Fermat'n suuren lauseen historia ja sen matemaattinen kehitys 1700- ja 1800-luvuilla

Mervi Luotonen

22. helmikuuta 2008

Sisältö

1 Johdanto

Pierre de Fermat oli 1600-luvulla elänyt matemaatikko. Hän kirjoitti kuuluisaksi tulleen suuren lauseensa Diofantoksen Arithmetica-kirjan marginaaliin arviolta vuonna 1637. Lause löytyi Fermat'n kuoltua vuonna 1665. Fermat'n suuri lause on seuraavanlainen: $x^n + y^n \neq z^n$ kun $n > 2$ ja x, y, z ja n ovat positiivisia kokonaislukuja. Fermat'n suuri lause on muodoltaan hyvin yksinkertainen lause, jota lukuisat matemaatikot yrittivät tuloksetta todistaa yli 350 vuoden ajan. Fermat itse väitti Arithmetica kirjan marginaalissa todistaneensa lauseen, mutta hän ei voinut kirjoittaa todistusta marginaaliin, sillä todistus oli niin pitkä. Tämä väitös on inspiroinut monia matemaatikoita etsimään todistusta lauseelle. Jotkut jopa väittivät keksineensä todistuksen, mutta näistä todistuksista löytyi kuitenkin aina virheitä.

Ensin lausetta lähdettiin todistamaan tapaus kerrallaan. Väitetään että Fermat itse todisti tapauksen $n = 4$. Tästä ei kuitenkaan ole varmaa tietoa. 100 vuotta myöhemmin Leonhard Euler todisti tapaukset $n = 3$ ja $n = 4$. Ranskalainen matemaatikko Marie-Sophie Germain oli ensimmäinen, joka sai vietyä Fermat'n suuren lauseen todistusta hieman yleisempään suuntaan. Hän ei tutkinut vain yksittäisiä tapauksia, vaan pyrki yleistämään tuloksensa koskemaan tietynlaisia lukuja. Ernst Eduard Kummer jatkoi yleistämistä todistamalla että lause pätee kaikille säännöllisille alkuluvuille. Lause pystyttiin todistamaan vasta 1990-luvulla. Lopullisen todistuksen teki Andrew Wiles monien epäonnisten vaiheiden jälkeen.

Fermat'n suuri lause on vain yksittäinen matemaattinen ongelma. Sitä tutkittaessa on kuitenkin saatu aikaan paljon matemaattisesti merkittäviä tuloksia. Lauseella on se erityinen ominaisuus, että ongelmana se kattaa koko matematiikan historian pronssikaudesta nykypäivään saakka. Lause liittyy läheisesti Pythagoraan lauseeseen, jonka jo babylonialaiset tunsivat. Lopullinen todistus pohjautuu hyvin nykyaikaiseen matematiikkaan, josta Fermat'n aikana ei varmastikaan ollut mitään tietoa. Fermat'n suuri lause on puhuttanut ihmisiä vielä Wilesin todistuksen jälkeenkin. Monet ovat yrittäneet löytää yksinkertaisen näköiselle lauseelle yksinkertaista todistusta. Mahdotonta se ei ehkä ole, mutta täytyy pitää mielessä että monet viime vuosisatojen parhaista matemaatikoista yrittivät ratkaista ongelmaa siinä kuitenkaan onnistumatta.

Tässä tutkielmassa tutustutaan Fermat'n suuren lauseen historiaan ja etenkin siihen, miten lausetta yritettiin todistaa 1700- ja 1800-luvuilla. Ensin tarkastellaan tapauksia $n = 4$ ja $n = 3$. Näissä todistuksissa käytetään äärettömän laskeutumisen menetelmää. Kyseinen menetelmä on Fermat'n keksimä. Menetelmää käytettäessä valitaan ongelman pienin ratkaisu ja näytetään, että on olemassa vielä pienempi ratkaisu. Näin päädytään ristirii-

taan. Näiden tapausten tarkastelun jälkeen tarkastellaan Sophie Germainin, Gabriel Lamén ja Ernst Eduard Kummerin vaikutusta lauseen kehitykseen. Lopussa tarkastellaan lyhyesti sitä, mitä Fermat'n suuren lauseen osalta on tapahtunut Andrew Wilesin todistuksen jälkeen. Wilesin todistus on aivan liian monimutkainen tässä esitettäväksi.

Tutkielmassa on tarkoitus keskittyä historiallisiin tapahtumiin, joten viime vuosisadan kehitystä ja lopullista todistusta ei käsitellä kovin tarkasti. Tutkielmassa käydään läpi, miten lopullinen todistus syntyi, mutta sen matemaattiseen puoleen ei juurikaan paneuduta. Tavoitteena on perehtyä siihen, miten kuuluisaa ongelmaa ryhdyttiin tarkastelemaan ja kuinka monimutkainen ongelma kokonaisuudessaan on.

2 Fermat'n suuren lauseen historiaa

2.1 Ennen Fermat'ta

Fermat'n kuuluisan 'suuren lauseen' tarina alkoi jo kauan ennen Fermat'n syntymää. Se alkoi jo ennen Diofantosta, jonka matematiikkaa Fermat yritti yleistää. Voidaan ajatella, että lauseen juuret ovat pronssikauden aikaisessa Mesopotamiassa, hedelmällisen puolikuun alueella Eufratin ja Tigriin välissä, alueella, joka tunnetaan myös Kaksoisvirran maana. Nykyisin tämä alue kuuluu Irakiin. Fermat'n lauseen alku voidaan ajoittaa Mesopotamian arkipäivään, neljän tuhannen vuoden taakse. Mesopotamiassa kukoisti n.2000 eKr - 600 eKr kulttuuri, jota tässä yksinkertaistaen kutsutaan Babylonian ajaksi. Tällöin kehitettiin muun muassa kirjoitustaito. Babyloniassa arkipäivään kuuluivat myös lukujen neliöt, joiden voidaan katsoa edustavan vaurautta. Maanviljelijän varallisuus riippui sadon suuruudesta, joka puolestaan riippui siitä, miten suuri on pellon pinta-ala. Koska neliön muotoisen pellon pinta-ala oli $sivu \cdot sivu = sivu^2$, niin voidaan sanoa, että vauraus tulee neliöstä. ([11], s.22-23).

Babylonialaisia kiinnosti tieto siitä, miten kokonaislukujen muodostamat neliöt voidaan jakaa muiden kokonaislukujen neliöiden summiksi. Jos talonpojalla oli esimerkiksi pelto, jonka kummankin sivun pituus oli 5 mittayksikköä, eli pellon ala oli 25 neliötä, niin sen saattoi vaihtaa kahteen peltoon, joista toisen sivut olivat 3 mittayksikköä (ala 9 neliötä) ja toisen 4 mittayksikköä (ala 16 neliötä). Tämä oli tärkeä tieto käytännön maanjako-ongelmia ratkaistaessa. Lukuja 5,4 ja 3 kutsutaan Pythagoraan luvuiksi, vaikka lähes 4000 vuotta vanhojen savitaulujen perusteella tiedämmekin, että babylonialaiset tunsivat Pythagoraan lukujen ominaisuudet jo tuhat vuotta ennen kuin Pythagoras oli syntynytkään. Pythagoraan luvut ovat kolmen kokonaisluvun, x, y ja z, joukkoja, jotka toteuttavat Pythagoraan lauseen $x^2+y^2 = z^2$. ([11], s.24).

Babyloniassa käytettiin kuusikymmenjärjestelmää. Babylonialaiset tekivät nuolenpääkirjoituksella savitauluille paljon erilaisia taulukoita. Tällaisia taulukoita on myös säilynyt paljon. ([11], s.25). Eräs säilyneistä tauluista on Plimpton-kokoelman savitaulu numero 322. Taulu on peräisin Babylonian vanhemman valtakunnan kaudelta (n.1900-1600 eKr). Plimpton 322 on suuremman savitaulun osa. ([13], s.66). Taulukossa on 15 vaakasuoraa riviä. Jokaisella rivillä on erilainen Pythagoraan lukujen ryhmä. Eräällä rivillä on esimerkiksi 169, 144 ja 25 ($13^2 = 12^2 + 5^2$). Kaikki tutkijat eivät usko, että babylonialaisia olisi sen kummemmin kiinnostanut tämä neliöiden välinen yhteys. Erään teorian mukaan kyse oli puhtaasti käytännön laskemisesta, koska kuusikymmenjärjestelmässä oli kätevää käyttää murto-osien laskemi-

sessa myös kokonaislukujen neliöitä. Jotkut tutkijat puolestaan uskovat, että babylonialaisia kiinnosti myös pelkät lukujen ominaisuudet eikä niihin välttämättä tarvinnut liittyä käytännön tavoitteita. ([11], s.25-26). Yleisesti on kuitenkin oletettu, että kaikki esihelleeninen tiede ja matematiikka oli puhtaasti käytännöllistä. ([13], s.66). On mahdollista, että Plimpton 322-taulua käytettiin opetusvälineenä, kun oppilaita opetettiin ratkaisemaan sellaisia tehtäviä, joissa tarvitaan lukujen neliöitä. Babylonialaiset eivät kuitenkaan yrittäneet kehittää yleisiä ratkaisumenetelmiä tällaisille ongelmille. ([11], s.26).

Seuraavan kehitysaskeleen kohti Fermat'n lauseen syntyä otti Pythagoras Samoslainen ja hänen koulukuntansa. Pythagoras syntyi kreikkalaisella Samoksen saarella noin 580 eKr. Hän matkusteli muun muassa Egyptissä ja Babyloniassa. Babyloniassa hän perehtyi matematiikkaan, ja on mahdollista, että hän tutustui siellä Pythagoraan lukuihin. Matkoillaan hän omaksui myös tähtitieteellistä tietämystä ja uskonnollisia kertomuksia. ([11], s.26-30). Palattuaan Kreikkaan Pythagoras asettui Krotoniin, nykyiseen Kaakkois-Italiaan. Sinne hän perusti salaseuran, pythagoralaiset, joka omistautui tutkimaan lukuja. Pythagoralaiset halusivat selvittää lukujen perimmäisen olemuksen ja pitää tiedon vain sisäpiirin hallussa. Heidän paneutumisensa lukuihin oli paljolti uskonnollista perua. Pythagoraalta tai hänen välittömiltä seuralaisiltaan ei säilynyt kirjoituksia, eikä niitä luultavasti ole edes olemassa, mutta myöhemmin hänen jälkeensä kirjoitetuissa teksteissä kerrotaan tämän salaseuran toiminnasta. ([13], s.83-86).

Pythagoralaiset käsittelivät jo babylonialaisille tuttua neliöiden välistä yhteyttä geometrisesti ja saattoivat tällä tavalla yleistää sen koskemaan muitakin kuin vain luonnollisia lukuja. ([11], s.30-31). Pythagoraan teoreeman nimen oikeutusta on perusteltu sillä, että pythagoralaiset esittivät teoreemalle ensimmäisen todistuksen. Tätä oletusta ei ole kuitenkaan vahvistettu. ([13], s.86). Pythagoras tiesi myös sen, että kokonaislukujen neliöt saadaan laskemalla järjestyksessä yhteen parittomia lukuja. Esimerkiksi luvun 2 neliö on $4 = 1+3$, luvun 3 neliö on $9 = 1+3+5$ ja luvun 4 neliö on $16 = 1+3+5+7$. ([11], s.30-31).

Pythagoras kuoli noin 500 eKr. Hänen salaseuransa hajosi vuonna 510 eKr puhjenneen mellakan seurauksena, kun sybariiteiksi kutsuttu kilpaileva poliittinen ryhmä yllätti pythagoralaiset ja murhasi heistä useimmat. Ne, jotka jäivät henkiin, levittäytyivät eri puolille Kreikkaa ja veivät mukanaan lukumystiikkansa ja filosofiset oppinsa. Eräs heistä, Filaos, kirjoitti muistiin pythagoraan koulukunnan historian ja tieteelliset teoriat. Oletettavasti Eukleideen alkeiden kaksi ensimmäistä kirjaa pohjautuvat kokonaan Pythagoraan ja hänen salaseuransa töille. ([11], s.34-38). Ensimmäisessä kirjassa Eukleides käy muun muassa läpi Pythagoraan lauseen todistuksen. Eukleides käy myös läpi käänteisen Pythagoraan lauseen todistuksen: jos kolmion sivun

neliö on yhtä suuri kuin kahden muun sivun neliöiden summa, jälkimmäisten sivujen välinen kulma on suora. ([13], s.164-166).

Vuoden 250 jKr tienoilla eli Aleksandriassa Diofantos-niminen matemaatikko. Diofantos Aleksandrialaisen tarkkoja synnyin- ja kuolinvuosia ei tiedetä. Varmaksi tiedetään, että Diofantos viittaa kirjoituksissaan Hypsiklesnimiseen matemaatikkoon, jonka tiedetään eläneen noin 150 eKr. Toisaalta vuonna 364 jKr elänyt Theon Aleksandrialainen mainitsee Diofantoksen, joten hänen on täytynyt elää tässä välissä. ([11], s.43-44).

Tuntemistamme Diofantoksen töistä tärkein on Arithmetica. Alunperin se sisälsi kolmetoista kirjaa, joista vain kuusi on säilynyt. Teos muistuttaa melkoisesti babylonialaista algebraa, sillä se ei käytä geometrisia menetelmiä. Diofantoksen Arithmetica (sellaisena kuin se on säilynyt) on omistettu lähes kokonaan sekä yksikäsitteisen ratkaisun tuottavien että sellaisten yhtälöiden, joiden ratkaisujoukko on ääretön, kokonaislukuratkaisuille. ([13], s.261-265). Tässä teoksessa Diofantos täsmensi algebran ja lukuteorian käsitteitä ja tutki tietyntyyppisiä yhtälöitä, joita kutsutaan nykyisin Diofantoksen yhtälöiksi. ([11], s.44).

Keskiajalla matemaattinen kulttuuri säilyi islamilaisissa maissa, kuten Iranissa ja Egyptissä. Euroopassa matemaattinen kehitys ei juurikaan edennyt. Mutta kun Diofantoksen ajoista oli kulunut 1300 vuotta, renesanssi ja uuden ajan alku alkoivat nousta pimeänä pidetyn ajatusmaailman tilalle. Eurooppa alkoi taas janota tietoa, ja katseet kohdistuivat antiikin kulttuuriin. Tietoa ja valistusta tavoiteltaessa kaikki käsiin saatu antiikin kirjallisuus käännettiin latinaksi, joka oli tuolloin oppineiden yhteinen kieli. Ranskalainen aatelismies Claude Bachet paneutui kääntämään matematiikan kirjoja. Hän sai hankituksi Diofantoksen kreikankielisen Arithmetican ja julkaisi sen 1621 Pariisissa latinankielisenä nimellä Diophanti alexandrini arithmeticorum libri sex. Tässä tekstissä mainitaan ongelma 8, jossa kysytään, miten tietty kokonaisluvun neliö voidaan ilmaista kahden kokonaisluvun neliön summana. Juuri tämä ongelma sai Fermat'n kirjoittamaan kirjan marginaaliin kuuluisan reunahuomautuksensa. ([11], s.44-45, 53-54).

2.2 Pierre de Fermat 1601-1665

Monien mielestä 1600-luvun suurin matemaatikko oli Pierre de Fermat. Väitetään, että puhtaana matemaatikkona Fermat oli vähintään Newtonin veroinen. Pierre de Fermat syntyi elokuussa 1601 Beaumont-de-Lomagnessa, Ranskassa. Tarkkaa syntymäpäivää ei tiedetä, mutta kastepäivä oli 20. elokuuta. ([12], s.58-59). Hänen isänsä oli Beaumontin toinen konsuli, nahkakauppias Dominique Fermat ja hänen äitinsä oli Claire de Long, erään laki-

miehen tytär. ([11], s.15).

Ensimmäiset tiedonalkeensa Fermat sai kotona synnyinkaupungissaan. Vanhemmat halusivat pojasta virkamiehen, ja siksi hänet lähetettiin opiskelemaan Toulouseen. ([11], s.15-18). Fermat'n opiskeluajalta ei ole säilynyt juurikaan tietoa. Voidaan kuitenkin päätellä, että hänen opintonsa sujuivat loistavasti, sillä ilman tarkkoja ja perusteellisia tietoja ei hänestä olisi voinut tulla sitä klassikkoa ja kirjailijaa, mikä hänestä myöhemmin tuli. Koulutus ei kuitenkaan ollut perustana hänen saavutuksiinsa matematiikan alalla, sillä hänen opiskeluaikanaan ei vielä opetettu niitä aloja, joilla hän teki myöhemmin huomattavimmat työnsä. On siis todennäköistä ettei hän saanut alkusysäystä töihinsä opinnoistaan. Fermat oli erittäin oppinut niissä aineissa, joita yleensä kutsutaan yleissivistykseksi. Hän tunsi Euroopan pääkielet ja kirjallisuuden. Kreikkalainen ja latinalainen filologia ovat hänelle kiitollisuudenvelassa monista tärkeistä korjauksista. Hän myös sepitti latinan, ranskan ja espanjan kielisiä runoja. ([12], s.59-60).

Fermat oli ammatiltaan lakimies, joka tutki matematiikkaa vain harrastuksenaan ([11], s.15-17). Hän on epäilemättä eräs tieteen historian kuuluisimmista harrastelijoista ([12], s.59). Vuonna 1631 30-vuotias Fermat nimitettiin oikeusistuimen jäseneksi Toulousessa. Samana vuonna hän solmi avioliiton äitinsä serkun, Louise Longin, kanssa. ([11], s.15-17). Avioliitosta syntyi viisi lasta, 3 poikaa ja 2 tytärtä. Molemmat tyttäristä menivät luostariin. ([12], s.60). Yksi pojista, Clément Samuel de Fermat otti myöhemmin tehtäväkseen vaalia isänsä tieteellistä perintöä ja julkaisi isän kuoleman jälkeen hänen kootut matemaattiset kirjoituksensa. Juuri tässä teoksessa mainitaan se kuuluisa huomautus, jota nykyisin kutsutaan Fermat'n suureksi lauseeksi. ([11], s.15-17).

Vuonna 1648 Fermat ylennettiin kuninkaan neuvosmieheksi Toulousen paikallisessa parlamentissa. Tätä virkaa hän hoiti 17 vuotta, kuolemaansa saakka. Parlamentin neuvoston virkailijoiden edellytettiin pysyvän erillään muista kaupunkilaisista ja pidättyvän tarpeettomasta sosiaalisesta toiminnasta. ([12], s.61). Tämän eristäytymisen oli tarkoitus varmistaa, ettei neuvosmiestä voida lahjoa eikä kiristää ([11], s.15-17). Tästä syystä Fermat'lla oli aikaa tutkia matematiikkaa ([12], s.61). Fermat'n elämää on luonnehdittu tyyneksi, hiljaiseksi ja tasaiseksi ([11], s.15-17). Hänen elämänsä oli työteliästä ja yksitoikkoista, mutta hän sai siitä irti suunnattoman paljon. Fermat kuoli Castresissa 12.1.1665, ollessaan 63-vuotias. ([12], s.60).

Fermat'ta kiinnosti erityisesti puhdas matematiikka, vaikka hänen osuutensa matematiikan soveltamisessa luonnontieteisiin on myös huomattava. René Descartes (1596-1650) ja Fermat keksivät analyyttisen geometrian toisistaan riippumatta. Fermat oli ensimmäinen, joka sovelsi analyyttistä geometriaa kolmiulotteiseen avaruuteen, kun taas Descartes tyytyi kahteen ulot-

tuvuuteen. ([12], s.65). Yhdessä nuoremman aikalaisensa Blaise Pascalin (1623-1662) kanssa Fermat muotoili todennäköisyyslaskennan periaatteet. ([16], s.28).

Fermat'n loistavimpia saavutuksia oli differentiaali- ja integraalilaskennan pääperiaatteiden hahmotteleminen. Fermat oli käsitellyt differentiaali- ja integraalilaskentaa jo 30 vuotta ennen Isaac Newtonin (1642-1727) syntymää, jolle kunnia differentiaali- ja integraalilaskennan keksimisestä yleensä kuuluu. ([11], s.15-17). Fermat keksi ääriarvomenetelmän, josta Newton oman kertomansa mukaan sai lähtökohdan differentiaalilaskennan kehittämiseen. Ääriarvoja koskevaa tulostaan Fermat sovelsi valo-oppiin: hän totesi, että valo kulkee pisteestä toiseen eri väliaineissa nopeinta mahdollista tietä. Tästä 'minimiajan periaatteesta' Fermat johti fysiikassa keskeiset valon heijastumis- ja taittumislait. ([16], s.27-28).

Jälkimaailman silmissä Fermat'n suurimmat saavutukset ovat lukuteoriaan liittyviä. Tämä johtuu ehkä siitä, että hänen työnsä muilla matematiikan aloilla olivat voimakkaana jatkuneen kehityksen ensi askelia, jotka ajan kuluessa jäivät uusien tulosten varjoon. ([16], s.28).

Fermat oli erityisen ihastunut kokonaislukuihin, joista hän löysi kauneutta ja mielekkyyttä ([11], s.19). Hän kehitti monia kokonaislukuihin liittyviä teoreemia, joista esimerkiksi yksi väittää, että muotoa $2^{2^n}+1$, missä $n \in Z$, olevat luvut ovat alkulukuja. Hän ei kuitenkaan väittänyt todistaneensa arvaustaan. Paljon myöhemmin, 1700-luvulla, Euler huomasi, etteivät kaikki tällä kaavalla tuotetut luvut olekaan alkulukuja. Muotoa $2^{2^n}+1$ olevia alkulukuja kutsutaan Fermat'n alkuluvuiksi. Fermat esitti myös niin sanotun pienen lauseensa todistamatta sitä. Lauseen mukaan $a^{p-1} \equiv 1(\text{mod p})$ aina kun ei ole $p \mid a$, tässä p on alkuluku. Leibniz antoi Fermat'n pienelle lauseelle ensimmäisen todistuksen eräässä päiväämättömässä käsikirjoituksessaan, mutta hän näyttää tunteneen sen ennen vuotta 1683. ([12], s.67-69).

Fermat esitti myös, että jokainen alkuluku, joka on muotoa $4n+1$ voidaan esittää kahden neliön summana yhdellä ja vain yhdellä tavalla. Esimerkiksi $37 = 1 + 36 = 1^2 + 6^2$, eikä ole muita neliöitä, joille $37 = x^2 + y^2$. Fermat ei jättänyt tällekään teoreemalle mitään todistusta. Fermat kuitenkin kuvaa sen nerokkaan keksimänsä metodin, jonka avulla hän todisti tämän ja eräitä muitakin ihmeellisistä tuloksistaan. Sitä kutsutaan 'äärettömäksi laskeutumiseksi', ja se vastaa matemaattista induktiota. Ensimmäisenä tämän lauseen todisti Leonhard Euler vuonna 1749 ponnisteltuaan herkeämättä seitsemän vuoden ajan todistuksen keksimiseksi. ([12], s.70).

Antiikin kreikan matemaattiset saavutukset viehättivät Fermat'ta. Fermat'n suuresti arvostamien kirjojen joukossa oli Claude Bachetin kreikasta latinaksi kääntämä Diofantoksen Arithmetica. ([11], s.15-21, 53-54). Kirja käsitteli muun muassa yhtälön $x^2 + y^2 = z^2$ ratkaisuja ([16], s.26). Tämän kir-

jan marginaaliin Fermat kirjoitti kuuluisan lauseensa arviolta vuonna 1637. Lause sanoo, että $x^n + y^n \neq z^n$, kun $n > 2$ ja x, y, z, n ovat positiivisia kokonaislukuja. Väittämän alapuolelle hän kirjoitti latinaksi: 'Cuius rei demonstrationem mirabilem sane detexi hanc marginis exiguitas non caperet', eli 'olen keksinyt väittämälle ihmeellisen todistuksen, mutta marginaalissa ei riitä sille tilaa'. Tämä lause löytyi Fermat'n kuoltua vuonna 1665. Fermat'n alkuperäiset merkinnät eivät ole säilyneet, mutta väittämät esiintyvät hänen poikansa julkaisemassa teoksessa. Tämä huomautus on kannustanut matemaatikkoja vuosisatojen ajan etsimään tuota 'ihmeellistä' todistusta. ([11], s.19-21). Joidenkin mukaan on mahdollista, että Fermat tarkasteli potenssitaulukoita ns. nexus-lukujen eli perättäisten kokonaislukujen saman potenssin erotuksen summana. Kun kokonaislukujen potenssit kirjoitetaan muotoon $1 + (2^n - 1^n) + (3^n - 2^n) + \ldots + (x^n - (x-1)^n)$, siis nexus-lukujen summana, voidaan huomata, että vain neliötaulukossa ($n = 2$) nexus-lukujen ja niiden perättäissummien joukossa on neliöitä. Minkään korkeamman potenssin taulukossa nexus-lukujen ja nexussummien joukossa ei esiinny kokonaislukujen ko. potensseja. Kahden kokonaisluvun saman potenssin erotus (eli etäisyys ko. potenssitaulukossa) on aina nexus-luku tai perättäisten nexus-lukujen summa, joka ei voi olla minkään kokonaisluvun ko. potenssi, jos n on suurempi kokonaisluku kuin 2. Tällainen havainto on Fermat'n suuren lauseen kanssa loogisesti yhtäpitävä ja mahdollinen selitys sille, ettei 'demonstraatio' mahtunut marginaaliin. ([2]).

On merkkejä, että Fermat itse olisi ratkaissut tapauksen $n = 4$ käyttämällä 'äärettömän laskeutumisen' menetelmää, mistä hän näyttää kirjeissään kertovan ([16], s.29). Hän myös huomasi, että jos hänen väitteensä pitää paikkansa jollain luvulla n, niin se pitää paikkansa myös kaikilla luvun n monikerroilla ([11], s.55). Fermat eli vielä pitkään kuuluisan huomautuksensa jälkeen, mutta ei kertaakaan palannut siihen uudelleen ([11], s.148).

Fermat ei julkaissut yhtään työtään. Hänen töidensä selvittämiseksi joudutaankin turvautumaan aikalaisten saamiin kirjeisiin. Suurimmassa osassa lauseistaan Fermat oli kirjoittanut marginaaliin viitteitä oman todistuksensa kulkuun. Näiden viitteiden avulla myöhempi todistaminen helpottui huomattavasti. Suuren lauseen kohdalla oli aloitettava alusta. ([16], s.29).

2.3 Seuraavat vuosisadat

On siis mahdollista, että Fermat todisti itse suuren lauseen tapauksen $n = 4$, mutta muuten lauseen todistus ei ollut edennyt. Vasta 100 vuotta myöhemmin Sveitsiläinen Leonhard Euler (1707-1783) todisti tapaukset $n = 3$ ja $n = 4$. ([16], s.29).

Euler oli ensimmäinen matemaatikko, joka sai edistystä aikaan Fermat'n

suuren lauseen parissa. Euler oli tuottelias matemaatikko. Hän kehitti muun muassa lukuteoriaa, differentiaalilaskentaa, differentiaaliyhtälöitä, kompleksilukujen teoriaa ja topologiaa. ([1]). Euler teki kuitenkin virheen todistaessaan tapausta $n = 3$. Virhe koski muotoa $a^2 + 3b^2$ olevien kokonaislukujen jaollisuusominaisuuksia. ([18], s.24).

Saksalainen Carl Friedrich Gauss (1777-1855) korjasi virheen, jonka Euler teki todistaessaan tapausta $n = 3$ ([11], s.62). Yleisesti ajatellaan, että Gauss on yksi kolmesta kaikkien aikojen parhaasta matemaatikosta. Muut kaksi ovat Arkhimedes ja Isaac Newton. ([1]). Gauss tutki muun muassa lukuteoriaa, ja hän julkaisi lukuteoriaan liittyviä tutkimuksiaan vuonna 1801 latinankielisessä kirjassaan Disquisitiones arithmeticae. Mutta jos Gauss arvosti erityisesti lukuteoriaa, niin miksei hän yrittänyt todistaa Fermat'n suurta lausetta? Gaussin ystävä H.W.M Olbers (1758-1840) lähetti 7.3.1816 kirjeen Gaussille, jossa hän kertoi, että Ranskan tiedeakatemia oli luvannut suuren palkinnon sille, joka osoittaa Fermat'n suuren lauseen oikeaksi tai vääräksi. Olbers sanoi kirjeessään, että Gauss oli lukuteoriassa selvästi muita parempi, ja hän kehoittikin Gaussia paneutumaan lauseen todistukseen. Gauss ei kuitenkaan innostunut ajatuksesta. Hän kirjoitti Olbersille, että Fermat'n lause oli hänen mielestään niin erillinen ongelma, ettei se kiinnostanut häntä. Hän väitti, että voisi esittää koko joukon samankaltaisia otaksumia, joita ei pystytä todistamaan, eikä myöskään käyttämään mihinkään. Ehkä Gauss arvasi, kuinka kavala Fermat'n suuri lause oli. Voi olla, että koko Euroopassa vain Gaussin kyvyt riittivät oivaltamaan, miten suuri ongelma lause todellisuudessa on. ([11], s.64-65). Jotkut historijoitsijat arvelevat, että Gauss olisi yrittänyt todistaa lausetta, mutta epäonnistunut siinä ([8]).

Gauss erehtyi ainakin arvioidessaan lauseen merkitystä. Myöhempi lukuteoria kehittyi nimittäin suurelta osin Fermat'n suurta lausetta tutkittaessa, kuten Kalle Väisälä sanoo, pitäen väittämää ehkä kuuluisimpana matemaattisena ongelmana. ([16], s.30). Gauss kehitti huomattavasti funktioteoriaksi eli kompleksianalyysiksi kutsuttua matematiikan alaa, joka perustuu jo Eulerin tutkimiin imaginäärilukuihin. ([11], s.64-65).

Fermat'n suuren lauseen todistusta 1800-luvun alkupuolella etsineet matemaatikot käyttivät hyväkseen niitä tuloksia, joita Gauss oli saavuttanut lukuteoriassa. He olivat niistä hyvin perillä, koska Euroopan matemaatikot kirjoittivat paljon kirjeitä toisilleen. 1800-luvun alkupuolelle mennessä kaikki muut Fermat'n esittämät lauseet oli osoitettu oikeiksi tai vääriksi. Sen sijaan tämä yksi oli yhä todistamatta. ([11], s.19-20, 64). Englannin kielessä lauseesta käytetään yleensä nimitystä Fermat's last theorem tai FLT.

Sophie Germain (1776-1831) oli Fermat'n suurta lausetta tutkineista matemaatikoista merkittävimpiä, ja hän saavutti tällä alalla hienoja tuloksia. Germain kävi kirjeenvaihtoa muun muassa Gaussin kanssa, näissä kirjeissä

hän käytti kuitenkin salanimeä 'Monsieur Le Blanc'. ([11], s.77). Germain pyrki yleistämään Fermat'n lauseen todistusta useammille luvuille. Sophie Germain pystyikin osoittamaan, että jos Fermat'n yhtälöllä on ratkaisu, kun $n = 5$, niin silloin yhtälön luvuista x, y ja z yhden on oltava jaollinen luvulla 5. Lause merkitsi, että Fermat'n yhtälön mahdolliset ratkaisut eksponentin arvolla $n = 5$ voitiin jakaa kahteen ryhmään: niihin, joissa yksikään luvuista x, y tai z ei ole jaollinen eksponentilla 5 (tapaus 1) ja niihin, joissa yksi luvuista x, y tai z on jaollinen eksponentilla 5 (tapaus 2). Tämä lähestymistapa voitiin laajentaa koskemaan muitakin eksponentteja. Sophie Germain osoitti, että tapaus 1:n mukaisia ratkaisuja ei ole alkulukueksponenteille yhdestä sataan. Siis jos mikään luvuista x, y ja z ei ole jaollinen eksponentilla n, niin Fermat'n yhtälöllä ei ole ratkaisua millään lukua 100 pienemmällä alkuluvulla n. Tämä oli erittäin merkittävä tulos, sillä se rajasi tutkittavien yhdistelmien joukkoa: jäljelle jäi tapaus 2 eli jos n on alkuluku ja $n < 100$, niin nyt tarvitsi tutkia vain niitä tapauksia, joissa x, y tai z on jaollinen luvulla n. ([11], s.68-69).

Fermat'n suuren lauseen tapauksessa $n = 5$ todistivat Peter Gustav Dirichlet (1805-1859) ja Adrian Legendre (1752-1833). Dirichlet onnistui osoittamaan tapauksen $n = 5$ todeksi silloin kun joku luvuista x, y tai z on jaollinen kymmenellä. Tämä tulos sai paljon huomiota, ja yksi sen arvostelijoista oli Legendre. Hieman Dirichletin tuloksen jälkeen Legendre pystyi todistamaan tapauksen $n = 5$. Hieman sen jälkeen myös Dirichlet sai tapauksen $n = 5$ todistettua kokonaisuudessaan. ([1]). 1832 Dirichlet julkaisi todistuksen tapaukselle $n = 14$. Hän oli yrittänyt todistaa tapausta $n = 7$, mutta ei onnistunut siinä. ([11], s.55).

Vuonna 1839 Gabriel Lamé (1795-1870) todisti tapauksen $n = 7$. Victor Lebesgue (1791-1875) täydensi Lamén todistusta vuonna 1840. ([7]). Lamé ilmoitti Ranskan tiedeakatemian kokouksessa 1.3.1847, että hän oli löytänyt Fermat'n suurelle lauseelle täydellisen todistuksen. Aiemmin todistettujen tulosten $n = 3$, $n = 4$, $n = 5$ ja $n = 7$ sijasta Lamé ehdotti ongelmalle yleistä ratkaisumenetelmää, joka pätisi kaikilla luvun n arvoilla. Hän jakoi ensin kompleksilukuja käyttäen Fermat'n yhtälön vasemman puolen x^n+y^n tekijöihin, ja todisti lauseen tätä apuna käyttäen. Lamén mukaan tätä menetelmää hänelle oli ehdottanut Joseph Liouville (1809-1882). Liouville kuitenkin epäili, ettei tekijöihinjako olisi tässä tapauksessa yksikäsitteinen. Kokonaisluvuille tekijöihinjako on tietenkin yksikäsitteinen. Lamé käytti todistuksessaan kuitenkin kompleksilukuja, ja Liouville epäilikin kompleksilukujen tekijöihinjaon yksikäsitteisyyttä. Myöhemmin selvisi, että Liouvillen epäilyt olivat perusteltuja. Ernst Eduard Kummer (1810-1893) oli vuonna 1844 julkaissut muistion, jossa hän oli näyttänyt toteen yksikäsitteisen tekijöihinjaon pätemättömyyden tässä kyseessä olevassa tapauksessa. Kummerin julkaisu ei ol-

lut levinnyt kovin laajalle, joten Liouville ei tiennyt asiasta aiemmin. Lamén yritys oli hyvä, muttei tuottanut tulosta. ([11], s.55,77-78).

Ernst Eduard Kummer pääsi Fermat'n ongelman käsittelyssä lähemmäksi ratkaisua kuin kukaan muu tuohon aikaan. Sekä näiden yritystensä että muiden matemaattisten projektiensa avulla hän tuli keksineeksi uuden matematiikan haaran, ideaalilukujen teorian. Ideaaliluvut tunnetaan nykyalgebrassa ideaaleina tai ihanteina. Ideaalilukujen avulla Kummer pystyi osoittamaan, että 'säännöllisillä alkuluvuilla' n Fermat'n suuri lause pitää paikkansa. Säännölliset alkuluvut ovat tietyntyyppisiä parittomia alkulukuja. Tämä todistus laajeni käsittämään äärettömän monta eksponenttia n, sillä lause piti paikkansa myös kaikilla niillä luvun n arvoilla, jotka ovat jaollisia 'säännöllisillä' alkuluvuilla. 'Epäsäännöllisistä' alkuluvuista Kummer ei saanut otetta. Sataa pienemmissä alkuluvuissa, niitä on kolme: 37, 59 ja 67. Hän pystyi kyllä osoittamaan lauseen todeksi näissäkin tapauksissa, muttei löytänyt yleistä ratkaisua 'epäsäännöllisille' alkuluvuille. Kummerin saavutusten ansiosta 1850-luvulla tiedettiin jo, että lause pätee kaikilla lukua 100 pienemmillä kokonaisluvuilla samoin kuin niillä äärettömän monilla kokonaisluvuilla, jotka ovat lukujen 2, ..., 97 monikertoja. Jäljellä oli kuitenkin vielä äärettömän monta sellaista eksponenttia n, joista ei tiedetty, voisiko yhtälö toteutua. ([11], s.78-80).

Vuonna 1816 Ranskan tiedeakatemia oli julistanut palkinnon sille, joka todistaisi lauseen. Tämä lupaus uudistettiin vuonna 1850. Nyt luvattiin kultamitali ja 3000 frangia. Vuonna 1856 tiedeakatemia kuitenkin perui palkinnon, koska ratkaisu näytti siirtyvän hamaan tulevaisuuteen. Vuonna 1908 Wolfskehlin säätiö Saksassa julisti uuden 100000 saksanmarkan palkinnon lauseen todistajalle. Ratkaisuyrityksiä tuli tuhansia, mutta kaikki ne olivat vääriä. 1920-luvun inflaatiossa palkinnon rahallinen arvo hupeni, mutta silti säätiö sai uusia ratkaisuehdotuksia. ([11], s.81-82). Mainittakoon, että kuuluisa saksalainen matemaatikko Lindemann, joka selvitti yli 2000 vuotta vanhan ympyrän neliöimisongelman todistamalla, että π on transkendenttiluku, esitti 1900-luvun alussa parikin virheellistä todistusta Fermat'n suurelle lauseelle. ([16], s.37).

1800-luvun lopulla ja 1900-luvun alussa kehitettiin huomattavasti abstraktia algebraa, muun muassa Galois'n teoria ja Abelin ryhmä. Abstrakti algebra oli tärkeässä osassa todistuksen lopulta löytyessä. ([11], s.83-89).

2.4 Lopullinen todistus

Vuonna 1955 Yutaka Taniyama (1927-1958) mietti, että automorfifunktiot tuntuivat monine kompleksitason symmetriaominaisuuksineen olevan jotenkin yhteydessä Diofantoksen yhtälöihin. Goro Shimuran (1930-), Taniyaman

ystävän, mukaan jokainen elliptinen käyrä, jonka kertoimet ovat rationaalilukuja, voidaan lausua modulaarisessa muodossa. Modulaariset muodot olivat erikoistapaus Taniyaman käsittelemistä automorfifunktioista. Myöhemmin osoittautui merkittäväksi se, että modulaaristen muotojen sarjakehitelmän kertoimet voitiin rajata rationaalilukuihin. ([11], s.111-112).

Taniyaman-Shimuran otaksuman mukaan jokainen elliptinen käyrä on modulaarinen. Joskus otaksumaa kutsutaan virheellisesti Weilin-Taniyaman otaksumaksi. 1900-luvulla modulaaristen muotojen ja automorfifunktioiden teoriaa kehitti myös Henri Poincaré (1854-1912). ([11], s.94-96, 116).

Englantilainen matemaatikko Louis J. Mordell (1888-1972) tarkasteli muiden tutkimustensa ohessa, kuinka monta kokonaislukuratkaisua yhtälöllä $x^n + y^n = z^n$ voi olla. Vuonna 1922 hän arvioi, että kun $n \geq 3$, niin tiettyä eksponentin n arvoa kohti on vain äärellinen määrä ratkaisuja. Vuonna 1983 saksalainen matemaatikko Gerd Faltings (1954-) todisti erään lisälauseen, johon sisältyi myös Mordellin lause. Hiukan myöhemmin David Rodney Heath-Brown mukaili Faltingin todistusta osoittaen, että kun n kasvaa, niin mahdollisuus sille, että Fermat'n väittämä on oikein, kasvaa. ([16], s.31).

Heath-Brownin ja Andrew Granvillen mukaan Fermat'n lauseen toteuttavia positiivisia kokonaislukuja ei voi löytyä, kun n on hyvin suuri. On siis olemassa N siten että millekään $n \geq N$ ei ole olemassa sellaisia lukuja x, y ja z, joille $x^n + y^n = z^n$. Tämä tarkoitti, että lause 'melkein varmasti' piti paikkansa. Joka tapauksessa ratkaisuja olisi vähän ja ne olisivat hyvin kaukana toisistaan. Vuoteen 1983 mennessä lause oli todistettu oikeaksi luvun n arvolle miljoona saakka. ([16], s.31).

Gerhard Frey (1944-) esitti ajatuksen siitä, että Fermat'n yhtälön ratkaisusta seuraa välttämättä, että on olemassa sellainen elliptinen käyrä, joka ei ole modulaarinen. Tämä oli ristiriidassa Taniyaman-Shimuran otaksuman kanssa. Frey ei kuitenkaan todistanut, että tällainen elliptinen käyrä on olemassa, hän vain hahmotteli todistusidean asiantuntijoiden täydennettäväksi. Freyn väite tunnetaan nimellä epsilon-otaksuma. Siis jos Taniyaman-Shimuran otaksuma pitäisi paikkansa, niin silloin Fermat'n suuri lause voitaisiin osoittaa todeksi. Kenneth Ribet, Kalifornian yliopiston matematiikan professori, todisti 1980-luvulla, että Taniyaman-Shimuran otaksumasta seuraa Fermat'n suuren lauseen oikeellisuus. Enää tarvittiin joku, joka voisi osoittaa että Taniyaman-Shimuran otaksuma pitää paikkansa. Jos joku siinä onnistuisi, samalla tulisi Fermat'n suuri lause todistetuksi. ([11], s.128-129).

Andrew Wiles (1953-) päätti yrittää todistaa Taniyaman-Shimuran otaksuman. Hän uskoi vakaasti onnistuvansa yrityksessään, vaikka lähes kaikki muut matemaatikot ajattelivat, ettei otaksumaa kyettäisi osoittamaan oikeaksi vielä pitkään aikaan. Wiles jätti kaiken muun tutkimustyönsä. Hän keskittyi lapsuuden haaveeseensa, Fermat'n suuren lauseen todistamiseen.

Wilesin oli osoitettava, että jokainen elliptinen käyrä, jonka kertoimet ovat rationaalilukuja, on rakenteeltaan modulaarinen. Modulaarisuus ja elliptisyys näyttivät olevan niin täysin eri maailmoista, ettei kenelläkään ollut aavistustakaan miten niiden välinen eriskummallinen yhteys voitaisiin osoittaa todeksi. ([11], s.132). Modulaarisilla muodoilla tarkoitetaan funktioryhmiä, jotka on määritelty neliulotteisen kompleksiavaruuden ylemmässä puoliskossa ja jotka noudattavat hyperbolista geometriaa. Elliptiset käyrät taas ovat tasokäyriä, jotka ovat epäsingulaarisia ja jotka määrittelee yhtälö $y^2 = x^3+ax+b$, missä a ja b kuuluvat annettuun kuntaan K. Niiden kuvaajissa ei siis ole teräviä kohtia, eivätkä ne leikkaa itseään.

Ensin Wiles ajatteli tarkastella elliptisten käyrien joukkoja ja katsoa, mitä niistä saisi irti. Nyt ongelma pilkkoutui pienempiin osiin ja hän saattoi tutkia kutakin käyräparvea erikseen. Monet muut lukuteoreetikot olivat jo osoittaneet, että tietyt elliptiset käyrät ovat modulaarisia. Pian Wiles kuitenkin havaitsi, ettei olisi sittenkään antoisaa keskittyä vain vertailemaan elliptisiä käyriä modulaarisiin muotoihin, koska näin hän joutuisi käsittelemään kahta ääretöntä joukkoa. ([11], s.133).

Kaksi vuotta kestäneiden tuloksettomien ponnistelujen jälkeen Wiles päätti kokeilla toista keinoa. Hän arveli voivansa muuntaa elliptiset käyrät Galois'n esitykseksi ja verrata sitten näin saatua käyrien määrää modulaaristen muotojen määrään. Ajatus ei ollut Wilesin oma keksintö. Tässä lähestymistavassa käytetään hyväksi lukukuntia. Galois'n teoria antaa lukuteoreetikoille mahdollisuuden siirtyä sopivan muunnoksen avulla äärettömän suuresta lukukunnasta äärelliseen joukkoon. Se helpottaa huomattavasti muun muassa tämän ongelman käsittelyä, sillä äärellisten joukkojen kokoa voidaan verrata. Tämän alan Wiles tunsi hyvin, sillä hän oli soveltanut sitä väitöskirjassaan, jossa hän oli käsitellyt Iwasawan teoriaa. Puhuttaessa Iwasawan teoriasta, tarkoitetaan Kenkichi Iwasawan 1950-luvulla kehittämää Galois'n modulien teoriaa. Teoria liittyy lukuteoriaan sekä luokkakuntateoriaan. Nyt Wiles pääsi vauhtiin, mutta vuoden kuluttua hän törmäsi jälleen seinään. ([11], s.134-135).

Vuonna 1991 Wiles hylkäsi aiemmat lähestymistapansa ja alkoi tutkia Viktor Kolyvaginin ja Matthias Flachin töitä, jotka liittyvät ns. Eulerin systeemeihin. Wiles arveli pystyvänsä osoittamaan Taniyaman-Shimuran otaksuman oikeaksi näiden töiden pohjalta. Tämä vaati Wilesilta ankaraa uurastusta, sillä ala ei liittynyt lainkaan Iwasawan teoriaan. Kuusi vuotta jatkuneen yksinäisen uurastamisen jälkeen Wiles otti tammikuussa 1993 yhteyttä professori Nick Katziin (1943-), joka, kuten Wiles, työskenteli Princetonin matematiikan laitoksella. Katz tunsi hyvin ne teoriat, joita Wiles käytti. Wiles luotti Katziin ehdottomasti, eikä kukaan ulkopuolinen saanut tietää Wilesin todistusyrityksestä. ([11], s.135-136).

Nyt Wiles eteni Taniyaman-Shimuran otaksuman todistuksessa. Hän oli jo osoittanut, että elliptisistä käyristä useimmat olivat modulaarisia, mutta muutaman käyrän modulaarisuus oli vielä todistamatta. Lukiessaan Barry Mazurin (1937-) tutkimusta Eisensteinin ideaaleista, hän kuitenkin keksi ratkaisun näihin ongelmiin. Jälleen kerran jonkun toisen matemaatikon oivallus ja tutkimus auttoi Wilesia ylittämään toivottoman korkealta näyttäneen esteen. Nyt Wiles oli valmis astumaan julkisuuteen. ([11], s.140).

Kesäkuun lopulla 1993 Andrew Wilesia pyydettiin pitämään luento vapaavalintaisesta aiheesta Cambridgen yliopistossa. Wiles halusi kuitenkin pitää kolme luentoa, muttei kertonut tarkkaa aihetta kenellekään. Näillä luennoilla hän käsitteli erinäisiä lauseita liittyen modulaarisiin muotoihin, elliptisiin käyriin ja Galois'n esityksiin. Viimeisen luennon lopulla hän sanoi, että näiden luentojen esitysten perusteella Fermat'n suuri lause pitää paikkansa. Kaikki lukuteorian huiput olivat paikalla Cambridgessa. ([11], s.11-14, 140).

Yleensä tieteelliset tulokset julkaistaan alan lehdissä, mutta Wiles halusi kertoa tuloksestaan toisin. Luentojen jälkeen Wilesin 200-sivuisen raportin kopiot lähetettiin johtaville lukuteorian tutkijoille. Eräät heistä kertoivat pian epäilyistään, mutta yleisesti ottaen matemaatikot arvelivat, että Wiles oli todella todistanut Fermat'n suuren lauseen. ([11], s.141-142).

Asiantuntijat löysivät Wilesin raportista ongelmakohdan. Wiles oli päätellyt erään systeemin olevan Eulerin systeemi, vaikkei se todellisuudessa ole sitä. Aukko Wilesin käyttämässä Eulerin systeemissä romahdutti koko päättelyn. Wilesin täytyi ryhtyä miettimään, voisiko todistuksen jollain keinolla saada päteväksi. ([11], s.143-144).

Kun yli vuosi oli kulunut Cambridgen luennoista, Wiles oli jo valmis luopumaan toivosta ja unohtamaan jumiin jääneen todistuksensa. 19.9.1994 Wiles päätti vielä kerran silmäillä monivuotista työtään, ennen kuin mapittaisi paperit ja jättäisi haaveet Fermat'n suuren lauseen todistamisesta. Hän halusi vielä kerran katsoa, mikä oli estänyt häntä rakentamasta todistusketjuun Eulerin systeemin. Pian Wiles oivalsi, miksi todistelu ontui. Hän tajusi, että juuri sama asia, joka esti häntä käyttämästä Eulerin systeemiä, tekisi mahdolliseksi käyttää Iwasawan teoriaa, jonka hän oli kolme vuotta aiemmin hylännyt. ([11], s.145-146).

Wiles viimeisteli todistuksen. Kaikki näytti asettuvan täydellisesti kohdalleen. Käsikirjoitus oli nyt uudelleen valmis asiantuntijoiden tarkastettavaksi. Richard Taylor (1962-) oli auttanut Wilesia todistuksessa ja Wiles lupasi Taylorille panna molempien nimet seuraavaan raporttiin. Näin hän myös teki, vaikka todellisuudessa Wiles onnistui korjaamaan todistuksen vasta Taylorin jo lähdettyä Princetonista Cambridgeen, mistä hän oli tullut. ([11], s.147).

Nyt Wiles noudatti julkistamisessa tuttuja muotoja. Hän lähetti raport-

tinsa alansa arvostetuimpaan julkaisuun, Annals of Mathematics-lehteen. Ennen julkaisemista lehti tarkastutti tekstin monella matemaatikolla, mutta nyt virheitä ei löytynyt. Toukokuussa 1995 ilmestynyt Annals of Mathematics sisälsi Wilesin Cambridgessa pitämät luennot ja niihin liitetyt korjaukset, jotka oli kirjattu Wilesin ja Taylorin nimiin. Fermat'n suuri lause oli viimeinkin todistettu oikeaksi. ([11], s.147).

Wiles työsti todistusta yhteensä 7 vuotta. Hän käytti pitkässä todistuksessa syvällisiä matemaattisia teoreemia, joista ei kenelläkään voinut Fermat'n aikana olla vielä aavistustakaan, koska ne oli kehitetty vasta 1900-luvulla. Wilesin rakennelmassa oli valtavasti osia, jotka olivat perua lukemattoman monilta edeltäjiltä. Wiles on sanonut todistuksestaan, että se on '1900-luvun todistus', koska hän käytti siitä monia sellaisia matematiikan keinoja, jotka opittiin tuntemaan vasta silloin. Hän käytti myös hyväkseen varhaisempien matemaatikoiden käyttämiä menetelmiä. Matematiikan eri haarojen väliset yhteydet olivat lopulta avain, jolla Andrew Wiles avasi Fermat'n suuren lauseen arvoituksen. ([11], s.21, 46, 147-148). Wolfskehlin säätiön vuonna 1908 julistama palkinto on annettu Andrew Wilesille ([9]).

2.5 Andrew Wilesin mietteitä Fermat'n suuresta lauseesta ja sen todistamisesta

Tämä kappale perustuu Andrew Wilesin antamaan haastatteluun, ks. tarkemmin [10].

Andrew Wiles omisti suuren osan urastaan Fermat'n suuren lauseen todistamiselle. Hän tutustui ongelmaan jo lapsena paikallisessa kirjastossa. Hän selaili hyllyä, jossa oli matematiikan kirjoja, ja löysi kirjan jossa ongelma esiintyi. Se oli ollut ratkaisematta noin 300 vuotta. Se näytti helpolta ja siltikään historian suuret matemaatikot eivät olleet pystyneet ratkaisemaan sitä. Tässä oli ongelma, jonka 10-vuotias pystyi ymmärtämään. Anrew Wiles sanoo tienneensä heti, ettei voi päästää irti ongelmasta. Hänen oli ratkaistava se.

Wiles yritti ratkaista ongelmaa jo teininä. Hän yritti tarttua ongelmaan niin kuin ajatteli Fermat'n yrittäneen sitä. Wiles ajatteli, että Fermat ei olisi tiennyt matematiikasta paljoakaan enempää kuin mitä Wiles teininä tiesi. Myöhemmin Wiles huomasi, että monet ihmiset olivat yrittäneet ratkaista ongelmaa aiempina vuosisatoina, joten hän alkoi opiskella kyseisiä menetelmiä. Wiles ei siltikään edennyt todistuksessaan. Kun hänestä tuli tutkija, hän päätti siirtää ongelman syrjään. Ongelma Fermat'n suuren lauseen kanssa työskennellessä on siinä, että siihen voi käyttää vuosikausia pääsemättä yhtään mihinkään.

Kesällä 1986 Wiles sai kuulla Kenneth Ribetin todistaneen että Fermat'n suurella lauseella ja Taniyaman-Shimuran otaksumalla on yhteys toisiinsa. Wiles kertoi tienneensä heti, että hänen elämänsä suunta olisi muuttumassa. Tieto tarkoitti sitä, että lauseen todistamiseen riitäisi Taniyaman-Shimuran otaksuman todistaminen. Wiles oli jo tätä alaa tutkinut. Nyt oli aika tarttua lapsuuden unelmaan uudelleen. Kenelläkään ei ollut ajatusta siitä, miten lähestyä Taniyaman-Shimuran otaksumaa. Wiles oli kuitenkin päättänyt tarttua ongelmaan. Nyt rakkaus Fermat'n ongelmaan yhdistyi ongelmaan, joka oli myös ammatillisesti hyväksyttävä.

Wiles sanoi ymmärtäneensä, että kaikki mikä liittyy Fermat'n suureen lauseeseen, herättää suurta kiinnostusta, mikä vaikeuttaa omaan työhön keskittymistä. Siksi hän ei kertonut yrityksistään muille. Ainut, joka tiesi Wilesin puuhista oli hänen vaimonsa.

Wiles kertoi kantaneensa ongelmaa päässään koko ajan. Hän mietti sitä heti herätessään, koko päivän ja nukkumaan käydessään. Ainut hetki jolloin hän pystyi rentoutumaan oli se kun hän oli lastensa kanssa. Lapsia kun ei Fermat kiinnostanut. Kun Wiles juuttui johonkin ongelmaan, eikä tiennyt, mitä tehdä seuraavaksi, hän lähti kävelylle. Siellä hän selvitteli ajatuksiaan ongelman suhteen.

Wiles kuvaa todistusprosessia matkaksi halki pimeän, tutkimattoman kartanon. Ensin astut sisään ensimmäiseen huoneeseen ja on täysin pimeää. Kompastelet ympäriinsä ja törmäilet huonekaluihin, mutta lopulta opit, missä mikäkin huonekalu on. Lopulta, kuukausien jälkeen, löydät valokatkaisimen ja käännät sen päälle. Äkkiä kaikki on valoisaa, näet tarkkaan, missä olit. Sitten siirryt seuraavaan huoneeseen ja vietät taas kuukausia pimeässä. Näin tutustut taloon pala palalta.

Wiles uskoi olevansa oikealla polulla, muttei voinut olla varma siitä, että tulisi ratkaisemaan ongelman. Mahdollisesti niitä metodeja, joita ongelman lopulliseen ratkaisemiseen tarvitaan ei keksittäisi vielä satoihin vuosiin. Wiles kertoi että vaikka hän oli oikealla polulla, hän saattoi elää väärällä vuosisadalla.

1993 eräänä toukokuun aamuna Wiles keksi lopulta viimeisen palan todistukseen. Hän työskenteli sen kanssa niin, että unohti lounaankin. Todistuksessa oli kuitenkin virhe, joka myöhemmin saatiin korjattua.

Jotkut ongelmat näyttävät helpoilta. Niitä yritetään ratkaista vuosia, satoja vuosia ja ne osoittautuvat erittäin vaikeiksi ratkaista. Ei ole mitään syytä, mikseivät nämä todistukset voisi olla helppoja ja silti ne osoittautuvat todella monimutkaisiksi. Fermat'n suuri lause on hyvä esimerkki tästä. Miksi ihmiset sitten näkevät niin paljon vaivaa löytääkseen todistuksen? Wilesin mukaan puhtaat matemaatikot rakastavat ongelmien ratkaisua, he rakastavat haasteita. Ja kun aikaa kuluu, eikä todistusta löydy, siitä tulee todelli-

nen haaste. Tästä lauseesta tekee erityisen se, että Fermat itse on väittänyt todistaneensa sen.

Wilesin mukaan ei ole mitenkään mahdollista, että hänen keksimänsä todistus olisi sama, jonka Fermat aikanaan väitti keksineensä. Fermat ei olisi voinut keksiä sitä. Todistus on 150 sivua pitkä. Sitä ei olisi voitu tehdä 1800-luvulla saati sitten 1600-luvulla. Wiles ei usko että Fermat'lla oli todistusta. Hän ajattelee, että Fermat narrasi itsensä luulemaan että hänellä on todistus. On kuitenkin olemassa vielä pieni todennäköisyys, että on olemassa elegantti, 1600-luvun todistus.

Wilesin mukaan mikään ongelma ei tule merkitsemään hänelle yhtä paljon. Fermat oli hänen lapsuuden intohimonsa. Tulevaisuudessa hän sanoo yrittävänsä ratkaista ongelmia, ehkä erittäin vaikeitakin, mutta mikään niistä ei tule olemaan hänelle yhtä tärkeä. Jonkinlaista kaihoa on kuitenkin ilmassa. Jokin kauan ilmassa ollut ongelma on nyt poissa ja meidän täytyy löytää tilalle uusia huomion kohteita. Wiles toivoo, että nuoret matemaatikot ovat nähneet ongelman ratkaisemisen jännityksen ja että he ymmärtäisivät, että matematiikassa on paljon muitakin ongelmia, jotka ovat yhtä haastavia. Wilesin mukaan matematiikan suurin ongelma on nyt Riemannin hypoteesi.

Ratkaistavan ongelman valitseminen riippuu paljolti siitä, kuinka paljon siitä välittää. Wiles itse sanoo yrittävänsä aina ratkaista ongelmaa, jolla on merkitystä hänelle. Wiles myöntää että hänellä on ollut etuoikeus ajaa takaa ongelmaa, joka oli hänen lapsuuden unelmansa. Hän tietää että se on harvinainen etuoikeus, mutta jos joku voi aikuisiällä tehdä jotain omasta mielestään niin tärkeää, niin se on palkitsevampaa kuin mikään muu, mitä voi kuvitella.

3 Tapaus $n = 4$

Tapaus $n = 4$ on Fermat'n suuren lauseen helpoin tapaus. Jotkut väittävät, että Fermat todisti suuren lauseensa tapauksessa $n = 4$ ([16], s.29). Tästä ei kuitenkaan ole varmaa tietoa. Fermat käytti monissa muissa todistuksissaan keksimäänsä menetelmää, jota kutsutaan äärettömän laskeutumisen menetelmäksi. Menetelmää käytettäessä oletetaan, että on valittu ongelman pienin mahdollinen ratkaisu ja näytetään, että pitäisi olla olemassa vielä pienempi ratkaisu. Näytetään siis että ei ole olemassa pienintä ratkaisua, ja kun käsitellään positiivisia kokonaislukuja, niin ratkaisuja ei ole ollenkaan. Fermat'n suuren lauseen tapauksessa $n = 4$ äärettömän laskeutumisen menetelmä tarkoittaa seuraavaa: olkoon $n = 4$ ja $R = \{m \in N | \exists x, y, z$ s.e $x^n + y^n = z^n$ ja $m = \max\{x, y, z\}\}$. Olkoon $r = \min R$. Osoitetaan, että on olemassa sellainen $r_0 < r$ että $r_0 \in R$. Tästä saadaan ristiriita. Menetelmä oli yksi Fermat'n suurimmista keksinnöistä. ([15], s.4-7). Ennen kuin todistamme lauseen tapauksessa $n = 4$, käymme läpi kaksi lemmaa, jotka ovat tärkeitä itse todistuksessa. Lemma 3.1 on yleisesti tunnettu lukuteoriassa, joten sitä ei tässä todisteta.

Lemma 3.1 *Eukleideen lemma*
Olkoon p alkuluku. Jos $p \mid ab$, niin $p \mid a$ tai $p \mid b$.

Lemma 3.2 *Jos $(v, w) = 1$ ja $vw = z^n$, niin silloin on olemassa sellaiset x, y että $v = x^n$ ja $w = y^n$.*

Todistus

Olkoot $(v, w) = 1$ ja $vw = z^n$. Antiteesi: Oletetaan, että $v \neq x^n$ kaikilla x ja n. Silloin $v \neq 1$, koska $1^n = 1$. Nyt v on jaollinen alkuluvulla p, sillä jokainen kokonaisluku on joidenkin alkulukujen tulo. Joten on olemassa sellainen luku k että $v = pk$. Nyt $p \mid z$, sillä $z^n = vw = pkw$. On siis olemassa sellainen luku m että $z = pm$, joten $z^n = vw = pkw = (pm)^n = p^n m^n$. Kun jaetaan molemmat puolet luvulla p, saadaan $kw = p^{(n-1)}m^n$. Lemman 3.1 mukaan $p \mid k$ tai $p \mid w$. Luku p ei voi jakaa lukua w, sillä se jakaa luvun v ja $(v, w) = 1$. Siten $p \mid k$. Lisäksi $p^n \mid v$. Voimme päätellä, että $p^{(n-1)} \mid k$. On siis olemassa sellainen r että $k = p^{(n-1)}r$, joten $kw = p^{(n-1)}m^n = p^{(n-1)}rw$. Siten $m^n = rw$. Nyt $(r, w) = 1$ koska $r \mid v$ ja $(v, w) = 1$. Luku r ei voi olla n:s potenssi, koska jos se olisi, niin $v = pk = p \cdot p^{(n-1)}r = p^n r$ tekisi luvusta v n:nnen potenssin, mikä on vastoin oletusta. Lopuksi $r < v$, koska $p^{(n-1)} > 1$. Osoitimme että jos oletetaan, että n:nnen potenssin tekijä ei itse ole n.s potenssi niin on oltava pienempi tekijä, joka ei myöskään ole n.s potenssi ja

niin edelleen ja niin edelleen. On siis näytetty että ei ole pienintä ratkaisua, ja kun käsitellään positiivisia kokonaislukuja niin ratkaisuja ei ole ollenkaan. Joten äärettömän laskeutumisen menetelmällä meillä on ristiriita. Samalla tavalla voidaan osoittaa, että $w = y^n$ jollekin y.

Seuraavassa lauseessa käytetään termiä primitiivinen ratkaisu. Sillä tarkoitetaan sitä, että $x, y, z > 0$ ja $(x, y, z) = 1$.

Lause 3.1 *Olkoot a ja b kokonaislukuja siten että $a > b > 0$ ja $(a, b) = 1$. Olkoon toinen niistä pariton ja toinen parillinen. Silloin kolmikko (x, y, z), jossa*

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

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

Kääntäen: Jos x, y, z on primitiivinen ratkaisu yhtälölle $x^2 + y^2 = z^2$, niin silloin $a > b > 0$ ja $(a, b) = 1$. Lisäksi toinen luvuista a ja b on parillinen ja toinen pariton.

Todistus

Olkoot a ja b kokonaislukuja, jotka täyttävät lauseen ehdot. Määritellään x, y ja z kuten edellä. Silloin

$x^2 + y^2 = (2ab)^2 + (a^2 - b^2)^2 = 4a^2b^2 + a^4 - 2a^2b^2 + b^4 = a^4 + 2a^2b^2 + b^4 = (a^2 + b^2)^2 = z^2$

Selvästi $x > 0, y > 0, z > 0$ ja x on parillinen. $(x, y, z) = 1$ koska jos $d \mid x, d \mid y$ ja $d \mid z$ niin silloin $d \mid 2a^2$ ja $d \mid 2b^2$, joten $d = 1$ tai $d = 2$ (koska $(a, b) = 1$). Mutta $d \neq 2$, koska y on pariton (sillä toinen luvuista a ja b on pariton ja toinen parillinen).

Kääntäen: Olkoon (x, y, z) yhtälön $x^2 + y^2 = z^2$ primitiivinen ratkaisu, joten $x^2 + y^2 = z^2$. Koska $(x, y, z) = 1$, niin $(x, z) = 1$. Koska x on parillinen, niin z on pariton ja siksi $(z - x, z + x) = 1$. $y^2 = z^2 - x^2 = (z - x)(z + x)$. Lemman 3.2 perusteella $z - x$ ja $z + x$ ovat kokonaislukujen neliöitä. Olkoot $z + x = t^2$, $z - x = u^2$. Silloin t:n ja u:n on oltava positiivisia parittomia kokonaislukuja, $t > u > 0$. Olkoot a ja b kokonaislukuja, siten että $2a = t + u$

ja $2b = t - u$. Silloin $t = a + b$ ja $u = a - b$, missä $a > b > 0$. Aiemmin todettiin, että $z + x = t^2$ ja $z - x = u^2$. Nyt $z = u^2 + x$, joten

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

$$y^2 = (z - x)(z + x) = u^2t^2 = (a - b)^2(a + b)^2 = (a^2 - b^2)^2.$$

Joten $y = a^2 - b^2$.

Edelleen, koska $z + x = t^2$, niin $x = t^2 - z$. Nyt $z - (t^2 - z) = u^2$, joten $z - t^2 + z = u^2$ ja $2z = u^2 + t^2$. Siis

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

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

Koska $(z - x, z + x) = 1$, niin huomaamme että $(a, b) = 1$. Lopuksi, koska $a + b = t$ on pariton, niin a ja b eivät molemmat voi olla parittomia.

Lause 3.2 *Yhtälöllä $x^4 - y^4 = z^2$ ei ole kokonaislukuratkaisuja, kun $x \neq 0$, $y \neq 0$ ja $z \neq 0$.*

Todistus

Antiteesi: yhtälöllä $x^4 - y^4 = z^2$ on kokonaislukuratkaisuja. Valitaan pienin mahdollinen $x \in N$, jolle on olemassa luvut $y \in N$ ja $z \in N$ siten että $x^4 - y^4 = z^2$. Nyt $(x, y) = 1$. Tämä voidaan osoittaa seuraavasti. Jos alkuluku p jakaa molemmat, x:n ja y:n, niin $x = px'$ ja $y = py'$. Koska

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

niin $p^4 \mid z^2$, joten $p^2 \mid z$. Kun $x = px'$, $y = py'$ ja $z = p^2z'$, niin

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

missä $0 < x' < x$, koska $x = px'$. Tämä on vastoin sitä oletusta, että x on pienin mahdollinen, jolle $x^4 - y^4 = z^2$. Siis $(x, y) = 1$.

$z^2 = x^4 - y^4 = (x^2 + y^2)(x^2 - y^2)$. Koska $(x, y) = 1$, niin $(x^2 + y^2, x^2 - y^2)$ on joko 1 tai 2. Käsitellään molemmat tapaukset erikseen.

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

Koska $x^4 - y^4 = (x^2 + y^2)(x^2 - y^2) = z^2$, niin $(x^2 + y^2)(x^2 - y^2)$ on neliö. Silloin $x^2 + y^2$ ja $x^2 - y^2$ ovat neliöitä (Lemma 3.2); tarkalleen ottaen, on olemassa sellaiset positiiviset kokonaisluvut s ja t, $(s, t) = 1$ että

$x^2 + y^2 = s^2$ ja

$x^2 - y^2 = t^2$.

Koska $s^2 + t^2 = x^2 + y^2 + x^2 - y^2 = 2x^2$, niin s ja t ovat molemmat joko parittomia tai parillisia. $(s, t) = 1$, joten ne eivät voi olla parillisia. Siis s ja t ovat parittomia. Tästä seuraa, että $s+t$ ja $s-t$ ovat parillisia. Merkitään

$u = \frac{(s+t)}{2}$ ja

$v = \frac{(s-t)}{2}$.

$(u, v) = 1$, koska s ja t ovat parittomia ja $(s, t) = 1$.

Nyt

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

ja siksi $y^2 = 2uv$.

Tästä ja tiedosta $(u, v) = 1$ seuraa, että on olemassa positiiviset kokonaisluvut l ja m siten että

$u = 2l^2$ ja $v = m^2$ tai

$u = l^2$ ja $v = 2m^2$.

Se että u ja v ovat juuri tämän muotoisia voidaan perustella seuraavasti: Koska y^2 on neliö, $\frac{y^2}{2}$ voi olla kokonaisluku vain, jos se on parillinen kokonaisluku. Siksi $\frac{1}{2}uv = \frac{1}{4}y^2$ on kokonaisluku, ja koska se on kahden neliön osamäärä, se on neliö. Joko u:n tai v:n on oltava parillinen, koska $\frac{1}{2}uv$ on kokonaisluku, mutta molemmat eivät voi olla parillisia, sillä $(u, v) = 1$. $\frac{1}{2}uv$

on neliö, ja siksi tekijät ovat neliöitä.

Käydään läpi ensimmäinen vaihtoehto, toinen tehdään vastaavasti.

Siis u on parillinen, $(u, v, x) = 1$ ja

$u^2 + v^2 = (\frac{s+t}{2})^2 + (\frac{s-t}{2})^2 = \frac{(s+t)^2}{4} + \frac{(s-t)^2}{4} = \frac{(s+t)^2+(s-t)^2}{4}$

$= \frac{s^2+2st+t^2+s^2-2st+t^2}{4} = \frac{2s^2+2t^2}{4} = \frac{s^2+t^2}{2} = \frac{2x^2}{2} = x^2.$

Lauseesta 3.1 seuraa, että on olemassa positiiviset kokonaisluvut a ja b, $0 < b < a$, $(a, b) = 1$ siten että

$2l^2 = u = 2ab$

$m^2 = v = a^2 - b^2$

$x = a^2 + b^2.$

Tästä seuraa, että $l^2 = ab$. Siten on olemassa sellaiset positiiviset kokonaisluvut c ja d, $(c, d) = 1$ että

$a = c^2$ ja

$b = d^2,$

ja siten $m^2 = a^2 - b^2 = c^4 - d^4$. Huomaamme, että $0 < c < a < x$. Nyt positiivisten kokonaislukujen kolmikko (c, d, m) olisi yhtälön $x^4 - y^4 = z^2$ ratkaisu, mikä on vastoin sitä oletusta, että x on pienin mahdollinen. Siis tapaus 1 on mahdoton.

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

Nyt x ja y ovat parittomia ja z on parillinen. Lauseesta 3.1 seuraa, että on olemassa sellaiset positiiviset kokonaisluvut a ja b, $0 < b < a$, $(a, b) = 1$ että

$x^2 = a^2 + b^2,$

$y^2 = a^2 - b^2$ ja

$z = 2ab$.

Tästä syystä $x^2y^2 = (a^2 + b^2)(a^2 - b^2) = a^4 - b^4$, missä $0 < a < x$ ja tämä on vastoin sitä oletusta, että x valittiin pienimmäksi mahdolliseksi. Siis antiteesi on väärä ja voidaan todeta, että yhtälöllä $x^4 + y^4 = z^2$ ei ole kokonaislukuratkaisuja, kun $x, y, z \neq 0$.

Tässä todistuksessa on käytetty äärettömän laskeutumisen menetelmää.

Lause 3.3 *Yhtälöllä $x^4 + y^4 = z^4$ ei ole kokonaislukuratkaisua, kun $x \neq 0$, $y \neq 0$ ja $z \neq 0$.*

Todistus

Jos x, y ja z ovat kokonaislukuja ($\neq 0$) siten että $x^4 + y^4 = z^4$, niin silloin $z^4 - y^4 = (x^2)^2$, mikä on ristiriidassa lauseen 3.2 kanssa.

Fermat'n suuren lauseen eksponentille $n = 4$ ovat todistaneet myös muun muassa:

Bernard Frénicle De Bessy 1676
Leonhard Euler 1738
Adrien-Marie Legendre 1823,1830
Victor Lebesgue 1853, 1859, 1862

Seuraus 3.1 *Jos n on jaollinen 4:llä, niin ei ole olemassa kokonaislukuja a, b ja c, joille $a^n + b^n = c^n$.*

Miten tulosta voidaan hyödyntää etsittäessä ratkaisuja joihinkin samantyyppisiin Diofantoksen yhtälöihin? Seuraavat lauseet ovat Legendren todistamia.

Lause 3.4 *Jos x, y ja z ovat kokonaislukuja ($\neq 0$) ja $x^4 + y^4 = 2z^2$, niin $x^2 = y^2$ ja $z^2 = x^4$.*

Todistus

$$4z^4 = (x^4 + y^4)^2 = x^8 + 2x^4y^4 + y^8 = x^8 + 2x^4y^4 + y^8 + 2x^4y^4 - 2x^4y^4$$

$= x^8 - 2x^4y^4 + y^8 + 4x^4y^4 = (x^4 - y^4)^2 + 4x^4y^4$

.

Siis $4z^4 = (x^4 - y^4)^2 + 4x^4y^4$. Tästä seuraa, että

$z^4 - x^4y^2 = (\frac{x^4-y^4}{2})^2 \Rightarrow z^4 - (xy)^4 = (\frac{x^4-y^4}{2})^2$.

Erityisesti $x^4 - y^4$ on parillinen.

Koska $x, y, z \neq 0$, niin lauseen 3.2 perusteella luvun $(\frac{x^4-y^4}{2})^2$ on oltava nolla, joten $x^4 = y^4$ ja nyt $x^4 + y^4 = x^4 + x^4 = 2x^4 = 2z^2$, joten $x^4 = z^2$.

Lause 3.5 *Jos x, y ja z ovat kokonaislukuja ($\neq 0$) ja $2x^4 + 2y^4 = z^2$, niin $x^2 = y^2$ ja $z^2 = 4x^4$*

Todistus

Kertomalla 8:lla saadaan $(2x)^4 + (2y)^4 = 2(2z)^2$. Lauseesta 3.4 seuraa, että $(2x)^2 = (2y)^2$ ja $(2z)^2 = (2x)^4$, joten $x^2 = y^2$ ja $z^2 = 4x^4$.

4 Tapaus $n = 3$

Fermat esitti, että $x^3 + y^3 \neq z^3$ kun $xyz \neq 0$. Tämä käy ilmi Fermat'n kirjoittamista kirjeistä Mersennelle. Euler uskoi keksineensä todistuksen tälle lauseelle. Todistus perustuu äärettömän laskeutumisen menetelmään ja se esiintyy Eulerin kirjassa Algebra, joka julkaistiin vuonna 1770. Eulerin todistuksen kriittinen tarkastelu paljasti kuitenkin virheen, joka koski muotoa $a^2 + 3b^2$ olevien kokonaislukujen jaollisuusominaisuuksia. ([1], [14], s.39-43).

Euler tarvitsi lemmaa, joka sanoo seuraavaa: Olkoon $p^2 + 3q^2$ kuutio. Silloin on olemassa a ja b siten että $p = a^3 - 9ab^2$ ja $q = 3a^2b - 3b^3$. Käydään ensin läpi oikea todistus (lemma 4.5) ja sitten tarkastellaan hieman sitä, mitä Euler yritti tehdä.

Lemma 4.1 *Jos* $2 \mid (a^2 + 3b^2)$*, niin* $4 \mid (a^2 + 3b^2)$*. Ja jos* $4 \mid (a^2 + 3b^2)$*, niin silloin on olemassa* c *ja* d *siten että* $a^2 + 3b^2 = 4(c^2 + 3d^2)$*.*

Todistus

a ja b ovat molemmat joko parillisia tai parittomia, sillä muuten ei voisi olla $2 \mid (a^2 + 3b^2)$.

Jos a ja b ovat parillisia, niin on olemassa c ja d siten että $a = 2c$ ja $b = 2d$. Silloin $a^2 + 3b^2 = (2c)^2 + 3(2d)^2 = 4(c^2 + 3d^2)$, joten $4 \mid (a^2 + 3b^2)$.

Jos a ja b ovat parittomia, niin on olemassa m ja n siten että $a = 4m \pm 1$ ja $b = 4n \pm 1$. Joten tiedämme, että $4 \mid (a + b)$ tai $4 \mid (a - b)$. Käydään läpi molemmat tapaukset.

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

$4(\mathrm{a}^2 + 3b^2)$

$=(1^2 + 3 \cdot 1^2)(a^2 + 3b^2)$

$=(\mathrm{a}^2 + 3b^2) + 3(a^2 + 3b^2)$

$=\mathrm{a}^2 + 3b^2 + 3a^2 + 9b^2$

$=4\mathrm{a}^2 + 12b^2$

$=a^2 - 6ab + 9b^2 + 3b^2 + 6ab + 3a^2$

$=a^2 - 6ab + 9b^2 + 3(b^2 + 2ab + a^2)$

$=(a\text{-}3b)^2 + 3(b + a)^2$

Koska $a - 3b = (a + b) - 4b$, niin tiedämme että $4 \mid (a - 3b)$

Tästä seuraa että $4^2 \mid ((a - 3b)^2 + 3(a + b)^2)$, josta seuraa että $4^2 \mid (4(a^2 + 3b^2))$ ja siksi $4 \mid (a^2 + 3b^2)$. Koska $4 \mid (a - 3b)$ ja $4 \mid (a + b)$, niin tiedämme että on olemassa u ja v siten että $u = \frac{a-3b}{4}$ ja $v = \frac{a+b}{4}$.

$4(u^2 + 3v^2) = 4((\frac{1}{4}(a - 3b))^2 + 3(\frac{1}{4}(a + b))^2) = \frac{1}{4}(a^2 + 9b^2 + 3a^2 + 3b^2) = \frac{1}{4}(4a^2 + 12b^2) = a^2 + 3b^2$

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

Tämä tapaus menee samalla periaatteella kuin edellinen tapaus. Nyt asetetaan

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

$=a^2+3b^2+3a^2+9b^2 = a^2+6ab+9b^2+3b^2-6ab+3a^2 = (a+3b)^2+3(a-b)^2.$

Sitten kun on todistettu, että $4^2 \mid ((a + 3b)^2 + 3(a - b)^2)$, niin asetetaan $u = \frac{1}{4}(a + 3b)$ ja $v = \frac{1}{4}(a - b)$. Silloin $4(u^2 + 3v^2) = a^2 + 3b^2$.

Lemma 4.2 *Jos muotoa $p^2 + 3q^2$ oleva alkuluku jakaa luvun $a^2 + 3b^2$, niin silloin on olemassa sellaiset c ja d että $a^2 + 3b^2 = (p^2 + 3q^2)(c^2 + 3d^2)$.*

Todistus

On olemassa sellainen f että $a^2 + 3b^2 = (p^2 + 3q^2)f$. Alkuluku $p^2 + 3q^2$ jakaa joko luvun $pb - aq$ tai luvun $pb + aq$, sillä:

$(pb\text{-}aq)(pb+aq)=p^2b^2 - a^2q^2$

$=p^2b^2 + 3q^2b^2 - a^2q^2 - 3q^2b^2$

$=b^2(p^2 + 3q^2) - q^2(a^2 + 3b^2)$

$=\mathrm{b}^2(p^2+3q^2)-q^2((p^2+3q^2)f)$

$=\mathrm{b}^2p^2+3b^2q^2-p^2q^2f+3q^4f$

$=(\mathrm{p}^2+3q^2)(b^2+3q^2f)$

On siis olemassa sellainen g että $(p^2+3q^2)g=pb+aq$ tai $(p^2+3q^2)g=pb-aq$.

Nyt

$(p^2+3(\pm q)^2)(a^2+3b^2)=p^2a^2+3p^2b^2+3a^2q^2+9b^2q^2$

$=p^2a^2\pm 6paqb+9q^2b^2+3p^2b^2\mp 6paqb+3a^2q^2$

$=(pa\pm 3qb)^2+3(pb\pm aq)^2$

Siis p^2+3q^2 jakaa luvun $pa\pm 3qb$, sillä:

$(pa\pm 3qb)^2=p^2a^2\pm 6abpq+9q^2b^2$

$=p^2a^2+3b^2p^2+3a^2q^2+9b^2q^2-3p^2b^2\pm 6abpq-3a^2q^2$

$=p^2a^2+3b^2p^2+3q^2a^2+9q^2b^2-3(pb\pm aq)^2$

$=p^2a^2+3b^2p^2+3q^2a^2+9q^2b^2-3(\frac{p(pb\pm aq)}{p+3q}+\frac{3q(pb\pm aq)}{p+3q})^2$

$=p^2a^2+3b^2p^2+3q^2a^2+9q^2b^2-3(\frac{p^2(pb\pm aq)^2)}{(p+3q)^2}+\frac{6pq(pb\pm aq)^2}{(p+3q)^2}+\frac{9q^2(pb\pm aq)^2}{(p+3q)^2})$

$=p^2a^2+3b^2p^2+3q^2a^2+9q^2b^2-\frac{3p^2(pb\pm aq)^2(p^2+3q^2)}{(p+3q)^2(p^2+3q^2)}-\frac{18pq(pb\pm aq)^2(p^2+3q^2)}{(p+3q)^2(p^2+3q^2)}$

$-\frac{27q^2(pb\pm aq)^2(p^2+3q^2)}{(p+3q)^2(p^2+3q^2)}$

$=p^2(a^2+3b^2)+3q^2(a^2+3b^2)$

$-(p^2+3q^2)(\frac{3p^2(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)}+\frac{18pq(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)}+\frac{27q^2(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)})$

$=(p^2+3q^2)(a^2+3b^2-(\frac{3p^2(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)}+\frac{18pq(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)}+\frac{27q^2(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)}))$

Nyt koska $(pb-aq)(pb+aq)=(p^2+3q^2)(b^2+3q^2f)$ ja

$(pa \pm 3qb)^2$

$= (p^2+3q^2)(a^2+3b^2 - (\frac{3p^2(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)} + \frac{18pq(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)} + \frac{27q^2(pb\pm aq)^2}{(p+3q)^2(p^2+3q^2)}))$,

niin $pa \pm 3qb = c(p^2+3q^2)$ ja $pb \pm aq = d(p^2+3q^2)$.

Koska $(p^2+3(\pm q)^2(a^2+3b^2) = (pa \pm 3qb)^2 + 3(pb \pm aq)^2$, niin

$a^2+3b^2 = \frac{(pa\pm 3qb)^2+3(pb\pm aq)^2}{p^2+3q^2}$

$= \frac{(c(p^2+3q^2))^2+3(d(p^2+3q^2))^2}{p^2+3q^2}$

$= \frac{c^2(p^4+6p^2q^2+9q^4)+3(d^2(p^4+6p^2q^2+9q^4))}{p^2+3q^2}$

$= \frac{c^2(p^4+6p^2q^2+9q^4)+3d^2(p^4+6p^2q^2+9q^4)}{p^2+3q^2}$

$= \frac{(c^2+3d^2)(p^2+3q^2)^2}{p^2+3q^2}$

$= (c^2+3d^2)(p^2+3q^2)$

Lemma 4.3 *Jos luvulla a^2+3b^2 on pariton tekijä, joka ei ole tätä muotoa, niin silloin osamäärällä on pariton tekijä, joka ei ole tätä muotoa.*

Siis toisin sanoen: olkoon f luvun a^2+3b^2 pariton tekijä, f ei ole muotoa p^2+3q^2. Silloin on olemassa sellainen g että $fg = a^2+3b^2$ ja on olemassa sellainen f' että f' on pariton ja $f' \mid g$ ja f' ei ole muotoa p^2+3q^2.

Todistus

Vastaoletus: lukua f' ei voida valita niin, että f' on pariton ja f' ei ole muotoa s^2+3t^2, vaan jokainen luvun g pariton tekijä on muotoa s^2+3t^2.

On siis olemassa sellaiset f ja g että $fg = a^2+3b^2 = (2n+1)hf'$, missä $f = (2n+1)$ on pariton, ja f ei ole muotoa p^2+3q^2. Luku g voidaan esittää alkulukujen tulona; $g = p_1p_2\cdots p_n$, missä $p_1, p_2, \ldots p_n$ ovat alkulukuja. Lemman 4.1 perusteella kaikki tulossa mukana olevat luvut 2 eli 2^α voidaan korvata luvulla $4^{\frac{\alpha}{2}} = 4^\beta$, missä α on parillinen tai 0. Nyt siis $g = 4^\beta \cdot p_\sigma \cdots p_n$, missä $p_\sigma, \cdots p_n$ ovat alkulukuja $\neq 2$.

Nyt voimme poistaa luvun 4^β luvusta g ja luvusta $a^2 + 3b^2$ ja näin saadaan luku, joka on edelleen muotoa $p^2 + 3q^2$.

Siis

$c^2 + 3d^2 = f \cdot \frac{g}{4^\beta} = f \cdot p_\sigma \cdots p_n$, missä p_i on alkuluku.

Lemman 4.2 perusteella voimme poistaa luvusta g myös kaikki parittomat alkuluvut, koska oletimme, että kaikki luvun g parittomat tekijät ovat muotoa $p^2 + 3q^2$.

Nyt siis $f = e^2 + 3h^2$, joka on ristiriidassa sen kanssa, että f ei ole muotoa $p^2 + 3q^2$. Vastaoletus on siis väärä ja väite pätee.

Lemma 4.4 *Jos* $(a, b) = 1$, *niin jokainen* $a^2 + 3b^2$*:n pariton tekijä on tätä samaa muotoa.*

Todistus

Olkoon x luvun $a^2 + 3b^2$ tekijä siten että on olemassa kokonaisluku f niin että $a^2 + 3b^2 = xf$. Tämä on totta ainakin kun $x = 1$, joten oletamme, että $x > 1$. Jakoyhtälön perusteella on olemassa m ja n siten että

$a = mx + c$ ja

$b = nx + d$.

Nyt voimme olettaa, että $|c| < \frac{1}{2}x$ ja $|d| < \frac{1}{2}x$. Tästä saamme

$\mathrm{a}^2 + 3b^2 = m^2x^2 + 2mxc + c^2 + 3n^2x^2 + 6nxd + 3d^2$

$=\mathrm{x}(\mathrm{m}^2 + 2mc + 3n^2x + 6nd) + c^2 + 3d^2$

Nyt $x \mid (c^2 + 3d^2)$, sillä

$x(f - (m^2x + 2mc + 3n^2x + 6nd))$

$= x(f - m^2x - 2mc - 3n^2x - 6nd)$

$= xf - m^2x^2 - 2mcx - 3n^2x^2 - 6ndx$

$= a^2 + 3b^2 - m^2x^2 - 2mcx - 3n^2x^2 - 6ndx$

$= (mx + c)^2 + 3(nx + d)^2 - m^2x^2 - 2mcx - 3n^2x^2 - 6ndx$

$= m^2x^2 + 2mxc + c^2 + 3n^2x^2 + 6nxd + 3d^2 - m^2x^2 - 2mcx - 3n^2x^2 - 6ndx$

$= c^2 + 3d^2.$

Siis on olemassa sellainen arvo y että $c^2 + 3d^2 = xy$. Nyt

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

Koska $xy \geq 0$ ja $xy < x^2$, niin $y < x$, koska $xy < x^2$. Tiedämme myös, että $c^2 + 3d^2 \neq 0$. Tämä voidaan osoittaa seuraavasti:

Antiteesi: Oletetaan $c^2 + 3d^2 = 0$. Silloin $c = 0$ ja $d = 0$. Mutta silloin $a = mx$ ja $b = nx$ ja $x \mid a$ ja $x \mid b$. Tämä on ristiriidassa sen kanssa, että $(a, b) = 1$. Siis $c^2 + 3d^2 \neq 0$.

Voimme olettaa, että sekä $c^2 + 3d^2$ että y ovat parittomia. Tämä voidaan osoittaa seuraavasti:

Lemman 4.1 perusteella, jos $2 \mid (c^2 + 3d^2)$ niin myös $4 \mid (c^2 + 3d^2)$. Koska $4 = 2^2 + 3 \cdot 0^2$ ja koska x on pariton, niin voimme edelleen lemman 3.1 perusteella jakaa luvun y luvulla 4 niin että se on edelleen yhtä suuri kuin arvo, joka on muotoa $p^2 + 3q^2$. Voimme jatkaa tätä kunnes meillä on arvo $c^2 + 3d^2$, joka ei ole parillinen ja y:n arvo, joka ei ole parillinen. Siis $c^2 + 3d^2$ ja y ovat parittomia.

Olkoon nyt $g = (c, d)$. Tiedämme että on olemassa h ja f siten että $c = gh$ ja $d = gf$, $(h, f) = 1$. Nyt voimme osoittaa, että $g^2 \mid y$. Tämä voidaan tehdä seuraavasti:

$xy = (gh)^2 + 3(gf)^2 = g^2(h^2 + 3f^2)$. Silloin on olemassa r ja s siten että $x = rp$ ja $g = sp$. Koska

$a = mx + c = mpr + sph = p(mr + sh)$ ja

$b = nx + d = npr + spf = p(nr + sf)$,

niin $p \mid a$ ja $p \mid b$. Tämä on kuitenkin mahdotonta, sillä $syt(a, b) = 1$. Joten ei ole olemassa alkulukua p niin että se jakaisi g:n muttei y:tä. Siis $g^2 \mid y$.

Siten on olemassa z siten että $y = g^2 z$ ja $xy = x(g^2 z) = g^2(h^2 + 3f^2)$, mikä tarkoittaa sitä, että $xz = h^2 + 3f^2$, missä $(h, f) = 1$ ja $h^2 + 3f^2$ on pariton.

Nyt meillä on tarpeeksi tietoa, jotta voimme tehdä sen johtopäätöksen että x on muotoa $p^2 + 3q^2$.

Antiteesi: Oletetaan, että x ei ole tätä muotoa. Silloin lemman 4.3 perusteella on olemassa w siten että $w \mid z$ ja w ei ole muotoa $p^2 + 3q^2$. Nyt $w \neq 1$ sillä $1 = 1^2 + 3 \cdot 0^2$. $w < x$ sillä $w > 1$ ja $w \mid z$, ja $z < y < x$. Mutta nyt olemme osoittaneet, että x:n olemassaolo todistaa pienemmän tekijän, w:n, olemassaolon. Samoin voimme osoittaa että on olemassa w' ja w'' siten että $w'' < w' < w$. Äärettömän laskeutumisen menetelmän perusteella tämä ei ole mahdollista.

Lemma 4.5 *Olkoot olemassa p ja q, joilla on seuraavat ominaisuudet:*

1. $syt(p, q) = 1$
2. *toinen luvuista p ja q on parillinen ja toinen pariton*
3. $p^2 + 3q^2$ *on kuutio.*

Silloin on olemassa a ja b siten että

$p = a^3 - 9ab^2$,

$q = 3a^2 b - 3b^3$ *ja*

$(a, b) = 1$.

Todistus

Koska $p^2 + 3q^2$ on kuutio, voimme olettaa, että $p^2 + 3q^2 = u^3$. Ehdon 2) nojalla u:n on oltava pariton. Lemman 4.4 perusteella luvun u on oltava muotoa $a^2 + 3b^2$. Nyt

$(a^2 + 3b^2)^3$

$= (a^2 + 3b^2)(a^2 + 3b^2)^2$

$= (a^2 + 3b^2)(a^4 + 6a^2b^2 + 9b^4)$

$= (a^2 + 3b^2)(a^4 + 6a^2b^2 + 9b^4 + 6a^2b^2 - 6a^2b^2)$

$= (a^2 + 3b^2)(a^4 - 6a^2b^2 + 9b^4 + 12a^2b^2)$

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

Edelleen

$(a^2 + 3b^2)((a^2 - 3b^2)^2 + 3(2ab)^2)$

$= a^2((a^2 - 3b^2)^2 + 3(2ab)^2) + 3b^2((a^2 - 3b^2)^2 + 3(2ab)^2)$

$= a^2(a^2 - 3b^2)^2 + 3a^2(2ab)^2 + 3b^2(a^2 - 3b^2)^2 + 9b^2(2ab)^2$

$= a^2(a^2 - 3b^2)^2 - 6ab(a^2 - 3b^2)(2ab) + 9b^2(2ab)^2 + 3a^2(2ab)^2$

$+6ab(a^2 - 3b^2)(2ab) + 3b^2(a^2 - 3b^2)^2$

$= (a(a^2 - 3b^2))^2 - 6ab(a^2 - 3b^2)(2ab) + (3b(2ab))^2 +$

$3((a(2ab))^2 + 2ab(a^2 - 3b^2)(2ab) + (b(a^2 - 3b^2))^2$

$= (a(a^2 - 3b^2) - 3b(2ab))^2 + 3(a(2ab) + b(a^2 - 3b^2))^2$

$= (a^3 - 3ab^2 - 6ab^2)^2 + 3(2a^2b + a^2b - 3b^3)^2$

$= (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2$.

Koska oli oletettu, että $p^2 + 3q^2 = u^3$, niin saadaan

$p^2 + 3q^2 = (a^3 - 9ab^2)^2 + 3(3a^2b - 3b^3)^2$.

On siis olemassa a ja b siten että

$p = a^3 - 9ab^2$

$q = 3a^2b - 3b^3$

$(a, b) = 1$, sillä muu yhteinen tekijä jakaisi p:n ja q:n.

Euler yritti todistaa edellistä lemmaa. Käydään lyhyesti läpi ajatus siitä, mitä Euler yritti tehdä. Eulerin todistusta ei tässä käydä läpi. Eulerin ajatus oli lähteä liikkeelle oletuksesta, että on olemassa luvut, jotka ovat muotoa $p + q\sqrt{-3}$. Jos hyväksymme, että tällaisia lukuja on, saamme seuraavanlaisen yhtälön: $p^2 + 3q^2 = (p + q\sqrt{-3})(p - q\sqrt{-3})$. Oletetaan, että $p^2 + 3q^2$ on kuutio. Euler jatkoi näyttämällä, että kaksi kompleksilukua $p + q\sqrt{-3}$ ja $p - q\sqrt{-3}$ eivät voi olla jaollisia samalla alkuluvulla. Tästä Euler teki johtopäätöksen, että näiden kahden kompleksiluvun on oltava kuutioita. Tätä hän perusteli lemmalla 3.2, suhteellisen alkulukujakajan lemmalla. Mutta tässä kohdassa hän teki virheen, sillä tätä muotoa olevat luvut eivät käyttäydy täysin samalla tavalla kuin kokonaisluvut. Euler yritti siis todistaa lemmaa 4.5 käyttämällä imaginaarilukuja. Imaginaariluvut eivät olleet vieraita Eulerille, sillä hän keksi muun muassa yhtälön, jota kutsutaan nimellä Eulerin identiteetti: $e^{i\pi} = -1$. Ei siis ole kovin yllättävää, että Euler yritti ratkaista myös tämän lemman imaginaarilukujen avulla. Eulerin todistusyritys ei kuitenkaan mennyt hukkaan, sillä muun muassa Kummer käytti samaa tekniikkaa todistaessaan Fermat'n suuren lauseen todeksi säännöllisille alkuluvuille. ([1], [14], s.39-43).

Käydään nyt läpi, miten todistetaan Fermat'n suuren lauseen tapaus $n = 3$. Ennen kyseisen lauseen todistusta tarkastelemme kahta todistuksessa tarvittavaa lemmaa.

Lemma 4.6 *Voimme esittää minkä tahansa ratkaisun $x^n + y^n = z^n$ sellaisessa muodossa, jossa mitkään kaksi arvoista x, y ja z eivät ole jaollisia samalla alkuluvulla.*

Todistaaksemme tämän, meidän on todistettava kaksi asiaa:

1. jos tekijä jakaa mitkä tahansa tämän yhtälön kaksi arvoa, silloin sen n:s potenssi jakaa kolmannen arvon n:nnen potenssin.

2. jos tekijän n:s potenssi jakaa arvon n:nnen potenssin, niin silloin tekijä jakaa arvon.

Todistus

Vaihe 1: Yhtälön $x^n + y^n = z^n$ kahden arvon yhteisen tekijän n:s potenssi jakaa kolmannen arvon n:nnen potenssin. Tässä voidaan erottaa kaksi tapausta. Tapaus 1: $d \mid x$ ja $d \mid y$. Tapaus 2: $d \mid z$ ja $d \mid x$ tai $d \mid y$.

Tapaus 1: Oletetaan että $d \mid x$ ja $d \mid y$. Silloin on olemassa x' ja y' siten että $x = dx'$ ja $y = dy'$. Silloin $z^n = x^n + y^n = (dx')^n + (dy')^n = d^n(x')^n + d^n(y')^n = d^n((x')^n + (y')^n)$. Eli $d^n \mid z^n$.

Tapaus 2: Oletetaan että $d \mid z$ ja $d \mid x$ tai $d \mid y$. Oletetaan että $d \mid x$ (vastaavasti tehdään, kun $d \mid y$). Silloin on olemassa x' ja z' siten että $x = dx'$ ja $z = dz'$. Nyt $y^n = z^n - x^n = (dz')^n - (dx')^n = d^n((z')^n - (x')^n)$. Eli $d^n \mid y^n$.

Vaihe 2: $d^n \mid x^n \rightarrow d \mid x$.

Olkoon $(d, x) = c$. Olkoon $e = \frac{d}{c}$ ja $f = \frac{x}{c}$. Nyt $(e, f) = 1$, joten myös $(e^n, f^n) = 1$. Koska $d^n \mid x^n$, niin on olemassa k siten että $x^n = kd^n$. Koska $e = \frac{d}{c}$ ja $f = \frac{x}{c}$, niin $x^n = (cf)^n = kd^n = k(ce)^n$ ja siten $c^n f^n = kc^n e^n$ ja siis $f^n = ke^n$. Tästä seuraa, että $(e^n, k) = 1$. Tämä voidaan osoittaa seuraavalla tavalla: Oletetaan että $(e^n, k) = a$ siten että $a > 1$. Silloin $a \mid e^n$ ja $a \mid f^n$, sillä $f^n = e^n k$. Mutta nyt olisi $(e^n, f^n) \neq 1$, mikä on ristiriidassa sen kanssa, että $(e^n, f^n) = 1$. Siis $(e^n, k) = 1$. Lemman 3.2 nojalla voimme päätellä, että k on n:s potenssi. Tästä seuraa, että on olemassa u siten että $u^n = k$. Ja nyt $e^n u^n = f^n$ ja $(eu)^n = f^n$, joten $eu = f$ ja kertomalla c:llä saadaan $ceu = fc \Rightarrow du = x$, joten $d \mid x$.

Lemma 4.7 *Jos a ja b eivät ole jaollisia samalla alkuluvulla ja toinen luvuista on pariton ja toinen parillinen, niin silloin $(2a, a^2 + 3b^2) = 1$ tai 3*

Todistus

Oletetaan, että a ja b eivät ole jaollisia samalla alkuluvulla. Oletetaan että on olemassa alkuluku f, jolle $f \mid 2a$ ja $f \mid (a^2 + 3b^2)$. Tiedämme, että f ei voi olla 2, sillä $a^2 + 3b^2$ on pariton. Oletetaan että $f > 3$. Koska $f \mid 2a$, niin $f \mid a$, joten $f \mid a^2$. Koska $f \mid (a^2 + 3b^2)$, niin $f \mid 3b^2$. Oletettiin että a ja b eivät ole jaollisia samalla alkuluvulla, joten ei voi olla $f \mid b^2$. Täten $f \mid 3$. Nyt siis $(2a, a^2 + 3b^2) = 1$ tai 3.

Lause 4.1 $x^3 + y^3 + z^3 = 0$ *vain kun* $xyz = 0$.

Todistus

Lemman 4.6 nojalla voimme olettaa, etteivät mitkään kaksi luvuista x, y ja z ole jaollisia samalla alkuluvulla. Silloin vain yksi näistä luvuista voi olla parillinen. Oletetaan että x ja y ovat parittomia ja z on parillinen. Kaikista näistä ratkaisuista valitsemme sen, missä $|z|$ on pienin mahdollinen. Koska $x+y$ ja $x-y$ ovat parillisia, niin on olemassa kokonaisluvut a ja b siten että

$2a = x + y$ ja

$2b = x - y$,

joten

$x = a + b$ ja

$y = a - b$.

Nyt $a, b \neq 0$ ja $(a, b) = 1$. Koska x ja y ovat parittomia, niin toinen luvuista a ja b on parillinen ja toinen pariton. Nyt

$$-z^3 = x^3 + y^3 = (a+b)^3 + (a-b)^3$$

$$= (a+b)(a^2+2ab+b^2)(a-b)(a^2-2ab+b^2)$$

$$= a^3 + 2a^2b + ab^2 + a^2b + 2ab^2 + b^3 + a^3 - 2a^2b + ab^2 - a^2b + 2ab^2 - b^3$$

$$= 2a^3 + 6ab^2$$

$$= 2a(a^2 + 3b^2).$$

$a^2 + 3b^2$ on pariton, z on parillinen ja $8 \mid z^3$. Tästä seuraa, että $4 \mid a$ joten a on parillinen ja b on pariton. Lemman 4.7 perusteella $(2a, a^2 + 3b^2)$ on joko 1 tai 3.

Tarkastelemme näitä kahta tapausta erikseen:

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

Nyt a ei ole jaollinen luvulla 3. Koska $-z^3 = 2a(a^2 + 3b^2)$, niin lemman 2.2 perusteella $2a$ ja $a^2 + 3b^2$ ovat kuutioita:

$2a = r^3$ ja

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

missä s on pariton eikä se ole jaollinen luvulla 3. Lemmojen 4.4 ja 4.5 perusteella s on muotoa $s = u^2 + 3v^2$, missä $u, v \in Z$ ja

$a = u^3 - 9uv^2 = u(u^2 - 9v^2)$ ja

$b = 3u^2v - 3v^3 = 3v(u^2 - v^2)$.

Nyt v on pariton ja u on parillinen, sillä b on pariton. $u \neq 0$ ja u ei ole jaollinen luvulla 3, sillä a ei ole jaollinen luvulla 3. $(u, v) = 1$ ja $2a = 2u(u^2 - 9v^2) = 2u(u - 3v)(u + 3v)$. Siksi mitkään kaksi luvuista $2u$, $u + 3v$ ja $u - 3v$ eivät ole jaollisia samalla alkuluvulla. Koska $r^3 = 2a = 2u(u - 3v)(u + 3v)$, niin lemman 3.2 nojalla $2u$, $u + 3v$ ja $u - 3v$ ovat kuutioita:

$2u = -n^3$,

$u - 3v = l^3$,

$u + 3v = m^3$,

missä $l, m, n \neq 0$ ja mitkään kaksi luvuista l, m ja n eivät ole jaollisia samalla alkuluvulla. Nyt $l^3 + m^3 + n^3 = u - 3v + u + 3v - 2u = 0$, missä n on parillinen.

$|z^3| = |2as^3| = |2u(u^2 - 9v^2)s^3| > |2u| = |n^3|$

joten $|z| > |n|$. Tämä on vastoin sitä oletusta, että $|z|$ on pienin mahdollinen.

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

Koska nyt $3 \mid a$, niin kirjoitamme $a = 3c$. c on parillinen ja $4 \mid c$. Luku b ei ole jaollinen luvulla 3, sillä a ja b eivät ole jaollisia samalla alkuluvulla. Nyt $-z^3 = x^3 + y^3 = (a + b)^3 + (a - b)^3 = 2a(a^2 + 3b^2) = 6c((3c)^2 + 3b^2) =$

$6c(9c^2+3b^2) = 18c(3c^2+b^2)$. Koska c on parillinen ja b pariton, niin $3c^2+b^2$ on pariton ja $(18c, 3c^2+b^2) = 1$. Nyt $(3c^2+b^2)$ ei ole jaollinen luvulla 3 ja $(b,c) = 1$. Lemman 3.2 perusteella $18c$ ja $3c^2+b^2$ ovat kuutioita:

$18c = r^3$ ja

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

missä s on pariton ja $3 \mid r$. Lemmojen 4.4 ja 4.5 perusteella $s = u^2+3v^2$, missä $u, v \in Z$ ja

$b = u(u^2 - 9v^2)$ ja

$c = 3v(u^2 - v^2)$.

Koska b on pariton ja c on parillinen, niin u on pariton ja v parillinen. $v \neq 0$, $(u,v) = 1$. Koska $r^3 = 18(3v(u^2-v^2)) = 18c = 54v(u+v)(u-v)$, niin $(\frac{r}{3})^3 = 2v(u+v)(u-v)$. Mitkään kaksi luvuista $2v, u+v, u-v$ eivät ole jaollisia samalla alkuluvulla. Lemman 3.2 perusteella $2v, u+v$ ja $u-v$ ovat kuutioita:

$2v = -n^3$,

$u + v = l^3$ ja

$u - v = -m^3$.

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

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

Tämä on ristiriidassa sen kanssa, että $|z|$ valittiin pienimmäksi mahdolliseksi. Siis $x^3 + y^3 + z^3 \neq 0$ kun $xyz \neq 0$.

Fermat'n lauseen eksponentilla 3 ovat todistaneet myös muun muassa seuraavat matemaatikot:

Christoph Friedrich Kausler 1795
Adrien-Marie Legendre 1823, 1830
Gabriel Lamé 1865

Nyt käymme läpi Leopold Kroneckerin (1823-1891) tuloksen vuodelta 1859. ([18], s.31-32).

Lause 4.2 *1. Kaikille kokonaisluvuille $m \neq 0$ ainoat yhtälön $4x^3 - 3my^2 = m^3$ kokonaislukuratkaisut ovat (m, m) ja $(m, -m)$*

2. Ainoat yhtälön $4u^3 + 27t^2 = -1$ rationaalilukuratkaisut ovat $(-1, \frac{1}{3})$ ja $(-1, -\frac{1}{3})$

3. $x^3 - x \pm \frac{1}{3}$ ovat ainoat kolmannen asteen polynomit, joilla on rationaalikerroin, siten että juurien summa on 0 ja diskriminantti on -1.

Todistus

1. Jos x ja y ovat kokonaislukuja ja (x, y) toteuttaa yhtälön $4x^3 - 3my^2 = m^3$, niin olkoot $u = -2x, v = y + m$. Silloin

   $u^3 + v^3$

   $= (-2x)^3 + (y + m)^3$

   $= -8x^3 + y^3 + 3y^2m + 3ym^2 + m^3$

   $= -8x^3 + y^3 + 3y^2m + 3ym^2 + m^3 - 6y^2m + 6y^2m$

   $= -2(4x^3 - 3y^2m) + y^3 + 3y^2m + 3ym^2 + m^3 - 6y^2m$

   $= -2m^3 + y^3 - 3y^2m + 3ym^2 + m^3$

   $= y^3 - 3y^2m + 3ym^2 - m^3$

   $= (y - m)^3$.

   Täten joko $x = 0$, mistä seuraisi $-3my^2 = m^3$ eli $-3y^2 = m^2$, mikä on mahdotonta tai $y = \pm m$. Tässä tapauksessa on oltava $x = m$.

2. Olkoot u, t rationaalilukuja siten että $4u^3 + 27t^2 = -1$. Kirjoitamme $u = -\frac{x}{m}$, $t = \frac{y}{3m}$, joten $-4\frac{x^3}{m^3} + 27\frac{y^2}{9m^2} = -1 \Rightarrow -4x^3 + 3my^2 = -m^3$. Kohdan 1 perusteella $x = m$, $y = \pm m$ ja täten $u = -\frac{m}{m} = -1$, $t = \pm\frac{m}{3m} = \pm\frac{1}{3}$.

3. Jos yhtälöllä $x^3 + ax + b$ on rationaaliset kertoimet ja diskriminantti $\delta = -1$, kun $\delta = 4a^3 + 27b^2$, niin kohdan 2 perusteella $a = -1$ ja $b = \pm\frac{1}{3}$.

Vuonna 1944 Schmid sai aikaan seuraavan ekvivalenssin ja osoitti Fermat'n teoreeman todeksi eksponentille 3: ([18], s.32-33)

Lause 4.3 *Seuraavat väittämät ovat yhtäpitäviä*

1. *Fermat'n suuri lause on totta eksponentille 3*

2. *Kaikista kokonaisluvuista $m \neq 0$ ainoat kokonaislukuratkaisut yhtälölle $4x^3 - 3my^2 = m^3$ ovat (m, m) ja $(m, -m)$*

3. *Ainoat rationaaliratkaisut yhtälölle $4u^3 + 27t^2 = -1$ ovat $(-1, \frac{1}{3})$ ja $(-1, -\frac{1}{3})$.*

Todistus

Edellisen lauseen todistuksessa näimme, että (1) $\Rightarrow$ (2) ja (2) $\Rightarrow$ (3). Nyt oletamme, että (3) on totta ja johdamme tästä että Fermat'n lause on totta eksponentille 3.

Antiteesi: Oletetaan että on olemassa luvut $x, y, z \neq 0$ siten että mitkään kaksi luvuista x, y ja z eivät ole jaollisia samalla alkuluvulla. Oletetaan että $x^3 + y^3 = z^3$, joten $y \neq z$. Olkoot $u = \frac{x}{y-z}$ ja $t = \frac{y+z}{3(y-z)}$. Siten

$$4u^3 + 27t^2$$

$$= 4\frac{x^3}{(y-z)^3} + 27\frac{(y+z)^2}{(3(y-z))^2}$$

$$= \frac{4x^3}{(y-z)^3} + \frac{27(y+z)^2}{9(y-z)^2}$$

$$= \frac{4x^3}{(y-z)^3} + \frac{3(y+z)^2(y-z)}{(y-z)^3}$$

$$= \frac{4x^3+3(y^2+2yz+z^2)(y-z)}{(y-z)(y^2-2yz+z^2)}$$

$$= \frac{4x^3+3(y^3-y^2z+2y^2z-2yz^2+yz^2-z^3)}{y^3-2y^2z+yz^2-y^2z+2y^2z-z^3}$$

$$= \frac{4x^3+3y^3-3y^2z+6y^2z-6yz^2+3yz^2-3z^3}{y^3-2y^2z+yz^2-y^2z+2y^2z-z^3}$$

$$= \frac{4z^3-4y^3+3y^3-3y^2z+6y^2z-6yz^2+3yz^2-3z^3}{y^3-2y^2z+yz^2-y^2z+2y^2z-z^3}$$

$$= \frac{-y^3+3y^2z-3yz^2+z^3}{y^3-3y^2z+3yz^2-z^3}$$

$$= \frac{-(y^3-3y^2z+3yz^2-z^3)}{y^3-3y^2z+3yz^2-z^3}$$

$$= -1.$$

Oletuksen nojalla $u = -1$ ja $t = \pm\frac{1}{3}$ ja täten $\frac{y+z}{3(y-z)} = \pm\frac{1}{3} \Rightarrow \frac{y+z}{y-z} = \pm 1 \Rightarrow y + z = \pm(y - z)$, joten $y = 0$ tai $z = 0$, mikä on vastoin oletusta. Siis Fermat'n suuri lause on totta eksponentille 3.

5 Sophie Germainin teoreema

5.1 Sophie Germain (1776 - 1831)

Marie-Sophie Germain syntyi Pariisissa 1.4.1776, juuri Ranskan vallankumouksen alla. Hän alkoi opiskella matematiikkaa 13-vuotiaana. Germainin vanhemmat vastustivat tytön matematiikan opiskelua, sillä he eivät halunneet Sophien ryhtyvän 'miesten' ammattiin. ([1]).

Vuonna 1794, Sophien ollessa 18-vuotias, École Polytechnique aukesi Pariisissa. Sinne pääsivät opiskelemaan Ranskan lahjakkaimmat matemaatikot, mutta vain miehet. Sophie Germain onnistui kuitenkin saamaan joitain luentomuistiinpanoja École Polytechniquen kursseilta. Hän kiinnostui erityisesti Joseph-Louis Lagrangen opetuksista. Polytechniquessa oli opiskellut mies nimeltä Monsieur Le Blanc. Tämän nimen Germain otti salanimekseen oikean Le Blancin ollessa matkoilla Pariisin ulkopuolella. Germain lähetti tutkimuksia ja tehtäviä École Polytechniqueen salanimellään. Lagrange, joka oli työskennellyt läheisesti oikean Le Blancin kanssa oli yllättynyt nähdessään entisen oppilaansa tekevän huomattavia matemaattisia töitä. Hän oli niin vaikuttunut töistä, että halusi tavata Le Blancin, joten Germain joutui paljastamaan oikean henkilöllisyytensä. Lagrange piti Germainia lahjakkaana matemaatikkona, ja alkoi hänen neuvonantajakseen. ([1], [8]).

Vuonna 1804 Germain alkoi kirjeenvaihtoon Carl Friedrich Gaussin kanssa, luettuaan Gaussin kuuluisan teoksen Disquisitiones Arithmeticae (1801). Jälleen Germain käytti salanimeä Monsieur Le Blanc. Germain kävi kirjeenvaihtoa myös Adrien-Marie Legendren kanssa. Näissä kirjeissä Germain sai tuotua matemaattisia tuloksiaan kuuluisien matemaatikoiden tietoisuuteen. Kirjeessään Gaussille Germain todisti, että jos x, y ja z ovat kokonaislukuja ja $x^5 + y^5 = z^5$, niin silloin joko luvun x, y tai z on oltava jaollinen viidellä. Myöhemmin kirjeessään Legendrelle Germain todisti, että jos n on pariton alkuluku ja jos $2n + 1$ on myös alkuluku, niin silloin siitä että $x^n + y^n = z^n$ seuraa että joko x, y tai z on jaollinen luvulla n. Germain kehittikin kokonaan uuden linjan Fermat'n suuren lauseen ratkaisuyrityksiin. Hän ei etsinyt todistusta vain tietyille arvoille, vaan osoitti, että jos ratkaisu on, sen täytyy täyttää tietyt ehdot. Tätä voidaankin pitää suurena edistyksenä kohti yleistä todistusta. ([1], [11], s.68-69).

Oli Napoleonin ansiota, että Gauss sai tietää Germainin todellisen henkilöllisyyden. Napoleonin armeija suuntasi kohti Braunschweigia, missä Gauss asui. Hyökkääjiä johti kenraali Pernety, joka oli Sophie Germainin henkilökohtainen ystävä. Germain pyysi kenraalia takaamaan Gaussin turvallisuuden. Kenraali kertoi Gaussille, että tämä oli Sophie Germainin suojeluksessa. Gauss ei ollut koskaan kuullutkaan Germainista. Tämän jälkeen Sophie tun-

nusti todellisen henkilöllisyytensä. Gauss oli hyvin vaikuttunut saadessaan sen selville, sillä hän todella ihaili Germainin matemaattista lahjakkuutta. Vuonna 1808 Gauss nimitettiin astronomian professoriksi Göttingenin yliopistoon. Gaussin yllytyksestä Göttingenin yliopisto suostui myöntämään Germainille kunniatutkinnon. Sophie Germain kuoli rintasyöpään 27.6.1831. ([1]).

5.2 Fermat'n suuren lauseen kaksi osaa

Fermat'n suuri lause ($x^n + y^n \neq z^n$) voidaan jakaa kahteen osaan:

1. Tapaus 1: mikään arvoista x, y ja z ei ole jaollinen luvulla n.
2. Tapaus 2: n jakaa yhden arvoista x, y, z.

5.3 Sophie Germainin alkuluvut

Jos molemmat p ja $2p+1$ ovat alkulukuja, niin silloin p on Sophie Germainin alkuluku. Ensimmäiset tällaiset alkuluvut ovat 2,3,5,11,23,29,41,53,83,89,113 ja 131. 1820-luvun alussa Germain todisti, että Fermat'n suuren lauseen ensimmäinen tapaus on totta tällaisille alkuluvuille. Pian tämän jälkeen Legendre alkoi yleistää tätä näyttämällä, että Fermat'n suuren lauseen ensimmäinen tapaus pätee myös sellaisille parittomille alkuluvuille p, joille $kp + 1$ on alkuluku, $k = 4, 8, 10, 14, 16$. ([18], s.109-122).

Tällä hetkellä ei tiedetä, onko Sophie Germainin alkulukuja ääretön määrä. Suurin tällä hetkellä tunnettu Germainin alkuluku on $p = 137211941292195 \cdot 2^{171960} - 1$. Luvussa on 51780 desimaalia, ja se löydettiin 3.5.2006. ([4]).

5.4 Germainin teoreema

Lemma 5.1 *Fermat'n pieni lause*

Jos kokonaisluku a ei ole jaollinen alkuluvulla p, niin $a^{p-1} \equiv 1 (mod\ p)$.

Todistus
Yleisesti tunnettu

Fermat'n pieni lause on yksi Pierre de Fermat'n tärkeimmistä tuloksista. Fermat esitteli sen ensi kertaa kirjeissään ilman todistusta vuonna 1640.

([1]). Leibniz todisti lauseen ensimmäisenä eräässä päiväämättömässä käsikirjoituksessa, mutta hän näyttää tunteneen todistuksen ennen vuotta 1683 ([12], s.69). Euler teki lauseelle ensimmäisen julkisen todistuksen vuonna 1736 ([1]). Lause on käytännöllinen muun muassa testattaessa suuria alkulukuja. Lause voidaan myös kirjoittaa muotoon $a^p \equiv a(\mathrm{mod}\ p)\ \forall a \in Z$. ([1]).

Määritelmä 5.1 *Merkitään* $Q_n(x,y) = \frac{x^n - y^n}{x-y}$, *missä* $n \geq 1$, x *ja* y *ovat kokonaislukuja* $(\neq 0)$.

Lemma 5.2 *Olkoot* $n > m \geq 1$ *ja* x, y $(\neq 0)$ *kokonaislukuja, joille* $(x,y) = 1$. *Silloin* $(Q_n(x,y), x-y) = (n, x-y)$.

Todistus

$Q_n(x,y) = \frac{x^n - y^n}{x-y} = \frac{[(x-y)+y]^n - y^n}{x-y} = (x-y)^{n-1} + \frac{n!}{(n-1)!}(x-y)^{n-2}y + \cdots$

$+\frac{n!}{2\cdot(n-2)!}(x-y)y^{n-2} + ny^{n-1} = (x-y)e + ny^{n-1}$

missä $e \in Z$.

Koska $(x,y) = 1$, niin $(Q_n(x,y), x-y) = ((x-y)e + ny^{n-1}, x-y) = (n, x-y)$.

Lemma 5.3 *Jos* x, y *ja* z *ovat kokonaislukuja* $(\neq 0)$, *niin että mitkään kaksi niistä ei ole jaollisia samalla alkuluvulla,* $x^p + y^p + z^p = 0$ *ja jos alkuluku* $p \neq 2$ *ei jaa lukua* z, *niin on olemassa kokonaisluvut* t *ja* t_1 *siten että*

$x + y = t^p$,

$\frac{x^p + y^p}{x+y} = {t_1}^p$ *ja*

$z = -tt_1$.

Lisäksi p *ei jaa lukua* tt_1, $(t, t_1) = 1$, t_1 *on pariton ja* $t_1 > 1$.

Todistus

Lemman 5.1 mukaan $x^{p-1} \equiv 1 \pmod{p}$, joten $x \equiv x^p \pmod{p}$. Samoin $y \equiv y^p \pmod{p}$ ja $z \equiv z^p \pmod{p}$. Nyt koska $x+y+z \equiv x^p+y^p+z^p \equiv 0 (\mathrm{mod}\ p)$, niin $-z \equiv x+y (\mathrm{mod}\ p)$, joten p ei jaa lukua $x+y$. Nyt $(-z)^p = x^p+y^p = Q_p(x,-y)(x+y)$.

$$Q_p(x,-y) = \tfrac{x^p+y^p}{x+y} = x^{p-1} - x^{p-2}y + \cdots - xy^{p-2} + y^{p-1}.$$

Lemman 5.2 perusteella $(Q_p(x,-y), x+y) = 1$. Koska $(-z)^p = Q_p(x,-y)(x+y)$, niin $x+y$ ja $Q_p(x,-y)$ ovat p:nsiä potensseja. On siis olemassa kokonaisluvut t ja t_1 siten että $x+y = t^p$ ja $Q_p(x,-y) = {t_1}^p$. Nyt $(-z)^p = Q_p(x,-y)(x+y) = {t_1}^p t^p = (tt_1)^p$, joten $z = -tt_1$ ja $(t, t_1) = 1$.

Nyt näytämme että t_1 on pariton. $Q_p(x,-y)$ on parittoman määrän termien summa. Näistä aina x^{p-1} tai y^{p-1} on pariton, sillä x ja y eivät molemmat ole parillisia. Joten $Q_p(x,-y)$ on pariton, ja täten t_1 on myös pariton. Lopuksi koska $x > y$ (tai $y > x$), niin $x - y \geq 1$ (tai $y - x \geq 1$) ja täten ${t_1}^p = Q_p(x,-y) = Q_p(y,-x) \geq p$ joten $t_1 > 0$ ja itse asiassa $t_1 > 1$.

Lauseesta seuraa, että jos x, y ja z toteuttavat yhtälön $x^p + y^p + z^p = 0$, jos p ei jaa lukuja x, y ja z ja jos $(x,y,z) = 1$, niin on olemassa kokonaisluvut r, s, t, r_1, s_1, t_1, jotka eivät ole luvun p monikertoja siten että

$$x + y = t^p \text{ ja } \tfrac{x^p+y^p}{x+y} = {t_1}^p \text{ ja } z = -tt_1,$$

$$y + z = r^p \text{ ja } \tfrac{y^p+z^p}{y+z} = {r_1}^p \text{ ja } x = -rr_1,$$

$$z + x = s^p \text{ ja } \tfrac{z^p+x^p}{z+x} = {s_1}^p \text{ ja } y = -ss_1.$$

Näitä kutsutaan Barlow-Abel relaatioiksi. Luvut r_1, s_1, t_1 ovat parittomia, $(t, t_1) = (r, r_1) = (s, s_1) = 1$ ja $(r, s, t) = (r_1, s_1, t_1) = 1$. Joten mitkään kaksi luvuista r, s, t, r_1, s_1, t_1 eivät ole jaollisia samalla alkuluvulla. Luvut r_1, s_1, t_1 ovat suurempia kuin 1. Tästä saamme, että

$$r^p + s^p + t^p = y + z + z + x + x + y = 2x + 2y + 2z = 2(x + y + z) \neq 0.$$

Tästä seuraa että

$$x = -r^p + \tfrac{r^p+s^p+t^p}{2} = \tfrac{-r^p+s^p+t^p}{2},$$

$y = -s^p + \frac{r^p+s^p+t^p}{2} = \frac{r^p-s^p+t^p}{2}$ ja

$z = -t^p + \frac{r^p+s^p+t^p}{2} = \frac{r^p+s^p-t^p}{2}$.

Määritelmä 5.2 *Olkoon $(a, n) = 1$ ja $n \geq 1$. Luvun a kertaluku (mod n) on pienin luonnollinen luku $k(= ord_n(a))$, jolle $a^k \equiv 1$ (mod n).*

Määritelmä 5.3 *Eulerin funktio $\varphi(n)$ merkitsee niiden luonnollisten lukujen $m \leq n$ lukumäärää, joille $(m, n) = 1$.*

Määritelmä 5.4 *Jos $ord_n(a) = \varphi(n)$, luku a on primitiivinen juuri (mod n).*

Lause 5.1 *Olkoon q alkuluku ja $n \geq 3$ pariton kokonaisluku. Seuraavat väitteet ovat yhtäpitäviä:*

1. *On olemassa kokonaisluvut a, b ja c, jotka eivät ole q:n monikertoja, siten että $a^n + b^n + c^n \equiv 0(mod\ q)$.*
2. *On olemassa kokonaisluvut d ja e, jotka eivät ole q:n monikertoja, siten että $d^n \equiv e^n + 1(mod\ q)$.*

   Lisäksi jos $q-1 = 2kn$, niin ylläolevat ehdot ovat yhtäpitäviä seuraavan kanssa
3. *On olemassa kongruenssin $x^{2k} - 1 \equiv 0(mod\ q)$ juuret u ja u', siten että $u' \equiv u + 1(mod\ q)$.*

Todistus

(1) $\rightarrow$ (2):

Oletetaan että $a^n + b^n + c^n \equiv 0(\text{mod } q)$. Koska c ei ole jaollinen luvulla q ja $q \mid (a^n + b^n + c^n)$ ja a, b ja c eivät ole jaollisia luvulla q, niin on olemassa sellaiset kokonaisluvut d ja e että

$dc \equiv -a(\text{mod } q)$ ja

$ec \equiv b (\text{mod } q)$.

Silloin de ei ole jaollinen luvulla q ja $(dc)^n \equiv (ec)^n + c^n (\text{mod } q)$, joten $d^n \equiv e^n + 1 (\text{mod } q)$.

(2) $\rightarrow$ (1):

Oletetaan, että $d^n \equiv e^n + 1 \pmod{q}$. Nyt jos $a = -d, b = e$ ja $c = 1$, niin $a^n + b^n + c^n \equiv 0 \pmod{q}$.

Nyt oletamme, että $q - 1 = 2kn$

(2) $\rightarrow$ (3):

Oletetaan että $d^n \equiv e^n + 1 (\text{mod } q)$. Asetetaan $u = e^n$, $u' = d^n$. Silloin $u^{2k} = e^{2kn} = e^{q-1} \equiv 1 (\text{mod } q)$. Samoin $(u')^{2k} = d^{2kn} = d^{q-1} \equiv 1 (\text{mod } q)$, missä $u' \equiv u + 1 (\text{mod } q)$.

(3) $\rightarrow$ (2):

Olkoon h primitiivinen juuri modulo q. Olkoon $u = h^m$, joten $h^{2km} \equiv u^{2k} \equiv 1 (\text{mod } q)$ ja täten $q - 1 = 2kn$ jakaa $2km$:n, joten $n \mid m$. Täten $u \equiv e^n (\text{mod } q)$. Samoin $u' \equiv d^n (\text{mod } q)$ ja $d^n \equiv e^n + 1 (\text{mod } q)$.

Nyt käymme läpi Legendren version Sophie Germainin teoreemasta.

Lause 5.2 *Olkoot p ja q erillisiä parittomia alkulukuja. Oletetaan että seuraavat ehdot täyttyvät:*

1. *Kun a, b ja c ovat kokonaislukuja siten että $a^p + b^p + c^p \equiv 0 (mod\ q)$, niin $q \mid abc$.*
2. *p ei ole kongruentti d^p:n kanssa modulo q millään kokonaisluvulla d.*

Silloin Fermat'n suuren lauseen ensimmäinen tapaus on totta eksponentille p.

Todistus

Olkoon niin että mitkään kaksi luvuista x, y ja z eivät ole jaollisia samalla alkuluvulla ja x, y ja z eivät ole luvun p monikertoja. Olkoon niin että

$x^p + y^p + z^p = 0$. Silloin $x^p + y^p + z^p \equiv 0 (\mathrm{mod}\ q)$ ja oletuksen 1 perusteella $q \mid xyz$. Voimme olettaa esimerkiksi että $q \mid x$, jolloin q ei jaa lukua yz. Koska p ei jaa lukua xyz, niin lemman 5.3 perusteella on olemassa sellaiset kokonaisluvut r, s, t, r_1, s_1, t_1 että

$x + y = t^p$ joten $\frac{x^p+y^p}{x+y} = {t_1}^p$ ja $z = -tt_1$

$y + z = r^p$ joten $\frac{y^p+z^p}{y+z} = {r_1}^p$ ja $x = -rr_1$

$z + x = s^p$ joten $\frac{z^p+x^p}{z+x} = {s_1}^p$ ja $y = -ss_1$

Nyt

$x = -r^p + \frac{r^p+s^p+t^p}{2} = \frac{-r^p+s^p+t^p}{2}$,

$y = -s^p + \frac{r^p+s^p+t^p}{2} = \frac{r^p-s^p+t^p}{2}$ ja

$z = -t^p + \frac{r^p+s^p+t^p}{2} = \frac{r^p+s^p-t^p}{2}$.

Koska $q \mid x$ niin $-r^p + s^p + t^p \equiv 0 (\mathrm{mod}\ q)$. Oletuksen 1 perusteella q jakaa jonkin luvuista r, s, t. Koska $s \mid y$, $t \mid z$ ja q ei jaa lukua yz ja q ei jaa lukua st, niin $q \mid r$. Mutta ${t_1}^p = \frac{x^p+y^p}{x+y} \equiv y^{p-1} (\mathrm{mod}\ q)$, koska $q \mid x$. Koska $q \mid r$ niin $y \equiv -z (\mathrm{mod}\ q)$. Täten

$${r_1}^p = \frac{y^p+z^p}{y+z} = y^{p-1} + y^{p-2}(-z) + \ldots + (-z)^{p-1} \equiv py^{p-1} \equiv p{t_1}^p (\mathrm{mod}\ q).$$

Koska t_1 ei ole kongruentti nollan kanssa modulo q, niin on olemassa sellainen kokonaisluku t' että $t't_1 \equiv 1 (\mathrm{mod}\ q)$ ja täten $p \equiv (t'r_1)^p (\mathrm{mod}\ q)$. Tämä on ristiriidassa oletuksen 2 kanssa.

Lause 5.3 *Jos p ja q ovat parittomia alkulukuja ja $q - 1 = 2pk$, k on luonnollinen luku, niin silloin edellisen lauseen ehto 2 on ekvivalentti seuraavien kanssa:*

2') $(2k)^{2k}$ ei ole kongruentti 1:n kanssa modulo q ja

2") p^{2k} ei ole kongruentti 1:n kanssa modulo q.

Todistus

$(2) \rightarrow (2')$:

Olkoon h primitiivinen juuri modulo q ja olkoon $p = h^s (\text{mod } q)$. Jos $(2k)^{2k} \equiv 1 (\text{mod } q)$, niin $h^{2ks} \equiv p^{2k} \equiv (2k)^{2k} p^{2k} \equiv (2kp)^{2k} \equiv (q-1)^{2k} \equiv 1 (\text{mod } q)$, täten $q - 1 = 2kp$ jakaa $2ks$:n, joten $p \mid s$ ja $p \equiv d^p (\text{mod } q)$, missä $d \equiv h^{\frac{s}{p}} (\text{mod } q)$.

$(2') \rightarrow (2'')$:

Jos $p^{2k} \equiv 1 (\text{mod } q)$ niin $(2k)^{2k} \equiv (2k)^{2k} p^{2k} \equiv (q-1)^{2k} \equiv 1 (\text{mod } q)$. Mutta oletuksen nojalla $(2k)^{2k}$ ei ole kongruentti 1:n kanssa modulo q, joten p^{2k} ei ole kongruentti 1:n kanssa modulo q.

$(2'') \rightarrow (2)$:

Jos on olemassa sellainen d että $p \equiv d^p (\text{mod } q)$ niin $p^{2k} \equiv d^{2kp} \equiv d^{q-1} \equiv 1 (\text{mod } q)$.

Seuraavat lauseet ovat yhtäpitäviä Sophie Germainin teoreeman kanssa.

Lause 5.4 *Jos p on pariton alkuluku ja $q = 2p + 1$ on myös alkuluku, niin silloin Fermat'n lauseen ensimmäinen tapaus on totta luvulle p.*

Todistus

Näytämme, että q täyttää lauseen 5.2 oletukset. Oletetaan että x, y ja z ovat kokonaislukuja, eivätkä ole luvun q monikertoja ja $x^p + y^p + z^p \equiv 0 (\text{mod } q)$. Koska $p = \frac{q-1}{2}$, niin lemman 5.1 perusteella $x^{2p} \equiv 1 \ (\text{mod } q)$, joten $(x^p)^2 \equiv 1 \ (\text{mod } q)$ ja $x^p \equiv \pm 1 \ (\text{mod } q)$. Samalla perusteella myös $y^p \equiv \pm 1 (\text{mod } q)$ ja $z^p \equiv \pm 1 (\text{mod } q)$. Täten $0 \equiv x^p + y^p + z^p \equiv \pm 1 \pm 1 \pm 1$ joka ei ole kongruentti nollan kanssa modulo q, mikä on mahdotonta. Nyt siis $q \mid xyz$. Samoin, jos $p \equiv a^p (\text{mod } q)$, niin ehto (2') ei täyty, joten $2p + 1 = q$ jakaa $2^2 - 1 = 3$:n, mikä on mahdotonta.

Seuraus 5.1 $x^5 + y^5 = z^5 \rightarrow 5 \mid xyz$.

Edellisen lauseen perusteella tämä on totta, koska 5 on alkuluku ja $2 \cdot 5 + 1 = 11$ on alkuluku.

Legendre laajensi lausetta 5.4 vuonna 1823:

Lause 5.5 *Jos p on alkuluku, $p > 3$ ja $q = 4p+1$ tai $q = 8p+1$ tai $q = 10p+1$ tai $q = 14p+1$ tai $q = 16p+1$ on myös alkuluku, niin silloin Fermat'n suuren lauseen ensimmäinen tapaus on totta eksponentille p.*

Todistus

Ks. [18] s.112-117.

6 Gabriel Lamé ja Ernst Eduard Kummer

6.1 Lamén virheellinen todistusyritys

1.3.1847 Gabriel Lamé ilmoitti Pariisin Akatemialle ja Preussilaiselle Akatemialle, että hän oli löytänyt todistuksen sille, että $x^n + y^n \neq z^n$, kun $n > 2$, ja että hän oli näin täydellisesti ratkaissut pitkään ratkaisemattomana olleen ongelman. Hänen perusideansa oli yksinkertainen ja kiinnostava, ja se on keskeinen teorian myöhemmän kehityksen kannalta. Lamé käytti hyväkseen sellaisia kompleksilukuja r, joille $r^n = 1$. Tällaisten lukujen avulla hän jakoi $x^n + y^n$:n tekijöihin. Siis, kun n on pariton, niin

$$x^n + y^n = (x + y)(x + ry)(x + r^2y) \cdots (x + r^{n-1}y)$$

ESIMERKKI:

Jos $r = \cos(\frac{2\pi}{n}) + i\sin(\frac{2\pi}{n}) = e^{\frac{2\pi i}{n}}$, niin silloin polynomilla $x^n - 1$ on n erillistä juurta $1, r, r^2, \ldots, r^{n-1}$ ja algebran perusteiden nojalla

$$X^n - 1 = (X - 1)(X - r)(X - r^2) \cdots (X - r^{n-1}).$$

Kun oletetaan, että $X = -\frac{x}{y}$ ja kerrotaan yhtälön molemmat puolet $-y^n$:llä, saadaan

$$(-\tfrac{x^n}{y^n} - 1)(-y^n) = (-\tfrac{x}{y} - 1)(-\tfrac{x}{y} - r)(-\tfrac{x}{y} - r^2) \cdots (-\tfrac{x}{y} - r^{n-1})(-y^n)$$

joten

$$(-\tfrac{x^n}{y^n})(-y^n) - (-y^n)$$

$$= (-\tfrac{x}{y}(-y) - 1(-y))(-\tfrac{x}{y}(-y) - r(-y)) \cdots (-\tfrac{x}{y}(-y) - r^{n-1}(-y))$$

ja

$$x^n + y^n = (x + y)(x + ry)(x + r^2y) \cdots (x + r^{n-1}y).$$

Lamé ajatteli näyttää, että jos x ja y ovat sellaisia, että tekijöillä $x+y$, $x+ry, \ldots, x+r^{n-1}y$ ei ole yhteisiä positiivisia tekijöitä (paitsi 1), niin silloin siitä, että $x^n + y^n = z^n$ seuraa että jokaisen tekijän $x + y$, $x + ry$, ... on itsessään oltava n.s potenssi. Tästä saadaan mahdottomuus äärettömän laskeutumisen menetelmän avulla. ([14], s.76-86).

Jos tekijöillä $x+y$, $x+ry$, ... on yhteinen tekijä, niin Lamé ajatteli näyttää, että on olemassa tekijä m, joka on yhteinen, siten että luvuilla $\frac{x+y}{m}$, $\frac{x+ry}{m}$, ..., $\frac{x+r^{n-1}y}{m}$ ei ole yhteistä positiivista tekijää (paitsi 1). Tässä tapauksessa voidaan perustella samoilla argumenteilla kuin edellisessä tapauksessa, että Fermat'n suuri lause pätee. ([14], s.76-86).

Lamé oli varma, että idea käyttää kompleksilukuja oli avain, joka ratkaisisi Fermat'n suuren lauseen arvoituksen. Lamé kertoi Akatemialle, että hän ei voisi ottaa keksinnöstä kunniaa kokonaan itselleen, koska idea oli noussut esiin hänen ja hänen kollegansa Joseph Liouvillen välisessä keskustelussa joitain kuukausia aiemmin. Liouville ei kuitenkaan ollut yhtä innoissaan todistuksesta kuin Lamé. Lamén esityksen jälkeen hän kertoi Akatemialle epäilyksistään todistusta kohtaan. Hän myös kieltäytyi ottamasta kunniaa itselleen esitetystä kompleksilukujen ideasta, sillä monet muut, kuten Euler, Lagrange, Gauss, Cauchy ja Jacobi olivat käyttäneet kompleksilukuja samaan tapaan aiemmin. ([14], s.76-86).

Liouville huomasi, että Lamén todistuksessa oli erittäin suuri aukko. Liouville kyseenalaisti sen, että voiko Lamé päätellä, että jos tekijöiden tulo on n.s potenssi, ja tekijöillä ei ole yhteisiä positiivisia tekijöitä (paitsi 1), niin myös jokainen tekijä on n.s potenssi. Tämä pitäisi tietenkin paikkaansa tavallisille kokonaisluvuille, mutta pätisikö se niille kompleksiluvuille, joita Lamé todistuksessaan käytti? Liouville ei halunnut innostua todistuksesta, ennen kuin tämä vaikeus olisi selvitetty. Liouvillen jälkeen puheenvuoron piti Cauchy, joka puolestaan uskoi, että Lamé voisi mahdollisesti onnistua todistuksessaan. ([14], s.76-86).

Seuraavien viikkojen aikana Cauchy ja Lamé jatkoivat näiden ideoiden käsittelyä. Lamé myönsi Liouvillen kritiikin oikeellisuuden, mutta hän ei hetkeäkään epäillyt lopullisen tuloksen oikeellisuutta. Hän väitti että hänellä on keino ratkaista kyseisten kompleksilukujen tekijöihinjaon ongelma, ja että kaikki esimerkit vahvistivat yksikäsitteisen tekijöihinjaon olemassaolon. Hän oli varma, että hän saisi todistuksen tehtyä. ([14], s.76-86).

15 maaliskuuta 1847 Pierre Laurent Wantzel väitti todistaneensa yksikäsitteisen tekijöihinjaon oikeellisuuden. Hänen argumenttinsa kattoivat kuitenkin vain tapaukset $n \leq 4$, mitkä ovat helposti todistettavissa (ja jotka oli jo todistettu). Wantzel sanoi, että nähdään selvästi, että sama argumentti pätee tapauksille $n > 4$. Tämän jälkeen Cauchy yritti todistaa ongelmaa, mutta hänkään ei onnistunut siinä. ([14], s.76-86).

24 toukokuuta 1847 Liouville luki Ernst Eduard Kummerin lähettämän kirjeen, joka lopetti , tai jonka olisi pitänyt lopettaa, koko keskustelun. Kummer kirjoitti Liouvillelle kertoakseen hänelle että hänen epäilyksensä Lamén käyttämään tekijöihinjakoon olivat perusteltuja. Kummer ei vain väittänyt,

että yksikäsitteinen tekijöihinjako ei päde, hän myös sisällytti kirjeeseesnä kopion muistiosta, jonka hän oli julkaissut vuonna 1844. Tässä julkaisussa Kummer oli näyttänyt yksikäsitteisen tekijöihinjaon pätemättömyyden siinä tapauksessa, missä Lamé väitti sen pätevän. Kummerin julkaisu ei ollut levinnyt kovinkaan laajalle, joten Liouville ei tiennyt asiasta aiemmin. Idea oli siinä, että tekijöihinjaon teoria ei päde käytettäessä uudenlaisia kompleksilukuja, joita hän kutsui ideaalisiksi kompleksiluvuiksi. Tämän tuloksen hän oli julkaissut vuotta aiemmin Berliinin Akatemian julkaisussa lyhennetyssä muodossa ja täydellisenä sen piti pian ilmestyä eräässä lehdessä. ([14], s.76-86).

Kummerin kirjeen tultua julki Lamé pysyi hiljaa. Cauchy julkaisi edelleen epämääräisiä ja tuloksettomia artikkeleita usean kuukauden ajan. Hän jätti Kummerin ajatuksen omaan arvoonsa. ([14], s.76-86).

6.2 Kummer

Kummer oli tutkinut jonkin verran kompleksilukuja. Monet uskovat, että Kummer keksi 'ideaaliset kompleksiluvut' sen seurauksena, että hän oli kiinnostunut Fermat'n suuresta lauseesta. Tämä luulo on kuitenkin todennäköisesti väärä. On totta että Kummer tutki Fermat'n suurta lausetta 1830-luvulla. On myös mahdollista että hän tiesi kompleksilukujen teorioillaan olevan vaikutusta Fermat'n suureen lauseeseen. Fermat'n suuri lause ei ollut Kummerin suurin kiinnostuksen kohde. Hän tutki enemmänkin muita 'ideaalisiin kompleksilukuihin' liittyviä asioita. Fermat'n suuren lauseen tutkiminen on kuitenkin osaltaan vaikuttanut 'ideaalisten kompleksilukujen' kehitykseen. Kummer käytti seuraavanlaisia merkintöjä: λ =alkuluku ja α = yhtälön $\alpha^\lambda = 1$ imaginaarinen juuri, joka ei ole 1. Hän tutki lukuja, jotka ovat muotoa

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{\lambda-1}\alpha^{\lambda-1}$$

missä $a_0, a_1, a_2, \ldots, a_{\lambda-1}$ ovat kokonaislukuja. Cauchy kutsui näitä lukuja radikaaleiksi polynomeiksi ja Kummer ja Jacobi kutsuivat niitä erityisiksi kompleksiluvuiksi. Nykyään niistä käytetään nimeä syklotominen kokonaisluku. ([14], s.76-86).

Lamén ongelmana olivat olleet syklotomisten kokonaislukujen tekijöihinjako. Syklotomisilla kokonaisluvuilla laskettaessa voidaan käyttää kommutatiivisuutta, assosiatiivisuutta ja distributiivisyyttä sekä yhtälöä $\alpha^\lambda = 1$. Syklotomisille kokonaisluvuille pätee myös se, että jos $f(\alpha)h(\alpha) = g(\alpha)h(\alpha)$ ja $h(\alpha) \neq 0$, niin $f(\alpha) = g(\alpha)$. Näistä laskusäännöistä on hieman yllättävä seuraus, sillä syklotomisten kokonaislukujen esitys muodossa

$$a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{\lambda-1}\alpha^{\lambda-1}$$

ei ole yksikäsitteinen. Esimerkiksi siitä, että

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{\lambda-1}$$

$$= \alpha^\lambda + \alpha + \alpha^2 + \cdots + \alpha^{\lambda-1}$$

$$= \alpha(1 + \alpha + \alpha^2 + \cdots + \alpha^{\lambda-1}).$$

seuraa että joko

$$1 + \alpha + \alpha^2 + \cdots + \alpha^{\lambda-1} = 0 \text{ tai } \alpha = 1.$$

Koska on erityisesti oletettu, että $\alpha \neq 1$, niin $1 + \alpha + \alpha^2 + \cdots + \alpha^{\lambda-1} = 0$. Tästä seuraa se, että

$$a_0 + a_1\alpha + \cdots + a_{\lambda-1}\alpha^{\lambda-1}$$

$$= (a_0 + c) + (a_1 + c)\alpha + \cdots + (a_{\lambda-1} + c)\alpha^{\lambda-1}$$

mille tahansa kokonaisluvulle c. Tämä on syklotominen kokonaisluku, joka pysyy muuttumattomana, jos sama kokonaisluku c lisätään kaikkiin sen kertoimiin a_i. ([14], s.76-86).

Kummer tutki paljon näitä syklotomisia kokonaislukuja. Hän ratkaisi muun muassa seuraavan ongelman: Olkoon annettu kaksi syklotomista kokonaislukua $f(\alpha)$ ja $h(\alpha)$. Onko olemassa syklotomista kokonaislukua $g(\alpha)$ siten että $f(\alpha)g(\alpha) = h(\alpha)$ ja jos on, niin mikä on $g(\alpha)$? ([14], s.76-86).

Vuonna 1847 Kummer todisti Fermat'n suuren lauseen säännöllisille alkuluvuille. Säännöllinen alkuluku on tietyntyyppinen pariton alkuluku. Se voidaan määrittää syklotomisen kunnan luokkalukujen tai Bernoullin lukujen avulla. Bernoullin luvut $B_0, B_1, B_2, ...$ ovat rationaalilukujen sarja. $B_0 = 1$ ja kun $n \geq 1$, niin

$$\frac{(n+1)!}{n!}B_n + \frac{(n+1)!}{2\cdot(n-1)!}B_{n-1} + \cdots + \frac{(n+1)!}{n!}B_1 + 1 = 0.$$

Joten $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$, $B_5 = 0$, $B_6 = \frac{1}{42}\ldots$ $B_{2k+1} = 0$ kaikille $k \geq 1$. Alkuluku p on säännöllinen jos p ei jaa Bernoullin luvun $B_2, B_4, \ldots, B_{n-5}, B_{n-3}$ osoittajaa. Ensimmäiset säännölliset alkuluvut

ovat 3,5,7,11,13,17,19,23,29,31 ja 41. Pariton alkuluku, joka ei ole säännöllinen on epäsäännöllinen alkuluku. Ensimmäiset epäsäännölliset alkuluvut ovat 37,59,67,101,103,131 ja 149. ([18], s.359-361).

Sataa pienempiä säännöllisiä alkulukuja on kolme: 37,59 ja 67. Kummer pystyi osoittamaan Fermat'n suuren lauseen todeksi myös näissä kolmessa tapauksessa, muttei pystynyt yleistämään tapauksia koskemaan kaikkia epäsäännöllisiä alkulukuja. Epäsäännöllisiä alkulukuja on äärettömän monta. ([11], s.80).

7 Wilesin todistuksen jälkeen

Sen jälkeen kun Andrew Wiles todisti Fermat'n suuren lauseen todeksi, jotkut ovat yrittäneet etsiä virheitä Wilesin todistuksessa. Virheitä ei kuitenkaan ole löytynyt. Jotkut ovat myös yrittäneet löytää lauseelle yksinkertaisempaa todistusta. Toukokuussa 2005 venäläinen matematiikan professori väitti keksineensä todistuksen Fermat'n suurelle lauseelle. Seuraavaksi käydään läpi kyseinen todistuksen sellaisenaan. ([1]).

Oletetaan että Fermat'n suuri lause ei ole totta. Silloin on olemassa $x^n + y^n = z^n$, missä $n \geq 3$ ja sekä x että y ovat kokonaislukuja. Mille tahansa x ja y voimme tehdä suorakulmaisen kolmion, ja voimme olettaa arvon r, siten että $r^2 = x^2 + y^2$. Koska $n \geq 3$, tiedämme että $z < r$. Lukuihin x, y ja z perustuen voimme muodostaa kolmion. Koska $z < r$, tiedämme että lukua z vastaava kulma (olkoon se α) on pienempi kuin lukua r vastaava kulma, joka on 90°. Siis $0° < \alpha < 90°$.

Kosinilauseen mukaan $z^2 = x^2 + y^2 - 2xy\cos\alpha$.

Koska $0° < \alpha < 90°$, niin $\cos\alpha$ ei voi olla kokonaisluku, siis Fermat'n suuri lause on totta.

Kalifornialaisen matemaatikon Larry Freemanin mukaan todistus ei kuitenkaan ole pätevä. Ongelma on siinä, että vaikka $\cos\alpha$ ei ole kokonaisluku, niin se ei todista sitä, etteikö z voisi olla kokonaisluku. Professorin olisi todistettava joko että $\cos\alpha$ on irrationaalinen tai hänen olisi osoitettava, että z ei voi olla kokonaisluku perustuen lukuun $2xy\cos\alpha$. Koska $\cos\alpha$ on jatkuva funktio, se pitää välttämättä sisällään myös rationaalisia arvoja ja siksi on täysin mahdollista, että $2xy\cos\alpha$ on kokonaisluku. ([1]).

Larry Freemanin mukaan on kaksi selvää merkkiä siitä, että todistusyritys on virheellinen. Ensimmäinen on se, että todistuksen laatija ei ole lukuteorian ammattilainen. Toinen on se, että todistusta ei ole tarkastutettu kenelläkään lukuteorian ammattilaisella. ([1]).

8 Yhteenveto

Fermat'n suuri lause on ollut etenkin matemaatikoiden keskuudessa hyvin tunnettu ongelma viimeisten vuosisatojen aikana. Lukuisat matemaatikot, ja muutkin, ovat yrittäneet ratkaista ongelmaa. Fermat'n suuri lause on muodoltaan seuraavanlainen: $x^n + y^n \neq z^n$ kun $n > 2$ ja x, y, z ja n ovat positiivisia kokonaislukuja. Fermat itse väitti todistaneensa lauseen, mutta tätä todistusta tai edes mitään viitteitä todistuksen olemassaolosta ei ole koskaan löydetty. Todistuksen historiaa tarkasteltaessa voidaan hyvinkin olettaa, että Fermat'n mahdollinen todistus ei ole ollut täydellinen. Täyttä varmuutta asiaan ei kuitenkaan ole saatu.

Fermat'n suuren lauseen todistaminen on ollut pitkä ja monimutkainen prosessi. Monet matemaatikot veivät lauseen todistusta pienen askeleen eteenpäin ja lopulta 1990-luvulla Anrew Wiles löysi palapelin viimeisen palan. Wilesin todistuksessa hyödynnetään useita matematiikan eri haaroja, ja näiden haarojen väliset yhteydet oli lopulta se avain, joka avasi kuuluisan arvoituksen.

On väitetty että Fermat itse todisti tapauksen $n = 4$. Tästäkään ei olla kuitenkaan varmoja. Varmuudella tiedetään, että Leonhard Euler todisti 1700-luvulla tapaukset $n = 3$ ja $n = 4$. Euler teki kuitenkin virheen todistaessaan tapausta $n = 3$. Virhe koski muotoa a^2+3b^2 olevien kokonailukujen jaollisuusominaisuuksia. Carl Friedrich Gauss korjasi Eulerin tekemän virheen. Tapausten $n = 3$ ja $n = 4$ todistukset perustuvat hyvin vahvasti lukuteoriaan. Molempien tapausten todistaminen on mahdollistanut myös joidenkin muiden lauseiden todistamisen siten kuin ne on todistettu, ks. esimerkiksi lause 3.4.

Sophie Germain oli Fermat'n suurta lausetta tutkineista matemaatikoista merkittävämpiä. Hän saavutti tällä alalla hienoja tuloksia. Germain pyrki yleistämään todistuksensa koskemaan tietynlaisia lukuja, hän ei tyytynyt todistamaan yhtä tapausta kerrallaan. Germain todisti muun muassa sen, että jos p on pariton alkuluku ja $q = 2p + 1$ on myös alkuluku, niin silloin Fermat'n suuren lauseen ensimmäinen tapaus on totta p:lle. Ensimmäinen tapaus pitää sisällään ne tilanteet kun mikään arvoista x, y ja z ei ole jaollinen luvulla n. Toinen tapaus on puolestaan se kun n jakaa yhden luvuista x, y, z.

Muun muassa Gabriel Lamé ja Ernst Eduard Kummer käyttivät Fermat'n suurta lausetta tutkiessaan hyväksi kompleksilukuja. Kummer käytti teorioissaa erityisesti syklotomisia kokonaislukuja. Ne ovat lukuja, jotka ovat muotoa $a_0 + a_1\alpha + a_2\alpha^2 + \cdots + a_{\lambda-1}\alpha^{\lambda-1}$, missä $a_0, a_1, a_2, \ldots, a_{\lambda-1}$ ovat kokonaislukuja. Kummer todisti myös Fermat'n suuren lauseen todeksi säännöllisille alkuluvuille.

Suurin osa todistuksista on otettu lähdekirjallisuudesta. Todistukset ovat samankaltaisia kuin alkuperäiset todistukset. Itse olen todistanut lähinnä pieniä lemmoja ja todistusten sisällä olevia välivaiheita. Paulo Ribenboimin kirjoittamien kirjojen lisäksi erittäin tärkeä lähde oli internet-sivusto http://fermatslasttheorem.blogspot.com/. Sivuston on koonnut Kalifornialainen Larry Freeman. Hän on käyttänyt lähteinään lukuisia aiheeseen liittyviä kirjoja, osa niistä on samoja, joita olen itse käyttänyt lähteenä. Sivuston tarkoituksena on selvittää lukuteorian kehitystä suhteessa Fermat'n suureen lauseeseen. Freeman on pyrkinyt keskittymään ihmisiin, ideoihin ja matemaattisiin yksityiskohtiin.

Lähdeluettelo

[1] http://fermatslasttheorem.blogspot.com/

[2] http://fi.wikipedia.org/wiki/Fermat

[3] http://homepages.cwi.nl/ dik/english/mathematics/flt4.html

[4] http://mathworld.wolfram.com/SophieGermainPrime.html

[5] http://primes.utm.edu/top20/page.php?id=2

[6] http://www.geocities.com/fermatnow/flt/flt3.htm

[7] http://www.rinconmatematico.com/foros/index.php?action=dlattach ;topic=7796.0;attach=2172 -

[8] http://www.simonsingh.com/Sophie_Germain.html

[9] http://www.simonsingh.net/Wolfskehl_Prize_Article.html

[10] http://www.pbs.org/wgbh/nova/proof/wiles.html

[11] Aczel, A.D., Fermat'n teoreema, 1997, WSOY, Porvoo Helsinki Juva

[12] Bell, E.T., Matematiikan miehiä, 1963, WSOY, Porvoo

[13] Boyer, C., Tieteiden Kuningatar 1-2, 2000, WS Bookwell Oy, Juva

[14] Edwards, H.M., Fermat's Last Theorem: A Genetic Introduction to Algebraic Number Theory, 1977, Springer-Verlag, New York

[15] Hellegouarch, Y., Invitation to the Mathematics of Fermat-Wiles, 2002, Academic Press, London

[16] Hintikka, P., Arvoitus vuosisatojen takaa, Fermat'n suuri lause, 2003, Helsinki

[17] Ribenboim, P., 13 Lectures on Fermat's Last Theorem, 1979, Springer-Verlag, New York

[18] Ribenboim, P., Fermat's Last Theorem For Amateurs, 1999, Springer-Verlag, New York

[19] Singh, S., Fermat'n viimeinen teoreema, 1998, Gummerus Kirjapaino Oy, Jyväskylä