.

Seetõttu on arv $(n-1)\cdot n\cdot(n+1)$ astmeline arv. Nüüd saame kasutada võrratust (11):

$$\begin{aligned} \mathrm{rad}((n-1)\cdot n\cdot(n+1)) &\leq \sqrt{(n-1)\cdot n\cdot(n+1)} \\ &= \sqrt{(n^2-1)\cdot n} \\ &< \sqrt{n^2\cdot n} \\ &= n^{\frac{3}{2}} \quad \forall n \in A. \end{aligned}$$

Seega oleme saanud

$$n^2 \leq K_\varepsilon \cdot \mathrm{rad}((n^2-1)\cdot n^2)^{1+\varepsilon} < K_\varepsilon \cdot \left(n^{\frac{3}{2}}\right)^{1+\varepsilon} \quad \forall n \in A.$$

Võttes $\varepsilon = \frac{1}{10}$, saame

$$n^2 < K_{\frac{1}{10}} \cdot \left(n^{\frac{3}{2}}\right)^{1+\frac{1}{10}} \quad \forall n \in A$$

ehk

$$n^2 < K_{\frac{1}{10}} \cdot n^{\frac{33}{20}} \quad \forall n \in A$$

ehk

$$n^{\frac{7}{20}} < K_{\frac{1}{10}} \quad \forall n \in A$$

ehk

$$n < \left(K_{\frac{1}{10}}\right)^{\frac{20}{7}} \quad \forall n \in A.$$

Kuna $K_{\frac{1}{10}} \in \mathbb{R}$ on konstant, siis võrratuse paremal pool on konstant. See tähendab, et võrratus saab kehtida vaid lõpliku arvu n korral. Järelikult ei saa kehtida võrrand iga $n \in A$ korral, mis on vastuolu eeldusega. Seega saab olla järjestikuseid astmeliste arvude kolmikuid lõplik arv. □

6 *abc*-hüpoteesi kongruentsvariant

Oesterlé näitas, et *abc*-hüpotees on samaväärne modifitseeritud Szpiro hüpoteesile (Oesterlé, 1988). Ta märkas tõestuse käigus, et kui *abc*-hüpotees kehtib iga arvukolmiku (a, b, c) korral, kus $16 \mid abc$, siis kehtib ka hüpotees ilma selle üldistuseta. See tõstab hunniku järgmiseid hüpoteese ja lauseid.

Hüpotees 15. *Olgu täisarv $m \geq 2$. abc-hüpoteesi kongruentsvariant mooduli m jaoks ütleb, et iga $\varepsilon > 0$ korral leidub $K(m, \varepsilon) \in \mathbb{R}$ nii, et kui arvud a, b ja c on positiivsed paarikaupa ühistegurita täisarvud, mille korral*

$$a + b = c$$

ja

$$abc \equiv 0 \pmod{m},$$

siis kehtib võrratus

$$c \leq K(m, \varepsilon) \cdot \operatorname{rad}(abc)^{1+\varepsilon}.$$

Lisaeelduse tõttu on tegemist nõrgema väitega kui tavaline *abc*-hüpotees (vt hüpoteesi 2). Me tõestame, et kui *abc*-hüpoteesi kongruentsvariant kehtib mingi mooduli m korral, siis kehtib ka tavaline *abc*-hüpotees.

Lause 5. *Olgu a, b ja c täisarvud, mille korral kehtib võrdus $a+b = c$. Siis vähemalt üks täisarvudest a, b või c peab olema paarisarv.*

Tõestus. Kehtigu lause eeldused. Näitame, et vähemalt üks täisarvudest a, b või c peab olema paarisarv.

Kui arvudest a ja b on vähemalt üks paarisarv, siis ongi juba üks kolmest arvust paarisarv. Oletame nüüd, et arvud a ja b on mõlemad paaritud arvud, st c on kahe paaritu arvu summa, mis on paarisarv. Sellega oleme näidanud, et vähemalt üks arv arvudest a, b ja c on paarisarv. □

Eelneva lause tõttu näeme, et $abc \equiv 0 \pmod 2$. Seega on abc-hüpoteesi kongruentsvariant mooduli 2 korral samaväärne tavalise abc-hüpoteesiga ehk vaatleme edaspidi mooduleid $m \geq 3$.

Lause 6. *Olgu a, b ja c paarikaupa ühistegurita täisarvud, mille korral kehtib võrdus $a + b = c$. Kui arv c on paaritu, siis arv $b - a$ on ka paaritu. Kui arv c on paaris, siis arv $b - a$ on ka paaris.*

Tõestus. Kehtigu lause eeldused. Näitame esmalt, et kui arv c on paaritu, siis arv $b - a$ on ka paaritu. Kui arv c on paaritu, siis arv $b - a$ on ka paaritu, sest $b - a = b - (c - b) = 2b - c$ ehk paarisarvu $2b$ ja paaritu arvu c vahe.

Näitame nüüd, et kui arv c on paaris, siis arv $b - a$ on ka paaris. Kui arv c on paaris, siis sellest, et arvud a, b ja c on paarikaupa ühistegurita ei saa olla arvud a ja b paarisarvud ning arv $b - a$ on kahe paaritu arvu vahe ehk paarisarv. □

Kui a, b ja c on erinevad positiivsed paarikaupa ühistegurita täisarvud, siis üldisust kitsendamata saab eeldada, et $a < b < c$, mida ka edaspidi teeme.

Lemma 7. *Olgu a, b, c positiivsed täisarvud nii, et SÜT$(a, b, c) = 1$ ja kehtigu $a + b = c$. Siis kehtib SÜT$(a, b) =$ SÜT$(a, c) =$ SÜT$(b, c) = 1$. Lisaks $a = b$ ainult siis, kui $a = 1$ ja $c = 2$.*

Tõestus. Kehtigu lemma eeldused. Näitame esmalt, et $\text{SÜT}(a, b) = \text{SÜT}(a, c) = \text{SÜT}(b, c) = 1$. Oletame vastuväiteliselt, et $\text{SÜT}(a, b) = d > 1$. Siis $d \mid a$ ja $d \mid b$. Seega leiduvad täisarvud k ja l nii, et $a = kd$ ning $b = ld$. Nüüd avaldame $c = a+b = kd + ld = (k + l)d$ ehk $d \mid c$ ning seega $d \mid \text{SÜT}(\text{SÜT}(a, b), c) = \text{SÜT}(a, b, c) = 1$, mis on vastuolu. Sellega näitasime, et $\text{SÜT}(a, b) = 1$. Analoogiliselt saab näidata, et ka $\text{SÜT}(a, c) = \text{SÜT}(b, c) = 1$.

Lõpetuseks tõestame, et $a = b$ ainult siis, kui $a = 1$ ja $c = 2$. Kui $a = b$, siis saame võrduse $a + b = c$ kirjutada kujul $a + a = c$ ehk $2a = c$. Sellest järeldub, et $a \mid c$.

Kuna eelnevalt näitasime, et $\text{SÜT}(a, c) = 1$, siis järelikult peab kehtima $a = 1$. Seega saame, et $c = 2$. □

Lemma 8. *Olgu a, b, c positiivsed paarikaupa ühistegurita täisarvud nii, et arv c on paaritu, kehtib $a < b < c$ ja $a + b = c$. Olgu iga positiivse täisarvu n korral defineeritud*

$$A_n = (b - a)^n,$$
$$B_n = c^n - (b - a)^n,$$
$$C_n = c^n.$$

Arvud A_n, B_n ja C_n on erinevad paarikaupa ühistegurita positiivsed täisarvud nii, et $A_n + B_n = C_n$.

Tõestus. Kehtigu lemma eeldused. On ilmne, et kehtib $A_n + B_n = C_n$.

Näitame järgmisena, et arvude A_n, B_n ja C_n suurim ühistegur on 1.

Esmalt oletame vastuväiteliselt, et leidub algarv p nii, et $p \mid d = \text{SÜT}(A_n, B_n, C_n)$. Suurima ühisteguri definitsioonist ja sellest, et $p \mid d$ saame, et $p \mid A_n$, $p \mid B_n$ ja $p \mid C_n$. Järelikult $p \mid \text{SÜT}(A_n, C_n)$. Sarnaselt saame, et $p \mid A_n = (b - a)^n$ ja $p \mid C_n = c^n = (a + b)^n$. Kuna p on algarv, siis kehtivad $p \mid (b - a)$ ja $p \mid (a + b)$ ehk $p \mid c$.

Jaguvusseose omaduste põhjal kehtivad ka $p \mid ((b - a) + (a + b)) = 2b$ ning $p \mid ((a + b) - (b - a)) = 2a$. Seega järelduse 2 põhjal $p \mid 2$ või $p \mid a$ ja $p \mid b$. Viimane variant aga ei kehti, sest lemma eelduste põhjal $\text{SÜT}(a, b) = 1$ ja järelikult $p = 2$ või $p = 1$. Kuna aga teame, et $p \mid c$ ning lemma eelduste põhjal on arv c paaritu, siis ei saa kehtida võrdus $p = 2$, mistõttu $p = 1$. Kuna arv 1 pole algarv, siis saime vastuolu eeldusega. Järelikult peab kehtima $\text{SÜT}(A_n, B_n, C_n) = 1$.

Näitame nüüd, et arvud A_n, B_n ja C_n on erinevad positiivsed täisarvud. See, et need arvud on positiivsed on ilmne, sest eelduste põhjal kehtib $a < b < c$. Eelnevalt

näitasime, et $\text{SÜT}(A_n, B_n, C_n) = 1$, seega lemma 7 põhjal on arvud A_n, B_n ja C_n paarikaupa ühistegurita ja arvud $A_n = B_n$ vaid siis, kui $A_n = 1$. Kuna arvud A_n, B_n ja C_n rahuldavad lemmat 7 ja arv C_n peab kindlasti teistest suurem olema, siis ainus võrdumise variant on $A_n = B_n = 1$, millest saame $C_n = 2$. See pole aga võimalik, sest eeldustest $a < b < c$ ja $a + b = c$ saame, et $C_n = c^n \geq 3^n \geq 3$. Järelikult on arvud A_n, B_n ja C_n erinevad positiivsed täisarvud. □

Lemma 9. *Olgu arvud a, b ja c positiivsed paarikaupa ühistegurita täisarvud nii, et arv c on paarisarv, kehtib $a < b < c$ ja $a + b = c$. Olgu iga positiivse täisarvu n korral defineeritud*

$$A_n = \left(\frac{b-a}{2}\right)^n,$$
$$B_n = \left(\frac{c}{2}\right)^n - \left(\frac{b-a}{2}\right)^n,$$
$$C_n = \left(\frac{c}{2}\right)^n.$$

Siis $A_n + B_n = C_n$, arvud A_n, B_n ja C_n on paarikaupa ühistegurita positiivsed täisarvud ning kui $n \geq 2$, siis ka üksteisest erinevad.

Tõestus. Kehtigu lemma eeldused. On ilmne, et kehtib $A_n + B_n = C_n$. Samuti on tegemist täisarvudega, sest arv c on paarisarv ehk arv $\frac{c}{2}$ on täisarv. Lauses 6 näitasime, et kui arv c on paaris, siis on ka arv $b - a$ paaris ehk arv $\frac{b-a}{2}$ on samuti täisarv.

Näitame järgmisena, et arvude A_n, B_n ja C_n suurim ühistegur on 1.

Esmalt oletame vastuväiteliselt, et leidub algarv p nii, et $p \mid d = \text{SÜT}(A_n, B_n, C_n)$. Suurima ühisteguri definitsioonist ja sellest, et $p \mid d$ saame, et $p \mid A_n$, $p \mid B_n$ ja $p \mid C_n$. Järelikult $p \mid \text{SÜT}(A_n, C_n)$. Sarnaselt saame, et $p \mid A_n = (\frac{b-a}{2})^n$ ja $p \mid C_n = (\frac{c}{2})^n = (\frac{a+b}{2})^n$. Kuna p on algarv, siis kehtivad $p \mid \frac{b-a}{2}$ ja $p \mid \frac{c}{2} = \frac{a+b}{2}$.

Jaguvusseose omaduste põhjal kehtivad ka $p \mid (\frac{b-a}{2} + \frac{a+b}{2}) = b$ ning $p \mid (\frac{a+b}{2} - \frac{b-a}{2}) = a$. Kuna lemma eelduste põhjal $\text{SÜT}(a, b) = 1$, siis $p = 1$. Saime vastuolu eeldusega,

et arv p on algarv. Järelikult peab kehtima $\text{SÜT}(A_n, B_n, C_n) = 1$.

Näitame nüüd, et arvud A_n, B_n ja C_n on positiivsed ning $n \geq 2$ korral erinevad. See, et need arvud on positiivsed on ilmne, sest eelduste põhjal kehtib $a < b < c$.

Näitame, et arvud A_n, B_n ja C_n on erinevad $n \geq 2$ korral. Eelnevalt näitasime, et $\text{SÜT}(A_n, B_n, C_n) = 1$, seega lemma 7 põhjal on arvud A_n, B_n ja C_n paarikaupa ühistegurita. See on ainult siis võimalik, kui need arvud on kõik erinevad või vähemalt kaks neist on võrdsed arvuga 1. Kuna arvud A_n, B_n ja C_n rahuldavad lemmat 7 ja arv C_n peab kindlasti teistest suurem olema, siis ainus võrdumise variant on $A_n = B_n = 1$, millest saame $C_n = 2$. See pole aga võimalik, sest eeldustest $n \geq 2$, $a < b < c$, $a + b = c$ ja arv c on paaris saame, et $C_n = (\frac{c}{2})^n \geq (\frac{4}{2})^n \geq 2^n \geq 2^2 = 4$. Järelikult on arvud A_n, B_n ja C_n erinevad positiivsed täisarvud $n \geq 2$ korral. □

Lemma 10. *Olgu arvud a, b ja c paarikaupa ühistegurita täisarvud nii, et kehtib võrdus $a+b = c$. Kui arv c on paarisarv, siis täpselt üks arvudest c ja $b-a$ jaguvad arvuga 4.*

Tõestus. Kehtigu lemma eeldused. Teame, et $a + b = c$. Seega saame kirjutada, et

$$b - a = b - (c - b) = 2b - c,$$

mis on paarisarv, sest eelduse põhjal on arv c paarisarv ja kahe paarisarvu vahe on paarisarv. Kuna teame, et $\text{SÜT}(b, c) = 1$, siis peab arv b olema paaritu. Seega $2 \nmid b$ ja järelikult jaguvusseose omaduste tõttu ka $4 \nmid 2b$. Järelikult $2b \equiv 2 \pmod 4$.

Edasi vaatame kahte juhtu: $4 \mid c$ ja $4 \nmid c$.

Olgu $4 \mid c$ ehk $c \equiv 0 \pmod 4$. Seega $b - a = 2b - c \equiv 2 - 0 = 2 \pmod 4$. Sellega oleme näidanud, et $4 \nmid (b - a)$.

Olgu nüüd $4 \nmid c$. Kuna arv c on paarisarv, siis $c \equiv 2 \pmod 4$. Seega $b - a = 2b - c \equiv 2 - 2 = 0 \pmod 4$. Sellega oleme näidanud, et $4 \mid (b - a)$.

Seega oleme näidanud, et juhul kui $4 \mid c$, siis $4 \nmid b-a$ ja juhul kui $4 \nmid c$, siis $4 \mid b-a$ ehk täpselt üks arvudest c ja $b-a$ jaguvad arvuga 4. □

Lemma 11. *Olgu a, b ja c positiivsed paarikaupa ühistegurita täisarvud nii, et*

$$a < b < c$$

ja

$$a + b = c.$$

Olgu $n \geq 2$. Kui arv c on paaritu arv, siis defineerime

$$\begin{aligned} A_n &= (b-a)^n, \\ B_n &= c^n - (b-a)^n, \\ C_n &= c^n. \end{aligned}$$

Kui arv c on paarisarv, siis defineerime

$$\begin{aligned} A_n &= \left(\frac{b-a}{2}\right)^n, \\ B_n &= \left(\frac{c}{2}\right)^n - \left(\frac{b-a}{2}\right)^n, \\ C_n &= \left(\frac{c}{2}\right)^n. \end{aligned}$$

Nüüd on arvud A_n, B_n, C_n erinevad positiivsed paarikaupa ühistegurita täisarvud nii, et

$$A_n + B_n = C_n.$$

Kui $m \geq 3$ ja $n = \varphi(m)$, siis

$$A_n B_n C_n \equiv 0 \pmod{m}.$$

Tõestus. Lemmade 8 ja 9 põhjal saime, et arvud A_n, B_n ja C_n on erinevad paari-

kaupa ühistegurita positiivsed täisarvud nii, et kehtib võrdus $A_n + B_n = C_n$.

Olgu $m \geq 3$ ja $n = \varphi(m)$. Lemma 4 põhjal on arv n paarisarv ehk $n \geq 2$. Peame tõestama, et

$$A_n B_n C_n \equiv 0 \pmod{m}.$$

Lemma 1 põhjal piisab näidata, et kui arv p on algarv ja arv p^r jagab arvu m, siis

$$A_n B_n C_n \equiv 0 \pmod{p^r}. \tag{13}$$

Paneme tähele, et kui arv p on algarv ning kehtib $p^r \mid m$, siis teoreemi 2 põhjal kehtib $(p-1)p^{r-1} \mid n$ ning järelikult

$$r \leq 2^{r-1} \leq (p-1)p^{r-1} \leq n.$$

Esimese võrratuse kehtimine $r \in \mathbb{N}$ korral on ilmne. Teine võrratus kehtib, sest minimaalne arvu p väärtus ongi 2 ning siis kehtib võrdus, suuremate algarvude korral on vasak pool väiksem kui parem. Viimane võrratus kehtib jaguvuse $(p-1)p^{r-1} \mid n$ tõttu.

Oletame esmalt, et arv p on paaritu algarv.

Kui $p \mid c$, siis järelikult leidub täisarv k nii, et kehtib võrdus $c = kp$. Saame avaldada $c^n = (kp)^n = k^n p^n$ ehk $p^n \mid c^n$. Juhul, kui c on paaritu arv, siis viimane jaguvus on sama, mis $p^n \mid C_n$. Juhul kui c on paaris, siis leidub täisarv k nii, et $c = 2k$, seega eelnevalt saadud $p^n \mid c^n$ saame kirjutada kujul $p^n \mid (2k)^n = 2^n k^n$. Paneme tähele, et kuna p oli paaritu algarv, siis $p \nmid 2$ ehk $p^n \nmid 2^n$ ja seega lemma 2 põhjal $p^n \mid k^n = (\frac{c}{2})^n$. Seega ka paaris c korral $p^n \mid C_n$. Kuna $r \leq n$, siis $p^r \mid p^n$ ja jaguvusseose transitiivsuse tõttu saame $p^r \mid C_n$ ehk $C_n \equiv 0 \pmod{p^r}$.

Analoogiliselt, kui $p \mid (b-a)$, siis $A_n \equiv 0 \pmod{p^r}$. Kui arv p ei jaga kumbagi

arvu c ega $b-a$, siis teoreemi 3 põhjal saame

$$c^{(p-1)p^{r-1}} \equiv 1 \pmod{p^r}$$

ja

$$(b-a)^{(p-1)p^{r-1}} \equiv 1 \pmod{p^r}.$$

Olgu arvu c järk l mooduli p^r järgi. Siis lemma 5 põhjal saame, et $l \mid (p-1)p^{r-1}$. Kuna eelnevalt näitasime, et $(p-1)p^{r-1} \mid n$, siis järelikult $l \mid n$. Nüüd lemma 5 kaudu saame

$$c^n \equiv 1 \pmod{p^r}.$$

Analoogiliselt saame

$$(b-a)^n \equiv 1 \pmod{p^r}.$$

Kui arv c on paaris, siis on ka arv $(b-a)$ paaris lause 6 põhjal. Sellest, et $p \nmid c$ ja $p \nmid (b-a)$ järeldub, et $p \nmid \frac{c}{2}$ ja $p \nmid \frac{b-a}{2}$. Nüüd teoreemi 3 põhjal saame

$$\left(\frac{c}{2}\right)^{(p-1)p^{r-1}} \equiv 1 \pmod{p^r}$$

ja

$$\left(\frac{b-a}{2}\right)^{(p-1)p^{r-1}} \equiv 1 \pmod{p^r},$$

millest jällegi saame $(p-1)p^{r-1} \mid n$ tõttu, et

$$\left(\frac{c}{2}\right)^n \equiv \left(\frac{b-a}{2}\right)^n \equiv 1 \pmod{p^r}.$$

Seega paaritu c korral saame

$$B_n = c^n - (b-a)^n \equiv 1 - 1 \equiv 0 \pmod{p^r}$$

ning ka paaris c korral saame

$$B_n = \left(\frac{c}{2}\right)^n - \left(\frac{b-a}{2}\right)^n \equiv 1 - 1 \equiv 0 \pmod{p^r}.$$

Sellega oleme näidanud, et paaritute algarvude korral kehtib kongruents (13).

Oletame nüüd, et arv $p = 2$.

Kuna kehtib $2^r \mid m$, siis teoreemi 2 põhjal $2^{r-1} \mid n$ ning $r \leq n$. Tuletame meelde, et kui arv c on paarisarv, siis arv $b-a$ on samuti paarisarv. Lemma 10 põhjal teame, et vähemalt üks neist arvudest jagub arvuga 4. Nüüd saame, et kehtib kas $4^n \mid c^n$ või $4^n \mid (b-a)^n$. Järelikult üks arvudest C_n või A_n jagub arvuga 2^n, mis omakorda jagub arvuga 2^r.

Kui arv c on paaritu, siis on ka arv $b-a$ paaritu ning teoreemi 3 põhjal saame

$$c^{2^{r-1}} \equiv (b-a)^{2^{r-1}} \equiv 1 \pmod{2^r}.$$

Kuna kehtib $2^{r-1} \mid n$, siis järelikult leidub täisarv k nii, et kehtib $2^{r-1}k = n$. Kuna teame, et

$$c^{2^{r-1}} \equiv 1 \pmod{2^r}, \tag{14}$$

siis kongruentsusseose astendamise omaduse tõttu saame

$$c^n = (c^{2^{r-1}})^k \equiv 1^k = 1 \pmod{2^r}.$$

Analoogiliselt jõuame järgmise tulemuseni:

$$(b-a)^n \equiv 1 \pmod{2^r}.$$

Nüüd saame, et

$$B_n = c^n - (b-a)^n \equiv 1 - 1 = 0 \pmod{2^r}.$$

Järelikult kehtib kongruents (13) ka $p = 2$ korral. Kokkuvõttes oleme tõestanud lemma 11. □

Lemma 12. *Kui naturaalarv n on paarisarv, siis kehtib võrdus*

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

Tõestus. Tähistame $X := (b+a)$ ja $Y := (b-a)$. Tõestame väite induktsiooniga.

Baas. Näitame, et tulemus kehtib $n = 2$ ja $n = 4$ korral.

Kui $n = 2$, siis

$$X^2 - Y^2 = (b+a)^2 - (b-a)^2 = b^2 + 2ab + a^2 - (b^2 - 2ab + a^2) = 4ab.$$

Kui $n = 4$, siis

$$X^4 - Y^4 = (X^2 - Y^2)(X^2 + Y^2) = 4ab(X^2 + Y^2).$$

Samm. Olgu n paarisarv ja oletame, et väide kehtib $n-2$ ja n korral ehk kehtivad

$$X^{n-2} - Y^{n-2} = 4ab(X^{n-4} + X^{n-6}Y^2 + \ldots Y^{n-4}),$$
$$X^n - Y^n = 4ab(X^{n-2} + X^{n-4}Y^2 + \ldots Y^{n-2}).$$

Näitame, et väide kehtib $n+2$ korral. Saame kirjutada

$$\begin{aligned}
X^{n+2} - Y^{n+2} &= X^n X^2 - Y^n Y^2 \\
&= (X^n X^2 + X^n Y^2 - Y^n X^2 - Y^n Y^2) - X^n Y^2 + Y^n X^2 \\
&= X^n (X^2 + Y^2) - Y^n (X^2 + Y^2) - X^n Y^2 + Y^n X^2 \\
&= (X^n - Y^n)(X^2 + Y^2) - X^n Y^2 + Y^n X^2 \\
&= (X^n - Y^n)(X^2 + Y^2) - X^2 Y^2 (X^{n-2} - Y^{n-2}) \\
&= 4ab(X^{n-2} + X^{n-4} Y^2 + \ldots + Y^{n-2})(X^2 + Y^2) \\
&\quad - X^2 Y^2 4ab(X^{n-4} + X^{n-6} Y^2 + \ldots + Y^{n-4}) \\
&= 4ab\Big(\big(X^n + X^{n-2} Y^2 + \ldots + X^2 Y^{n-2} \\
&\quad + X^{n-2} Y^2 + X^{n-4} Y^4 + \ldots + Y^n\big) - \\
&\quad - \big(X^{n-2} Y^2 + X^{n-4} Y^4 + \ldots + X^2 Y^{n-2}\big)\Big) \\
&= 4ab(X^n + X^{n-2} Y^2 + \ldots + X^2 Y^{n-2} + Y^n).
\end{aligned}$$

□

Teoreem 14. *Olgu $m \geq 3$. Kui abc-hüpoteesi kongruentsvariant on tõene mooduli m korral, siis abc-hüpotees kehtib.*

Tõestus. Olgu $0 < \varepsilon < 1$. Vaatame täisarvukolmikuid (a, b, c), mis on kõik erinevad paarikaupa ühistegurita positiivsed täisarvud nii, et kehtib võrdus $a + b = c$. Defineerime uue funktsiooni:

$$\Phi_\varepsilon(a, b, c) = \log c - (1 + \varepsilon) \log(\mathrm{rad}(abc)). \tag{15}$$

Saame selle ümber kirjutada kujule

$$\log(\mathrm{rad}(abc)) = \frac{\log c}{1+\varepsilon} - \frac{\Phi_\varepsilon(a, b, c)}{1+\varepsilon} = \log c - \frac{\varepsilon \log c}{1+\varepsilon} - \frac{\Phi_\varepsilon(a, b, c)}{1+\varepsilon} \tag{16}$$

Olgu arvud A, B ja C erinevad paarikaupa ühistegurita positiivsed täisarvud nii, et kehtivad $ABC \equiv 0 \pmod{m}$ ja $A + B = C$. Kui *abc*-hüpoteesi kongruentsvariant kehtib mooduli m jaoks, siis leidub konstant $K(m, \varepsilon) > 0$ nii, et

$$C \leq K(m, \varepsilon) \cdot \mathrm{rad}(ABC)^{1+\varepsilon}.$$

Võttes mõlemalt poolt logaritmi, saame

$$\log C \leq \log(K(m, \varepsilon)) + (1 + \varepsilon) \log(\mathrm{rad}(ABC))$$

ehk

$$\log C - (1 + \varepsilon) \log(\mathrm{rad}(ABC)) \leq \log(K(m, \varepsilon))$$

ehk võrdust (15) kasutades saame

$$\Phi_\varepsilon(A, B, C) \leq \log(K(m, \varepsilon)) = K^*(m, \varepsilon).$$

Olgu arvud a, b ja c paarikaupa ühistegurita positiivsed täisarvud nii, et kehtivad $a < b < c$ ja $a + b = c$. Olgu $n = \varphi(m)$. Kuna $m \geq 3$, siis lemma 4 põhjal on arv n alati paarisarv ja seega ka $n \geq 2$.

Defineerime täisarvud A_n, B_n ja C_n lemma 11 järgi. Siis saame, et kehtivad $A_n B_n C_n \equiv 0 \pmod{m}$, arvud A_n, B_n ja C_n on paarikaupa ühistegurita ning $A_n + B_n = C_n$. Järelikult tänu eelnevale

$$\Phi_\varepsilon(A_n, B_n, C_n) \leq K^*(m, \varepsilon).$$

Kuna $m \geq 3$, siis nagu enne näidatud, on arv n paarisarv. Kasutades lemmat 12 saame paaritu c korral

$$\begin{aligned}
B_n &= c^n - (b-a)^n \\
&= (b+a)^n - (b-a)^n \\
&= 4ab((b+a)^{n-2} + (b+a)^{n-4}(b-a)^2 + \ldots + (b-a)^{n-2}) \\
&\leq 4ab((b+a)^{n-2} + (b+a)^{n-4}(b+a)^2 + \ldots + (b+a)^{n-2}) \\
&= 4ab\left(\frac{n}{2}\right)(b+a)^{n-2} \\
&= 2abnc^{n-2}.
\end{aligned}$$

Kuna $ab \mid B_n$, siis saame kirjutada

$$A_nB_nC_n = (b-a)^nB_nc^n = (b-a)^n\left(\frac{B_n}{ab}\right)abc^n.$$

Järelikult

$$\begin{aligned}
\mathrm{rad}(A_nB_nC_n) &= \mathrm{rad}\left((b-a)^n\left(\frac{B_n}{ab}\right)abc^n\right) \\
&= \mathrm{rad}\left((b-a)\left(\frac{B_n}{ab}\right)abc\right) \\
&\leq \mathrm{rad}(b-a)\mathrm{rad}\left(\frac{B_n}{ab}\right)\mathrm{rad}(abc) \\
&\leq (b-a)\left(\frac{B_n}{ab}\right)\mathrm{rad}(abc) \\
&= (b-a)(2nc^{n-2})\mathrm{rad}(abc) \\
&< c(2nc^{n-2})\mathrm{rad}(abc) \\
&= 2nc^{n-1}\mathrm{rad}(abc).
\end{aligned}$$

Esimene võrratus kehtib, sest kui täisarvudel x, y ja z on ühiseid algtegureid, siis $\mathrm{rad}(xyz) < \mathrm{rad}(x)\mathrm{rad}(y)\mathrm{rad}(z)$. Kui täisarvudel x, y ja z pole ühiseid algtegureid, siis $\mathrm{rad}(xyz) = \mathrm{rad}(x)\mathrm{rad}(y)\mathrm{rad}(z)$.

Paaris c korral saame juba paaritu c korral saadud tulemusi kasutades kirjutada järgnevalt

$$\begin{aligned} B_n &= \left(\frac{c}{2}\right)^n - \left(\frac{b-a}{2}\right)^n \\ &= \frac{(b+a)^n - (b-a)^n}{2^n} \\ &\leq \frac{2abnc^{n-2}}{2^n} \\ &= \frac{abnc^{n-2}}{2^{n-1}}. \end{aligned}$$

Paneme tähele, et kuna arv c on paaris, siis $2^{n-2} \mid c^{n-2}$ ja kuna n on paariasrv, siis $2 \mid n$. Seega $2^{n-1} \mid nc^{n-2}$ ning järelikult $ab \mid B_n$. Nüüd saame kirjutada

$$A_nB_nC_n = \left(\frac{b-a}{2}\right)^n B_n \left(\frac{c}{2}\right)^n = \left(\frac{b-a}{2}\right)^n \left(\frac{B_n}{ab}\right) ab \left(\frac{c}{2}\right)^n.$$

Järelikult

$$\begin{aligned} \mathrm{rad}(A_nB_nC_n) &= \mathrm{rad}\left(\left(\frac{b-a}{2}\right)^n \left(\frac{B_n}{ab}\right) ab \left(\frac{c}{2}\right)^n\right) \\ &\leq \mathrm{rad}\left((b-a)^n \left(\frac{c^n - (b-a)^n}{2^n} \cdot \frac{1}{ab}\right) abc^n\right) \\ &\leq \mathrm{rad}\left((b-a)^n \left(\frac{c^n - (b-a)^n}{ab}\right) abc^n\right) \\ &< 2nc^{n-1}\mathrm{rad}(abc), \end{aligned}$$

kus viimane võrratus saadi jällegi kasutades juba eelnevalt leitud tulemusi paaritu c korral.

Seega saime nii paaris kui ka paaritu c korral, et kehtib $\mathrm{rad}(A_nB_nC_n) < 2nc^{n-1}\mathrm{rad}(abc)$.

Võttes mõlemalt poolt logaritmi ja seejärel kasutades võrdust (16), saame

$$\begin{aligned}
\log(\mathrm{rad}(A_nB_nC_n)) &< (n-1)\log c + \log(\mathrm{rad}(abc)) + \log(2n) \\
&= n\log c - \log c + \log c - \frac{\varepsilon \log c}{1+\varepsilon} - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + \log(2n) \\
&= \log(c^n) - \frac{\varepsilon \log c}{1+\varepsilon} - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + \log(2n) \\
&= \log(c^n) - \frac{\varepsilon}{n(1+\varepsilon)}\log(c^n) - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + \log(2n) \\
&= \left(1 - \frac{\varepsilon}{(1+\varepsilon)n}\right)\log(c^n) - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + \log(2n) \\
&\leq \left(1 - \frac{\varepsilon}{(1+\varepsilon)n}\right)(\log C_n + n\log 2) - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + \log(2n) \\
&\leq \left(\frac{n+(n-1)\varepsilon}{(1+\varepsilon)n}\right)\log C_n - \frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} + 2n\log 2.
\end{aligned}$$

Eelviimane võrratus kehtib, sest arv $\left(1 - \frac{\varepsilon}{(1+\varepsilon)n}\right)$ on alati positiivne ning paaritu c korral $\log(c^n) = \log(C_n) \leq \log(C_n) + n\log 2$ ja paaris c korral $\log(c^n) = \log(2^nC_n) = \log(C_n) + n\log 2$. Viimase võrratuse saamiseks kasutati fakte, et $\log 2n < \log 2^n = n\log 2$ ja $\frac{n+(n-1)\varepsilon}{(1+\varepsilon)n} = (1 - \frac{\varepsilon}{(1+\varepsilon)n}) < 1$, sest $\varepsilon < (1+\varepsilon)n$.

Paneme tähele, et

$$\frac{\Phi_\varepsilon(a,b,c)}{1+\varepsilon} < \left(\frac{n+(n-1)\varepsilon}{(1+\varepsilon)n}\right)\log C_n + 2n\log 2 - \log(\mathrm{rad}(A_nB_nC_n))$$

ehk

$$\begin{aligned}
\Phi_\varepsilon(a,b,c) &\leq \left(\frac{n+(n-1)\varepsilon}{n}\right)\log C_n + 2n\log 2(1+\varepsilon) - \log(\mathrm{rad}(A_nB_nC_n))(1+\varepsilon) \\
&= \left(\frac{n+(n-1)\varepsilon}{n}\right)\left(\log C_n - \frac{n(1+\varepsilon)}{n+(n-1)\varepsilon}\log(\mathrm{rad}(A_nB_nC_n))\right) \\
&\quad + (1+\varepsilon)2n\log 2 \\
&< 2\left(\log C_n - \left(\frac{(1+\varepsilon)n}{n+(n-1)\varepsilon}\right)\log(\mathrm{rad}(A_nB_nC_n))\right) + 4n\log 2 \\
&= 2(\log C_n - (1+\varepsilon')\log \mathrm{rad}(A_nB_nC_n)) + 4n\log 2,
\end{aligned}$$

kus

$$\varepsilon' = \frac{(1+\varepsilon)n}{n+(n-1)\varepsilon} - 1 = \frac{n+\varepsilon n - n - n\varepsilon + \varepsilon}{n+(n-1)\varepsilon} = \frac{\varepsilon}{\varphi(m)+(\varphi(m)-1)\varepsilon}.$$

Teise võrratuse juures kasutasime eeldust, et $\varepsilon < 1$ ehk arv $1+\varepsilon < 2$ ning kehtib võrratus $\frac{n+(n-1)\varepsilon}{n} < 2$.

Kuna

$$\log C_n - (1+\varepsilon')\log(\mathrm{rad}(A_nB_nC_n) = \Phi_{\varepsilon'}(A_n, B_n, C_n) \leq K^*(m, \varepsilon'),$$

siis järelikult

$$\Phi_\varepsilon(a,b,c) < 2K^*(m,\varepsilon') + 4\varphi(m)\log 2.$$

Nüüd oleme näidanud, et $0 < \varepsilon < 1$ korral on funktsioon $\Phi_\varepsilon(a,b,c)$ ülalt tõkestatud ja seega on ka $e^{\Phi_\varepsilon(a,b,c)}$ ülalt tõkestatud, st leidub arv K nii, et $e^{\Phi_\varepsilon(a,b,c)} < K$. Nüüd võrduse 15 põhjal saame kirjutada

$$\Phi_\varepsilon(a,b,c) = \log \frac{c}{\mathrm{rad}(abc)^{1+\varepsilon}}$$

ehk

$$e^{\Phi_\varepsilon(a,b,c)} = \frac{c}{\mathrm{rad}(abc)^{1+\varepsilon}}$$

ehk

$$K \cdot \mathrm{rad}(abc)^{1+\varepsilon} > e^{\Phi_\varepsilon(a,b,c)}\mathrm{rad}(abc)^{1+\varepsilon} = c.$$

Saime nüüd võrratuse

$$c < K \cdot \mathrm{rad}(abc)^{1+\varepsilon}$$

ehk abc-hüpotees kehtib kui $0 < \varepsilon < 1$.

Olgu nüüd $0 < \varepsilon < 1$ ja $\varepsilon_u > \varepsilon$ ja leidugu K_ε nii, et kehtib $c < K_\varepsilon \cdot \mathrm{rad}(abc)^{1+\varepsilon}$. Siis $c < K_\varepsilon \cdot \mathrm{rad}(abc)^{1+\varepsilon} < K_\varepsilon \cdot \mathrm{rad}(abc)^{1+\varepsilon_u}$. Seega leidub ka ε_u korral $K_{\varepsilon_u} = K_\varepsilon$ nii, et kehtib abc-hüpotees.

Järelikult ka iga $\varepsilon_u \geq 1$ korral leidub $K_{\varepsilon_u} = \frac{1}{2}$ nii, et kehtib *abc*-hüpoteesi väide.

□

Kasutatud allikad

American Mathematical Society (i.a). *Beal Conjecture*. URL: https://www.ams.org/profession/prizes-awards/ams-supported/beal-conjecture (vaadatud 18.08.2022).

Baker, A. (1998). „Logarithmic forms and the abc-conjecture". *Number theory (Eger, 1996)*, lk. 37–44.

– (2004). „Experiments on the abc-conjecture". 65.3-4, lk. 253–260.

Ball, P. (2012). „Proof claimed for deep connection between primes". *Nature* 10.

Barlow, P. (1811). *An elementary investigation of the theory of numbers: With its application to the indeterminate and diophantine analysis, the analytical and geometrical division of the circle, and several other curious algebraical and arithmetical problems*. J. Johnson, lk. 144–145.

Bordg, A. (2021). „A Replication Crisis in Mathematics?" *Math. Intelligencer* 43.4, lk. 48–52.

Browkin, J. ja Brzeziński, J. (1994). „Some remarks on the *abc*-conjecture". *Math. Comp.* 62.206, lk. 931–939.

Browkin, J., Filaseta, M., Greaves, G. ja Schinzel, A. (1997). „Squarefree values of polynomials and the abc-conjecture". *Sieve Methods, Exponential Sums, and Their Applications to Number Theory* 237, lk. 65–85.

Castelvecchi, D. (2020). „Mathematical proof that rocked number theory will be published." *Nature* 580.7802, lk. 177–178.

Chen, C. (2013). „The paradox of the proof". *Project Wordsworth*.

Cochrane, T. ja Dressler, R. (1999). „Gaps between integers with the same prime factors". *Mathematics of computation* 68.225, lk. 395–401.

Croot, E., Li, R.-C. ja Zhu, H. J. (2004). „The abc conjecture and correctly rounded reciprocal square roots". *Theoret. Comput. Sci* 315.2-3, lk. 405–417.

Dabrowski, A. (1996). „On the Diophantine Equation $x! + A = y^2$". *Nieuw Arch. Wiskd.* 14, lk. 321–324.

de Smit, B. (2019). *ABC-triples*. URL: https://www.math.leidenuniv.nl/~desmit/abc/ (vaadatud 18.08.2022).

Elkies, N. D. (1991). „ABC implies Mordell". *Int. Math. Res. Not. IMRN* 1991.7, lk. 99–109.

Erdős, P. (1976). „Problems and results on consecutive integers". *Publ. Math. Debrecen* 23.1976, lk. 271–282.

Erdős, P. ja Szekeres, G. (1934). „Über die Anzahl der Abelschen Gruppen gegebener Ordnung und über ein verwandtes zahlentheoretisches Problem". *Acta Litt. Sci. Szeged* 7, lk. 95–102.

Euler, L. (1770). *Vollständige Anleitung zur Algebra*. Roy.Acad. Sci., St. Petersburg.

Faltings, G. (1983). „Endlichkeitssätze für abelsche Varietäten über Zahlkörpern". *Invent. Math.* 73.3, lk. 349–366.

Fesenko, I. (2015). „Arithmetic deformation theory via arithmetic fundamental groups and nonarchimedean theta-functions, notes on the work of Shinichi Mochizuki". *Eur. J. Math.* 1.3, lk. 405–440.

Goldfeld, D. (1996). „Beyond the Last Theorem". *Math Horizons* 4.1, lk. 26–34.

Golomb, S. W. (1970). „Powerful numbers". *Amer. Math. Monthly* 77, lk. 848–852.

Hall Jr., M. (1971). „The Diophantine equation $x^3 - y^2 = k$". *Computers in number theory*, lk. 173–198.

Hartnett, K. (2015). *Hope Rekindled for Perplexing Proof*. URL: https://www.quantamagazine.org/hope-rekindled-for-abc-proof-20151221/ (vaadatud 18.08.2022).

Klarreich, E. (2018). *Titans of Mathematics Clash Over Epic Proof of ABC Conjecture*. URL: https://www.quantamagazine.org/titans-of-mathematics-clash-over-epic-proof-of-abc-conjecture-20180920/ (vaadatud 18.08.2022).

Laan, V. ja Tart, L. (2020). *Arvuteooria loengukonspekt*. URL: http://kodu.ut.ee/~ltart/Arvuteooria_k2020/kon_2020.pdf (vaadatud 18.08.2022).

Langevin, M. (1992). „Partie sans facteur carré d'un produit d'entiers voisins". Teoses: *Approximations Diophantiennes et Nombres Transcendants. Diophantine Approximations and Transcendental Numbers*. de Gruyter, lk. 203–214.

– (1993). „Cas d'égalité pour le théorème de Mason et applications de la conjecture (abc)". *C. R. Acad. Sci.* 317.5, lk. 441–444.

Lebesgue, V.-A. (1843). „Théorèmes nouveaux sur l'équation indéterminée $x^5 + y^5 = az^5$". *J. Math. Pures Appl* 8, lk. 49–70.

– (1850). „Sur l'impossibilité, en nombres entiers, de l'équation $x^m = y^2 + I$". *Nouvelles annales de mathématiques : journal des candidats aux écoles polytechnique et normale*, lk. 178–181.

Luca, F. (2003). „On the diophantine equation $p^{x_1} - p^{x_2} = q^{y_1} - q^{y_2}$". *Indag. Math.*, lk. 207–222.

Lygeros, N. (2021). *Erdos-Woods numbers*. URL: https://oeis.org/A059756 (vaadatud 18.08.2022).

Masser, D. W. (1985). „Open problems". Teoses: *Proceedings of the symposium on Analytic Number Theory*. Imperial College.

Matson, R. D. (2017). *Brocard's Problem 4th Solution Search Utilizing Quadratic Residues*.

Mihăilescu, P. (2004). „Primary cyclotomic units and a proof of Catalans conjecture", lk. 167–195.

Mochizuki, S. (2018a). *Comments on the manuscript (2018-08 version) by Scholze-Stix concerning Inter-universal Teichmüller theory (IUTCH)*. URL: https://www.kurims.kyoto-u.ac.jp/~motizuki/Cmt2018-08.pdf (vaadatud 16.08.2022).

– (2018b). *Comments on the manuscript by Scholze-Stix concerning Inter-universal Teichmüller theory (IUTCH)*. URL: https://www.kurims.kyoto-u.ac.jp/~motizuki/Cmt2018-05.pdf (vaadatud 16.08.2022).

– (2019). *Report on discussions, held during the period March 15-20, 2018, concerning Inter-universal Teichmüller theory (IUTCH)*. URL: https://www.kurims.kyoto-u.ac.jp/~motizuki/Rpt2018.pdf (vaadatud 16.08.2022).

– (2021). „Inter-universal Teichmüller theory I: Construction of Hodge theaters". *Publ. Res. Inst. Math. Sci.* 57.1, lk. 3–207.

Mollin, R. A. ja Walsh, P. G. (1986). „On powerful numbers". *Int. J. Math. Math. Sci.* 9.4, lk. 801–806.

Mordell, L. J. (1922). *On the rational solutions of the indeterminate equation of the third and fourth degrees*. Proc. Cambridge Philos. Soc., lk. 179–192.

Nathanson, M. B. (2000). *Elementary methods in number theory*. Springer.

Nitaj, A. (2021). *The ABC Conjecture home page*. URL: https://nitaj.users.lmno.cnrs.fr/abc.html (vaadatud 18.08.2022).

Oesterlé, J. (1988). „Nouvelles approches du « théorème » de Fermat". Teoses: *Séminaire Bourbaki : volume 1987/88, exposés 686-699*. Astérisque 161-162. Bull. Soc. Math. France.

Overholt, M. (1993). „The Diophantine equation $n! + 1 = m^2$". *Bull. Lond. Math. Soc* 25.2, lk. 104–104.

Pasten, H. (2017). „Definability of Frobenius orbits and a result on rational distance sets". *Monatsh. Math.* 182.1, lk. 99–126.

Pickover, C. A. (1995). *Keys to infinity*. Wiley.

Revell, T. (2017). *Mathematician set to publish ABC proof almost no one understands*. URL: https://www.newscientist.com/article/2156623-mathematician-set-to-publish-abc-proof-almost-no-one-understands/ (vaadatud 16.08.2022).

Roth, K. F. (1955). „Rational approximations to algebraic numbers". *Mathematika* 2.1, lk. 1–20.

Schmidt, W. M. (2006). *Diophantine approximations and Diophantine equations*. Springer.

Scholze, P. (2021). *Review of "Inter-universal Teichmüller theory", parts I-V*. URL: https://zbmath.org/?format=complete&q=an:1465.14002 (vaadatud 16.08.2022).

Scholze, P. ja Stix, J. (2018). *Why abc is still a conjecture*. URL: https://ncatlab.org/nlab/files/why_abc_is_still_a_conjecture.pdf (vaadatud 16.08.2022).

Silverman, J. H. (1988). „Wieferich's criterion and the abc-conjecture". *J. Number Theory* 30.2, lk. 226–237.

Sloane, N. J. A. (2021). *Wieferich primes*. URL: https://oeis.org/A001220 (vaadatud 15.08.2021).

Stewart, C. L. ja Tijdeman, R. (1986). „On the œsterlé-Masser conjecture". *Monatsh. Math.* 102.3, lk. 251–257.

Stewart, C. L. ja Yu, K. (1991). „On the abc conjecture". *Math. Ann* 291.1, lk. 225–230.

Stewart, C. L. ja Yu, K. (2001). „On the abc conjecture, II". *Duke Math. J.* 108.1, lk. 169 –181.

Szpiro, L. (2007). „Finiteness Theorems for Dynamical Systems". Teoses: *Conference on L-functions and Automorphic Forms.*

Taylor, R. ja Wiles, A. (1995). „Ring-Theoretic Properties of Certain Hecke Algebras". *Ann. of Math.* 141.3, lk. 553–572.

Walsh, P. G. (2012). „On a conjecture of Schinzel and Tijdeman". Teoses: *Number theory in progress.* De Gruyter, lk. 577–582.

Wieferich, A. (1909). „Zum letzten Fermatschen Theorem." *J. für die Reine und Angew. Math.* 1909.136, lk. 293–302.

Wiles, A. (1995). „Modular elliptic curves and Fermat's last theorem". *Ann. of Math.* 141.3, lk. 443–551.

Wright, T. (2016). *Trolling Euclid: An Irreverent Guide to Nine of Mathematics' Most Important Problems.* CreateSpace Independent Publishing Platform.

Lihtlitsents lõputöö reprodutseerimiseks ja üldsusele kättesaadavaks tegemiseks

Mina, Jon Hendrik Aruväli,

1. Annan Tartu Ülikoolile tasuta loa (lihtlitsentsi) minu loodud teose „*abc*-hüpoteesist ja selle järeldustest", mille juhendaja on Lauri Tart, reprodutseerimiseks eesmärgiga seda säilitada, sealhulgas lisada digitaalarhiivi DSpace kuni autoriõiguse kehtivuse lõppemiseni.

2. Annan Tartu Ülikoolile loa teha punktis 1 nimetatud teos üldsusele kättesaadavaks Tartu Ülikooli veebikeskkonna, sealhulgas digitaalarhiivi DSpace kaudu Creative Commonsi litsentsiga CC BY NC ND 3.0, mis lubab autorile viidates teost reprodutseerida, levitada ja üldsusele suunata ning keelab luua tuletatud teost ja kasutada teost ärieesmärgil, kuni autoriõiguse kehtivuse lõppemiseni.

3. Olen teadlik, et punktides 1 ja 2 nimetatud õigused jäävad alles ka autorile.

4. Kinnitan, et lihtlitsentsi andmisega ei riku ma teiste isikute intellektuaalomandi ega isikuandmete kaitse õigusaktidest tulenevaid õigusi.

Jon Hendrik Aruväli
18.08.2022