Fermat'n suuri lause

Ilari Kinnunen

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Syksy 2016

Tiivistelmä: Ilari Kinnunen, *Fermat'n suuri lause* (engl. *Fermat's Last Theorem*), matematiikan pro gradu -tutkielma, 52 s., Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, syksy 2016.

Tässä tutkielmassa perehdytään Pierre de Fermat'n 1600-luvulla esittämään Fermat'n suureen lauseeseen. Fermat'n suuri lause on lukuteoriaan liittyvä yksinkertaisen näköinen väite, jonka perustaa on luotu jo n. 2000 vuotta ennen Fermat'n syntymää. Fermat'n suuri lause matemaattisesti muotoiltuna on: yhtälöllä

$$x^n + y^n = z^n, (x, y, z) \in \mathbb{N}, n \in \mathbb{N}$$

ei ole kokonaislukuratkaisua, kun $n \geq 3$ ja $x > 0, y > 0, z > 0$.

Fermat'n suuri lause on kiinnostava sen takia, että Fermat väitti keksineensä lauseelleen "ihmeellisen" todistuksen, jota hän ei kuitenkaan milloinkaan julkaissut. Monet tunnetut ja tuntemattomammatkin matemaatikot ovat vuosien varrella yrittäneet löytää lauseelle pitävän todistuksen, mutta se osoittautui erittäin haastavaksi. Vasta 1990-luvulla brittiläinen matemaatikko Andrew Wiles keksi pitävän todistuksen lauseelle. Ennen Wilesiä oli lause saatu todistettua jo melkein kaikilla eksponentin arvoilla, mutta Wiles sai todistettua viimeisetkin arvot ja sai ansaitusti itselleen kunnian lauseen todistuksesta.

Tutkielmassa todistetaan lause eksponentin arvolla 4 käyttämällä hyödyksi muun muassa primitiivistä ratkaisua Pythagoraan lauseelle sekä Fermat'n itse keksimää äärettömän laskeutumisen menetelmää. Todistetusti Fermat itsekin todisti tämän tapauksen. Äärettömän laskeutumisen menetelmää muutkin matemaatikot hyödynsivät todistaessaan lauseen muita tapauksia, esimerkiksi tapauksen $n = 3$ todistuksessa Euler hyödynsi samaa menetelmää. Kyseinen tapaus todistetaan tutkielmassa mukaillen juuri Eulerin 1770-luvulla julkaisemaa todistusta.

Tutkielmassa todistetaan myös tapaus $n = 5$, mikä on hieman teknisempi kuin tapaukset $n = 4$ ja $n = 3$. Todistuksessa tarvitaan apuna hieman algebraa ja erityisesti kvadraattisia lukuja. Lopuksi tutustutaan hieman *abc*-konjektuuriin, joka oikeaksi todistettuna antaisi seurauksena todistuksen Fermat'n suurelle lauseelle, kun $n > 6$.

Sisältö

Johdanto

Tämän kirjoitelman tarkoituksena on tutustua Fermat'n suuren lauseen historiaan ja sen todistamiseen. Fermat'n suuren lauseen alkujuuret ovat jo Babylonian ajassa eli noin 2000–600 eKr. Noin kaksi tuhatta vuotta myöhemmin Pierre de Fermat esitti ongelman nykyisessä muodossaan. Fermat'n suuressa lauseessa yhdistyy siis jo antiikin aikaan Pythagoraan luoman matematiikan perusteet ja nykypäivän matematiikan edistyneimmät käsitteet. Fermat'n suuri lause matemaattisesti muotoiltuna on: yhtälöllä

$$x^n + y^n = z^n, (x, y, z) \in \mathbb{N}, n \in \mathbb{N}$$

ei ole kokonaislukuratkaisua, kun $n \geq 3$ ja $x > 0, y > 0, z > 0$.

Fermat väitti keksineensä lauseelle ihmeellisen todistuksen, jota hän ei kuitenkaan julkaissut missään, koska se ei mahtunut Diofantoksen kirjoittaman Arithmetica-kirjan marginaaliin. Vielä tänäkään päivänä ei tiedetä, onko Fermat'lla todella ollut todistus kyseiselle lauseelle. Tiedetään, että Fermat on todistanut lauseen ainakin tapauksessa $n = 4$. Fermat jätti jälkeensä useita erilaisia väitteitä, joiden todistuksia hän ei julkaissut. Näitä monet matemaatikot ovat yrittäneet todistaa ja suurimman osan todistaminen kävikin suhteellisen helposti. Fermat'n suureksi lauseeksi nimetyn ongelman todistaminen osoittautui kuitenkin erittäin haastavaksi.

Fermat'n suurta lausetta todistettiin aluksi pala kerrallaan melko hitaasti edeten. Muun muassa Leonhard Euler todisti lauseen tapauksissa $n = 4$ ja $n = 3$. Tämän jälkeen siitä todistettiin tapaus $n = 5$ ja jonkin ajan päästä oli lause todistettu jo kaikilla eksponenteilla $n < 100$ ja niiden monikerroilla. Yleistä todistusta ei kuitenkaan vielä löydetty. Lopulta monien epäonnistuneiden yrittäjien jälkeen brittiläinen matemaatikko Andrew Wiles sai todistettua kokonaisuudessaan Fermat'n suuren lauseen. Wilesin todistus pohjautui 1900-luvulla kehitettyihin matematiikan menetelmiin, joita Fermat aikanaan tuskin tunsi. Monet ihmiset ovatkin yrittäneet löytää lauseelle yksinkertaisempaa todistusta, jonka Fermatkin olisi voinut aikanaan tuntea. Sellaista ei kuitenkaan ole vielä löytynyt, siksi useimmat matemaatikot ja tiedehistorioitsijat eivät usko Fermat'n itse todistaneen lausettaan kaikilla $n \in N, n \geq 3$.

Fermat'n suuren lauseen todistaminen on kehittänyt merkittävästi monia matematiikan osa-alueita ja se on antanut paljon uusia työkaluja erilaisten matemaattisten ongelmien ratkaisuun. Vaikka lause itsessään on melko hyödytön ja huonosti sovellettavissa mihinkään, on sen todistaminen vienyt matematiikkaa erittäin paljon eteenpäin useiden tunnettujen matemaatikkojen yrittäessä ratkaista tätä kuuluisaa ongelmaa.

Tämän tutkielman ensimmäisessä luvussa esitellään historiaa Fermat'n suuren lauseen kehittymisestä nykyiseen muotoonsa, Fermatista ja lauseen todistusyrityksistä. Samalla tutustutaan hieman Wilesin lopulliseen todistukseen ja siinä käytettyihin

menetelmiin. Ensimmäisen luvun päälähteinä ovat Simon Singhin teos *Fermat'n viimeinen teoreema* [**22**] ja Amir Aczelin teos *Fermat'n teoreema* [**1**]. Luvuissa 2, 3 ja 4 todistetaan lause tapauksissa $n = 4$, $n = 3$ ja $n = 5$. Tapauksen $n = 4$ todistus pohjautuu pääasiassa Ribenboimin teokseen *Fermat's Last Theorem For Amateurs* [**21**]. Lukujen 3 ja 4 todistukset pohjautuvat pääasiassa Larry Freemanin kirjoittamaan *Fermat's Last Theorem*-blogiin [**8**] ja [**9**] sekä lähteisiin [**21**] ja [**6**].

Tutkielman viimeisessä luvussa tutustutaan Josph Oesterlén ja David Masserin vuonna 1985 esittämään *abc*-konjektuuriin. Mikäli kyseinen konjektuuri saadaan osoitettua todeksi, sitä soveltamalla saadaan helposti todistettua Fermat'n suuri lause tapauksissa $n > 6$. Tämän luvun päälähteenä on käytetty Marko Lamminsalon tutkielmaa [**15**].

LUKU 1

Fermat'n suuren lauseen historiaa

1.1. Alkujuuret

Fermat'n suuren lauseen alkujuuret ovat pronssikauden aikaisessa Mesopotamiassa, hedelmällisen puolikuun alueella Eufratin ja Tigrisin välissä, joka tunnetaan myös Kaksoisvirran maana. Nykyään alue kuuluu Irakiin. Mesopotamiassa kukoisti noin vuodesta 2000 eKr. noin vuoteen 600 eKr. kulttuuri, jota kutsutaan Babylonian ajaksi. Tämä aikakausi tunnetaan monien keksintöjen aikakautena. Tuolloin muun muassa kehitettiin kirjoitustaito ja keksittiin pyörä. Babylonian ajan tiedemiehet huomasivat ympyrän kaaren pituuden ja halkaisijan välisen yhteyden, laskivat pinta-aloja ja tilavuuksia [**1**, s. 22–23].

Babylonian arkipäivään kuuluivat myös lukujen neliöt. Niiden katsottiin edustavan vaurautta. Maanviljelijän varallisuus riippuu sadon suuruudesta. Sadon suuruus taas riippuu siitä, kuinka suuri on pellon pinta-ala. Suorakulmaisen pellon pinta-ala lasketaan kertomalla pellon pituus sen leveydellä. Jos pellon leveys a ja pituus b sattuvat olemaan yhtä suuret, niin tällöin pinta-alaksi tulee neliö a^2. Babylonialaiset olivat kiinnostuneet kokonaislukujen neliöistä enemmänkin. He halusivat tietää, kuinka kokonaislukujen neliöt voidaan jakaa toisten kokonaislukujen neliöiksi [**1**, s. 23–24]. Siihen aikaan heitä on kiinnostanut esimerkiksi seuraavaa tilannetta vastaava tieto: Jos talonpojalla oli pelto, jonka kummankin sivun pituus oli 10 mittayksikköä eli pellon ala oli 100 neliötä. Niin sen hän saattoi vaihtaa kahteen peltoon, joiden sivujen pituudet olivat 6 ja 8 mittayksikköä. Tällöin näiden kahden pellon pinta-alat olivat 36 ja 64 neliötä. Tämä tieto oli tärkeä, kun maiden jaosta seuranneita ongelmia ratkaistiin. Nykyään kirjoittaisimme vastaavan ongelman lyhyesti $10^2 = 8^2+6^2$. Näitä lukuja kutsutaan Pythagoraan luvuiksi, vaikka 4000 vuotta vanhojen savitaulujen avulla tiedämmekin, että Babyloniassa on tiedetty Pythagoraan lukujen ominaisuudet jo ennen Pythagoraan syntymistä [**1**, s. 24].

Babylonialaiset tekivät aikanaan paljon erilaisia taulukoita nuolenpääkirjoituksella savitauluihin. Näitä tauluja on säilynyt paljon meidän päiviimme asti. Eräs näistä tauluista on luettelonimeltään Plimpton 322. Siinä on viisitoista kolmen luvun ryhmää, joista jokaisella lukuryhmällä on se ominaisuus, että ryhmän ensimmäinen luku on kahden seuraavan luvun summa. Savitauluissa on siis viisitoista erilaista Pythagoraan lukujen ryhmää. Tutkijat ovat arvelleet, että taulujen avulla oli kätevää laskea käytännön laskuja, kuten murto-osia. Luultavasti tauluja on käytetty myös opetusvälineinä. Babylonialaiset eivät yrittäneet kehittää tällaisille ongelmille yleisiä ratkaisumenetelmiä, vaan he käyttivät hyväksi valmiiksi laskettuja lukuja [**1**, s. 25–26].

Viisisataa vuotta ennen ajan laskumme alkua elänyt Pythagoras Samoslainen oli yksi matematiikan vaikutusvaltaisimpia ihmisiä. Pythagoras hankki matemaattiset taitonsa matkustelemalla ympäri antiikin maailmaa [**22**, s. 27–28]. Hän matkusti muun muassa Egyptissä ja Babyloniassa [**1**, s. 26]. Todennäköisimmin Pythagoras

oppi juuri egyptiläisiltä ja babylonialaisilta matematiikan tutkimusmenetelmiä. Näissä molemmissa maissa oli siirrytty yksinkertaisista laskuista vaativiin laskutoimituksiin, joiden avulla esimerkiksi suunniteltiin ja pystytettiin taidokkaita rakennelmia. Pythagoras huomasi, että egyptiläiset ja babylonialaiset tekivät jokaisen laskutoimituksen tietyllä kaavalla. Näiden kaavojen avulla saatiin aina oikea vastaus. Kukaan ei vaivautunut tutkimaan tarkemmin laskujen perustana olevaa logiikkaa [**22**, s. 28].

Kreikkaan palattuaan Pythagoras perusti veljeskunnan, johon kuului kuusisataa jäsentä. Opiskelun lisäksi he tekivät omaakin tutkimustyötä. Pythagoraan koulukunnan omaksuma elämänkatsomus muutti matematiikan kehitystä. Veljeskunta oli salamyhkäinen ja hengellinen yhteisö, joka piti matemaattiset keksinnöt omana tietonaan [**22**, s. 30–31]. Veljeskunta tutki paljon lukuja ja luontoa yhdistäviä tekijöitä [**22**, s. 35]. Keskeisin niistä on tämä sääntö, joka sai nimensä keksijältään, Pythagoraalta. Pythagoraan lause antaa yhtälön, joka pätee kaikkiin suorakulmaisiin kolmioihin ja se myös määrittelee suorakulmaisen kolmion. Vaikka babylonialaiset ja kiinalaisetkin olivat käyttäneet Pythagoraan lausetta paljon ennen Pythagorasta, annetaan lauseesta kunnia Pythagoraalle, koska hän oli ensimmäinen, joka todisti lauseen [**22**, s. 40–41].

Vuonna 510 eKr. puhjenneen mellakan seurauksena Pythagoraan veljeskunta hajosi ja Pythagoras sai surmansa. Henkiin jääneiden jäsenten oli vainojen seuraksena paettava ulkomaille, jossa he alkoivat levittää matematiikan sanomaansa perustamalla kouluja ja opettamalla loogisen todistuksen metodia [**22**, s. 49–50]. Veljeskunnan hajoamisen jälkeen matematiikan opiskelun painopiste oli siirtynyt Kreikan Krotonista Aleksandrian kaupunkiin Egyptiin. Aleksandriaan perustettu yliopisto ja etenkin kaupungin suuri kirjasto veti puoleensa matemaatikkoja ja muita älymystön edustajia [**22**, s. 70].

Vuoden 330 eKr. tienoilla syntyi yksi aikansa merkittävimmistä matemaatikoista. Eukleides omisti suuren osan elämästään historian menestyksekkäimmän oppikirjan Alkeita-kirjan kirjoittamiseen. Eukleideen Alkeita koostuu kolmestatoista kirjasta, joista kaksi kirjaa on omistettu kokonaan pythagoralaisen veljeskunnan työlle [**22**, s. 71]. Vaikka Eukleides oli selvästikin kiinnostunut lukuteoriasta, hänen suurin mielenkiinnon kohteensa oli geometria. Eukleideen Alkeita tarjosi sellaisen tietopaketin, että sitä käytettiin geometrian oppikirjana kouluissa ja yliopistoissa seuraavat kaksituhatta vuotta ja käytetään yhä edelleenkin [**22**, s. 76].

Fermat'n suuren lauseen syntyyn on vaikuttanut merkittävästi Aleksandriassa eläneen matemaatikko Diofantos Aleksandrialaisen (n. 250 jKr.) kokoama matematiikan suurteos Arithmetica. Tämä teos koostui kolmestatoista kirjasta, joista kuitenkin vain kuusi selvisi keskiajan ylitse renessanssin matemaatikkojen, mm. Pierre de Fermat'n, käsiin [**22**, s. 77]. 1300 vuotta Diofantoksen aikojen jälkeen Euroopassa alkoi renessanssi ja uuden ajan alku. Euroopassa alettiin janota tietoa, joten katseet kääntyivät antiikin kulttuuriin. Kaikkea antiikin kirjallisuutta käännettiin latinaksi, joka oli tuolloin oppineiden yhteinen kieli [**1**, s. 537]. Myös antiikin aikaisia kirjoja käännettiin latinaksi. Näin ollen myös Fermat'lla oli käytössään latinankielinen versio Diofantoksen kirjoittamasta Arithmeticasta. Sen oli kääntänyt Ranskan oppineimmaksi mieheksi mainittu Claude Gaspar Bachet de Méziriac, jonka intohimona olivat erilaiset

matemaattiset pulmat, joita Arithmeticakin sisälsi [**22**, s. 83]. Tässä Bachetin kääntämässä kirjassa mainittiin Diofantoksen Probleemi 8, joka sai Fermat'n kirjoittamaan kirjan marginaaliin kuuluisan reunahuomautuksensa [**1**, s. 44–45].

1.2. Pierre de Fermat (1601–1665)

Pierre de Fermat syntyi 20.8.1601 Ranskan lounaisosassa sijaitsevassa Beaumont-de-Lomagnen kaupungissa [**22**, s. 59]. Fermat'n isä Dominique Fermat oli Beamountin toinen konsuli, rikas nahkakauppias ja äiti juristiperheen tytär Claire de Long [**2**, s. 59]. Vanhempien varallisuuden myötä Pierren oli mahdollista saada opetusta Grandselven fransiskaaniluostarissa ja sen jälkeen opiskella lakioppia Toulousen yliopistossa [**22**, s. 59]. Fermat'n opiskeluajoilta on harvinaisen vähän muistoja, mutta ilmeisesti hänen opintonsa ovat sujuneet loistavasti [**2**, s. 59]. Perheensä painostamana Fermat alkoi valtion virkamieheksi ja hänet nimitettiin Toulousen oikeusistuimen jäseneksi 30-vuotiaana [**1**, s. 16]. Vuonna 1648 hänet ylennettiin kuninkaan neuvosmieheksi Toulouse'n paikalliseen parlamenttiin [**1**, s. 17]. Fermat oli työssään rauhallinen ja oikeamielinen virkamies, joka toteutti velvollisuutensa harkiten ja oikeudentuntoisesti. Hän hoiti neuvosmiehen virkaa kuolemaansa, eli vuoteen 1665 asti [**12**, s. 27].

Leipätyönsä ohella Fermat oli erittäin oppinut, niin matematiikassa kuin kielissäkin [**12**, s. 27]. Matematiikka oli kuitenkin hänen lempiaiheensa ja esimerkiksi E.T.Bell (1963 s. 58) kutsuukin häntä "harrastelijain kuninkaaksi". Fermat'n aikaan Ranskan tuomareiden oletettiin välttävän seurustelua tavallisten kansalaisten kanssa [**22**, s. 82]. Tämän eristäytymisen tarkoituksena oli varmistaa, ettei tuomareita voitaisi lahjoa eikä kiristää [**1**, s. 17]. Fermat'n intohimoa matematiikkaa kohtaan selitetäänkin sillä, että hän halusi harrastaa jotain virkavelvollisuuksien vastapainoksi ja näin ollen Toulousen seurapiireistä eristäytyneellä Fermat'lla oli vapaa-ajallaan runsaasti aikaa keskittyä matematiikkaan [**1**, s. 17].

Matematiikassa Fermat oli salamyhkäinen omia tutkimuksiaan kohtaan, eikä paljastanut muille omia todistuksiaan ja tutkimustuloksiaan. Hän saattoi lähettää omia teoreemojaan toisille matemaatikoille, mutta ei paljastanut niiden todistuksia [**22**, s. 64]. Fermat'n töiden selvittämiseksi onkin jouduttu turvautumaan vain aikalaisten saamiin kirjeisiin [**12**, s. 29]. Eräs näistä on Fermat'ia parikymmentä vuotta nuorempi Blaise Pascal (1623–1662), jonka kanssa Fermat kävi kirjeenvaihtoa todennäköisyyslaskentaan liittyvistä asioista. Pascal ja Fermat muovailivatkin todennäköisyyslaskennan ensimmäisiä todistuksia ja perusteita [**12**, s. 28]. Kiinnostus todennäköisyyslaskentaa kohtaan alkoi ammattipeluri Chevalier de Méré'n Pascalille esittämästä uhkapeliin liittyvästä ongelmasta [**22**, s. 65].

Todennäköisyyslaskennan lisäksi Fermat oli luomassa toisen matematiikan alan, differentiaali- ja integraalilaskennan, perusteita. Tämän alan varsinaisina kehittäjinä on yleisesti pidetty englantilaista Isaac Newtonia (1642–1727) ja saksalaista Gottfrid Wilhelm Leibnizia (1646–1716). Myöhemmin on kuitenkin tullut ilmi, että Newton oli kirjoittanut kehittäneensä differentiaali- ja integraalilaskennan Fermat'n ääriarvomenetelmän pohjalta [**22**, s.68–69]. Fermat sovelsi keksimäänsä ääriarvomenetelmää valo-oppiin. Fermat keksi nk. "vähimmän ajan periaatteen", joka tarkoittaa sitä, että valonsäde kulkee pisteestä A pisteeseen B eri väliaineissa nopeinta mahdollista tietä. Eli kuljettaessa A:sta B:hen kuluva aika on ääriarvo. Tästä periaatteesta Fermat johti fysiikassa keskeisiä olevat heijastumis- ja taittumislait [**2**, s. 65].

Fermat keksi myös analyyttisen geometrian yhdessä René Descartes'in (1596–1650) kanssa toisistaan riippumatta [**2**, s. 58]. Fermat oli ensimmäinen, joka sovelsi analyyttistä geometriaa kolmiulotteiseen avaruuteen [**2**, s. 65]. Vaikka Fermat vaikutti useammallakin matematiikan alalla merkittävästi, muistetaan hänet nykypäivänä parhaiten lukuteorian saavutuksistaan. Tämä johtunee siitä, että muilla aloilla hänen työnsä olivat niiden ensiaskelia, jotka jäivät aikojen saatossa uusien tulosten varjoon. Lukuteorian alalla Fermat esitti paljon sellaista, jotka työllistivät matemaatikkoja vuosisatoja ja vielä nykypäivänäkin [**12**, s. 28–29].

Fermat oli ihastunut kokonaislukujen kauneuteen ja mielekkyyteen. Niinpä hän kehitti monia kokonaislukuihin liittyviä teorioita. Yhdessä niistä hän väittää, että muotoa $2^{(2^n)}+1$, $n \in \mathbb{Z}$ olevat luvut ovat alkulukuja [**1**, s. 19]. Tässä Fermat kuitenkin erehtyi. Kuitenkaan Fermat ei ole missään vaiheessa väittänyt todistaneensa arvaustaan. Edellä olevaa muotoa olevia alkulukuja kutsutaan Fermat'n alkuluvuiksi [**2**, s. 67–68]. Leonhard Euler (1707–1783) todisti vuonna 1732, että kaikki muotoa $2^{(2^n)}+1$ olevat luvut eivät ole alkulukuja [**1**, s. 54]. Yksi Fermat'n monista lukuteorian keksinnöistä on nk. "Fermat'n pieni lause": Jos n on mielivaltainen kokonaisluku ja p mielivaltainen alkuluku, niin tällöin luku $n^p - n$, on jaollinen p:llä. Tavoilleen uskollisena Fermat ei todistanut tätä "pientä lausettaankaan". Ensimmäisenä sen todisti Leibniz, jonka todistus on todennäköisesti peräisin ennen vuotta 1683 [**2**, s. 69].

Yksi Fermat'n hienoimmista huomioista on eräs alkulukuja koskeva lause. Fermat väitti, että muotoa $4n+1$ olevat alkuluvut voidaan esittää kahden neliöluvun summana yhdellä ja vain yhdellä tavalla, kun taas muotoa $4n-1$ olevia lukuja ei koskaan voida kirjoittaa kahden neliöluvun summana. Tähänkään Fermat ei ollut todistustaan jättänyt. Niinpä Euler otti tehtäväkseen todistaa kyseisen tuloksen, ja vuonna 1749, seitsemän vuoden uurastuksen jälkeen, hänen onnistui lopultakin todistaa tämä tulos [**22**, s. 91 ja 94].

On ilmennyt, että tutkiessaan Arithmetican toista kirjaa Fermat on törmännyt moniin Pythagoraan lauseeseen liittyviin huomioihin, ongelmiin ja ratkaisuihin [**22**, s. 87]. Vuonna 1637 Fermat oli kirjoittanut Arithmetican marginaaliin lukujen neliöiden summaa koskevien kirjoitusten kohdalle huomautuksen: *Cubem autem in duos cubos, aut quadratoquadratum in duos quaratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere. Cuius rei demonstrationem mirabilem sane detexi hanc margins exiguitas non caperet* [**22**, s. 89]. Eli "Toisaalta on mahdotonta jakaa kuutiota kahdeksi kuutioksi, neljättä potenssia kahdeksi neljänneksi potenssiksi tai yleisemmin mitään kahta korkeampaa potenssia kahdeksi saman asteen potenssiksi. Olen keksinyt siihen todella ihmeellisen todistuksen, jolle tämä marginaali ei kuitenkaan riitä" [**1**, s. 19–20]. Näin ilmeni, että Fermat oli tutkinut yhtälöä $x^n + y^n = z^n$, $n \in \mathbb{N}$ ja väitti, ettei tällä yhtälöllä ole kokonaislukuratkaisua, kun $n \geq 3$ ja $x > 0, y > 0, z > 0$ [**12**, s. 26].

Fermat ei itse julkistanut saamiaan tuloksiaan missään, niinpä hänen kuoltuaan oli vaarana, että kaikki hänen aikaansaannoksensa jäisivät unholaan. Pelastukseksi tuli kuitenkin Fermat'n vanhin poika Clément Samuel de Fermat, joka tutki isänsä kuoltua Pierreltä jääneitä papereita ja hän huomasi Arithmetican leveissä marginaaleissa olevia isänsä kirjoittamia päättelyitä ja merkintöjä. Fermat'lle riitti, että hän

itse vakuuttui ongelmien ratkaisusta, eikä hän siten vaivautunut kirjoittamaan muistiin ongelmien lopullisia todistuksia. Fermat'n marginaaleihin kirjoittamistaan päättelyistä tuli Fermat'n nerokkaiden päätelmien niukka todistuskappale. Onkin täysin Clément Samuelin ansiota, että nykyään tiedämme yhtään mitään Fermat'n tekemistä uurastuksista ja läpimurroista lukuteorian alalla [**22**, s. 84–85, 90–91].

Clément Samuelin vuonna 1670 julkaisema kirja oli Arithmetica varustettuna Pierre de Fermat'n huomioilla. Fermat'n tekemiä huomioita on kirjassa yhteensä 48 kappaletta [**22**, s.91]. Fermat'n jälkeen matemaatikot alkoivat todistella Fermat'n tekemiä teoreemoja tarkasti. Tämä oli tärkeää, koska ennen kuin teoreemoja voitiin käyttää, oli ne todistettava täsmällisesti. Teoreemoja käytetään usein seuraavan teoreeman todistamiseen, siten, jos aiemman teoreeman todistuksessa onkin virhe, ei myöskään seuraavien teoreemojen todistukset pätisi. Tällöin voisi käydä todella hullusti ja voisi saada täysin vääriäkin johtopäätöksiä [**22**, s. 94–95].

1.3. Fermat'n jälkeen

Kaikki muut Fermat'n teoreemat oli osoitettu oikeiksi tai vääriksi viimeistään 1800-luvun alkupuolella [**1**, s. 20]. Vain yksi oli enää todistamatta. Se oli edellä mainittu Fermat'n suuri lause, jota kutsutaan myös Fermat'n viimeiseksi teoreemaksi juuri siitä syystä, että se oli viimeinen Fermat'n lause, jota ei ollut saatu todistettua. Sitä yritettiin todistaa yli kolmesataa vuotta, minkä vuoksi se tulikin tunnetuksi matematiikan haastavimpana ongelmana, johon matemaatikot yksi toisensa jälkeen tarttuivat lähes tuloksetta [**22**, s. 95–96].

Tiedetään, että Fermat'n onnistui osoittaa suuri lauseensa todeksi ainakin silloin, kun eksponentti $n = 4$ ja $n = 3$. Myös Leonhard Euler osoitti saman eli sen, että yhtälölle ei ole kokonaislukuratkaisua, kun eksponentti on 3 tai 4 [**1**, s. 55–56]. Euler oli tunnetusti ensimmäinen henkilö, joka pääsi Fermat'n lauseen todistuksessa eteenpäin [**12**, s. 29]. Eulerin todistus oli valtava edistysaskel, mutta kuitenkaan Euler ei pystynyt yleistämään todistustaan Fermat'n suuren lauseen muihin tapauksiin [**22**, s.116].

Seuraava edistysaskel lauseen todistamisessa tapahtui Ranskan Sophie Germainin (1776–1831) ansiosta. Naismatemaatikot eivät olleet Germainin aikaan kovin suuressa arvossa. Esimerkiksi Ranskaan vuonna 1794 avattu huippuyliopisto oli vain miehille, joten Germainin joutui opiskelemaan yliopistossa valehenkilöllisyyden avulla. Germainin lahjakkuuden vuoksi hänen todellinen henkilöllisyytensä kuitenkin paljastui yliopiston opettajalle Joseph-Louis Lagrangelle. Lagrangesta tuli Germainin ohjaaja ja opettaja. Germain kiinnostui erityisesti lukuteoriasta ja alkoi tutkia myös Fermat'n suurta lausetta. Germain omaksui uuden strategian Fermat'n lauseen todistamiseen. Hänen ensisijainen tavoitteensa oli saada tuloksia monista eri tapauksista yhtä aikaa, sen sijaan, että olisi todistanut jonkin Fermat'n lauseen yksittäistapauksen [**22**, s. 132–137].

Germain halusi keskustella ideoistaan jonkun toisen matemaatikon kanssa, joten hän päätti mennä konsultoimaan maailman suurinta lukuteoreetikkoa Carl Friedrich Gaussia (1777–1855). Germain hahmotteli Gaussille päättelyn, joka kohdistui tietyn tyyppisiin alkulukuihin. Sellaisiin alkulukuihin p, että myös $2p + 1$ on alkuluku. Tämän tyyppinen alkuluku on esimerkiksi luku 5, koska myös 11 $(2 \cdot 5 + 1)$ on alkuluku. Näihin alkulukuja vastaaviin n:n arvoihin Germain sovelsi tyylikästä perustelua joka

osoitti, ettei yhtälöllä $x^n + y^n = z^n$ todennäköisesti ole lainkaan kokonaislukuratkaisuja. Jos ratkaisuja olisi ollut, niin tällöin joko x, y tai z olisi jaollinen n:llä, ja se asettaisi tiukkoja rajoituksia mahdollisille luvuille [**22**, s. 136–137]. Gauss itse ei ollut innostunut Fermat'n lauseen todistamisesta. Saattoi olla, että hän tiesi, kuinka vaikea se oli todistaa ja kieltäytyi siitä siksi. Gauss kehitti merkittävästi funktioteoriaksi kutsuttua matematiikan alaa. Juuri tämä funktioteoria oli ratkaisevassa asemassa, kun Fermat'n lause saatiin viimein todistettua [**1**, s. 64–65].

Germainin menetelmän ansiosta Peter Gustav Lejeune-Dirichlet (1805–1859) ja Adrien-Marie Legendre (1752–1833) onnistuivat toisistaan tietämättä todistamaan, ettei yhtälöllä ole ratkaisuja tapauksessa $n = 5$ [**22**, s. 137–138]. Legendre oli todistanut kyseisen tapauksen kaksi vuotta Dirichlet'n jälkeen, mutta ei ollut silloin tiennyt Dirichlet'n todistuksesta [**1**, s. 71]. Vuonna 1847 Ranskan tiedeakatemian kokouksessa matemaatikko Gabriel Lamé (1795–1870) ilmoitti löytäneensä Fermat'n suurelle lauseelle täydellisen todistuksen. Lamé oli pari vuotta aikaisemmin todistanut lauseen tapauksessa $n = 7$ [**1**, s. 77]. Augustin Louis Cauchy (1789–1857) kannatti Lamén ratkaisua [**12**, s. 29]. Lamé käytti todistuksessaan menetelmää, jossa hän jakoi ensin kompleksilukuja käyttäen Fermat'n yhtälön vasemman puolen tekijöihinsä. Lamé myönsi, ettei idea tästä ollut yksin hänen, vaan Joseph Liouville (1809–1882) oli sitä hänelle ehdottanut. Liouville kuitenkin huomautti, ettei Lamé ollut todistanut suurta lausetta, koska Liouvillen ehdottama tekijöihin jako ei ollut yksikäsitteinen. Näin ollen menetelmä ei riittänyt lauseen todistamiseen [**1**, s. 77–78].

Myös saksalainen matemaatikko Ernst Eduard Kummer (1810–1893) käytti tekijöihin jakoa Fermat'n suuren lauseen todistuksessa [**1**, s. 78]. Kummer otti käyttöönsä niin sanotut ideaaliluvut. Hän osoitti lauseen oikeaksi, kun p on ns. säännöllinen alkuluku. Lukua 100 pienemmistä alkuluvuista vain luvut 37, 59 ja 67 ovat epäsäännöllisiä lukuja [**12**, s. 29]. Myös näille kolmelle epäsäännölliselle alkuluvulle Kummer keksi todistuksen, mutta ei pystynyt yleistämään todistuksiaan kaikille epäsäännöllisille alkuluvuille. Kummerin saavutusten ansiosta Fermat'n lause oli todistettu oikeaksi kaikilla lukua 100 pienemmillä kokonaisluvuilla sekä kaikilla niillä äärettömän monilla kokonaisluvuilla, jotka olivat lukujen $2, ..., 99$ monikertoja [**1**, s. 80].

Saksassa Wolfskehlin säätiö julisti vuonan 1908 sadantuhannen Saksanmarkan palkinnon sille, joka pystyisi todistamaan Fermat'n suuren lauseen. Nykyrahassa summa vastaa suunnilleen miljoonaa dollaria [**22**, s. 155]. Jos joku olisi osoittanut Fermat'n suuren lauseen epätodeksi, ei siitä olisi saanut säätiöltä rahaa lainkaan. Wolfskehlin palkinnosta ilmoitettiin kaikissa matemaattisissa julkaisuissa ja niinpä uutinen palkinnosta levisi pian ympäri Eurooppaa [**22**, s. 158]. Ensimmäisenä vuonna säätiö sai 621 ratkaisuehdotusta ongelmalle, jotka kaikki osoitettiin kuitenkin vääriksi. Säätiö sai vuosien mittaan tuhansia ratkaisuyrityksiä, mutta ne kaikki osoitettiin vääriksi [**1**, s. 81–82]. Pääasiassa näitä todistuksia lähettivät useat matematiikan harrastelijat, jotka yrittivät palkintosumman siivittämänä saada todistuksen lauseelle, mutta järjestään jokainen todistus oli virheellinen. Jokainen todistus jouduttiin kuitenkin tarkastamaan ja käymään läpi siltä varalta, että joku tuntematon harrastelija olisikin onnistunut sattumalta todistamaan Fermat'n suuren lauseen [**22**, s. 164–165].

Valitettavasti suurin osa ammattimatemaatikoista piti Fermat'n suurta lausetta toivottomana tapauksena, ja he päättivät säätiön palkinnosta huolimatta olla vaarantamatta uraansa sellaisella uhkayrityksellä [**22**, s. 158]. Muutamat 1900-luvun merkittävimmistä hahmoista yrittivät ymmärtää lukujen syvällisimpiä ominaisuuksia keksiäkseen, mihin kaikkeen lukuteoria pystyy vastaamaan. Näitä merkittäviä hahmoja olivat esimerkiksi David Hilbert ja Kurt Gödel. Heidän työnsä on ollut merkittävä matematiikan perusteille ja vaikutti lopulta myös Fermat'n suureen lauseeseen [**22**, s. 167].

1.4. 1900-luvun kehitys

Henri Poincarè (1854–1912) tutki sinin ja kosinin tapaisia jaksollisia funktioita sekä niiden kautta kompleksitasoa. Funktion jaksollisuus voi ilmetä sekä reaaliakselin että imaginaariakselin suunnassa. Poincaré päätteli, että tällä keinolla löytyy funktioita, joilla on hyvin monipuolinen symmetria. Näitä funktioita hän kutsui automorfifunktioiksi. Poincaré laajensi automorfifunktiot vielä monimutkaisemmiksi funktioiksi, modulaarisiksi muodoiksi [**1**, s. 94–95]. Modulaaristen muotojen keskeinen piirre on niiden symmetrian suunnaton moninaisuus. Modulaarista muotoa on mahdoton piirtää tai edes kuvitella ja niitä tutkitaan paljon juuri niiden symmetrian takia [**22**, s. 215, 219, 222].

1900-luvulla alettiin tutkia kahdentuhannen vuoden takaisia Diofantoksen yhtälöitä yhä enemmän siten, että niiden ratkaisujen etsimiseen käytettiin elliptisten käyrien ominaisuuksia. Elliptiset käyrät eivät ole ellipsejä eivätkä ne kuvaa elliptisiä funktioitakaan. Ne liittyvät kolmannen asteen polynomien ratkaisuihin. Yksi esimerkki elliptisestä käyrästä on $y^2 = ax^3+bx^2+cx$. Lukuteoreetikot ovat kiinnostuneita elliptisistä käyristä, koska niiden avulla saadaan vastauksia moniin yhtälöitä ja niiden ratkaisuja koskeviin kysymyksiin. Elliptisistä käyristä kehittyi lukuteoreetikoille tehokas tutkimusmenetelmä [**1**, s. 104–105].

Vuonna 1954 Japanissa kaksi aloittelevaa matemaatikkoa, Yutaka Taniyma (1927–1958) ja Goro Shimura (1930–), tapasivat toisensa [**22**, s. 214]. Heidän tapaamisensa ja sitä kautta ystävyyden sai alulle jommankumman toiselle lähettämä kirjelappunen, jossa pyydettiin palauttamaan kirjastoon eräs matemaattinen lehti [**1**, s. 108]. Taniymaa ja Shimuraa kiehtoi eräs siihen aikaan epämuodikas aihe, Poincarén tutkimat modulaariset muodot. Taniyma väitti, että elliptiset yhtälöt ja modulaariset muodot ovat käytännöllisesti katsoen yksi ja sama asia. Niiden avulla voitaisiin yhdistää modulaarinen ja elliptinen maailma [**22**, s.215, 222]. Shimura uskoi ystävänsä idean paikkansapitävyyteen ja halusi löytää lisää todisteita modulaarisen ja elliptisen maailman välisen sukulaissuhteen vahvistamiseksi [**22**, s. 225–226]. Lopulta Shimura saikin sen verran todisteita elliptisten yhtälöiden ja modulaaristen muotojen vastaavuudesta, että se alkoi saada laajempaakin kannatusta. Todisteita oli sen verran, että siitä alettiin puhua Taniyman–Shimuran otaksumasta. Joskus hypoteesista puhutaan myös Taniyman–Shimuran–Weilin otaksumana ja virheellisesti Taniyman–Weilin otaksumana tai jopa vain Weilin otaksumana [**22**, s. 230].

Vuonna 1922 englantilainen matemaatikko Louis J. Mordell (1888–1972) keksi, että jos Fermat'n suuren lauseen eksponentti on suurempi kuin kaksi, niin yhtälöllä on vain äärellinen määrä ratkaisuja, sikäli kuin niitä ylipäätään olisi lainkaan. Mordell ei itse keksinyt väitteelleen todistusta, joten se sai nimekseen Mordellin konjektuuri.

Mordellin otaksuman todisti oikeaksi Gerd Falting (1954–) vuonna 1983. Pian tämän jälkeen D. R. Heath-Brown (1952–) ja Andrew Granville (1962–) osoittivat Faltingsin tuloksen avulla, että jos Fermat'n yhtälöllä oli ratkaisuja ne olisivat sitä harvemmassa mitä korkeammaksi eksponentti kasvaa. Heidän mukaansa Fermat'n yhtälön toteuttavia kokonaislukuja ei voi olla, kun eksponentti on hyvin suuri. Näin ollen Fermat'n suuri lause piti jo "melkein varmasti" paikkansa. Vuoteen 1983 mennessä Fermat'n suuri lause oli osoitettu oikeaksi, kun eksponentti on korkeintaan miljoona [**1**, s. 97–100].

Syksyllä 1984 pienessä saksalaiskylässä Oberwolfachissa järjestettiin tieteellinen keskustelutilaisuus. Yksi tilaisuuden puhujista, Gerhard Frey (1944–), esitti väitteen, jonka mukaan se, joka osaisi todistaa Taniyman–Shimuran otaksuman, pystyisi saman tien todistamaan myös Fermat'n suuren lauseen. Tähän väitteeseen Frey oli päätynyt muodostamalla Fermat'n yhtälön avulla elliptisen käyrän. Nyt Fermat'n suurella lauseella ja Taniyman–Shimuran olettamuksella oli selkeä yhteys. Nyt piti vain osoittaa, että elliptinen käyrä ei ole modulaarinen, jolloin Taniyman–Shimuran otaksuman todistaminen antaisi suoraan Fermat'n suuren lauseen. Freyn päättely oli siis seuraava:

(1) Jos Taniyman–Shimuran otaksuma voidaan todistaa, jokaisen elliptisen yhtälön on oltava modulaarinen.
(2) Jos jokaisen elliptisen yhtälön on oltava modulaarinen, Freyn elliptistä yhtälöä ei voi olla olemassa.
(3) Jos Freyn elliptistä yhtälöä ei ole olemassa, Fermat'n yhtälöllä ei ole ratkaisuja.
(4) Niinpä Fermat'n lause on tosi.

Ken Ribet (1948–) todisti, että Freyn elliptinen käyrä ei ole modulaarinen ja siten Taniyman–Shimuran otaksuman todistaminen antaa seurauksena Fermat'n suuren lauseen [**22**, s. 236–238, 242–243].

1.5. Lopullinen todistus

Eräänä iltana loppukesästä 1986 herra nimeltään Andrew Wiles (1953–) joi jääteetä ystävänsä luona. "Keskustelun lomassa hän mainitsi ohimennen, että Ken Ribet oli todistanut Taniyman–Shimuran otaksuman ja Fermat'n suuren lauseen välisen yhteyden. Valpastuin heti. Siitä hetkestä tiesin, että elämäni suunta oli vaihtumassa, koska tämä tarkoitti, että todistaakseni Fermat'n suuren lauseen minun tarvitsi vain todistaa Taniyman–Shimuran otaksuma. Se puolestaan tarkoitti, että lapsuuteni unelma oli muuttunut vakavasti otettavaksi tutkimuskohteeksi. Tiesin heti, etten enää koskaan voisi päästää sitä käsistäni. Tiesin myös, että palaisin kotiini ja ryhtyisin välittömästi tutkimaan Taniyman–Shimuran otaksumaa," Wiles muistelee [**22**, s. 247]. Wiles oli kymmenvuotias, kun hän meni Englannissa kotikaupunkinsa kirjastoon ja silmäili siellä erästä matematiikasta kertovaa kirjaa. Kirjassa kerrottiin Fermat'n suuresta lauseesta, joka näytti niin yksinkertaiselta, että lapsikin ymmärsi sen. Siinä hetkessä Wilesin unelmana oli todistaa lause joskus oikeaksi [**1**, s. 129].

Andrew Wiles aloitti yliopisto-opintonsa vuonna 1970. Suoritettuaan loppututkinnon, hänet hyväksyttiin Cambridgeen tekemään matematiikasta väitöskirjaa. Nyt Wiles joutui jättämään lapsuuden unelmansa Fermat'n suuren lauseen todistamisesta, koska siihen ei ollut väitöskirjaa tehdessä aikaa. Wiles kirjoitti väitöskirjansa

elliptisistä käyristä ja niitä sivuavasta Iwasawan teoriasta. Saatuaan väitöskirjan valmiiksi Wiles lähti Yhdysvaltoihin Princetonin yliopiston tutkijaksi. Siellä hän jatkoi elliptisten käyrien ja Iwasawan teorian parissa [**1**, s.130]. Nyt Ken Ribetin ansiosta hän alkoi taas tutkia Fermat'n suurta lausetta. Wiles teki erikoisen ratkaisun ja alkoi työskennellä täysin yksin ja salassa muilta. Hän perusteli sitä sillä, että näin hän takasi itselleen työrauhan. Toinen syy salamyhkäisyyteen oli varmaankin hänen halunsa saada tunnustusta. Wiles pelkäsi tilannetta, jossa hän olisi saanut päättelyn viimeisiä silauksia vaille valmiiksi ja tällöin hänen saavutuksensa vuotaisi julkisuuteen ja joku muu veisi häneltä kunnian täydentämällä todistuksen loppuun. Wiles saavutti useita huomattavia tuloksia parin vuoden aikana, mutta ei kertonut niistä julkisuuteen [**22**, s. 250–251].

Wiles tiesi, että todistaakseen Taniyman–Shimuran otaksuman oikeaksi hänen piti osoittaa kaikki elliptiset käyrät modulaarisiksi. Hänen piti siis osoittaa, että jokainen rationaalilukukertoiminen elliptinen käyrä on rakenteeltaan modulaarinen [**1**, s. 132]. Wiles päätti hyödyntää induktiotodistusta Taniyman-Shimuran otaksuman todistuksessa. Hänen haasteenaan oli laatia päättely, joka osoittaisi, että kukin äärettömän monesta elliptisestä yhtälöstä voitiin yhdistää johonkin äärettömän monesta modulaarisesta muodosta. Ensimmäinen askel kohti induktiivista todistusta löytyi 1800-luvulla eläneen ranskalaisen Évariste Galoisin tutkimuksista. Galois oli tutkinut muun muassa viidennen asteen yhtälöiden ratkaisua ja käytti apunaan ryhmäteoriaa. Ryhmäteorian avulla Wiles pystyi muodostamaan äärettömän monta äärettömän pitkää dominolaattajonoa, ja hänen onnistui kaataa jokaisen jonon ensimmäinen laatta. Dominolaattajonot kuvaavat tässä siis induktiotodistusta, jossa on äärettömän monta tapausta todistettavana. Wiles oli saanut otettua induktiotodistuksen ensimmäisen askeleen kohti lopullista todistusta [**22**, s. 253–255, 272–275].

Nyt Wilesin piti todistaa, että jokainen kaadettu dominolaatta kaataisi myös seuraavan. Seuraavan askeleen ottamisessa Wilesilla oli ongelma. Hän ajatteli käyttävänsä Iwasawan teoriaa, mutta se ei siihen sopinutkaan. Hän ei tiennyt, kuinka jatkaisi. Niinpä hän päätti lähteä viiden vuoden eristäytymisen jälkeen matematiikan alan kongressiin, josta ajatteli kuulevansa aivan viimeisimmät matematiikan keksinnöt. Kongressissa hän tapasi väitöskirjan ohjaajansa John Coatesin, joka mainitsi oppilaansa Matthias Flachin olevan laatimassa hienoa artikkelia elliptisistä yhtälöistä. Flachin tutkimus perustui Kolyvaginin vastikään kehittämään metodiin. Wiles sai idean hyödyntää tätä ns. Kolyvaginin–Flachin metodia todistuksessaan. Wiles luokitteli kaikki elliptiset yhtälöt erilaisiin perheisiin, joihin hän sitten Kolyvaginin–Flachin metodia sovelsi. Kuuden vuoden intensiivisen työskentelyn jälkeen Wiles otti yhteyttä professori Nick Katziin. Katz työskenteli Wilesin tavoin Princetonin yliopistossa ja hän oli läheinen henkilö Wilesin kanssa. Katzilta Wiles sai apua Kolyvaginin–Flachin metodin teknisiin päättelyihin [**22**, s. 283–287].

Lopulta Wilesin todistus oli siinä vaiheessa, että vain yksi elliptisten yhtälöiden perhe oli enää alistumatta hänen tekniikalleen. Siihen hän löysi ratkaisun 1800-luvulta peräisin olevasta konstruktiosta, jonka Barry Mazur mainitsi eräässä tutkimuksessaan. Näin hän sai Kolyvaginin–Flachin metodin toimimaan myös viimeiseen elliptisten yhtälöiden perheeseen ja hän uskoi olevansa todistanut Fermat'n suuren lauseen [**22**, s. 289]. Kesäkuussa 1993 järjestettiin Englannin Cambridgessa lukuteoriaa käsittelevä kongressi, jossa Wiles aikoi esittää todistuksensa. Wiles piti kolmen luennon

sarjan, jonka loppuhuipennuksena oli Fermat'n suuren lauseen todistus. Tämän jälkeen todistus lähti asiantuntijoiden tarkastettavaksi [**1**, s. 140–141].

Valitettavasti Wilesin todistuksesta löytyi kuitenkin ammottava aukko, jonka paikkaaminen ei käynytkään tuosta vain. Wiles eristäytyi taas ulkomaailmasta ja alkoi paikata todistustaan. Eristäytyminen oli nyt huomattavasti vaikeampaa, koska kaikki odottivat hänen lopullista todistustaan ja epäilivät jo, tuleekohan sitä edes. Wiles pyysi todistukseen apua entiseltä oppilaaltaan Richard Taylorilta. Vihdoin 19. syyskuuta 1994 Wilesin onnistui paikata todistuksessa ollut aukko kokonaan. Wiles lähetti raporttinsa matematiikan alan arvostetuimpaan julkaisuun, *Annals of Mathematics* -lehteen. Tämä oli matematiikassa normaali tapa julkistaa tutkimustuloksia. Ennen julkaisua lehti tarkistutti Wilesin tekstin usealla asiantuntijalla. Tarkistuksessa meni kuukausia, mutta virheitä ei löytynyt. Näin yli 350 vuotta vanha arvoitus oli lopullisesti todistettu oikeaksi [**1**, s. 142–147].

LUKU 2

Tapaus $n = 4$

Todistetaan tässä luvussa Fermat'n suuri lause, kun eksponentti $n = 4$. Tämä on lauseen helpoin tapaus. Tämän tapauksen ovat todistaneet muun muassa De Bessy vuonna 1676, Euler vuonna 1738 ja Kausler vuonna 1795 [**21**, s. 15]. Myös Fermat itse on todistetusti osoittanut lauseen todeksi tapauksessa $n = 4$. Fermat käytti todistuksessaan äärettömän laskeutumisen menetelmää [**22**, s. 108–109].

Äärettömän laskeutumisen menetelmää käyttäen Fermat aluksi oletti, että yhtälölle on olemassa hypoteettinen ratkaisu

$$x = X_1, y = Y_1, z = Z_1.$$

Tutkimalla ratkaisun (X_1, Y_1, Z_1) ominaisuuksia Fermat osoitti, että mikäli tämä hypoteettinen ratkaisu oli olemassa, silloin olisi oltava olemassa myös pienempi ratkaisu (X_2, Y_2, Z_2). Tutkimalla tätä uutta ratkaisua Fermat osoitti, että oli olemassa vieläkin pienempi ratkaisu (X_3, Y_3, Z_3). Näin Fermat oli löytänyt laskeutuvan portaikon ratkaisuja, jotka jatkuisivat äärettömiin, aina pienempiin lukuihin. Koska lukujen x, y, z on kuitenkin oltava luonnollisia lukuja ja koska yhtälölle on oltava olemassa pienin mahdollinen ratkaisu, niin äärettömiin jatkuva portaikko on tällöin mahdoton. Tämän ristiriidan nojalla alkuperäinen oletus, jonka mukaan on olemassa ratkaisu (X_1, Y_1, Z_1), on väärä [**22**, s. 109].

Jotta voidaan todistaa Fermat'n suuri lause tapauksessa $n = 4$, pitää ensin todistaa pari lemmaa. Näitä lemmoja käytetään apuna myös tapausten $n = 3$ ja $n = 5$ todistuksissa.

LEMMA 2.1 (Aritmetiikan peruslause). *Jokainen kokonaisluku $s > 1$, voidaan esittää yksikäsitteisesti alkulukujen tulona, $s = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, missä p_i:t ovat eri alkulukuja ja $a_i \in \mathbb{N}$.*

TODISTUS. Katso [**25**, s. 18–19]. □

LEMMA 2.2 (Eukleideen Lemma). *Olkoon p alkuluku ja $a, b \in \mathbb{Z}$. Jos $p \mid ab$, niin $p \mid a$ tai $p \mid b$. Jos $a_1, a_2, \ldots, a_n \in \mathbb{Z}$ ja $p \mid a_1 \cdots a_n$, niin $p \mid a_i$, jollain $i \in \{1, 2, ..., n\}$*

TODISTUS. Oletuksen mukaan $ab = rp$ jollekin $r \in \mathbb{Z}$. Jos luku a on jaollinen luvulla p, niin väite pitää paikkansa. Oletetaan sitten, että a ei ole jaollinen luvulla p, ja osoitetaan, että luku b on silloin jaollinen luvulla p. Koska luku p on alkuluku ja $p \nmid a$, niin silloin $syt\,(a, p) = 1$. Tällöin joillakin $m, n \in \mathbb{Z}$ on voimassa Bezout'n yhtälö: $1 = ma + np$ [**18**, s. 63]. Kertomalla molemmat puolet luvulla b, saadaan $b = mab + npb = mrp + npb = p\,(mr + nb)$. Tästä huomataankin, että nyt $p \mid b$. Yleinen tapaus todistetaan induktiolla. □

Seuraavan lemman todistuksessa hyödynnetään Fermat'n kehittelemää äärettömän laskeutumisen menetelmää. Lemma on tärkeä ja sitä käytetään jatkossa monessa tilanteessa.

LEMMA 2.3. *Jos* $syt\,(v, w) = 1$ *ja* $vw = z^n$*, niin silloin on olemassa luvut* x, y *siten, että* $v = x^n$ *ja* $w = y^n$*.*

TODISTUS. Oletuksen nojalla $syt\,(v, w) = 1$ ja $vw = z^n$.

Tehdään antiteesi: Oletetaan, että $v \neq x^n$ kaikilla x, n. Nyt $v \neq 1$, koska $1^n = 1$. Tällöin v on Lemman 2.1 nojalla jaollinen alkuluvulla p. On siis olemassa luku k siten, että $v = pk$. Nyt luku p jakaa luvun z, koska $z^n = vw = pkw$. Tällöin on olemassa luku m siten, että $z = pm$. Joten $z^n = vw = pkw = (pm)^n = p^n m^n$. Jakamalla molemmat puolet luvulla p, saadaan $kw = p^{n-1}m^n$. Nyt Lemman 2.2 nojalla joko $p \mid k$ tai $p \mid w$. Luku p ei voi jakaa lukua w, koska se jakaa luvun v ja $syt\,(v, w) = 1$. Tällöin $p \mid k$. Tämä sama päättely, mikä tehtiin luvulle p, voidaan tehdä myös luvulle p^{n-1}. Siten saadaan, että $p^{n-1} \mid k$. Tällöin on olemassa luku V siten, että $k = p^{n-1}V$. Tästä saadaan, että $kw = p^{n-1}m^n = p^{n-1}Vw$. Jakamalla molemmat puolet luvulla p^{n-1}, saadaan $Vw = m^n$. Nyt $syt\,(V, w) = 1$, koska $V \mid v$ ja $syt\,(v, w) = 1$. Luku V ei voi olla n. potenssi. Jos se olisi, niin $v = p^n V$ tekisi luvusta v n:nnen potenssin, mikä on kuitenkin vastoin oletusta. Lopuksi V on pienempi kuin v, koska $p^{n-1} > 1$.

Edellä osoitettiin, että olettamalla, että n:nnen potenssin jakaja ei ole itse n. potenssi, niin täytyy välttämättä olla pienempi jakaja, joka ei myöskään ole n. potenssi ja niin edelleen ja niin edelleen. Tätä jatkamalla päädytään tilanteeseen, missä positiivisia kokonaislukuja käsitellessä ei enää löydykään pienempää ratkaisua ja saadaan ristiriita. Näin saatiin todistettua Fermat'n kehittelemää äärettömän laskeutumisen menetelmää käyttäen, että $v = x^n$. Vastaavasti voidaan osoittaa, että $w = y^n$ jollekin y. □

MÄÄRITELMÄ 2.4. Jos kolmikko (x, y, z) positiivisia kokonaislukuja toteuttaa Pythagoraan yhtälön, eli yhtälön $x^2 + y^2 = z^2$, niin lukukolmikkoa kutsutaan *Pythagoraan kolmikoksi.*

ESIMERKKI 2.5. Kolmikko $(3, 4, 5)$ on Pythagoraan kolmikko, koska $3^2 + 4^2 = 5^2$.

MÄÄRITELMÄ 2.6. Kun $x > 0$, $y > 0$, $z > 0$, x on parillinen ja $syt\,(x, y, z) = 1$, niin kolmikko (x, y, z) on *primitiivinen ratkaisu* yhtälölle $x^2 + y^2 = z^2$.

Seuraavan lauseen avulla saadaan kaikki primitiiviset ratkaisut Pythagoraan lauseelle.

LAUSE 2.7. *Jos* a, b *ovat kokonaislukuja, joille* $a > b > 0$*,* $syt\,(a, b) = 1$*, toinen niistä on pariton ja toinen parillinen, niin tällöin kolmikko* (x, y, z)*, jossa*

$$\begin{cases} x = 2ab, \\ y = a^2 - b^2, \\ z = a^2 + b^2, \end{cases}$$

on primitiivinen ratkaisu Pythagoraan lauseelle $x^2 + y^2 = z^2$*.*

Myös käänteinen tulos pätee. Eli jos kolmikko (x, y, z) *on primitiivinen ratkaisu Pythagoraan lauseelle, niin tällöin* $a > b > 0$*,* $syt\,(a, b) = 1$ *ja toinen luvuista* a, b *on pariton ja toinen parillinen.*

TODISTUS. Olkoot a, b kokonaislukuja, joille lauseen ehdot ovat voimassa. Lisäksi olkoon x, y ja z määritelty, kuten edellä. Tällöin

$$x^2+y^2 = (2ab)^2+\left(a^2-b^2\right)^2 = 4a^2b^2+a^4-2a^2b^2+b^4 = a^4+2a^2b^2+b^4 = \left(a^2+b^2\right)^2 = z^2.$$

Selvästi $x > 0, y > 0, z > 0$, x on parillinen. Olkoon $d = syt\,(x, y, z)$. Tällöin $d \mid x$, $d \mid y$ ja $d \mid z$, siten $d \mid ((a^2+b^2)+(a^2-b^2))$ ja $d \mid ((a^2+b^2)-(a^2-b^2))$, eli $d \mid 2a^2$ ja $d \mid 2b^2$. Koska $syt\,(a, b) = 1$, niin täytyy olla joko $d = 1$ tai $d = 2$. Oletuksen mukaan toinen luvuista a ja b on parillinen ja toinen pariton, siten y on pariton. Ja koska y on pariton, niin $d \neq 2$. Eli täytyy olla $syt\,(x, y, z) = 1$.

Käänteisesti, olkoon (x, y, z) primitiivinen ratkaisu yhtälölle $x^2 + y^2 = z^2$, joten $x^2 + y^2 = z^2$. Koska tiedetään, että $syt\,(x, y, z) = 1$, niin myös $syt\,(x, z) = 1$. Koska x on parillinen, niin z on pariton ja tällöin $syt\,(z-x, z+x) = 1$. Koska $y^2 = z^2 - x^2 = (z-x)(z+x)$ ja $syt\,(z-x, z+x) = 1$, niin Lemmasta 2.3 seuraa, että $z-x$ ja $z+x$ ovat kokonaislukujen neliöitä. Olkoon ne $z+x = t^2$ ja $z-x = u^2$, missä lukujen t ja u täytyy olla positiivisia parittomia kokonaislukuja, $t > u > 0$. Olkoon a, b kokonaislukuja siten, että $2a = t+u$ ja $2b = t-u$. Tällöin $t = a+b$ ja $u = a-b$, $a > b > 0$. Koska $x = t^2 - z = t^2 - (u^2+x) = t^2 - u^2 - x$, $y^2 = u^2t^2$ ja $z = t^2 - x = t^2 - (z-u^2) = t^2 - z + u^2$, niin

$$x = \frac{(a+b)^2-(a-b)^2}{2} = \frac{a^2+2ab+b^2-a^2+2ab-b^2}{2} = \frac{4ab}{2} = 2ab,$$

$$y^2 = (a-b)^2(a+b)^2 = ((a+b)(a-b))^2 = \left(a^2-b^2\right)^2, \text{ joten } y = a^2-b^2,$$

$$z = \frac{(a+b)^2+(a-b)^2}{2} = \frac{a^2+2ab+b^2+a^2-2ab+b^2}{2} = \frac{2a^2+2b^2}{2} = a^2+b^2.$$

Huomataan, että $syt\,(a, b) = 1$, koska $syt\,(z-x, z+x) = 1$. Lisäksi, koska $t = a+b$ on pariton, niin toinen luvuista a, b on pariton ja toinen parillinen. □

Todistetaan seuraavaksi, että yhtälöllä $x^4 - y^4 = z^2$ ei ole yhtään positiivisista kokonaisluvuista muodostuvaa ratkaisua.

LAUSE 2.8. *Ei ole olemassa kokonaislukuja $x \neq 0, y \neq 0, z \neq 0$, jotka toteuttavat yhtälön $x^4 - y^4 = z^2$.*

TODISTUS. Antiteesi: On olemassa kokonaisluvut $x \neq 0, y \neq 0, z \neq 0$, jotka toteuttavat yhtälön $x^4 - y^4 = z^2$. Olkoon (x, y, z) näistä se ratkaisu, jossa x on pienin. Osoitetaan, että tällöin $syt\,(x, y) = 1$. Jos alkuluku p jakaa molemmat luvut x, y, voidaan merkitä $x = px', y = py'$. Nyt saadaan, että

$$z^2 = x^4 - y^4 = (px')^4 - (py')^4 = p^4(x')^4 - p^4(y')^4 = p^4\left((x')^4 - (y')^4\right).$$

Tämän nojalla selvästi p^2 jakaa luvun z. Olettamalla, että $z = p^2z'$, saadaan

$$(px')^4 - (py')^4 = \left(p^2z'\right)^2 \Rightarrow (x')^4 - (y')^4 = (z')^2,$$

missä $0 < x' < x$, mikä on ristiriita oletuksen kanssa. Siten $p = 1$ ja $syt\,(x, y) = 1$.

Yhtälö $z^2 = x^4 - y^4$ voidaan kirjoittaa muotoon $z^2 = (x^2+y^2)(x^2-y^2)$. Koska $syt\,(x, y) = 1$, niin nähdään helposti, että $syt\,(x^2+y^2, x^2-y^2)$ on 1 tai 2. Käsitellään nämä molemmat tapaukset.

Tapaus 1: $syt\,(x^2+y^2, x^2-y^2) = 1$.

Koska lukujen x^2+y^2 ja x^2-y^2 tulo on neliö, niin Lemman 2.3 nojalla luvut x^2+y^2 ja x^2-y^2 ovat neliöitä. On siis olemassa positiiviset kokonaisluvut $s, t, syt\,(s,t) = 1$ siten, että

$$x^2+y^2 = s^2,$$
$$x^2-y^2 = t^2.$$

Siitä seuraa, että lukujen s ja t täytyy olla parittomia ($s^2+t^2 = 2x^2$, siten s ja t ovat molemmat samaa parillisuutta ja koska $syt\,(s,t) = 1$, niin molemmat eivät voi olla parillisia). On olemassa positiiviset kokonaisluvut u, v siten, että

$$u = \frac{s+t}{2},$$
$$v = \frac{s-t}{2},$$

ja selvästi $syt\,(u,v) = 1$, koska luvut s, t ovat parittomia.

Nyt voidaan kirjoittaa

$$uv = \frac{(s+t)(s-t)}{4} = \frac{s^2-t^2}{4} = \frac{x^2+y^2-x^2+y^2}{4} = \frac{y^2}{2}.$$

Tällöin $y^2 = 2uv$. Ja koska $syt\,(u,v) = 1$, niin Lemman 2.3 nojalla on olemassa positiiviset kokonaisluvut l, m siten, että

$$\begin{cases} u = 2l^2, \\ v = m^2, \end{cases} \quad \text{tai} \quad \begin{cases} u = l^2, \\ v = 2m^2. \end{cases}$$

Käydään läpi ensimmäinen vaihtoehto, toinen tehdään vastaavasti. Tässä tapauksessa u on parillinen, $syt\,(u,v,x) = 1$ ja

$$u^2+v^2 = \left(\frac{s+t}{2}\right)^2 + \left(\frac{s-t}{2}\right)^2 = \frac{(s+t)^2}{4} + \frac{(s-t)^2}{4} = \frac{(s+t)^2+(s-t)^2}{4}$$
$$= \frac{s^2+2st+t^2+s^2-2st+t^2}{4} = \frac{s^2+t^2}{2} = x^2.$$

Lauseesta 2.7 seuraa, että on olemassa positiiviset kokonaisluvut $a, b, 0 < b < a$, $syt\,(a,b) = 1$ siten, että

$$2l^2 = u = 2ab,$$
$$m^2 = v = a^2-b^2,$$
$$x = a^2+b^2.$$

Huomataan, että tällöin $l^2 = ab$. Siten Lemman 2.3 nojalla on olemassa positiiviset kokonaisluvut c, d, $syt\,(c,d) = 1$ siten, että

$$a = c^2,$$
$$b = d^2,$$

ja siten $m^2 = c^4-d^4$. Huomataan, että $0 < c < a < x$ ja kolmikko (c,d,m) positiivisia kokonaislukuja olisi yhtälön $x^4-y^4 = z^2$ ratkaisu. Tämä on kuitenkin vastoin

sitä oletusta, että x on pienin mahdollinen. Näin ollen $syt\,(x^2 + y^2, x^2 - y^2) \neq 1$.

Tapaus 2: $syt\,(x^2 + y^2, x^2 - y^2) = 2$.

Nyt luvut x, y ovat parittomia ja z on parillinen. Lauseen 2.7 nojalla on olemassa positiiviset kokonaisluvut $a, b, 0 < b < a$, $syt\,(a, b) = 1$ siten, että

$$x^2 = a^2 + b^2,$$
$$y^2 = a^2 - b^2,$$
$$z = 2ab.$$

Tällöin $x^2y^2 = a^4 - b^4$, missä $0 < a < x$. Tämä on ristiriita, koska (x, y, z) oli se ratkaisukolmikko, jossa x on pienin mahdollinen. Näin ollen $syt\,(x^2 + y^2, x^2 - y^2) \neq 2$, ja siten antiteesin täytyy olla väärä. □

Nyt voidaan Lauseen 2.8 perusteella osoittaa, että Fermat'n suuri lause ei päde eksponentin ollessa 4.

LAUSE 2.9. *Yhtälöllä $x^4 + y^4 = z^4$ ei ole kokonaislukuratkaisua, kun $x \neq 0, y \neq 0, z \neq 0$.*

TODISTUS. Jos x, y, z ovat nollasta poikkeavia kokonaislukuja siten, että $x^4 + y^4 = z^4$, niin silloin $z^4 - y^4 = (x^2)^2$. Tämä on kuitenkin ristiriidassa Lauseen 2.8 kanssa. □

SEURAUS 2.10. *Yhtälöllä $x^n + y^n = z^n$ ei ole olemassa kokonaislukuratkaisua, kun n on jaollinen luvulla 4.*

LUKU 3

Tapaus $n = 3$

Tässä luvussa todistetaan Fermat'n suuri lause tapauksessa $n = 3$. Todistuksessa mukaillaan Eulerin kirjoittaman, vuonna 1770 julkaistun, Algebra-kirjan todistusta, jossa käytetään äärettömän laskeutumisen menetelmää. Tarkemmat tarkastelut paljastivat Eulerin tehneen erään virheen käsitellessään muotoa $a^2 + 3b^2$ olevien lukujen jaollisuutta [**21**, s. 24]. Tämä virhe on tässä todistuksessa kuitenkin korjattu.

Näytetään aluksi eräs lukujen suurimpaan yhteiseen tekijään liittyvä ominaisuus.

LEMMA 3.1. *Jos* $syt\,(a, b) = d$, *niin* $syt\left(\frac{a}{d}, \frac{b}{d}\right) = 1$.

TODISTUS. Oletetaan, että $syt\left(\frac{a}{d}, \frac{b}{d}\right) = e$. Tällöin $e \mid \frac{a}{d}$ ja $e \mid \frac{b}{d}$. Nyt on olemassa luvut x, y siten, että $\frac{a}{d} = ex$ ja $\frac{b}{d} = ey$. Tällöin $a = dex$ ja $b = dey$, mistä huomataan, että $de \mid a$ ja $de \mid b$. Koska $de > d$, jos $e > 1$ ja $syt\,(a, b) = d$, niin täytyy olla $e = 1$. □

Nyt todistetaan muutama muu tärkeä lemma, joita käytämme tapauksen $n = 3$ todistuksessa.

LEMMA 3.2. *Kertomalla keskenään muotoa* $a^2 + 3b^2$ *olevia lukuja, saadaan tulokseksi samaa muotoa oleva luku.*

TODISTUS.

$$\begin{aligned}\left(a^2 + 3b^2\right)\left(c^2 + 3d^2\right) &= a^2\left(c^2 + 3d^2\right) + 3b^2\left(c^2 + 3d^2\right) \\ &= a^2c^2 + 3a^2d^2 + 3b^2c^2 + 9b^2d^2 \\ &= a^2c^2 - 6abcd + 9b^2d^2 + 3a^2d^2 + 6abcd + 3b^2c^2 \\ &= (ac - 3bd)^2 + 3\,(ad + bc)^2\,.\end{aligned}$$

□

LEMMA 3.3. *Olkoon* s *pariton luku. Tällöin on olemassa* n *siten, että* $s = 4n \pm 1$.

TODISTUS. Todistetaan tämä induktiolla.

Jos $s = 1$, niin $n = 0$, koska $1 = 4 \cdot 0 + 1$.

Oletetaan, että kun $s = v$ löytyy jokin n siten, että $v = 4n \pm 1$.

Kun $v = 4n + 1$, niin $v + 2 = 4n + 1 + 2 = 4n + 3 = 4\,(n + 1) - 1$.

Kun $v = 4n - 1$, niin $v + 2 = 4n - 1 + 2 = 4n + 1$.

Näin ollen induktiotodistus osoittaa väitteen oikeaksi. □

LEMMA 3.4. *Jos luku* 2 *jakaa muotoa* $a^2 + 3b^2$ *olevan luvun, niin myös luku* 4 *jakaa tämän luvun ja tämän jaon tuloksena on samaa muotoa oleva luku.*

Toisin sanoen, jos $2 \mid a^2 + 3b^2$*, niin* $4 \mid a^2 + 3b^2$ *ja tällöin on olemassa luvut* c, d *siten, että* $a^2 + 3b^2 = 4\left(c^2 + 3d^2\right)$*.*

TODISTUS. Tiedetään, että luvut a ja b ovat samaa parillisuutta, eli molemmat ovat joko parittomia tai parillisia. Muussa tapauksessa luku $a^2 + 3b^2$ ei olisi jaollinen luvulla 2.

Jos molemmat ovat parillisia, niin tällöin on olemassa luvut c, d siten, että $a = 2c$ ja $b = 2d$. Silloin $a^2 + 3b^2 = (2c)^2 + 3\left(2d\right)^2 = 4\left(c^2 + 3d^2\right)$ ja nyt $4 \mid (a^2 + 3b^2)$.

Oletetaan sitten, että molemmat ovat parittomia. Tällöin Lemman 3.3 nojalla on olemassa luvut m, n siten, että $a = 4m \pm 1$ ja $b = 4n \pm 1$. Nyt tiedetään, että joko $4 \mid (a + b)$ tai $4 \mid (a - b)$. Tarkastellaan nämä molemmat tapaukset.

Tapaus 1: $4 \mid (a + b)$

Lemman 3.2 nojalla saadaan

$$4\left(a^2 + 3b^2\right) = \left(1^2 + 3 \cdot 1^2\right)\left(a^2 + 3b^2\right) = (a - 3b)^2 + 3\left(a + b\right)^2.$$

Koska $a - 3b = (a + b) - 4b$, niin tiedetään, että $4 \mid (a - 3b)$. Tästä saadaan, että $4^2 \mid (a - 3b)^2 + 3\left(a + b\right)^2$, ja silloin $4^2 \mid 4\left(a^2 + 3b^2\right)$ ja $4 \mid (a^2 + 3b^2)$. Nyt, koska $4 \mid (a - 3b)$ ja $4 \mid (a + b)$, niin on olemassa luvut u, v siten, että

$$u = \frac{a - 3b}{4} \text{ ja}$$
$$v = \frac{a + b}{4}.$$

Nyt saadaan

$$\begin{aligned}
4\left(u^2 + 3v^2\right) &= 4\left(\left(\frac{1}{4}\left(a - 3b\right)\right)^2 + 3\left(\frac{1}{4}\left(a + b\right)\right)^2\right) \\
&= 4\left(\left(\frac{1}{16}\left(a^2 - 6ab + 9b^2\right)\right) + 3\left(\frac{1}{16}\left(a^2 + 2ab + b^2\right)\right)\right) \\
&= \frac{1}{4}\left(a^2 - 6ab + 9b^2 + 3a^2 + 6ab + 3b^2\right) \\
&= \frac{1}{4}\left(4a^2 + 12b^2\right) \\
&= a^2 + 3b^2.
\end{aligned}$$

Tapaus 2: $4 \mid (a - b)$.

Vastaavasti, kuten tapauksen 1 käsittelyssä saadaan Lemman 3.2 nojalla

$$4\left(a^2 + 3b^2\right) = \left(1^2 + 3 \cdot (-1)^2\right)\left(a^2 + 3b^2\right) = (a + 3b)^2 + 3\left(a - b\right)^2.$$

Tästä saadaan, että $4^2 \mid (a+3b)^2 + 3(a-b)^2$, josta saadaan, että $4 \mid (a+3b)$ ja $4 \mid (a-b)$. Tällöin on olemassa u, v siten, että

$$u = \frac{a+3b}{4} \text{ ja}$$
$$v = \frac{a-b}{4}, \text{ jolloin}$$

$4(u^2+3v^2) = a^2+3b^2$. □

LEMMA 3.5. *Jos $(p^2+3q^2) \mid (a^2+3b^2)$, missä p^2+3q^2 on alkuluku, niin silloin on olemassa luvut l, m siten, että $a^2+3b^2 = (p^2+3q^2)(l^2+3m^2)$.*

TODISTUS. Koska $(p^2+3q^2) \mid (a^2+3b^2)$, niin on olemassa f siten, että $(a^2+3b^2) = f(p^2+3q^2)$. Koska

$$\begin{aligned}(pb-aq)(pb+aq) &= p^2b^2 - a^2q^2 + \left(3q^2b^2 - 3q^2b^2\right)\\ &= p^2b^2 + 3q^2b^2 - 3q^2b^2 - a^2q^2\\ &= b^2\left(p^2+3q^2\right) - q^2\left(a^2+3b^2\right)\\ &= b^2\left(p^2+3q^2\right) - q^2f\left(p^2+3q^2\right)\\ &= \left(p^2+3q^2\right)\left(b^2-fq^2\right),\end{aligned}$$

niin Lemman 2.2 nojalla luku p^2+3q^2 jakaa joko luvun $pb-aq$ tai luvun $pb+aq$. Tällöin on olemassa luku F siten, että joko $(p^2+3q^2)F = pb+aq$ tai $(p^2+3q^2)F = pb-aq$. Nyt

$$\begin{aligned}&\left(p^2+3(\pm q)^2\right)\left(a^2+3b^2\right)\\ &= p^2\left(a^2+3b^2\right) + 3(\pm q)^2\left(a^2+3b^2\right)\\ &= p^2a^2 + p^23b^2 + 3(\pm q)^2a^2 + 3(\pm q)^2 3b^2\\ &= p^2a^2 - 6p(\pm q)ab + 9(\pm q)^2b^2 + 3p^2b^2 + 6p(\pm q)ab + 3(\pm q)^2a^2\\ &= (pa \pm 3qb)^2 + 3(pb \pm aq)^2,\end{aligned}$$

mistä saadaan, että

$$\begin{aligned}(pa \pm 3qb)^2 &= \left(p^2+3q^2\right)\left(a^2+3b^2\right) - 3(pb \pm aq)^2\\ &= \left(p^2+3q^2\right)\left(a^2+3b^2\right) - 3\left(\left(p^2+3q^2\right)F\right)^2\\ &= \left(p^2+3q^2\right)\left(\left(a^2+3b^2\right) - 3\left(p^2+3q^2\right)F^2\right).\end{aligned}$$

Tämän ja aiemman perusteella huomataan, että

$$\left(p^2+3q^2\right) \mid (pa \pm 3qb) \text{ ja}$$
$$\left(p^2+3q^2\right) \mid (pb \pm aq).$$

Tällöin on olemassa luvut l, m siten, että

$$\begin{aligned}pa \pm 3qb &= l\left(p^2+3q^2\right)\\ pb \pm aq &= m\left(p^2+3q^2\right).\end{aligned}$$

Nyt

$$\begin{aligned}(pa \pm 3qb)^2 + 3(pb \pm aq)^2 &= \left(l\left(p^2+3q^2\right)\right)^2 + 3\left(m\left(p^2+3q^2\right)\right)^2 \\ &= \left(p^2+3q^2\right)^2\left(l^2+3m^2\right).\end{aligned}$$

Sijoittamalla tämä yhtälöön $(p^2+3q^2)(a^2+3b^2) = (pa \pm 3qb)^2 + 3(pb \pm aq)^2$ saadaan

$$\begin{aligned}a^2+3b^2 &= \frac{\left(p^2+3q^2\right)^2\left(l^2+3m^2\right)}{p^2+3q^2} \\ &= \left(p^2+3q^2\right)\left(l^2+3m^2\right).\end{aligned}$$

□

LEMMA 3.6. *Jos luvulla a^2+3b^2 on pariton tekijä, joka ei ole muotoa p^2+3q^2, niin silloin osamäärällä on pariton tekijä, joka ei ole muotoa p^2+3q^2.*

Toisin sanoen, jos f on luvun a^2+3b^2 tekijä ja f ei ole muotoa p^2+3q^2, niin silloin on olemassa g ja f' siten, että $fg = a^2+3b^2$, $f' \mid g$ ja f' ei ole muotoa p^2+3q^2.

TODISTUS. Oletetaan, että on olemassa f, g siten, että $fg = a^2+3b^2$, f on pariton ja f ei ole muotoa p^2+3q^2.

Antiteesi: Oletetaan, että kaikki parittomat tekijät g ovat muotoa p^2+3q^2. Nyt Lemman 2.1 nojalla g on alkulukujen tulo $g = p_1p_2p_3\cdots p_n$. Tämän tulon luvuissa mukana olevat luvut 2 eli 2^α voidaan Lemman 3.4 nojalla korvata luvulla 4^β. Eli tällöin luku 4^β jakaa luvun g. Nyt Lemman 3.4 perusteella jaettaessa lukua a^2+3b^2 luvulla 4^β saadaan muotoa c^2+3d^2 oleva luku. Siis

$$c^2+3d^2 = f \cdot \frac{g}{4^\beta} = f \cdot p_x \cdots p_n.$$

Koska oletettiin, että kaikki luvun g parittomat tekijät ovat muotoa p^2+3q^2, niin Lemman 3.5 nojalla luvusta g voidaan poistaa kaikki parittomat alkuluvut. Silloin päädytään tilanteeseen, missä $f = l^2+3m^2$. Tämä on kuitenkin ristiriita, koska luku f ei ollut tätä muotoa. □

LEMMA 3.7. *Jos lukujen a, b suurin yhteinen tekijä on 1, niin jokainen luvun a^2+3b^2 pariton tekijä on samaa muotoa.*

Toisin sanoen, jokaiselle luvun a^2+3b^2 parittomalle tekijälle on olemassa luvut c, d siten, että pariton tekijä $= c^2+3d^2$.

TODISTUS. Olkoon x positiivinen, pariton tekijä luvulle a^2+3b^2. Silloin on olemassa luku f siten, että $a^2+3b^2 = xf$. Jos $x = 1$, niin esimerkiksi $1 = 1^2+3(0)^2$. Siten voidaan olettaa, että $x > 1$ ja silloin on olemassa luvut m, n siten, että

$$\begin{aligned}a &= mx + c, \\ b &= nx + d,\end{aligned}$$

missä luvut c, d voivat olla positiivisia tai negatiivisia. Jakoyhtälön ominaisuuksista tiedetään, että $c < x$. Oletetaan, että $c \geq \frac{1}{2}x$. On olemassa luku c' siten, että $c' = x - c = -(c-x)$. Tällöin $a = mx+c = (m+1)x + c - x = (m+1)x - (x-c) = (m+1)x - c'$. Koska $c' = x-c$, niin $|c'| < \frac{1}{2}x$. Nyt on kuitenkin päädytty ristiriitaan, koska jakoyhtälö on yksikäsitteinen, eli ei voi olla $a = mx+c = (m+1)x - c'$, kun

$c \geq \frac{1}{2}x$ ja $|c'| < \frac{1}{2}x$. Nyt täytyy siis olla $|c| < \frac{1}{2}x$. Vastaavasti saadaan, että $|d| < \frac{1}{2}x$. Nyt sijoittamalla a:n ja b:n jakoyhtälöt lukuun $a^2 + 3b^2$ saadaan

$$\begin{aligned} a^2 + 3b^2 &= (mx + c)^2 + 3(nx + d)^2 = m^2x^2 + 2mxc + c^2 + 3n^2x^2 + 6ndx + 3d^2 \\ &= x\left(m^2x + 2mc + 3n^2x + 6nd\right) + c^2 + 3d^2. \end{aligned}$$

Koska x on luvun $a^2 + 3b^2$ tekijä, niin $x \mid c^2 + 3d^2$. Silloin on olemassa y siten, että $c^2 + 3d^2 = xy$. Nyt

$$xy = c^2 + 3d^2 < \left(\frac{1}{2}x\right)^2 + 3\left(\frac{1}{2}x\right)^2 = \frac{1}{4}x^2 + \frac{3}{4}x^2 = x^2.$$

Koska neliöt $c^2, d^2 \geq 0$, niin $xy \geq 0$. Lisäksi, koska $x \geq 0$ ja $xy < x^2$, niin tällöin $y < x$.

Tiedetään myös, että $c^2 + 3d^2 \neq 0$. Todistetaan tämä: Oletetaan, että $c^2 + 3d^2 = 0$. Tällöin $c = 0$ ja $d = 0$, koska neliöt $c^2, d^2 \geq 0$. Tällöin $a = mx$ ja $b = nx$, jolloin x jakaa sekä a:n että b:n. Tämä on ristiriita, koska $syt(a, b) = 1$. Eli täytyy olla $c^2 + 3d^2 \neq 0$.

Olkoon $g = syt(c, d)$. Tällöin Lemman 3.1 nojalla on olemassa luvut C, D siten, että $c = gC$, $d = gD$, $syt(C, D) = 1$. Nyt

$$xy = c^2 + 3d^2 = (gC)^2 + 3(gD)^2 = g^2\left(C^2 + 3D^2\right).$$

Oletetaan, että on olemassa alkuluku p, jolle pätee $p \mid g$ ja $p \nmid y$. Silloin $p \mid g$ ja $p \mid x$, eli on olemassa luvut X, G siten, että $x = Xp$ ja $g = Gp$. Koska

$$\begin{aligned} a = mx + c = mpX + GpC = p(mX + GC) \text{ ja} \\ b = nx + d = npX + GpD = p(nX + GD), \end{aligned}$$

niin $p \mid a$ ja $p \mid b$. Tämä ei ole mahdollista, koska $syt(a, b) = 1$. Tällöin ei ole olemassa alkulukua p, joka jakaa luvun g, muttei lukua y. Tämä todistaa, että $g \mid y$, josta seuraa, että $g^2 \mid y$.

Koska $g^2 \mid y$, niin on olemassa z siten, että $y = g^2z$. Sijoittamalla tämä yhtälöön $xy = g^2(C^2 + 3D^2)$, saadaan $xz = C^2 + 3D^2$, missä $syt(C, D) = 1$.

Nyt meillä on kaikki tarvittavat tiedot, jotta voimme osoittaa, että x on muotoa $p^2 + 3q^2$. Tehdään antiteesi: x ei ole tätä muotoa. Aiemmin saatiin, että $xz = C^2 + 3D^2$, missä $syt(C, D) = 1$. Tällöin Lemman 3.6 nojalla on olemassa w siten, että $w \mid z$ ja w ei ole muotoa $p^2 + 3q^2$. Nyt $w \neq 1$, koska jos olisi $w = 1$, niin se olisi muotoa $p^2 + 3q^2$ $(1 = 1^2 + 3(0)^2)$. Koska $w > 1$ ja $w \mid z$, niin $w < z$, ja koska $z < y$ ja $y < x$, niin $w < x$. Nyt on osoitettu, että x:n olemassaolo todistaa vielä pienemmän tekijän w olemassaolon. Vastaavasti voidaan osoittaa, että löytyy vielä pienempiä tekijöitä w', w'', joille $w'' < w' < w < x$. Tätä voidaan jatkaa edelleen pienempiin tekijöihin. Äärettömän laskeutumisen periaatteen nojalla tämä ei ole kuitenkaan mahdollista, joten x on muotoa $p^2 + 3q^2$. □

LEMMA 3.8. *Jos on olemassa luvut a, b, joilla on seuraavat ominaisuudet:*

(1) $syt(a, b) = 1$,
(2) *luvuista a, b toinen on parillinen ja toinen pariton ja*
(3) $a^2 + 3b^2$ *on kuutio, niin*

silloin on olemassa luvut u, v siten, että

(1) $a = u^3 - 9uv^2$,
(2) $b = 3u^2v - 3v^2$,
(3) $syt\,(u, v) = 1$ *ja*
(4) *luvuista* u, v *toinen on parillinen ja toinen pariton.*

TODISTUS. Oletuksen nojalla a^2+3b^2 on kuutio. Tällöin on olemassa luku s, jolle $s^3 = a^2 + 3b^2$. Tiedetään, että s on pariton, koska luvuista a, b toinen on pariton ja toinen parillinen. Lisäksi Lemman 3.7 perusteella tiedetään, että luvun s täytyy olla muotoa $u^2 + 3v^2$.

Nyt

$$\begin{aligned}\left(u^2+3v^2\right)^3 &= \left(u^2+3v^2\right)\left(u^2+3v^2\right)^2 = \left(u^2+3v^2\right)\left(u^4+6u^2v^2+9v^4\right)\\ &= \left(u^2+3v^2\right)\left(u^4+12u^2v^2-6u^2v^2+9v^4\right)\\ &= \left(u^2+3v^2\right)\left(\left(u^2-3v^2\right)^2+3\left(2uv\right)^2\right).\end{aligned}$$

Ja Lemman 3.2 nojalla

$$\begin{aligned}&\left(u^2+3v^2\right)\left(\left(u^2-3v^2\right)^2+3\left(2uv\right)^2\right)\\ &= \left(u\left(u^2-3v^2\right)-3v2uv\right)^2+3\left(u2uv+v\left(u^2-3v^2\right)\right)^2\end{aligned}$$

Edelleen

$$\begin{aligned}&\left(u\left(u^2-3v^2\right)-3v2uv\right)^2+3\left(u2uv+v\left(u^2-3v^2\right)\right)^2\\ &= \left(u^3-3uv^2-6uv^2\right)^2+3\left(2u^2v+u^2v-3v^3\right)^2\\ &= \left(u^3-9uv^2\right)^2+3\left(3u^2v-3v^3\right)^2.\end{aligned}$$

Oletuksen $s^3 = a^2 + 3b^2$ nojalla $a^2 + 3b^2 = (u^3 - 9uv^2)^2 + 3\,(3u^2v - 3v^3)^2$. Tämä tarkoittaa sitä, että me voimme määrittää luvut a, b siten, että

$$\begin{aligned}a &= u^3 - 9uv^2,\\ b &= 3u^2v - 3v^3,\end{aligned}$$

ja $syt\,(u, v) = 1$, koska muuten jokainen niiden yhteinen tekijä jakaisi sekä a:n että b:n. Tiedetään myös, että luvuista u, v toinen on parillinen ja toinen on pariton, koska

a) Jos luvut u, v ovat molemmat parittomia, niin a on kahden parittoman luvun erotuksena parillinen ja vastaavasti myös b on parillinen, mikä on kuitenkin mahdotonta, koska luvuista a ja b toinen on parillinen ja toinen on pariton.
b) Jos luvut u, v ovat molemmat parillisia, niin a on kahden parillisen luvun erotuksena parillinen ja vastaavasti myös b on parillinen, mikä on jälleen mahdotonta.

□

Seuraavan lemman avulla voidaan yhtälön $x^n + y^n = z^n$ ratkaisuja sieventää tiettyyn muotoon.

LEMMA 3.9. *Minkä tahansa yhtälön* $x^n + y^n = z^n$ *ratkaisu voidaan sieventää sellaiseen muotoon, jossa luvut* x, y, z *ovat keskenään jaottomia lukuja.*

TODISTUS. Jotta tämä voidaan todistaa, on todistettava kaksi asiaa:

(1) Jos tekijä jakaa mitkä tahansa kaksi arvoa tästä yhtälöstä, niin sen n. potenssi jakaa kolmannen arvon n:nnen potenssin.
(2) Jos tekijän n. potenssi jakaa jonkin arvon n:nnen potenssin, niin silloin tekijä jakaa myös kyseisen arvon.

Vaihe 1: Yhtälön $x^n + y^n = z^n$ kahden arvon yhteisen tekijän n. potenssi jakaa n:nnen potenssin kolmannesta arvosta.

Tapaus 1: Oletetaan, että $d \mid x$ ja $d \mid y$.

Koska $d \mid x$ ja $d \mid y$, niin on olemassa luvut x', y' siten, että $x = dx'$ ja $y = dy'$. Nyt

$$\begin{aligned} z^n = x^n + y^n &= (dx')^n + (dy')^n \\ &= d^n (x')^n + d^n (y')^n \\ &= d^n \left((x')^n + (y')^n \right). \end{aligned}$$

Tästä huomataan, että $d^n \mid z^n$.

Tapaus 2: Oletetaan, että $d \mid z$ ja $d \mid x$ tai $d \mid y$.

Oletetaan, että $d \mid z$ ja $d \mid x$. Tällöin on olemassa luvut x', z' siten, että $x = dx'$ ja $z = dz'$. Muotoillaan yhtälömuotoon $y^n = z^n - x^n$, jolloin

$$\begin{aligned} y^n = z^n - x^n &= (dz')^n - (dx')^n \\ &= d^n (z')^n - d^n (x')^n \\ &= d^n \left((z')^n + (x')^n \right). \end{aligned}$$

Tästä huomataan, että $d^n \mid y^n$. Vastaavasti saadaan tapaus, missä $d \mid z$ ja $d \mid y$.

Vaihe 2: Jos $d^n \mid x^n$, niin $d \mid x$.

Olkoon c suurin yhteinen tekijä luvuille d ja x. Lisäksi olkoon luvut D, X siten, että $d = cD$ ja $x = cX$. Nyt Lemman 3.1 nojalla $syt(X, D) = 1$. Koska $d^n \mid x^n$, niin olemassa k siten, että $x^n = kd^n$. Edellinen yhtälö saadaan esitettyä muodossa $(cX)^n = k(cD)^n$, mistä saadaan $c^n X^n = kc^n D^n$. Jakamalla molemmat puolet luvulla c^n, saadaan $X^n = D^n k$. Siitä seuraa, että $syt(D^n, k) = 1$. Osoitetaan tämä antiteesin avulla: Oletetaan, että $syt(D^n, k) = a, a > 1$. Silloin $a \mid D^n$ ja $a \mid X^n$. Nyt siis $syt(X, D) \neq 1$, joka on ristiriidassa aiemman tuloksen kanssa, jonka mukaan $syt(X, D) = 1$. Siten oletus on väärä ja $syt(D^n, k) = 1$.

Nyt voidaan Lemman 2.3 perusteella päätellä, että k on n. potenssi. Tämä tarkoittaa sitä, että on olemassa u siten, että $u^n = k$. Tästä tiedosta saadaan, että $D^n u^n = X^n$ ja $(Du)^n = X^n$. Nyt täytyy olla $Du = X$ ja siten kertomalla luvulla c saadaan, että $du = x$, mikä osoittaa, että $d \mid x$. □

Seuraavan lemman avulla voidaan tapauksen $n = 3$ todistaminen jakaa kahteen eri osaan.

LEMMA 3.10. *Olkoot a, b keskenään jaottomia lukuja, joista toinen on parillinen ja toinen pariton. Tällöin $syt\,(2a, a^2 + 3b^2) = 1$ tai 3.*

TODISTUS. Oletetaan, että on alkuluku f, joka jakaa luvut $2a$ ja $a^2 + 3b^2$. Luku f ei voi olla 2, koska a:n ja b:n ollessa eri parillisuutta $a^2 + 3b^2$ on pariton.

Oletetaan, että $f > 3$. Tällöin on luvut A, B siten, että $2a = fA$ ja $a^2 + 3b^2 = Bf$. Nyt $f \neq 2$, joten tiedetään, että luvun 2 täytyy jakaa luku A. Siten on luku H, joka on puolet luvusta A ja $a = fH$, eli $f \mid a$. Nyt yhdistämällä kaksi yhtälöä saadaan

$$3b^2 = Bf - a^2 = Bf - f^2H^2 = f\left(B - fH^2\right).$$

Koska f on suurempi kuin kolme, niin se ei voi jakaa lukua 3. Siten $f \mid b^2$ ja $f \mid b$. Tämä on kuitenkin ristiriita, koska oletimme, että luvut a ja b ovat keskenään jaottomia. Siten $syt\,(2a, a^2 + 3b^2) = 1$ tai 3. □

LAUSE 3.11. *Yhtälöllä $x^3 + y^3 = z^3$ ei ole kokonaislukuratkaisuja, kun $x, y, z \neq 0$.*

TODISTUS. Lemman 3.9 nojalla voidaan olettaa, että on nollasta eroavat pareittain keskenään jaottomat kokonaisluvut (eng. pairwise relatively prime) x, y ja z siten, että $x^3 + y^3 + z^3 = 0$. Koska luvut ovat pareittain jaottomia kokonaislukuja, niin $syt\,(x, y) = syt\,(x, z) = syt\,(y, z) = 1$. Tällöin korkeintaan yksi luvuista x, y, z on parillinen. Kuitenkin ainakin yksi luvuista on parillinen, koska jos x, y ovat parittomia, niin z on parillinen. Tällöin täsmälleen yksi luvuista on parillinen.

Oletetaan, että luvut x, y ovat parittomia ja luku z on parillinen. Kaikista yhtälön $x^3 + y^3 + z^3 = 0$ ratkaisuista valitaan se ratkaisu, missä $|z|$ on pienin mahdollinen. Nyt pitäisi äärettömän laskeutumisen menetelmällä osoittaa, että on olemassa nollasta eroavat pareittain jaottomat kokonaisluvut l, m, n siten, että $l^3 + m^3 = n^3$, n on parillinen ja $|z| > |n|$.

Koska tiedetään, että sekä $x + y$ että $x - y$ ovat molemmat parillisia, niin on olemassa kokonaisluvut a, b siten, että $2a = x + y$ ja $2b = x - y$, jolloin $x = a + b$ ja $y = a - b$, $a, b \neq 0$, $syt\,(a, b) = 1$. Koska luvut x, y ovat molemmat parittomia, niin toinen luvuista a, b on parillinen ja toinen pariton.

Siten

$$\begin{aligned} -z^3 = x^3 + y^3 &= (a+b)^3 + (a-b)^3 \\ &= a^3 + 3a^2b + 3ab^2 + b^3 + a^3 - 3a^2b + 3ab^2 - b^3 \\ &= 2a^3 + 6ab^2 \\ &= 2a\left(a^2 + 3b^2\right). \end{aligned}$$

Siitä seuraa helposti, että $a^2 + 3b^2$ on pariton, z on parillinen ja $8 \mid z^3$, joten $8 \mid 2a$. Tällöin $4 \mid a$, joten a on parillinen ja b on pariton. Nyt Lemman 3.10 nojalla $syt\,(2a, a^2 + 3b^2) = 1$ tai 3.

Tarkastellaan nämä molemmat tapaukset erikseen:

Tapaus 1: $syt\,(2a, a^2 + 3b^2) = 1$.

Koska $syt\,(2a, a^2 + 3b^2) = 1$ ja $-z^3 = 2a\,(a^2 + 3b^2)$, niin Lemman 2.3 nojalla $2a$ ja $a^2 + 3b^2$ ovat kuutioita:

$$2a = r^3,$$
$$a^2 + 3b^2 = s^3,$$

missä s on pariton. Lemmojen 3.7 ja 3.8 nojalla s on muotoa $s = u^2 + 3v^2$, missä on u, v siten, että

$$a = u^3 - 9uv^2,$$
$$b = 3u^2v - 3v^3.$$

Koska b on pariton, niin v on pariton ja u on parillinen. Lisäksi $u \neq 0$, $syt\,(u, v) = 1$ ja $3 \nmid u$. Luku r^3 voidaan esittää muodossa

$$r^3 = 2a = 2u\left(u^2 - 9v^2\right) = 2u\,(u + 3v)\,(u - 3v)\,.$$

Osoitetaan seuraavaksi, että luvut $2u$, $u + 3v$ ja $u - 3v$ ovat keskenään pareittain jaottomia kokonaislukuja. Ensiksi huomataan, että sekä $u + 3v$ että $u - 3v$ ovat parittomia, koska u on parillinen ja v on pariton. Jos luvulla u olisi yhteinen tekijä joko luvun $u + 3v$ tai luvun $u - 3v$ kanssa, niin tällöin tämä tekijä jakaisi myös luvun v, mikä olisi vastoin tietoa $syt\,(u, v) = 1$. Eli nyt $2u$ on jaoton sekä luvun $u + 3v$ että luvun $u - 3v$ kanssa. Jos jokin pariton alkuluku $p > 3$ jakaa luvut $u + 3v$ ja $u - 3v$, niin $p \mid u$, koska $2u = u - 3v + u + 3v$, ja tällöin $p \mid v$, koska $6v = u + 3v - (u - 3v)$. Myös tämä on mahdotonta. Nyt pitää vielä näyttää, että luku 3 ei jaa lukuja $u + 3v$ ja $u - 3v$. Jos luku 3 jakaa molemmat, niin $3 \mid u$, koska $2u = u - 3v + u + 3v$. Tällöin $3 \mid a$, koska $a = u^3 - 9uv^2$. Koska $syt\,(2a, a^2 + 3b^3) = 1$, niin $3 \nmid a$. Ja nyt luku 3 ei voi jakaa molempia. Näin ollen lukujen $2u$, $u - 3v$ ja $u + 3v$ täytyy olla pareittain keskenään jaottomia kokonaislukuja. Silloin Lemman 2.3 nojalla ne ovat kuutioita:

$$2u = -l^3,$$
$$u - 3v = m^3,$$
$$u + 3v = n^3,$$

missä l, m, n ovat nollasta poikkeavia lukuja. Tämä antaa toisen ratkaisun Fermat'n suurelle lauseelle tapauksessa $n = 3$:

$$l^3 = 2u = u - 3v + u + 3v = m^3 + n^3,$$

missä l on parillinen. Lisäksi, koska $b \neq 0$, $3 \nmid u$, niin

$$|z^3| = |2a\left(a^2 + 3b^2\right)| = |l^3\left(u^2 - 9v^2\right)\left(a^2 + 3b^2\right)| > |l^3|.$$

Tämä on ristiriita, koska oletimme, että $|z|$ on pienin mahdollinen ratkaisu.

Tapaus 2: $syt\,(2a, a^2 + 3b^2) = 3$.

Koska $3 \mid 2a$, niin $3 \mid a$. Koska $syt\,(a, b) = 1$, niin $3 \nmid b$. On siis olemassa luku c siten, että

$$a = 3c \text{ ja}$$
$$-z^3 = 2a\left(a^2 + 3b^2\right) = 2 \cdot 3c\left((3c)^2 + 3b^2\right) = 2 \cdot 3^2c\left(3c^2 + b^2\right) = 18c\left(3c^2 + b^2\right).$$

Osoitetaan, että luvut $18c$ ja $(3c^2 + b^2)$ ovat keskenään jaottomia: Koska $3 \nmid b$, niin $3 \nmid (3c^2 + b^2)$. Lisäksi, koska $a = 3c$, niin a:n ollessa parillinen myös c on parillinen. Jos luku c on parillinen ja b on pariton, niin $2 \nmid (3c^2 + b^2)$ ja tällöin $3c^2 + b^2$ on pariton. Lopuksi, koska $syt\,(a, b) = 1$, niin $syt\,(c, b) = 1$. Nyt on osoitettu, että $syt\,(18c, 3c^2 + b^2) = 1$. Tällöin Lemman 2.3 nojalla luvut $18c$ ja $(3c^2 + b^2)$ ovat kuutioita

$$18c = r^3,$$
$$3c^2 + b^2 = s^3,$$

missä s on pariton. Kuten Tapauksessa 1, myös tässä Lemmojen 3.7 ja 3.8 nojalla s on muotoa $s = u^2 + 3v^2$, missä on u, v siten, että

$$b = u^3 - 9uv^2,$$
$$c = 3u^2v - 3v^3.$$

Tällöin u on pariton, v on parillinen, $v \neq 0$, $syt\,(u, v) = 1$ ja luvut $2v$, $u + v$ ja $u - v$ ovat pareittain jaottomia kokonaislukuja. Koska

$$r^3 = 18c = 18\left(3u^2v - 3v^3\right) = 54v\,(u + v)\,(u - v) \text{ ja}$$
$$\left(\frac{r^3}{3}\right)^3 = 2v\,(u + v)\,(u - v)\,,$$

niin Lemman 2.3 nojalla ne ovat kuutioita:

$$2v = -l^3,$$
$$u + v = m^3,$$
$$u - v = -n^3.$$

Tällöin $l^3 + m^3 + n^3 = -2v + u + v - u + v = 0$, missä $l, m, n \neq 0$ ja l on parillinen. Nyt

$$|z^3| = 18|c|\left(3c^2 + b^2\right) = 54|v\left(u^2 - v^2\right)|\left(3c^2 + b^2\right) = 27|l|^3|u^2 - v^2|\left(3c^2 + b^2\right) > |l^3|.$$

Tämä on ristiriita, koska oletimme, että $|z|$ on pienin mahdollinen ratkaisu.

Siis yhtälöllä $x^3 + y^3 = z^3$ ei ole kokonaislukuratkaisuja, kun $x, y, z \neq 0$. □

Seuraus 3.12. *Yhtälöllä $x^n + y^n = z^n$ ei ole olemassa kokonaislukuratkaisua, kun n on jaollinen luvulla 3. Erityisesti yhtälöllä $x^6 + y^6 = z^6$ ei ole kokonaislukuratkaisua.*

LUKU 4

Tapaus $n = 5$

4.1. Kvadraattisista kokonaisluvuista

Tässä luvussa tutustutaan kvadraattisiin kokonaislukuihin, joita tarvitaan Fermat'n suuren lauseen tapauksen $n = 5$ todistamisessa. Luvussa huomataan, että kvadraattisilla kokonaisluvuilla on joitain parempia ominaisuuksia kuin rationaalisilla kokonaisluvuilla. Ne on esimerkiksi helpompi jakaa tekijöihin kuin rationaaliset kokonaisluvut. Lisäksi näytetään, että niin kauan kuin kvadraattisilla kokonaisluvuilla on yksikäsitteinen tekijöihin jako, voidaan niihin soveltaa jo olemassa olevia lemmoja, esim. Eukleideen Lemmaa 2.2. Tämän luvun tulokset ovat tärkeitä tapauksen $n = 5$ todistamiseksi, mutta eivät pääosassa tässä tutkielmassa, joten tämän luvun lemmojen todistuksia sivuutetaan.

Määritellään aluksi hieman algebran peruskäsitteitä ja esitetään niiden avulla määritelmä kvadraattisille kokonaisluvuille.

MÄÄRITELMÄ 4.1. Olkoon $A \neq \emptyset$ ja olkoon $*$ joukon A laskutoimitus. Alkio $e \in A$ on laskutoimituksen $*$ *neutraalialkio*, jos $e * g = g$ ja $g * e = g$ kaikilla $g \in A$.

MÄÄRITELMÄ 4.2. Olkoon $(A, *, \oplus)$ kahdella laskutoimituksella varustettu joukko. Laskutoimitus $*$ on *distributiivinen* laskutoimituksen $\oplus$ suhteen, jos

(1) $a * (b \oplus c) = (a * b) \oplus (a * c)$ kaikilla $a, b, c \in A$ ja
(2) $(b \oplus c) * a = (b * a) \oplus (c * a)$ kaikilla $a, b, c \in A$.

MÄÄRITELMÄ 4.3. Laskutoimituksella varustettu joukko $(G, *)$ on *ryhmä*, jos

(1) laskutoimitus $*$ on assosiatiivinen,
(2) laskutoimituksella $*$ on neutraalialkio ja
(3) jokaisella $g \in (G, *)$ on käänteisalkio.

MÄÄRITELMÄ 4.4. Ryhmä G on *kommutatiivinen*, jos sen laskutoimitus $*$ on kommutatiivinen eli $a * b = b * a$ kaikilla $a, b \in G$.

MÄÄRITELMÄ 4.5. Olkoon R epätyhjä joukko, jolle on määritelty kaksi assosiatiivista laskutoimitusta $+$ ja $\cdot$. Kolmikko $(R, +, \cdot)$ on *rengas*, jos

(1) $(R, +)$ on kommutatiivinen ryhmä,
(2) kertolasku on distributiivinen yhteenlaskun suhteen ja
(3) kertolaskulla on neutraalialkio $1 = 1_R \in R$.

MÄÄRITELMÄ 4.6. Jos A on rengas ja alkiolla $u \in A$ on käänteisalkio kertolaskun suhteen, niin u on renkaan A *yksikkö*.

MÄÄRITELMÄ 4.7. Olkoon R rengas ja olkoon $S \subset R$ vakaa yhteenlaskun ja kertolaskun suhteen. S on renkaan R *alirengas*, jos S varustettuna indusoiduilla laskutoimituksilla on rengas ja jos $1_S = 1_R$. (Katso tarvittaessa esitietoja lähteestä [**18**].)

MÄÄRITELMÄ 4.8. Rengas R on *kunta*, jos se on kommutatiivinen ja kaikki nollasta poikkeavat alkiot ovat yksiköitä.

MÄÄRITELMÄ 4.9. Olkoon K ja F kuntia. Jos F on kunnan K alirengas, niin F on kunnan K *alikunta* ja K on kunnan F *kuntalaajennus*. Kuntalaajennusta merkitään K/F.

MÄÄRITELMÄ 4.10. Olkoon R rengas, jossa on vähintään kaksi alkiota. Jos $a, b \in R$, $a, b \neq 0$ ja $ab = 0$, niin a ja b ovat nollan jakajia. Kommutatiivinen rengas R, jossa ei ole nollan jakajia, on *kokonaisalue*.

MÄÄRITELMÄ 4.11. Kunta K on kunnan $\mathbb{Q}$ *toisen asteen kuntalaajennus* eli *kvadraattinen lukukunta*, jos $K = \mathbb{Q}\left(\sqrt{d}\right) = \{a + b\sqrt{d} : a, b \in \mathbb{Q}\}$, missä $d \in \mathbb{Z}$ ei ole jaollinen minkään alkuluvun neliöllä.

MÄÄRITELMÄ 4.12. Olkoon L kunta ja K sen alikunta. Alkio $x \in L$ on *algebrallinen* kunnan K suhteen, jos on olemassa sellainen nollasta poikkeva polynomi f, jolle $f(x) = 0$ kunnassa L. Toisin sanoen, on olemassa $a_1, \ldots, a_n \in K$ siten, että $x^n + a_1 x^{n-1} + \cdots + a_n = 0$.

MÄÄRITELMÄ 4.13. Olkoon K/F kuntalaajennos ja olkoon $\alpha \in K$ algebrallinen F:n suhteen. Alinta positiivista astetta oleva polynomi $P \in K[X]$, jolle $P(a) = 0$, on a:n *minimipolynomi* kunnassa K. Merkintä $K[X]$ tarkoittaa kaikkien K-kertoimisten polynomien joukkoa. Katso tarkemmin [**18**, s. 75].

MÄÄRITELMÄ 4.14. Algebrallista lukua α, jonka minimipolynomin kertoimet ovat kaikki renkaassa $\mathbb{Z}$ kutsutaan *algebralliseksi kokonaisluvuksi* kunnassa $\mathbb{Q}(\alpha)$.

MÄÄRITELMÄ 4.15. Algebrallisia kokonaislukuja kunnassa $\mathbb{Q}\left(\sqrt{d}\right)$ kutsutaan *kvadraattisiksi kokonaisluvuiksi*. Tällöin jokainen kokonaisalueen $\mathbb{Z}\left[\sqrt{d}\right] = \{a+b\sqrt{d} : a, b \in \mathbb{Z}\}$ alkio on kvadraattinen kokonaisluku kunnassa $\mathbb{Q}\left(\sqrt{d}\right)$.

Seuraava lemma antaa tuloksen, jonka avulla voidaan esittää jokainen joukon $K = \mathbb{Q}\left(\sqrt{d}\right)$ alkio.

LEMMA 4.16. *Olkoon $K = \mathbb{Q}\left(\sqrt{d}\right)$, missä d ei ole jaollinen minkään alkuluvun neliöllä. Jos $d \equiv 1 \pmod 4$, niin joukon K kokonaisluvut ovat muotoa $\frac{a+b\sqrt{d}}{2}$, missä $a, b \in \mathbb{Z}$, a ja b ovat samaa parillisuutta. Jos $d \not\equiv 1 \pmod 4$, niin joukon K kokonaisluvut ovat muotoa $a + b\sqrt{d}$, missä $a, b \in \mathbb{Z}$.*

TODISTUS. Katso [**23**, s. 266–267]. □

MÄÄRITELMÄ 4.17. Funktiota $N : \mathbb{Z}\left[\sqrt{d}\right] \to \mathbb{Z}$,

$$N\left(s + t\sqrt{d}\right) = \left(s + t\sqrt{d}\right)\left(s - t\sqrt{d}\right) = s^2 - dt^2$$

kutsutaan *normiksi*.

LEMMA 4.18. *Olkoon d kokonaisluku, joka ei ole jaollinen minkään alkuluvun neliöllä. Silloin $u \in \mathbb{Z}\left[\sqrt{d}\right]$ on yksikkö, jos ja vain jos sen normi $N(u) = \pm 1$.*

TODISTUS. Katso [**13**, s. 347]. □

SEURAUS 4.19. *Jos* $\frac{a+b\sqrt{5}}{2}$ *on joukon* $K = \mathbb{Q}\left(\sqrt{d}\right)$ *yksikkö, niin*

$$\left(\frac{a+b\sqrt{5}}{2}\right)\left(\frac{a-b\sqrt{5}}{2}\right) = \frac{a-5b^2}{4} = \pm 1,$$

ts. $a - 5b^2 = \pm 4$.

Määritellään sitten Eukleideen alue. Sillä on useita mieluisia ominaisuuksia, joita on esitetty määritelmän jälkeen.

MÄÄRITELMÄ 4.20. Kokonaisalue R on *Eukleideen alue*, (eng. Euclidean domain), jos on olemassa funktio $d : R \setminus \{0\} \to \mathbb{N}$, jolle pätee:

(1) Jos $a, b \in R \setminus \{0\}$, niin $d(a) \leq d(ab)$.
(2) Kaikilla kokonaisluvuilla $a, b \in R$, $b \neq 0$ löydetään $q, r \in R$ siten, että $a = qb + r$ ja $r = 0$ tai $d(r) < d(b)$.

LEMMA 4.21. *Jokainen Eukleideen alueen nollasta poikkeava alkio, joka ei ole yksikkö, voidaan esittää järjestystä ja yksiköillä kertomista vaille yksikäsitteisesti jaottomien alkioiden äärellisenä tulona.*

TODISTUS. Katso [**18**, s. 88]. □

MÄÄRITELMÄ 4.22. Kokonaisalueen $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$ alkioita kutsutaan *Dirichlet'n kokonaisluvuiksi*. Nämä alkiot ovat muotoa $a + b\left(\frac{1+\sqrt{5}}{2}\right)$, missä $a, b \in \mathbb{Z}$.

LEMMA 4.23. $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$ *on Eukleideen alue.*

TODISTUS. [**23**, s. 292-293]. □

SEURAUS 4.24. *Kokonaisalueella* $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$ *on yksikäsitteinen tekijöihin jako. Tämän ansiosta voimme käyttää tässä joukossa yleisesti käytettäviä laskumenetelmiä, kuten Lemmoja 2.2 ja 2.3.*

LEMMA 4.25. *Kaikki Dirichlet'n yksiköt, eli kokonaisalueen* $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$ *yksiköt, ovat samaa muotoa* $\pm\left(\frac{1+\sqrt{5}}{2}\right)^{\pm n}$.

TODISTUS. Katso [**10**]. □

Kokonaisalueiden teoriassa on hieman erilainen määritelmä alkuluvulle kuin perinteinen kokonaislukujen määritelmä.

MÄÄRITELMÄ 4.26. Kokonaisalueen K alkio p, joka ei ole yksikkö, on *alkualkio* (tai alkuluku), jos kaikille $a, b \in K$ pätee $p \mid a$ tai $p \mid b$, jos $p \mid ab$.

Näin ollen alkualkio toteuttaa Eukleideen Lemman 2.2 vastineen tarkasteltavaksi renkaassa.

LEMMA 4.27. *Jos* α *on kokonaisluku kokonaisalueessa* $\mathbb{Q}\left(\sqrt{d}\right)$ *ja* $N(\alpha)$ *on jaoton luku, niin* α *on alkualkio, eli jaoton kokonaisalueessa* $\mathbb{Q}\left(\sqrt{d}\right)$.

TODISTUS. Katso [**23**, s. 277]. □

LEMMA 4.28. *$\sqrt{5}$ on alkualkio kokonaisalueessa $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$.*

TODISTUS. $\sqrt{5}$ on kokonaisalueessa $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$, koska $\frac{0+2\sqrt{5}}{2} = \sqrt{5}$. Koska $N\left(\sqrt{5}\right) = -5$, missä -5 on alkuluku, niin Lemman 4.27 nojalla $\sqrt{5}$ on alkualkio eli jaoton alueessa $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$. □

LEMMA 4.29. *2 on alkualkio kokonaisalueessa $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$.*

TODISTUS. Katso [**11**]. □

4.2. Sophie Germainin lause

Tässä luvussa esitellään ensin yksi Fermat'n tunnetuimmista tuloksista, joka on nimetty Fermat'n pieneksi lauseeksi. Fermat esitti kyseisen tuloksen vuonna 1640 [**9**]. Fermat'n pientä lausetta hyödynnetään Sophie Germainin lauseen todistamisessa. Kuten jo Luvussa 1 tuli ilmi, oli Sophie Germainilla merkittävä rooli Fermat'n suuren lauseen todistamisen edistämisessä. Hän keksi tunnetuksi tulleen lauseensa, jonka perusteella yhtälön $x^n + y^n = z^n$ mahdollisesti toteuttavien ratkaisujen täytyy toteuttaa tietyt ehdot [**22**, s. 137].

LAUSE 4.30 (Fermat'n pieni lause). *Jos p on alkuluku ja $p \nmid a$, niin $a^{p-1} \equiv 1 \pmod{p}$.*

TODISTUS. Katso [**7**, s. 24] □

LAUSE 4.31 (Sophie Germainin Lause). *Jos $x^n + y^n = z^n$, missä $n \geq 3$ ja $2n + 1$ ovat alkulukuja, niin silloin $n \mid xyz$.*

TODISTUS. Lemman 3.9 nojalla voidaan olettaa, että luvut x, y, z ovat keskenään jaottomia kokonaislukuja. Tehdään antiteesi, että n ei jaa tuloa xyz.

Koska n on pariton, niin $-z$ voidaan korvata luvulla z' ja saadaan

$$x^n + y^n + (z')^n = 0.$$

Nyt Lemman 4.35 nojalla

$$-x^n = (y + z)\left(y^{n-1} - y^{n-2}z + \ldots - yz^{n-2} + z^{n-1}\right).$$

Luvut $y + z$ ja $y^{n-1} - y^{n-2}z + \ldots - yz^{n-2} + z^{n-1}$ ovat keskenään jaottomia kokonaislukuja. Osoitetaan tämä: Tehdään antiteesi, jonka mukaan ne eivät ole keskenään jaottomia kokonaislukuja. Silloin on olemassa alkuluku p siten, että $p \mid (y + z)$ ja $p \mid (y^{n-1} - y^{n-2}z + \ldots - yz^{n-2} + z^{n-1})$. Tästä tiedetään, että $z \equiv -y \pmod{p}$. Käyttämällä kongruenssin ominaisuuksia saadaan, että

$$\begin{aligned} y^{n-1} - y^{n-2}z + ... - yz^{n-2} + z^{n-1} &\equiv y^{n-1} - y^{n-2}(-y) + \ldots - y(-y)^{n-2} + (-y)^{n-1} \\ &\equiv y^{n-1} + y^{n-1} + \ldots + y^{n-1} + y^{n-1} \equiv ny^{n-1}. \end{aligned}$$

Nyt Lemman 2.2 nojalla joko $p \mid n$ tai $p \mid y^{n-1}$. Jos $p \mid n$, niin n:n ollessa alkuluku pitäisi olla $p = n$ ja silloin luku $n \mid (-x)^n$. Eukleideen Lemman 2.2 nojalla saadaan, että $n \mid x$. Tämä on kuitenkin mahdotonta, koska n ei jaa tuloa xyz. Tällöin $p \nmid n$.

Jos $p \mid y^{n-1}$, niin Eukleideen Lemman avulla saadaan, että $p \mid y$. Koska $p \mid y$ ja $p \mid (y+z)$, niin $p \mid z$. Tämä on kuitenkin mahdotonta, koska $syt\,(y,z) = 1$. Tällöin $p \nmid y^{n-1}$. Eli nyt on saatu ristiriita sen oletuksen kanssa, jonka mukaan luvut $y+z$ ja $y^{n-1} - y^{n-2}z + ... - yz^{n-2} + z^{n-1}$ eivät ole keskenään jaottomia kokonaislukuja. Silloin niiden täytyy olla keskenään jaottomia kokonaislukuja.

Tällöin Lemman 2.3 nojalla on olemassa a siten, että

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

Vastaavasti voidaan kirjoittaa, että

$$-y^n = (x+z)\left(x^{n-1} - x^{n-2}z + \ldots - xz^{n-2} + z^{n-1}\right) \text{ ja}$$
$$-z^n = (x+y)\left(x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1}\right),$$

jolloin on olemassa luvut b ja c siten, että

$$z + x = b^n \text{ ja}$$
$$x + y = c^n.$$

Osoitetaan, että mikä tahansa $u^n \equiv \pm 1$ tai $0 \pmod{2n+1}$: Oletetaan, että $(2n+1) \nmid u^n$ (muussa tapauksessa $u^n \equiv 0 \pmod{2n+1}$). Koska $2n+1$ on alkuluku, niin Fermat'n pienen lauseen, eli Lauseen 4.30, nojalla $u^{2n} \equiv 1 \pmod{2n+1}$. Ja silloin $(u^n)^2 \equiv 1 \pmod{2n+1}$. Nyt kongruenssin ominaisuuksien mukaan $u^n \equiv \pm 1 \pmod{2n+1}$.

Nyt huomataan, että $(2n+1) \mid xyz'$. Koska, jos $(2n+1) \nmid xyz'$, niin

$$x^n \equiv \pm 1,$$
$$y^n \equiv \pm 1 \text{ ja}$$
$$z^n \equiv \pm 1.$$

Tämä on kuitenkin mahdotonta, koska $x^n + y^n + (-z)^n \equiv 0 \pmod{2n+1}$, mutta $\pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod{2n+1}$. Joten $(2n+1) \mid xyz'$. Oletetaan, että $(2n+1) \mid x$ (vastaavalla tavalla voidaan perustella tapaukset, missä $(2n+1) \mid y$ tai $(2n+1) \mid z'$). Silloin

$$2x = z + x + x + y - y - z = (z+x) + (x+y) + (-y-z) = b^n + c^n + (-a)^n.$$

Nyt voidaan käyttämällä samaa tapaa kuin edellä, osoittaa, että $(2n+1) \mid acb$. Koska oletettiin, että $(2n+1) \mid x$, niin $b^n + c^n + (-a)^n \equiv 0 \pmod{2n+1}$. Nyt oletetaan, että $(2n+1) \nmid acb$. Silloin

$$b^n \equiv \pm 1,$$
$$c^n \equiv \pm 1 \text{ ja}$$
$$(-a)^n \equiv \pm 1.$$

Tämä on kuitenkin mahdotonta, koska $\pm 1 \pm 1 \pm 1 \not\equiv 0 \pmod{2n+1}$. Tällöin $(2n+1) \mid acb$.

Kuitenkaan $2n+1$ ei voi jakaa lukua abc. Todistetaan tämä:

$(2n+1) \nmid b$: Jos $(2n+1) \mid b$, niin $(2n+1) \mid b^n$ ja silloin $(2n+1) \mid z + x$. Tiedetään, että $(2n+1) \mid x$, joten silloin $(2n+1) \mid z$. Tämä on kuitenkin mahdotonta,

koska $syt\,(x, z) = 1$.

Koska $syt\,(x, y) = 1$, niin vastaavasti kuin edellä saadaan $(2n + 1) \nmid c$.

$(2n + 1) \nmid a$: Oletetaan, että $(2n + 1) \mid a$. Silloin $(2n + 1) \mid (y + z)$ ja $z \equiv -y \pmod{2n + 1}$. Aiemman perusteella tiedetään, että on olemassa luvut d ja e siten, että

$$d^n = y^{n-1} - y^{n-2}z + \ldots - yz^{n-2} + z^{n-1} \text{ ja}$$
$$e^n = x^{n-1} - x^{n-2}y + \ldots - xy^{n-2} + y^{n-1}.$$

Käyttämällä tietoa $z \equiv -y \pmod{2n + 1}$ saadaan, että

$$d^n \equiv ny^{n-1} \pmod{2n + 1}.$$

Oletus $(2n + 1) \mid x$ on yhtäpitävää väitteen $x \equiv 0 \pmod{2n + 1}$ kanssa, jolloin saadaan

$$e^n \equiv 0^{n-1} - 0^{n-2}y + \ldots - 0y^{n-2} + y^{n-1} \equiv y^{n-1} \pmod{2n + 1}.$$

Yhdistämällä edelliset saadaan

$$d^n \equiv ne^n \pmod{2n + 1}.$$

Nyt tiedetään, että $d^n \equiv \pm 1$ tai $0 \pmod{2n + 1}$ ja $e^n \equiv \pm 1$ tai $0 \pmod{2n + 1}$. Tällöin molempien lukujen täytyy olla 0, koska $0 \equiv n \cdot 0$. Mutta jos $(2n + 1) \mid d^n$ ja $(2n + 1) \mid e^n$, niin Lemman 2.2 nojalla $(2n + 1) \mid d$ ja $(2n + 1) \mid e$. Koska $(2n + 1) \mid e$, niin $(2n + 1) \mid y$. Silloin $(2n + 1) \mid y$ ja $(2n + 1) \mid x$, mikä on vastoin oletusta $syt\,(x, y) = 1$. Joten $(2n + 1) \nmid a$.

Nyt siis $(2n + 1) \mid acb$, mutta $(2n + 1) \nmid abc$, mikä on ristiriita ja näin ollen $n \mid xyz$. □

Seuraus 4.32. *Jos $x^5 + y^5 = z^5$, niin $5 \mid xyz$.*

4.3. Fermat'n suuri lause tapauksessa $n = 5$

Jotta yhtälöllä $x^5 + y^5 = z^5$ voisi olla ratkaisu, niin Sophie Germainin lauseen 4.31 nojalla $5 \mid xyz$. Nyt tässä luvussa tutkitaan tapauksia, missä $5 \mid z$ tai $5 \mid x$ (tai $5 \mid y$). Näiden tapausten tutkimista varten todistamme ensin muutamia lemmoja. Lopulta luvun tuloksista seuraa Fermat'n suuren lauseen päteminen tapauksessa $n = 5$.

Esitellään aluksi niin sanottu binomikaava:

$$(a + b)^n = a^n + \sum_{m=1}^{n-1} \binom{n}{m} a^{n-m}b^m + b^n. \tag{4.1}$$

Binomikaavan avulla voidaan esittää tulos $(a + b)$:n viidennen potenssin ja $(a - b)$:n viidennen potenssin summalle.

Lemma 4.33. $(a + b)^5 + (a - b)^5 = 2a\,(a^4 + 10a^2b^2 + 5b^4)$

Todistus. Käyttämällä binomikaavaa (4.1) saadaan

$$(a + b)^5 = a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5$$
$$(a - b)^5 = a^5 - 5a^4b + 10a^3b^2 - 10a^2b^3 + 5ab^4 - b^5.$$

Summaamalla nämä kaksi lauseketta yhteen saadaan

$$\begin{aligned}(a+b)^5 + (a-b)^5 &= a^5 + 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 + b^5 \\ &\quad + \left(a^5 - 5a^4b + 10a^3b^2 + 10a^2b^3 + 5ab^4 - b^5\right) \\ &= 2a^5 + 20a^3b^2 + 10ab^4 = 2a\left(a^4 + 10a^2b^2 + 5b^4\right).\end{aligned}$$

□

Kaksi seuraavaa lemmaa auttavat tiettyä muotoa olevien lausekkeiden muokkaamista. Näiden lemmojen todistukset ovat suoraviivaisia laskuja.

LEMMA 4.34. *Jos*

a) $t = q^4 + 50q^2r^2 + 125r^4$,
b) $u = q^2 + 25r^2$ *ja*
c) $v = 10r^2$,

niin $t = u^2 - 5v^2$.

TODISTUS. Nyt

$$\begin{aligned}u^2 &= \left(q^2 + 25r^2\right)^2 = q^4 + 50q^2r^2 + 625r^4 \text{ ja} \\ -5v^2 &= -5\left(10r^2\right)^2 = -500r^4.\end{aligned}$$

Tällöin

$$\begin{aligned}u^2 - 5v^2 &= \left(q^2 + 25r^2\right)^2 - 5\left(10r^2\right)^2 \\ &= q^4 + 50q^2r^2 + 625r^4 - 500r^4 \\ &= q^4 + 50q^2r^2 + 125r^4 = t.\end{aligned}$$

□

LEMMA 4.35. *Jos* $n \geq 5$ *on pariton, niin*

$$a^n + b^n = (a+b)\left(a^{(n-1)} - a^{(n-2)}b + ... - ab^{(n-2)} + b^{(n-1)}\right).$$

TODISTUS.

$$\begin{aligned}&(a+b)\left(a^{n-1} - a^{n-2}b + \ldots - ab^{n-2} + b^{n-1}\right) \\ &= a\left(a^{n-1} - a^{n-2}b + a^{n-3}b^2 \ldots - ab^{n-2} + b^{n-1}\right) \\ &\quad + b\left(b^{n-1} + a^{n-1} - a^{n-2}b + \ldots + a^2b^{n-3} - ab^{n-2}\right) \\ &= a^n - a^{n-1}b + a^{n-2}b^2 \ldots - a^2b^{n-2} + ab^{n-1} \\ &\quad + b^n + a^{n-1}b - a^{n-2}b^2 + \ldots + a^2b^{n-2} - ab^{n-1} \\ &= a^n + b^n.\end{aligned}$$

□

LEMMA 4.36. *Olkoon kokonaisluvut* a, b *siten, että*

a) *toinen luvuista* a *ja* b *on pariton ja toinen on parillinen,*
b) *syt* $(a, b) = 1$,
c) $a, b \neq 0$,
d) $5 \nmid a$,
e) $5 \mid b$,

f) $a^2 - 5b^2$ *on viides potenssi,*

g) *on olemassa kokonaisluvut* h, k *siten, että* $a + b\sqrt{5} = \left(\frac{h+k\sqrt{5}}{2}\right)^5$,

h) h, k *ovat samaa parillisuutta.*

Tällöin h *ja* k *ovat parillisia.*

Todistus. Oletuksen ja kaavan (4.1) nojalla

$$\begin{aligned}\left(h + k\sqrt{5}\right)^5 &= h^5 + 5h^4k\sqrt{5} + 50h^3k^2 + 50h^2k^3\sqrt{5} + 125hk^4 + 25k^5\sqrt{5} \\ &= h^5 + 50h^3k^2 + 125hk^4 + \left(5h^4k + 50h^2k^3 + 25k^5\right)\sqrt{5} \\ &= 2^5\left(a + b\sqrt{5}\right) = 2^5a + 2^5b\sqrt{5},\end{aligned}$$

jolloin

$$2^5b = 5h^4k + 50h^2k^3 + 25k^5 = 5k\left(h^4 + 10h^2k^2 + 5k^4\right).$$

Oletetaan, että h ja k ovat parittomia. Nyt $2 \nmid 5$ ja $2 \nmid k$, joten Lemman 2.2 nojalla $2^5 = 32 \mid (h^4 + 10h^2k^2 + 5k^4)$. Koska h on pariton, niin $h \equiv 1 \pmod 2$. Tällöin $h \equiv \pm1, \pm3, \pm5, \ldots$ tai $\pm15 \pmod{32}$. Tällöin $h^2 \equiv 1, 9, 17$ tai $25 \pmod{32}$ ja edelleen $h^4 \equiv 1$ tai $17 \pmod{32}$. Vastaava päättely voidaan tehdä luvuille k, k^2 ja k^4. Tällöin $h^4 + 10h^2k^2 + 5k^4$ on kongruentti luvun 16 kanssa modulo 32, koska joko

$$1 + 10k^2 + 5k^4 \equiv \begin{cases} 1 + 10 + 5 \equiv 16, \\ 1 + 90 + 85 \equiv 16, \end{cases}$$

tai

$$17 + 26k^2 + 5k^4 \equiv \begin{cases} 17 + 26 + 5 \equiv 16, \\ 17 + 234 + 85 \equiv 16, \end{cases}$$

mikä on ristiriita sen kanssa, että $2^5 = 32 \mid (h^4 + 10h^2k^2 + 5k^4)$. Tällöin luvut h ja k ovat parillisia. □

Seuraavien lemmojen todistuksissa käytämme luvussa 4.1 kvadraattisille luvuille esitettyjä ominaisuuksia.

Lemma 4.37. *Olkoon kokonaisluvut* a, b *siten, että*

a) $syt\,(a, b) = 1$,

b) *toinen luvuista* a *ja* b *on pariton ja toinen on parillinen,*

c) $a, b \neq 0$,

d) $5 \nmid a$,

e) $5 \mid b$,

f) $a + b\sqrt{5} = \left(\frac{m+n\sqrt{5}}{2}\right)^5\left(\frac{t+u\sqrt{5}}{2}\right)$, *missä* $\left(\frac{t+u\sqrt{5}}{2}\right)$ *on yksikkö ja* $u = 0$.

Silloin:

i) $a = c\,(c^4 + 50c^2d^2 + 125d^4)$,

ii) $b = 5d\,(c^4 + 10c^2d^2 + 5d^4)$,

iii) $syt\,(c, d) = 1$,

iv) *toinen luvuista* c *ja* d *on pariton ja toinen on parillinen,*

v) $5 \nmid c$,

vi) $c, d \neq 0$.

TODISTUS. Olkoon $\frac{m'+n'\sqrt{5}}{2} = \left(\frac{m+n\sqrt{5}}{2}\right)^5$. Tällöin kaavan (4.1) nojalla

$$\frac{m'+n'\sqrt{5}}{2} = \frac{m^5+5m^4n\sqrt{5}+50m^3n^2+50m^2n^3\sqrt{5}+125mn^4+25n^5\sqrt{5}}{2^5}.$$

Edelleen

$$\begin{aligned} m'+n'\sqrt{5} &= \frac{m^5+5m^4n\sqrt{5}+50m^3n^2+50m^2n^3\sqrt{5}+125mn^4+25n^5\sqrt{5}}{2^4} \\ &= \frac{m^5+50m^3n^2+125mn^4}{2^4} + \frac{5m^4n+50m^2n^3+25n^5}{2^4}\sqrt{5}, \end{aligned}$$

ja näin ollen $m' = \frac{m^5+50m^3n^2+125mn^4}{2^4}$ ja $n' = \frac{5m^4n+50m^2n^3+25n^5}{2^4}$. Tästä seuraa, että $16m' \equiv m^5 \pmod 5$ ja $16n' \equiv 0 \pmod 5$ ja $5 \mid n'$. Nyt oletusta käyttämällä saadaan, että

$$a+b\sqrt{5} = \left(\frac{m'+n'\sqrt{5}}{2}\right)\left(\frac{t+u\sqrt{5}}{2}\right) = \frac{m't+m'u\sqrt{5}+n't\sqrt{5}+5n'u}{4},$$

ja silloin

$$\begin{aligned} 4a &= m't+5n'u, \\ 4b &= m'u+n't. \end{aligned}$$

Nyt, jos $5 \mid m'$, niin $5 \mid a$, mikä on vastoin oletusta. Siten $5 \nmid m'$. Koska $16m' \equiv m^5 \pmod 5$ ja $5 \nmid m'$, niin $5 \nmid m$. Lisäksi, koska $5 \mid n'$, $5 \mid 4b$ ja $5 \nmid m'$, niin $5 \mid u$. Koska $u = 0$ ja $\frac{t+u\sqrt{5}}{2}$ on yksikkö, niin $t = \pm 2$ ja siten $a+b\sqrt{5} = \pm\left(\frac{m+n\sqrt{5}}{2}\right)^5$. Tällöin Lemman 4.36 ja tiedon $m \equiv n \pmod 2$ nojalla m ja n ovat parillisia. Olkoon $c = \pm\frac{m}{2}$ ja $d = \pm\frac{n}{2}$. Silloin

$$a+b\sqrt{5} = \pm\left(c+d\sqrt{5}\right)^5 = c^5+5c^4d\sqrt{5}+50c^3d^2+50c^2d^3\sqrt{5}+125cd^4+25d^5\sqrt{5}$$

ja

$$\begin{aligned} a &= c^5+50c^3d^2+125cd^4 = c\left(c^4+50c^2d^2+125d^4\right), \\ b &= 5c^4d+50c^2d^3+25d^5 = 5d\left(c^4+10c^2d^2+5d^4\right). \end{aligned}$$

Koska $syt\,(a,b) = 1$, $c \mid a$ ja $d \mid b$, niin $syt\,(c,d) = 1$. Selvästi toinen luvuista c ja d on parillinen ja toinen pariton. $5 \nmid c$, koska $5 \nmid m$. Koska $a, b \neq 0$, niin myös $c, d \neq 0$. □

LEMMA 4.38. *Olkoon kokonaisluvut a, b siten, että*

a) $syt\,(a,b) = 1$,
b) *toinen luvuista a ja b on pariton ja toinen on parillinen,*
c) $a, b \neq 0$,
d) $5 \nmid a$,
e) $5 \mid b$,
f) $a+b\sqrt{5} = \left(\frac{m+n\sqrt{5}}{2}\right)^5\left(\frac{t+u\sqrt{5}}{2}\right)$, *missä* $\left(\frac{t+u\sqrt{5}}{2}\right)$ *on yksikkö ja* $u \neq 0$.

Silloin:

i) $a = c\,(c^4+50c^2d^2+125d^4)$,

ii) $b = 5d\,(c^4 + 10c^2d^2 + 5d^4)$,
iii) *syt* $(c, d) = 1$,
iv) *toinen luvuista* c *ja* d *on pariton ja toinen on parillinen,*
v) $5 \nmid c$,
vi) $c, d \neq 0$.

Todistus. Koska $\frac{t+u\sqrt{5}}{2}$ on yksikkö, niin Lemman 4.25 nojalla on olemassa kokonaisluku $e \neq 0$ siten, että

$$\frac{t + u\sqrt{5}}{2} = \pm \left(\frac{1 + \sqrt{5}}{2} \right)^e .$$

Korvaamalla $\frac{1+\sqrt{5}}{2}$ tarvittaessa käänteisalkiolla $-\frac{1-\sqrt{5}}{2}$, voidaan olettaa, että $e > 0$. Itse asiassa $e \geq 2$, koska jos $e = 1$, niin $u = \pm 1$, mikä ei ole jaollinen viidellä (edellisen Lemman 4.37 nojalla $5 \mid u$, koska $5 \mid b$). Nyt voidaan olettaa, että

$$\frac{t + u\sqrt{5}}{2} = \pm \frac{\left(1 + \sqrt{5}\right)^e}{2^e}.$$

Tästä seuraa, että

$$\pm \left(2^{e-1}\right) \left(t + u\sqrt{5} \right) = \left(1 \pm \sqrt{5} \right)^e .$$

Käyttämällä binomikaavaa (4.1) saadaan, että

$$\pm 2^{e-1} u = e + 5 \binom{e}{3} + 5^2 \binom{e}{5} + \cdots ,$$

joten $\pm 2^{e-1} u \equiv \pm e \pmod 5$ ja koska $5 \mid u$, niin $5 \mid e$. Silloin on olemassa f siten, että $e = 5f$. Olkoon

$$\frac{c' + d'\sqrt{5}}{2} = \left(\frac{m + n\sqrt{5}}{2} \right) \left(\frac{1 \pm \sqrt{5}}{2} \right)^f ,$$

missä $c' \equiv d' \pmod 2$. Silloin $a + b\sqrt{5} = \pm \left(\frac{c'+d'\sqrt{5}}{2} \right)^5$. Nyt, koska $c' \equiv d' \pmod 2$, niin Lemman 4.36 nojalla sekä c' että d' ovat parillisia. Silloin on olemassa luvut $c = \pm\frac{c'}{2}$ ja $d = \pm\frac{d'}{2}$ ja saadaan yhtälö $a + b\sqrt{5} = \pm \left(c + d\sqrt{5} \right)^5$. Loppu todistetaan täysin vastaavasti Lemman 4.37 kanssa. □

Lemma 4.39. *Olkoon kokonaisluvut* a, b *siten, että*

a) *syt* $(a, b) = 1$,
b) *toinen luvuista* a *ja* b *on pariton ja toinen on parillinen,*
c) $5 \nmid a$,
d) $5 \mid b$,
e) $a^2 - 5b^2$ *on viides potenssi.*

Silloin on kokonaisluvut c, d *siten, että*

i) $a = c\,(c^4 + 50c^2d^2 + 125d^4)$,
ii) $b = 5d\,(c^4 + 10c^2d^2 + 5d^4)$,
iii) *syt* $(c, d) = 1$,
iv) *toinen luvuista* c *ja* d *on pariton ja toinen on parillinen,*
v) $5 \nmid c$,

vi) $5 \mid d$,
vii) $c, d \neq 0$.

TODISTUS. Oletetaan, että $syt\left(a + b\sqrt{5}, a - b\sqrt{5}\right) = d > 1$. Tällöin on olemassa luvut e, f siten, että

$$de = a + b\sqrt{5},$$
$$df = a - b\sqrt{5}.$$

Nyt

$$a + b\sqrt{5} + a - b\sqrt{5} = 2a = de + df = d\,(e + f) \text{ ja}$$
$$a + b\sqrt{5} - \left(a - b\sqrt{5}\right) = 2b\sqrt{5} = d\,(e - f)\,.$$

Nyt, koska $\sqrt{5}$ on jaoton Lemman 4.28 nojalla, niin jos $d \mid \sqrt{5}$, täytyy olla $d = \sqrt{5}$. Koska $d \mid 2a$, niin tällöin $\sqrt{5} \mid 2a$ ja silloin $5 \mid 4a^2$. Tämä on kuitenkin mahdotonta, koska $5 \nmid a$. Siten $d \nmid \sqrt{5}$. Tällöin Lemman 2.2 nojalla $d \mid 2b$. Koska $d \mid 2a$, $d \mid 2b$ ja $syt(a, b) = 1$, niin $d \mid 2$. Lemman 4.29 nojalla 2 on jaoton, joten $d = 2$. Tällöin $4 \mid \left(a + b\sqrt{5}\right)\left(a - b\sqrt{5}\right) = a^2 - 5b^2$. Tämä on kuitenkin mahdotonta, koska lukujen a ja b ollessa eri parillisuutta, $a^2 - 5b^2$ on aina pariton. Näin ollen $syt(a + b\sqrt{5}, a - b\sqrt{5}) = 1$.

Koska kokonaisalueessa $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2}\right)$ on yksikäsitteinen tekijöihin jako, niin voidaan Lemmaa 2.3 ja oletusta $a^2 - 5b^2$ on viides potenssi apuna käyttäen päätellä, että $a + b\sqrt{5}$ ja $a - b\sqrt{5}$ ovat viidensiä potensseja. Tämä tarkoittaa sitä, että on olemassa luvut m, n, t, u siten, että $a + b\sqrt{5} = \left(\frac{m+n\sqrt{5}}{2}\right)^5 \left(\frac{t+u\sqrt{5}}{2}\right)$, missä $\frac{t+u\sqrt{5}}{2}$ on yksikkö. Nyt, jos $u = 0$, niin Lemman 4.37 nojalla saadaan haluttu tulos. Jos $u \neq 0$, niin tällöin Lemman 4.38 nojalla saadaan haluttu lopputulos. □

LEMMA 4.40. *Ei ole olemassa kokonaislukuja x, y, z siten, että $x^5 + y^5 = z^5$, missä $xyz \neq 0$, $syt\,(x, y, z) = 1$, x ja y ovat parittomia ja z on parillinen ja $5 \mid z$.*

TODISTUS. Antiteesi: On olemassa kokonaisluvut x, y, z siten, että $x^5 + y^5 = z^5$, missä $xyz \neq 0$, $syt\,(x, y, z) = 1$, x ja y ovat parittomia ja z on parillinen ja $5 \mid z$. Koska $5 \mid z$ ja z on parillinen, niin on olemassa luvut m, n, z' siten, että $z = 2^m 5^n z'$, missä $m \geq 1$, $n \geq 1$. Koska voidaan kasvattaa m:n ja n:n potenssit riittävän suuriksi, niin $syt\,(z', 2) = 1$, $syt\,(z', 5) = 1$. Koska $z = 2^m 5^n z'$ ja $z^5 = 2^{5m} 5^{5n} (z')^5$, niin $2^{5m} 5^{5n} (z')^5 = x^5 + y^5$.

Koska luvut x, y ovat parittomia, niin $x + y$ ja $x - y$ ovat parillisia. Tällöin on luvut p, q siten, että

$$x + y = 2p \text{ ja}$$
$$x - y = 2q.$$

Nyt

$$x = \frac{1}{2}(x + y + x - y) = \frac{1}{2}2x = \frac{1}{2}(2p + 2q) = p + q \text{ ja}$$
$$y = \frac{1}{2}(x + y - (x - y)) = \frac{1}{2}2y = \frac{1}{2}(2p - 2q) = p - q.$$

Jos on olemassa luku $d > 1$ siten, että $d \mid p$ ja $d \mid q$, silloin edellä olevien yhtälöiden nojalla $d \mid x$ ja $d \mid y$, mikä on mahdotonta, koska $syt\,(x, y) = 1$. Tällöin $syt\,(p, q) = 1$. Luvut p ja q eivät voi molemmat olla samaa parillisuutta, koska silloin myös x olisi parillinen. Tällöin toisen niistä täytyy olla pariton ja toisen parillinen. Lisäksi Lemman 4.33 avulla saadaan

$$2^{5m}5^{5n}\left(z'\right)^5 = x^5 + y^5 = (p+q)^5 + (p-q)^5 = 2p\left(p^4 + 10p^2q^2 + 5q^4\right).$$

Jos $x + y = 0$ tai $x - y = 0$, niin $x = y$ tai $x = -y$, mikä on mahdotonta, koska $syt\,(x, y) = 1$. Siten $p, q \neq 0$.

Nyt Lemman 2.2 perusteella joko $5 \mid 2p$ tai $5 \mid (p^4 + 10p^2q^2 + 5q^4)$. Jos $5 \mid 2p$, niin $5 \mid p$. Vastaavasti, jos $5 \mid (p^4 + 10p^2q^2 + 5q^4)$, niin tällöin $5 \mid p$. Nyt molemmissa tapauksissa $5 \mid p$, jolloin on olemassa kokonaisluku r siten, että $p = 5r$. Koska $syt\,(p, q) = 1$, niin $syt\,(r, q) = 1$. Luvut r ja p ovat samaa parillisuutta keskenään, joten toinen luvuista q ja r on pariton ja toinen on parillinen.

Lisäksi sijoittamalla $p = 5r$ yhtälöön $2^{5m}5^{5n}\left(z'\right)^5 = 2p\left(p^4 + 10p^2q^2 + 5q^4\right)$ saadaan

$$\begin{aligned} 2^{5m}5^{5n}\left(z'\right)^5 &= 2p\left(p^4 + 10p^2q^2 + 5q^4\right) = 2 \cdot 5r\left((5r)^4 + 10 \cdot (5r)^2 q^2 + 5q^4\right) \\ &= 2 \cdot 5r \cdot 5\left(125r^4 + 50r^2q^2 + q^4\right) = 2 \cdot 5^2 r\left(q^4 + 50q^2r^2 + 125r^4\right). \end{aligned}$$

Nyt huomataan, että

$$5^{5n} \mid \left(2 \cdot 5^2 r\left(q^4 + 50q^2r^2 + 125r^4\right)\right),$$

jolloin

$$5^{5n-2} \mid \left(2r\left(q^4 + 50q^2r^2 + 125q^4\right)\right).$$

Koska $n \geq 1$, niin $5n \geq 5$. Tällöin $5n > 2$, joten $5 \mid (2r\,(q^4 + 50q^2r^2 + 125q^4))$. Koska $5 \mid p$ ja $syt(p, q) = 1$, niin $5 \nmid q$ ja silloin $5 \nmid (q^4 + 50q^2r^2 + 125q^4)$. Tällöin Lemman 2.2 nojalla $5 \mid 2r$, eli $5 \mid r$. Ja koska $p \neq 0$, niin $r \neq 0$.

Määritetään seuraavaksi arvot a, b, t. Olkoot $t = q^4 + 50q^2r^2 + 125r^4$, $a = q^2 + 25r^2$ ja $b = 10r^2$. Nyt Lemman 4.34 nojalla $t = a^2 - 5b^2$. Huomataan, että $syt\,(a, b) = 1$: Tehdään antiteesi, jonka mukaan $syt\,(a, b) = f > 1$. Koska $f \mid b$, niin $f \mid 10r^2$, jolloin Lemman 2.2 nojalla $f \mid 2$, $f \mid 5$ tai $f \mid r$, eli $f = 2$, $f = 5$ tai $f = r$. Koska q ja r ovat eri parillisuutta, niin luku a on pariton ja tällöin $f \neq 2$. Koska $5 \mid p$ ja $syt\,(p, q) = 1$, niin $5 \nmid q$ ja tällöin $5 \nmid (q^2 + 25r^2) = a$, joten $f \neq 5$. Jos $f \mid r$ ja $f \mid a$, niin $f \mid q$, mikä on kuitenkin mahdotonta, koska $syt(r, q) = 1$. Koska kaikki tapaukset oli mahdottomia, niin on saatu ristiriita ja $syt\,(a, b) = 1$.

Selvästi $5 \mid b$, $5 \nmid a$ ja $a, b > 0$. Lisäksi huomataan, että b on parillinen, jolloin a on pariton. Voidaan osoittaa, että $syt\,(2 \cdot 5^2 r, t) = 1$. Oletetaan, että on olemassa alkuluku f, joka jakaa molemmat luvut. Tiedetään, että $f \neq 2$, koska t on aina pariton. Koska $5 \nmid q$, niin $5 \nmid t$ ja silloin $f \neq 5$. Koska $syt(r, t) = 1$, niin $f \nmid r$. Eli nyt on osoitettu, että ei ole olemassa lukua f, joka jakaa sekä luvun t että luvun $2 \cdot 5^2 r$. Nyt Lemman 2.3 nojalla luvut t ja $2 \cdot 5^2 r$ ovat joidenkin kokonaislukujen viidennet potenssit.

Nyt Lemman 4.39 nojalla on olemassa kokonaisluvut c, d siten, että

$$\begin{aligned} a &= c\left(c^4 + 50c^2d^2 + 125d^4\right), \\ b &= 5d\left(c^4 + 10c^2d^2 + 5d^4\right), \end{aligned}$$

$syt\,(c, d) = 1$, toinen luvuista c ja d on pariton ja toinen on parillinen, $5 \nmid c$ ja $5 \mid d$. Olkoon $u' = c + 5d^2$ ja $v' = 2d^2$. Tällöin selvästi $syt\,(u', v') = 1$, $5 \mid v'$, $5 \nmid u'$, u' on pariton ja v' on parillinen. Voidaan osoittaa, että $u' - 5\,(v')^2$ on viides potenssi:

$$c^4 + 10c^2d^2 + 5d^4 = c^4 + 10c^2d^2 + 25d^4 - 20d^4 = \left(c^2 + 5d^2\right) - 5\left(2d^2\right)^2.$$

Nyt koska $2 \cdot 5^2 r$ on viides potenssi, niin myös $\left(2 \cdot 5^2 r\right)^2$ on viides potenssi, ja

$$\begin{aligned}\left(2 \cdot 5^2 r\right)^2 &= 2 \cdot 5^3 \cdot 10r^2 = \left(2 \cdot 5^3\right) b \\ &= \left(2 \cdot 5^3\right)\left(5d\left(c^4 + 10c^2d^2 + 5d^4\right)\right) \\ &= \left(2 \cdot 5^4 d\right)\left(c^4 + 10c^2d^2 + 5d^4\right).\end{aligned}$$

Koska $syt\,(2 \cdot 5^4 d, c^4 + 10c^2d^2 + 5d^4) = 1$, niin Lemman 2.3 nojalla luvut $2 \cdot 5^4 d$ ja $c^4 + 10c^2d^2 + 5d^4$ ovat viidensiä potensseja. Tällöin myös $u' - 5\,(v')^2 = (c^2 + 5d^2) - 5\,(2d^2)^2$ on viides potenssi.

Tällöin Lemman 4.39 nojalla on luvut c', d' siten, että

$$\begin{aligned}c + 5d^2 &= c'\left((c')^4 + 50\,(c')^2\,(d')^2 + 125\,(d')^4\right), \\ 2d^2 &= 5d'\left((c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4\right),\end{aligned}$$

$syt\,(c', d') = 1$, toinen luvuista c' ja d' on pariton ja toinen on parillinen, $5 \nmid c'$ ja $5 \mid d'$. Kertomalla jälkimmäistä yhtälöä luvulla $2 \cdot 5^8$, saadaan

$$\left(2 \cdot 5^8\right)\left(2d^2\right) = 2^2 \cdot 5^8 d^2 = \left(2 \cdot 5^4 d\right)^2 = 2 \cdot 5^9 d'\left((c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4\right).$$

Nyt, koska $2 \cdot 5^4 d$ on viides potenssi, niin myös $\left(2 \cdot 5^4 d\right)^2$ on viides potenssi, ja tällöin edellisen yhtälön nojalla $2 \cdot 5^9 d'\left((c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4\right)$ on viides potenssi. Koska $syt\left(2 \cdot 5^9 d', (c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4\right) = 1$, niin Lemman 2.3 nojalla luvut $2 \cdot 5^9 d'$ ja $(c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4$ ovat viidensiä potensseja. Tämä on täysin analoginen edellisen vaiheen kanssa, jossa saimme, että luvut $2 \cdot 5^4 d$ ja $c^4 + 10c^2d^2 + 5d^4$ ovat viidensiä potensseja. Näin ollen samaa perustelua käyttämällä, voidaan käyttää Lemmaa 4.39 niin monta kertaa kuin halutaan. Lisäksi koska

$$\begin{aligned}25\,(d')^5 &\leq 25\,(d')^5 + 5d'\left((c')^4 + 10\,(c')^2\,(d')^2\right) \\ &= 5d'\left((c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4\right) = 2d^2,\end{aligned}$$

niin $0 < d' \leq \sqrt[5]{\frac{2d^2}{25}} < d$. Jos tätä menetelmää jatkettaisiin, lopulta saataisiin kokonaisluku d'' siten, että $0 < d'' < 1$, mikä on mahdotonta. Näin ollen antiteesi on väärä ja alkuperäinen väite on tosi. □

LEMMA 4.41. *Olkoon kokonaisluvut a, b siten, että*

a) $syt\,(a, b) = 1$,
b) $a \equiv b \pmod 2$,
c) $a, b \neq 0$,
d) $5 \nmid a$,
e) $5 \mid b$,
f) $\frac{a+b\sqrt{5}}{2} = \left(\frac{m+n\sqrt{5}}{2}\right)^5 \left(\frac{t+u\sqrt{5}}{2}\right)$, *missä* $\left(\frac{t+u\sqrt{5}}{2}\right)$ *on yksikkö ja* $u = 0$.

Silloin:

i) $a = \frac{c\left(c^4+50c^2d^2+125d^4\right)}{16}$,
ii) $b = \frac{5d\left(c^4+10c^2d^2+5d^4\right)}{16}$,
iii) $syt\,(c,d) = 1$,
iv) *c ja d ovat molemmat parittomia,*
v) $5 \nmid c$,
vi) $c, d \neq 0$.

Todistus. $\left(\frac{t+u\sqrt{5}}{2}\right)\left(\frac{t-u\sqrt{5}}{2}\right) = \frac{t^2-5u^2}{4}$, joten $t^2 - 5u^2 = \pm 4$, koska $\frac{t+u\sqrt{5}}{2}$ on yksikkö. Koska $u = 0$, niin $t = \pm 2$ ja edelleen $\frac{t}{2} = \pm 1$. Olkoon $c = \pm m$ ja $d = \pm n$. Tällöin $\frac{a+b\sqrt{5}}{2} = \pm\left(\frac{c+d\sqrt{5}}{2}\right)^5$. Nyt edelleen binomikaavan (4.1) nojalla

$$a + b\sqrt{5} = \frac{c^5 + 5c^4d\sqrt{5} + 50c^3d^2 + 50c^2d^3\sqrt{5} + 125cd^4 + 25d^5\sqrt{5}}{16}.$$

Näin ollen

$$a = \frac{c^5 + 50c^3d^2 + 125cd^4}{16} = \frac{c\left(c^4 + 50c^2d^2 + 125d^4\right)}{16}$$

ja

$$b = \frac{5c^4d + 50c^2d^3 + 25d^5}{16} = \frac{5d\left(c^4 + 10c^2d^2 + 5d^4\right)}{16}.$$

Koska $syt\,(a,b) = 1$, $c \mid a$ ja $d \mid b$, niin $syt\,(c,d) = 1$. Selvästi c ja d ovat molemmat parittomia. $5 \nmid c$, koska $5 \nmid a$. Koska $a, b \neq 0$, niin myös $c, d \neq 0$. □

Lemma 4.42. *Olkoon kokonaisluvut a, b siten, että*

a) $syt\,(a,b) = 1$,
b) $a \equiv b \pmod 2$,
c) $a, b \neq 0$,
d) $5 \nmid a$,
e) $5 \mid b$,
f) $\frac{a+b\sqrt{5}}{2} = \left(\frac{m+n\sqrt{5}}{2}\right)^5\left(\frac{t+u\sqrt{5}}{2}\right)$, *missä* $\left(\frac{t+u\sqrt{5}}{2}\right)$ *on yksikkö ja* $u \neq 0$.

Silloin:

i) $a = \frac{c\left(c^4+50c^2d^2+125d^4\right)}{16}$,
ii) $b = \frac{5d\left(c^4+10c^2d^2+5d^4\right)}{16}$,
iii) $syt\,(c,d) = 1$,
iv) *c ja d ovat molemmat parittomia,*
v) $5 \nmid c$,
vi) $c, d \neq 0$.

Todistus. $t^2 - 5u^2 = \pm 4$, koska $\frac{t+u\sqrt{5}}{2}$ on yksikkö. Nyt voidaan Lemman 4.25 nojalla olettaa, että

$$\frac{t + u\sqrt{5}}{2} = \pm\left(\frac{1+\sqrt{5}}{2}\right)^e,$$

missä Lemman 4.38 todistuksen mukaisesti $e \geq 2$ ja $5 \mid e$. Tällöin voidaan määritellä luvut c, d siten, että

$$\frac{c + d\sqrt{5}}{2} = \pm \left(\frac{m + n\sqrt{5}}{2} \right) \left(\frac{1 + \sqrt{5}}{2} \right)^f .$$

Nyt huomataan, että $\frac{a+b\sqrt{5}}{2} = \left(\frac{c+d\sqrt{5}}{2} \right)^5$. Tällöin edellisen Lemman 4.41 mukaisesti saadaan, että $a = \frac{c\left(c^4+50c^2d^2+125d^4\right)}{16}$, $b = \frac{5d\left(c^4+10c^2d^2+5d^4\right)}{16}$, $syt\,(c, d) = 1$, c ja d ovat molemmat parittomia, $5 \nmid c$ ja $c, d \neq 0$. □

LEMMA 4.43. *Olkoon kokonaisluvut a, b siten, että*

a) $syt\,(a, b) = 1$,
b) *toinen luvuista a ja b on pariton ja toinen on parillinen,*
c) $5 \nmid a$,
d) $5 \mid b$,
e) $\frac{a^2-5b^2}{4}$ *on viides potenssi.*

Silloin on kokonaisluvut c, d siten, että

i) $a = \frac{c\left(c^4+50c^2d^2+125d^4\right)}{16}$,
ii) $b = \frac{5d\left(c^4+10c^2d^2+5d^4\right)}{16}$,
iii) $syt\,(c, d) = 1$,
iv) *c ja d ovat molemmat parittomia,*
v) $5 \nmid c$,
vi) $5 \mid d$,
vii) $c, d \neq 0$.

TODISTUS. Oletetaan, että $syt\left(\frac{a+b\sqrt{5}}{2}, \frac{a-b\sqrt{5}}{2} \right) = d > 1$. Tällöin on olemassa luvut e, f siten, että

$$de = \frac{a + b\sqrt{5}}{2},$$
$$df = \frac{a - b\sqrt{5}}{2}.$$

Nyt

$$\frac{a + b\sqrt{5}}{2} + \frac{a - b\sqrt{5}}{2} = a = de + df = d\,(e + f) \text{ ja}$$
$$\frac{a + b\sqrt{5}}{2} - \frac{a - b\sqrt{5}}{2} = b\sqrt{5} = d\,(e - f)\,.$$

Lemman 4.28 nojalla $\sqrt{5}$ on jaoton, joten jos $d \mid \sqrt{5}$, täytyy olla $d = \sqrt{5}$. Tiedetään, että $d \mid a$, jolloin pitäisi olla $\sqrt{5} \mid a$. Tämä on kuitenkin mahdotonta, koska $5 \nmid a$. Siten $d \nmid \sqrt{5}$. Tällöin Lemman 2.2 nojalla $d \mid b$. Mutta tämäkin on mahdotonta, koska $syt\,(a, b) = 1$. Näin ollen $syt\left(\frac{a+b\sqrt{5}}{2}, \frac{a-b\sqrt{5}}{2} \right) = 1$.

Koska kokonaisalueella $\mathbb{Z}\left(\frac{1+\sqrt{5}}{2} \right)$ on yksikäsitteinen tekijöihin jako, niin voidaan oletusta $\frac{a^2-5b^2}{4}$ on viides potenssi ja Lemmaa 2.3 apuna käyttäen päätellä, että luvut

$\frac{a+b\sqrt{5}}{2}$ ja $\frac{a-b\sqrt{5}}{2}$ ovat viidensiä potensseja. Tämä tarkoittaa sitä, että on olemassa luvut m, n, t, u siten, että $\frac{a+b\sqrt{5}}{2} = \left(\frac{m+n\sqrt{5}}{2}\right)^5 \left(\frac{t+u\sqrt{5}}{2}\right)$, missä $\frac{t+u\sqrt{5}}{2}$ on yksikkö. Nyt, jos $u = 0$, niin Lemman 4.41 nojalla saadaan haluttu tulos. Jos $u \neq 0$, niin tällöin Lemman 4.42 nojalla saadaan haluttu lopputulos. □

LEMMA 4.44. *Ei ole olemassa kokonaislukuja x, y, z siten, että $x^5+y^5 = z^5$, missä $xyz \neq 0$, $syt\,(x, y, z) = 1$, x ja y ovat parittomia ja z on parillinen ja joko $5 \mid x$ tai $5 \mid y$.*

TODISTUS. Tehdään antiteesi: On olemassa kokonaisluvut x, y, z siten, että $x^5 + y^5 = z^5$, missä $xyz \neq 0$, $syt\,(x, y, z) = 1$, x ja y ovat parittomia ja z on parillinen ja $5 \mid x$ (jos $5 \mid y$, niin voidaan tehdä samat päättelyt korvaamalla y x:llä).

Koska $5 \mid x$, niin on olemassa n, x' siten, että $x = 5^n x', n \geq 1$, $syt(x', 5) = 1$ ja $5^{5n}\,(x')^5 = y^5 + z^5$. Nyt kertomalla jälkimmäisen yhtälön molemmat puolet luvulla 2^5 saadaan

$$2^5 \cdot 5^{5n}\,(x')^5 = 2^5\left(y^5 + z^5\right).$$

Olkoon luvut p, q siten, että $p = y + z$ ja $q = y - z$. Tällöin p ja q ovat molemmat parittomia.

$syt\,(p, q) = 1$: Jos on olemassa luku $f > 1$ siten, että $p = fp'$ ja $q = fq'$, niin f on pariton. Koska f on pariton ja $p + q = f\,(p' + q') = y + z + y - z = 2y$, niin $f \mid y$. Vastaavasti saadaan, että $f \mid z$ (koska $p - q = f\,(p' - q') = y + z - y + z = 2z$). Tämä on kuitenkin mahdotonta, koska $syt\,(y, z) = 1$, joten $syt\,(p, q) = 1$.

Lisäksi Lemman 4.33 avulla saadaan

$$\begin{aligned} 2^5 5^{5n}\,(x')^5 &= 2^5\left(y^5 + z^5\right) = (2y)^5 + (2z)^5 = (p+q)^5 + (p-q)^5 \\ &= 2p\left(p^4 + 10p^2q^2 + 5q^4\right). \end{aligned}$$

Jos $y + z = 0$ tai $y - z = 0$, niin $y = z$ tai $y = -z$, mikä on mahdotonta, koska $syt\,(y, z) = 1$. Siten $p, q \neq 0$.

Nyt Lemman 2.2 nojalla saadaan, että $5 \mid 2p$ tai $5 \mid (p^4 + 10p^2q^2 + 5q^4)$. Jos $5 \mid 2p$, niin $5 \mid p$. Vastaavasti, jos $5 \mid (p^4 + 10p^2q^2 + 5q^4)$, niin tällöin $5 \mid p$. Nyt molemmissa tapauksissa $5 \mid p$, jolloin on olemassa kokonaisluku r siten, että $p = 5r$. Koska $syt\,(p, q) = 1$, niin $syt\,(r, q) = 1$. Selvästi luvut q ja r ovat molemmat parittomia.

Lisäksi sijoittamalla $p = 5r$ yhtälöön $2^5 5^{5n}\,(x')^5 = 2p\,(p^4 + 10p^2q^2 + 5q^4)$ saadaan

$$\begin{aligned} 2^5 5^{5n}\,(x')^5 &= 2p\left(p^4 + 10p^2q^2 + 5q^4\right) = 2 \cdot 5r\left((5r)^4 + 10 \cdot (5r)^2\,q^2 + 5q^4\right) \\ &= 2 \cdot 5r \cdot 5\left(125r^4 + 50r^2q^2 + q^4\right) = 2 \cdot 5^2 r\left(q^4 + 50q^2r^2 + 125r^4\right). \end{aligned}$$

Nyt huomataan, että

$$5^{5n} \mid \left(2 \cdot 5^2 r\left(q^4 + 50q^2r^2 + 125r^4\right)\right),$$

jolloin

$$5^{5n-2} \mid \left(2r\left(q^4 + 50q^2r^2 + 125q^4\right)\right).$$

Koska $n \geq 1$, niin $5n \geq 5$. Tällöin $5n > 2$, joten $5 \mid (2r\,(q^4 + 50q^2r^2 + 125q^4))$. Koska $5 \mid p$ ja $syt\,(p, q) = 1$, niin $5 \nmid q$ ja silloin $5 \nmid (q^4 + 50q^2r^2 + 125q^4)$. Tällöin Lemman 2.2 nojalla $5 \mid 2r$, eli $5 \mid r$. Ja koska $p \neq 0$, niin $r \neq 0$.

Olkoon luvut a', b', t' siten, että

$$t' = q^4 + 50q^2r^2 + 125r^4,$$
$$a' = q^2 + 25r^2 \text{ ja}$$
$$b' = 10r^2.$$

Nyt Lemman 4.34 nojalla $t' = (a')^2 - 5(b')^2$. Huomataan, että molemmat luvut a', b' ovat parillisia, jolloin on luvut a, b siten, että $a = \frac{a'}{2} = \frac{q^2+25r^2}{2}$ ja $b = \frac{b'}{2} = 5r^2$. Olkoon

$$t = \frac{t'}{4} = \frac{(a')^2 - 5(b')^2}{4} = \left(\frac{a'}{2}\right)^2 - 5\left(\frac{b'}{2}\right)^2 = a - 5b^2.$$

Nyt $syt(a, b) = 1$: Tehdään antiteesi, jonka mukaan $syt(a, b) = f > 1$. Nyt siis $f \mid 5r^2$ ja $f \mid \frac{q^2+25r^2}{2}$, jolloin Lemman 2.2 nojalla $f \mid 2$, $f \mid 5$ tai $f \mid r$ ja $f \mid q$, eli $f = 2$, $f = 5$ tai f jakaa sekä luvun q että luvun r. Koska r on pariton, niin b on pariton ja $f \neq 2$. Jos $5 \mid a$, niin $5 \mid (q^2 + 25r^2)$. Koska $5 \mid p$ ja $syt(p, q) = 1$, niin $5 \nmid q$ ja tällöin $5 \nmid (q^2 + 25r^2)$, joten $f \neq 5$. Koska $syt(r, q) = 1$, niin ei voi olla mahdollista, että f jakaa sekä q:n että r:n. Koska kaikki tapaukset oli mahdottomia, niin on saatu ristiriita ja $syt(a, b) = 1$.

Selvästi $5 \mid b$, $5 \nmid a$ ja $a, b > 0$. Lisäksi huomataan, että a ja b ovat molemmat parittomia. Koska

$$2^5 5^{5n} (x')^5 = 2 \cdot 5^2 r \left(q^4 + 50q^2r^2 + 125r^4\right),$$

niin

$$2^5 5^{5n} (x')^5 = 2 \cdot 5^2 rt' = 2^3 5^2 rt,$$

ja edelleen

$$5^{5n} (x')^5 = \frac{5^2 rt}{4}.$$

Nyt voidaan osoittaa, että $syt\left(5^2 r, \frac{t}{4}\right) = 1$. Oletetaan, että on olemassa alkuluku f, joka jakaa molemmat luvut. Koska $5 \nmid q$, niin $5 \nmid t'$ ja silloin $f \neq 5$. Jos $f \mid r$ ja $f \mid t$, niin $f \mid q$. Tämä on kuitenkin mahdotonta, koska $syt(r, q) = 1$. Eli ei ole olemassa lukua f, joka jakaa sekä luvun $\frac{t}{4}$ että luvun $5^2 r$. Tällöin Lemman 2.3 nojalla luvut $\frac{t}{4} = \frac{a-5b^2}{4}$ ja $5^2 r$ ovat joidenkin kokonaislukujen viidennet potenssit.

Nyt Lemman 4.43 nojalla on olemassa kokonaisluvut c, d siten, että

$$a = \frac{c(c^4 + 50c^2d^2 + 125d^4)}{16},$$
$$b = \frac{5d(c^4 + 10c^2d^2 + 5d^4)}{16},$$

$syt(c, d) = 1$, c ja d ovat molemmat parittomia, $5 \nmid c$ ja $5 \mid d$. Koska

$$\left(5^2 r\right)^2 = 5^4 r^2 = 5^3 b = \frac{5^3 5d(c^4 + 50c^2d^2 + 5d^4)}{16} = \left(\frac{5^4 d}{4}\right)\left(\frac{c^4 + 50c^2d^2 + 5d^4}{4}\right)$$
$$= \left(\frac{5^4 d}{4}\right)\left(\frac{c^4 + 50c^2d^2 + 25d^4}{4} - \frac{20d^4}{4}\right) = \left(\frac{5^4 d}{4}\right)\left(\left(\frac{c^2 + 5d^2}{2}\right)^2 - 5d^4\right)$$

ja $syt\left(\frac{5^4 d}{4}, \left(\frac{c^2+5d^2}{2}\right)^2 - 5d^4\right) = 1$ (Oletetaan, että on $f > 1$ siten, että $f \mid \frac{5^4 d}{4}$ ja $f \mid \left(\left(\frac{c^2+5d^2}{2}\right)^2 - 5d^4\right)$. Lemman 2.2 nojalla joko $f \mid 5$ tai $f \mid d$. Koska $5 \nmid c$, niin $5 \nmid \left(\left(\frac{c^2+5d^2}{2}\right)^2 - 5d^4\right)$ ja silloin $f \nmid 5$. Jos $f \mid d$ ja $f \mid \left(\left(\frac{c^2+5d^2}{2}\right)^2 - 5d^4\right)$, niin silloin $f \mid c$. Tämä on kuitenkin mahdotonta, koska $syt\,(c, d) = 1$.), niin Lemman 2.3 nojalla $5^4 d$ ja $\left(\frac{c^2+5d^2}{2}\right)^2 - 5d^4$ ovat viidensiä potensseja.

Tällöin Lemman 4.43 nojalla on luvut c', d' siten, että

$$\frac{c+5d^2}{2} = \frac{c'\left((c')^4 + 50\,(c')^2\,(d')^2 + 125\,(d')^4\right)}{16},$$
$$d^2 = \frac{5d'\left((c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4\right)}{16},$$

$syt\,(c', d') = 1$, molemmat luvut c' ja d' ovat parittomia, $5 \nmid c'$ ja $5 \mid d'$. Kertomalla jälkimmäistä yhtälöä luvulla 5^8, saadaan

$$\begin{aligned} 5^8 d^2 &= \frac{5^9 d'\left((c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4\right)}{16} \\ &= \left(\frac{5^9 d'}{4}\right)\left(\frac{(c')^4 + 10\,(c')^2\,(d')^2 + 5\,(d')^4}{4}\right) \\ &= \left(\frac{5^9 d'}{4}\right)\left(\frac{\left((c')^2 + 5\,(d')^2\right)^2 - 20\,(d')^4}{4}\right) \\ &= \left(\frac{5^9 d'}{4}\right)\left(\left(\frac{(c')^2 + 5\,(d')^2}{2}\right)^2 - 5\left((d')^2\right)^2\right). \end{aligned}$$

$syt\left(5^9 d', \frac{1}{4}\left(\left(\frac{(c')^2+5(d')^2}{2}\right)^2 - 5\left((d')^2\right)^2\right)\right) = 1$: Oletetaan, että on luku $f > 1$, joka jakaa molemmat. Tällöin $f = 5$ tai $f \mid d'$. Koska $5 \nmid c'$, niin $f \neq 5$. Jos $f \mid d'$ ja $f \mid \frac{1}{4}\left(\left(\frac{(c')^2+5(d')^2}{2}\right)^2 - 5\left((d')^2\right)^2\right)$, niin tällöin $f \mid c'$. Se on kuitenkin mahdotonta, koska $syt\,(c', d') = 1$.

Koska $5^4 d$ on viides potenssi, niin myös luku $5^8 d^2 = (5^4 d)^2$ on viides potenssi. Tällöin Lemman 2.3 nojalla luvut $5^9 d'$ ja $\frac{1}{4}\left(\left(\frac{(c')^2+5(d')^2}{2}\right)^2 - 5\left((d')^2\right)^2\right)$ ovat viidensiä potensseja. Näin ollen samalla perusteella voidaan käyttää Lemmaa 4.43 aina uudelleen ja uudelleen. Lisäksi , koska

$$25\,(d')^5 < 16d^2 \text{ ja}$$
$$d' > 0,$$

niin $d > d'$.

Jos tätä menetelmää jatkettaisiin, lopulta saataisiin kokonaisluku d'' siten, että $0 < d'' < 1$, mikä on mahdotonta. Näin ollen antiteesi on väärä ja alkuperäinen väite on tosi. □

Nyt on helppo näyttää, että yhtälöllä $x^5 + y^5 = z^5$ on kokonaislukuratkaisu vain silloin, kun $xyz = 0$.

LAUSE 4.45. *Yhtälöllä $x^5 + y^5 = z^5$ on kokonaislukuratkaisu vain silloin, kun $xyz = 0$.*

TODISTUS. Oletetaan, että yhtälöllä on jokin ratkaisu, missä $xyz \neq 0$. Lemman 3.9 nojalla voidaan olettaa, että $syt\,(x, y, z) = 1$. Kuten Lauseen 3.11 todistuksessa, voidaan tässäkin olettaa, että luvut x ja y ovat parittomia ja z on parillinen. Sophie Germainin Lauseen 4.31 nojalla voidaan olettaa, että $5 \mid xyz$. Jos $5 \mid z$, niin tällöin voidaan Lemman 4.40 avulla näyttää, että yhtälöllä $x^5 + y^5 = z^5$ ei ole kokonaislukuratkaisua. Ja jos $5 \nmid z$, niin voidaan Lemman 4.44 perusteella sanoa, että yhtälöllä $x^5 + y^5 = z^5$ ei ole kokonaislukuratkaisua.

Näin on saatu ristiriita, jolloin alkuoletus ei päde ja yhtälöllä $x^5 + y^5 = z^5$ ei ole kokonaislukuratkaisua, kun $x, y, z \neq 0$. □

SEURAUS 4.46. *Yhtälöllä $x^n + y^n = z^n$ ei ole olemassa kokonaislukuratkaisua, kun n on jaollinen luvulla 5.*

LUKU 5

Abc-konjektuuri

Tässä luvussa tutustutaan Josph Oesterlén (1954–) ja David Masserin (1948–) vuonna 1985 esittämään *abc*-konjektuuriin. Konjektuuri on tyypillinen esimerkki yksinkertaisesta väitteestä, jota voidaan käyttää yhdistämään useita lukuteorian tuloksia, jotka muutoin olisivat hajanaisia väitteitä ilman yhteisiä yhteyksiä [**3**, s. 401].

Tämän tutkielman tekohetkellä *abc*-konjektuurille ei ole vielä olemassa pitävää todistusta. Varteenotettavin ratkaisuehdotus on tällä hetkellä japanilaisen matemaatikon Shinchi Mochizukin (1969–) elokuussa 2012 julkaisema 500-sivuinen ratkaisuehdotus. Mochizukin ratkaisu sisältää kuitenkin paljon hänen kehittämiään uusia tekniikoita ja matemaattisia käsitteitä, joita kukaan muu matemaatikko ei oikeastaan ymmärrä, joten hänen todistuksensa tarkistamisessa kestänee vuosia [**4**].

Luvun alussa esitetään konjektuurille kaksi ekvivalenttia muotoilua ja lopuksi näytetään, että jos *abc*-konjektuuri on tosi, niin siitä seuraa Fermat'n suuri lause.

MÄÄRITELMÄ 5.1. Kolmikko $(a, b, c) \in \mathbb{Z}^3$ muodostaa *abc-summan*, jos $a + b = c$ ja $syt\,(a, b) = 1$. *abc*-summan muodostavaa kolmikkoa $(a, b, c) \in \mathbb{Z}^3$ kutsutaan *abc-kolmikoksi*.

MÄÄRITELMÄ 5.2. Kokonaisluvun N *radikaali* $rad\,(N)$ on luvun N jakavien alkulukujen tulo, ts. alkutekijöiden tulo

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

missä p on alkuluku.

ESIMERKKI 5.3. Olkoon $n = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$, missä p_i:t ovat alkulukuja ja $a_i \in \mathbb{N}$. Tällöin radikaalin määritelmän nojalla $rad\,(n) = p_1 p_2 \cdots p_n$

LEMMA 5.4. *Olkoot* $a, b, m, n \in \mathbb{N}$. *Tällöin*

(a) $rad\,(a) \leq a$,
(b) $rad\,(ab) \leq rad\,(a)\,rad\,(b)$ *ja*
(c) $rad\,(a^m b^n) \leq rad\,(a)\,rad\,(b)$.

TODISTUS. Oletetaan, että $a, b, m, n \geq 2$. Muussa tapauksessa väitteet pätevät selvästi. Aritmetiikan peruslauseen, eli lauseen 2.1, nojalla luvut a ja b voidaan esittää muodossa $a = p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}$ ja $b = q_1^{d_1} q_2^{d_2} \cdots q_n^{d_n}$. Nyt

$$rad\,(a) = rad\,(p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n}) = p_1 p_2 \cdots p_n \leq p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n} = a$$

kaikilla $a \in \mathbb{N}$, $a \geq 2$, mistä väite (a) seuraa.

Jos $syt\,(a, b) \neq 1$, niin $p_i = q_j$, joillekin i ja j. Tällöin

$$\begin{aligned} rad\,(ab) &= rad\left(p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n} q_1^{d_1} q_2^{d_2} \cdots q_n^{d_n}\right) \leq p_1 p_2 \cdots p_n q_1 q_2 \cdots q_n \\ &= rad\,(p_1^{c_1} p_2^{c_2} \cdots p_n^{c_n})\,rad\left(q_1^{d_1} q_2^{d_2} \cdots q_n^{d_n}\right) = rad\,(a)\,rad\,(b)\,, \end{aligned}$$

jolloin väite (b) on tosi. Väite (c) seuraa väitteestä (b) ja radikaalin määritelmästä. □

Esitetään seuraavaksi Masserin mukainen muotoilu *abc*-konjektuurille.

KONJEKTUURI 5.5. *Kaikilla* $\epsilon > 0$ *on olemassa luku* $C(\epsilon) > 0$ *siten, että*

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

on totta kaikille abc-kolmikoille $(a, b, c) \in \mathbb{N}^3$.

HUOMAUTUS 5.6. Voidaan olettaa, että luvuilla a, b ja c on järjestys siten, että $0 < a < b < c$.

Hieman oletuksia muuttamalla saadaan konjektuuri yleisempään muotoon.

KONJEKTUURI 5.7. *Kaikilla* $\epsilon > 0$ *on olemassa reaaliluku* $C(\epsilon) > 0$ *siten, että*

$$max\{\mid a \mid, \mid b \mid, \mid c \mid\} \leq C(\epsilon)\, rad(abc)^{1+\epsilon}$$

on totta kaikille abc-kolmikoille $(a, b, c) \in \mathbb{Z}^3$, $abc \neq 0$.

Koska lukua $\epsilon > 0$ ei ole kiinnitetty eikä lukua $C(\epsilon) > 0$ ole tarkemmin määritelty, ovat nämä kaksi edellä esitettyä *abc*-konjektuuria ns. vahvassa muodossa. Usein *abc*-konjektuurin heikkoa muotoa on helpompi soveltaa kuin vahvaa muotoa. Heikosta muodosta puhutaan silloin, kun kiinnitetään ϵ. Esimerkiksi olettamalla, että $\epsilon = 1$, saadaan *abc*-konjektuurin heikko muoto.

KONJEKTUURI 5.8. *Kaikille abc-kolmikoille pätee*

$$c = a + b \leq rad(ab(a + b))^2.$$

Tämän heikon muodon sekä tutkielman aiempien lukujen avulla voidaan todistaa Fermat'n suuri lause kokonaisuudessaan. Tällöin konjektuurin ollessa tosi, on Fermat'n suuren lauseen todistus melko yksinkertainen todistus.

LAUSE 5.9. *Oletetaan, että* $syt(a, b) = 1$ *ja* $a + b = c$. *Oletetaan lisäksi, että Konjektuuri 5.8 on voimassa, eli* $c < rad(abc)^2$ *kaikilla* a, b *ja* c. *Tällöin yhtälöllä* $x^n + y^n = z^n$ *ei ole kokonaislukuratkaisua, kun* $n \geq 3$.

TODISTUS. Olkoon $a = x^n$, $b = y^n$ ja $c = z^n$. Silloin $abc = (xyz)^n$ ja nyt Konjektuurin 5.8 ja Lemman 5.4 nojalla

$$z^n \leq rad((xyz)^n)^2 = rad(xyz)^2 \leq (xyz)^2 \leq z^6.$$

Koska $z \in \mathbb{Z} \setminus \{0\}$, niin $n \leq 6$. Lisäksi tiedetään, että yhtälöllä $x^n + y^n = z^n$ ei ole kokonaislukuratkaisua, kun $n = 3, n = 4, n = 5$ tai $n = 6$, joten yhtälöllä $x^n + y^n = z^n$ ei ole kokonaislukuratkaisua, kun $n \geq 3$. □

Lähteessä [**17**] on esitetty eräs listaus *abc*-konjektuurin seurauksista, jotka ovat tosia *abc*-konjektuurin pitäessä paikkansa.

Kirjallisuutta

[1] Aczel, Amir D. *Fermat'n teoreema.* (Englanninkielinen alkuteos: Fermat's Last Theorem. Unlocking the Secret of an Ancient Mathematical Problem) Suomentanut Risto Varteva. WSOY 1998. 2. Painos.

[2] Bell, E.T. *Matematiikan miehiä.* (Englanninkielinen alkuteos: Men of Mathematics) Suomentaneet Helka ja Klaus Vala. WSOY 1963.

[3] Bombieri, Enrico & Gubler Walter. *Heights in Diophantine Geometry.* Cambridge University Press 2006.

[4] Castelvecchi, Davide *The biggest mystery in mathematics: Shinichi Mochizuki and the impenetrable proof.* Nature 526 (2015), s. 178-181.

[5] Dahmen S. R. *Lower bounds for numbers of ABC-hits.* Journal of Number Theory 128 (2008), s. 1864–1873

[6] Edwards, Harold M. *Fermat's Last Theorem: A Genetic Intoduction to Algebraic Number Theory.* Springer-Verlag 1977.

[7] Everest, Graham & Ward Thomas. *An Introduction to Number Theory.* Springer-Verlag 2005.

[8] Freeman, Larry (22.5.2005). Fermat's Last Theorem. [Fermat's Last Theorem: Proof for $n = 3$] Haettu 11.10.2016 osoitteesta
`http://fermatslasttheorem.blogspot.fi/2005/05/fermats-last-theorem-proof-for-n3.html`

[9] Freeman, Larry (28.10.2005). Fermat's Last Theorem. [Fermat's Last Theorem: Proof for $n = 5$] Haettu 1.11.2016 osoitteesta
`http://fermatslasttheorem.blogspot.fi/2005/10/fermats-last-theorem-proof-for-n5_28.html`

[10] Freeman, Larry (3.11.2005). Fermat's Last Theorem. [Dirichlet Integers] Haettu 5.12.2016 osoitteesta
`http://fermatslasttheorem.blogspot.fi/2005/11/dirichlet-integers.html`

[11] Freeman, Larry (16.1.2006). Fermat's Last Theorem. [Fermat's Last Theorem: Proof for $n = 5$: 2 is a prime in $Z[(1 + \sqrt{5})/2]$] Haettu 5.12.2016 osoitteesta
`http://fermatslasttheorem.blogspot.fi/2006/01/fermats-last-theorem-proof-for-n5-2-is_16.html`

[12] Hintikka, Pekka. *Fermat'n suuri lause, salaisuus kolmen vuosisadan takaa.* Gummerrus 2003.

[13] Hungerford, Thomas W. *Abstract Algebra: An Introduction.* Brooks/Cole 2014.

[14] Kahanpää, Lauri. *Algebrajatko.* Jyväskylän yliopisto. Luentomoniste 1993. Haettu 14.12.2016 osoitteesta `http://users.jyu.fi/~laurikah/Algebrajatko.pdf`

[15] Lamminsalo, Marko. *Abc*-konjektuuri. Itä-Suomen yliopisto. Pro gradu -tutkielma. 2014

[16] Luotonen, Mervi. Fermat'n suuren lauseen historia ja sen matemaattinen kehitys 1700- ja 1800-luvuilla. Jyväskylän yliopisto. Pro gradu -tutkielma. 2008

[17] Nitaj, Abderrahmanei. *The abc conjecture* Haettu 5.12.2016 osoitteesta
`http://www.math.unicaen.fr/~nitaj/abc.html`

[18] Parkkonen, Jouni. *Algebra 2014.* Jyväskylän yliopisto. Luentomoniste 2014. Haettu 2.11.2016 osoitteesta `http://users.jyu.fi/~parkkone/Algebra2014/Algebra2014.pdf`

[19] Ribenboim, Paulo. *13 Lectures on Fermat's Last Theorem.* Springer-Verlag 1979.

[20] Ribenboim, Paulo. *Classical Theory of Algebraic Numbers.* Springer-Verlag 2001.

[21] Ribenboim, Paulo. *Fermat's Last Theorem For Amateurs.* Springer-Verlag 1998.

[22] Singh, Simon. *Fermat'n viimeinen teoreema*. (Englanninkielinen alkuteos: Fermat's Enigma. The Epic Quest to Solve the World's Greatest Mathematical Problem) Suomentanut Katriina Savolainen. Tammi 1998.
[23] Stark, Harold M. *An Introduction to Number Theory*. Markham Publishing Company 1970.
[24] Underwood, Dudley. *A Guide To Elementary Number Theory*. Mathematical Association of America 2009.
[25] Väisälä, K.. *Lukuteorian ja korkeamman algebran alkeet* (1961). Näköispainos. Otava 2009.