Fermat'n suuren lauseen erikoistapauksia

Jussi Väisänen

Matematiikan pro gradu

Jyväskylän yliopisto
Matematiikan ja tilastotieteen laitos
Syksy 2018

Tiivistelmä: J.Väisänen, *Fermat'n suuren lauseen erikoistapauksia* (engl. *Special cases of Fermat's last theorem*), matematiikan pro gradu -tutkielma, 35 s., Jyväskylän yliopisto, Matematiikan ja tilastotieteen laitos, syksy 2018.

Tämän tutkielman tarkoituksena on perehtyä Fermat'n suuren lauseen todistuksen syntyyn ja etenkin muutamiin lauseen yksinkertaisimpiin erityistapauksiin. Fermat'n suuren lauseen mukaan ei ole olemassa kokonaislukuja x, y ja z, jotka toteuttavat yhtälön

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

kun n on lukua 2 suurempi luonnollinen luku. Vaikka lause on nimetty 1600-luvulla eläneen Pierre de Fermat'n mukaan, ulottuvat sen juuret tuhansien vuosien päähän Fermat'ta edeltävään aikaan. Fermat'n suuri lause onnistuttiin myös lopulta todistamaan vasta satojen vuosien kuluttua siitä, kun Fermat oli tämän väittämän esittänyt. Andrew Wiles yhdisti lopullisessa todistuksessa onnistuneesti vuosisatojen varrella kehittyneitä tuloksia monilta eri matematiikan aloilta ja lauseen todistaminen vaati häneltä seitsemän vuoden yhtäjaksoisen työn.

Tässä tutkielmassa otetaan katsaus Fermat'n suuren lauseen historiaan ja todistetaan lauseen paikkaansapitävyys tapauksissa $n = 4$ ja $n = 3$. Tapauksen $n = 4$ todistus pohjautuu jo Fermat'n käyttämään *äärettömän laskeutumisen menetelmään*, kun taas tapaus $n = 3$ on todistettu Eulerin laatiman todistuksen pohjalta.

Eulerin todistuksessa tapaukselle $n = 3$ hyödynnetään Gaussin resiprookkilakia. Jos p ja q ovat erisuuria parittomia alkulukuja ja tiedetään, onko q neliönjäännös vai neliönepäjäännös modulo p, niin Gaussin resiprookkilaki kertoo, onko p tällöin neliönjäännös vai neliönepäjäännös modulo q. Tämä resiprookkilain sisältö saadaan esitettyä suoraviivaisemmin Legendren symbolia hyödyntäen ja ennen lain todistamista todistetaan aputuloksina muun muassa Eulerin kriteeri sekä Gaussin lemma.

Sisältö

Johdanto

Tämän tutkielman tarkoituksena on perehtyä Fermat'n suuren lauseen todistuksen syntyyn ja etenkin muutamiin lauseen yksinkertaisimpiin erityistapauksiin. Fermat'n suuren lauseen mukaan ei ole olemassa kokonaislukuja x, y ja z, jotka toteuttavat yhtälön

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

kun n on lukua 2 suurempi luonnollinen luku. Vaikka lause on nimetty 1600-luvulla eläneen Pierre de Fermat'n mukaan, ulottuvat sen juuret tuhansien vuosien päähän Fermat'ta edeltävään aikaan. Fermat'n suuri lause onnistuttiin myös lopulta todistamaan vasta satojen vuosien kuluttua siitä, kun Fermat oli tämän väittämän esittänyt. Andrew Wiles yhdisti lopullisessa todistuksessa onnistuneesti vuosisatojen varrella kehittyneitä tuloksia monilta eri matematiikan aloilta ja lauseen todistaminen vaati häneltä seitsemän vuoden yhtäjaksoisen työn.

Tämän tutkielman ensimmäisessä luvussa otetaan katsaus Fermat'n suuren lauseen historiaan. Seuraavassa luvussa keskitytään kahteen lauseen erikoistapaukseen ja todistetaan tämän paikkaansapitävyys ensin tapauksessa $n = 4$ ja tämän jälkeen tapauksessa $n = 3$. Tapauksen $n = 4$ todistus pohjautuu jo Fermat'n käyttämään *äärettömän laskeutumisen menetelmään*, kun taas tapaus $n = 3$ on todistettu Eulerin laatiman todistuksen pohjalta. Molemmat näistä todistuksista on tehty lähteeseen [**7**, s. 1–31] tukeutuen ja näiden todistusten myötä huomataan lauseen olevan samalla tosi myös aina, kun luku n on mikä tahansa luvun 3 tai 4 monikerta. Yleisemmin, jos lause pätee luvulle n, niin se pätee myös kaikille luvun n monikerroille. Tämän vuoksi riittää todistaa lause vain kaikissa sellaisissa tapauksissa, joissa n on alkuluku.

Eulerin todistuksessa tapaukselle $n = 3$ hyödynnetään Gaussin resiprookkilakia, jonka mukaan, jos p ja q ovat erisuuria parittomia alkulukuja, niin

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}},$$

missä $\left(\frac{p}{q}\right)$ on Legendren symboli. Tämä tulos todistetaan tässä tutkielmassa omana kappaleenaan 2.4 ja lauseen todistus on tehty kokonaisuudessaan lähteen [**8**, s. 418–438] pohjalta. Ennen Gaussin resiprookkilakia kappaleessa 2.4 todistetaan aputuloksina myös Eulerin kriteeri sekä Gaussin lemma.

Seuraavien Fermat'n suuren lauseen erikoistapausten todistaminen on historian saatossa osoittautunut selvästi näitä kahta tutkielmassa esitettyä tapausta haastavammaksi, mistä kielii jo se, että sata vuotta Fermat'n kuoleman jälkeen ainoastaan nämä kaksi tapausta oli todistettu. Tapaus $n = 5$ todistettiin vasta vuonna 1825, kun

osattiin ensimmäistä kertaa hyödyntää Sophie Germainin tuoretta, muotoa $2p+1$ oleviin lukuihin kohdistuvaa, päättelyä ja 14 vuotta tämän jälkeen Gabriel Lamé todisti tapauksen $n = 7$.

Niin Augustin Louis Cauchyn kuin Laménkin vuonna 1847 laatimia Fermat'n suuren lauseen täydellisiä todistusyrityksiä leimasi sellainen perusongelma, että nämä nojasivat yksikäsitteiseen tekijöidenjakoon, joka onnistui ainoastaan reaaliluvuille, kun samaan aikaan molempien todistusyritykset edellyttivät kuitenkin imaginaarilukujen käyttöä. Ernst Kummer onnistui osoittamaan, että erään uudenlaisen menetelmän avulla yksikäsitteinen tekijöidenjako oli mahdollista säilyttää monissa tapauksissa. Lukua $n = 100$ pienemmistä alkuluvuista tapaukset $n = 31$, $n = 59$ ja $n = 67$ vaativat kuitenkin kukin erillisen todistuksen, mutta nämä yksittäistapaukset Kummer onnistui todistamaan 1850-luvulla, joten jo silloin tiedettiin, että Fermat'n suuri lause pätee, kun $n \leq 100$. Vielä tämän jälkeenkin saatiin kuitenkin odottaa lähes 150 vuoden ajan ennen Wilesin lopullisen todistuksen valmistumista.

LUKU 1

Fermat'n suuren lauseen historiaa

1.1. Ennen Fermat'ta

Fermat'n suuren lauseen tarinan voidaan katsoa alkaneen jo kauan ennen Fermat'n syntymää. Sen juuret ulottuvat aina pronssikauden aikaiseen Mesopotamiaan, hedelmällisen puolikuun alueelle Eufratin ja Tigrisin välissä. Tämä nykyisin Irakiin kuuluva alue tunnetaan historiassa myös Kaksoisvirran maana. Mesopotamiassa kukoisti vuosien 2000 eKr. ja 600 eKr. välissä kulttuuri, jota kutsutaan Babylonian ajaksi. Tänä aikakautena siellä kehitettiin kirjoitustaito, keksittiin pyörä ja opittiin käsittelemään metalleja. Lisäksi Eufratin ja Tigrisin väliseen maastoon raivattujen laajojen peltojen kastelemiseksi kaivettiin kattava kanavaverkko.

Kulttuurin kukoistaessa ihmiset alkoivat käydä kauppaa ja rakentaa vauraita kaupunkeja. Näiden pohjaksi tarvittiin täsmällinen ja yhtenäinen mittajärjestelmä. Babylonian ajan tiedemiehet oppivatkin arvioimaan, kuinka paljon ympyrän kehä on ympyrän halkaisijaa pidempi. Tälle suhteelle he käyttivät lukuarvoa, joka vastasi melko tarkkaan nykyään käytössä olevaa lukua pii. Jättimäisten porraspyramidien ja Baabelin tornin rakentajilla oli myös oltava tiedossa, kuinka lasketaan pinta-aloja ja tilavuuksia. [**1**, s. 22–23]

Myös lukujen neliöt kuuluivat Babylonian ajan arkipäivään. Näiden katsottiin edustavan vaurautta, sillä maanviljelijän varallisuus riippuu sadon suuruudesta, joka puolestaan riippuu siitä, miten suuri on pellon pinta-ala. Neliönmuotoisella pellolla sekä pellon leveys että pituus ovat a, jolloin pellon pinta-alaksi tulee a^2. Tässä mielessä voidaankin sanoa, että vauraus tulee neliöistä. Babylonialaiset halusivat myös tietää, miten kokonaislukujen muodostamat neliöt voidaan jakaa muiden kokonaislukujen neliöiksi. Esimerkiksi pelto, jonka kummankin sivun pituus oli 5 mittayksikköä ja ala 25 neliötä, voitiin vaihtaa kahteen peltoon, joista toisen sivut olivat 3 mittayksikköä eli 9 neliötä ja toisen 4 mittayksikköä eli 16 neliötä. Tämä oli olennainen tieto käytännön maanjako-ongelmia ratkaistaessa. Nykyään kirjoitamme tämän yhteyden muodossa $3^2 + 4^2 = 5^2$. Lukuja 3, 4 ja 5, kuten kaikkia muitakin yhtälön $x^2 + y^2 = z^2$ toteuttavia kokonaislukukolmikoita, kutsutaan Pythagoraan kolmikoiksi, vaikka vanhojen savitaulujen perusteella tiedämmekin babylonialaisten tunteneen näiden lukujen ominaisuudet jo tuhat vuotta ennen itse kreikkalaisen matemaatikko Pythagoraan syntymää. [**1**, s. 23–24]

Edellä mainittuja Babylonian ajan kirjoituksia sisältäneitä savitauluja on säilynyt paljon aina meidän päiviimme saakka. Esimerkiksi pelkästään Nippurin kaupungin alueelta on löydetty noin 50 000 savitaulua, joita säilytetään Yhdysvalloissa Yalen yliopistossa, Columbia-yliopistossa ja Pennsylvanian yliopistossa. Yhtä tutkituista savitauluista pidetään matematiikan historian kannalta erityisen merkittävänä. Tätä luettelonimekseen Plimpton 322 saanutta taulua säilytetään New Yorkissa Columbia-yliopistossa ja siinä on lueteltu ainoastaan viisitoista kolmen kokonaisluvun ryhmää.

Jokaisella näistä ryhmistä on kuitenkin se ominaisuus, että ryhmän ensimmäinen luku on kahden seuraavan luvun summa ja jokainen taulussa mainituista luvuissa on lisäksi kokonaisluvun neliö. Edellämainitun lukukolmikon 3,4 ja 5 lisäksi Plimpton 322 mainitsee muun muassa luvut 169, 144 ja 25, joiden välillä on yhteys $5^2 + 12^2 = 13^2$. Osa tutkijoista uskoo, että jo babylonialaisia kiinnosti tämä neliöiden välinen yhteys itsessään, kun taas osa epäilee heidän miettineen puhtaasti käytännön laskemista, sillä babylonialaisten käyttämässä 60-järjestelmässä oli kätevää hyödyntää kokonaislukujen neliöitä murto-osien laskemisessa. Niin tai näin, babylonialaiset eivät mitä ilmeisimmin yrittäneet kehittää yleisiä ratkaisumenetelmiä tämäntyyppisille ongelmille, vaan esimerkiksi tauluja käyttäneitä oppilaita opetettiin lukemaan ja käyttämään hyväksi niissä valmiina olevia lukuja. [**1**, s. 24–26]

Yksi avainhenkilö matkalla kohti Fermat'n suurta lausetta ja tämän todistamista oli eittämättä Pythagoras, joka syntyi noin vuonna 580 eKr. kreikkalaisella Samoksen saarella. Pythagoras matkusteli paljon ja hän vierailikin paitsi Egyptissä ja Babyloniassa, mahdollisesti myös jopa Intiassa saakka. Matematiikkaan hän perehtyi etenkin Babyloniassa ja siellä hän saattoikin tutustua myös näihin edellä mainittuihin kolmen kokonaisluvun ryhmiin, joita myöhemmin alettiin siis kutsua Pythagoraan luvuiksi. Kreikkaan palattuaan Pythagoras päätti jatkaa matkaansa Krotoniin, joka oli Etelä-Italiassa sijaitseva kreikkalainen siirtokunta. Sinne hän perusti salaseuran, joka omistautui täysin lukujen tutkimiselle. Tätä peräti 600 jäsenen veljeskuntaa alettiinkin myöhemmin kutsua pythagoralaisiksi. [**1**, s. 26–27]

Pythagoralaiset halusivat selvittää lukujen perimmäisen olemuksen ja pitää tietonsa sekä tutkimustuloksensa vain sisäpiirinsä hallussa. Kun aiemmin lukuja oli käytetty lähinnä luettelemiseen ja laskemiseen, arvostivat pythagoralaiset niitä niiden itsensä vuoksi. He pyrkivätkin pelkkien kaavojen käyttämisen ja kehittämisen sijaan ymmärtämään näitä syvällisemmin sekä selvittämään, minkä vuoksi käytetyt kaavat yleensä toimivat. Pythagoraan väitetään keksineen nimeään kantavan Pythagoraan lauseen, jonka mukaan suorakulmaisen kolmion pisimmän sivun neliö on yhtä suuri kuin kahden muun sivun neliöiden summa. Olennaisena lisäyksenä babylonialaisilla käytössä olleeseen matematiikkaan oli tämän neliöiden välisen yhteyden geometrinen tarkastelu, sillä tällä tavalla pythagoralaiset saattoivat yleistää sen koskemaan muitakin kuin positiivisia kokonaislukuja sekä osoittamaan, että väite pitää paikkansa. [**1**, s. 27–30] [**9**, s. 27–30, 40–42]

Pythagoras kuoli noin vuonna 500 eKr. Hänen salaseuransa hajosi, kun sybariiteiksi kutsuttu kilpaileva poliittinen ryhmä yllätti pythagoralaiset ja surmasi heistä useimmat. Henkiinjääneet levittäytyivät ympäri tuolloin suuren osan Välimeren rannikkoseudusta kattanutta Kreikkaa ja eräs pakoon päässeistä oppineista, Filolaos, kirjoitti muistiin Pythagoraan koulukunnan historian ja tieteelliset teoriat. Oletettavasti noin 200 vuotta myöhemmin eläneen Eukleides Aleksandrialaisen klassikkoteos *Elementan*, suomeksi *Alkeiden*, kaksi ensimmäistä kirjaa pohjautuvat kokonaan Pythagoraan ja hänen salaseuransa töille. Tähän pohjautuvaa geometrian järjestelmää on opetettu kouluissa lähes sellaisenaan useiden vuosisatojen ajan, minkä vuoksi teosta pidetään yhtenä kaikkien aikojen merkittävimmistä oppikirjoista. [**1**, s. 34–38]

1.2. Pierre de Fermat 1601–1665

Matemaatikko Pierre Fermat syntyi elokuussa 1601 Beaumont-de-Lomagnen kaupungissa eteläisessä Ranskassa. Fermat'n isä oli Beaumontin toinen konsuli, nahkakauppias Dominique Fermat, ja äiti oli lakimiehen tytär Claire de Long. Ensimmäiset tiedon alkeensa Pierre sai kotona synnyinkaupungissaan ja myöhemmin hän lähti vanhempiensa vaatimuksesta jatkamaan opintojaan Toulousen yliopistoon valmistuakseen virkamieheksi. Siellä Fermat nimitettiin 30-vuotiaana keväällä 1631 oikeusistuimen jäseneksi ja samana vuonna hän meni naimisiin äitinsä serkun, Louise de Longin, kanssa. He saivat kaksi tytärtä ja kolme poikaa, joista Clément Samuel de Fermat jatkoi myöhemmin isänsä jalanjäljissä ja julkaisi tämän kuoleman jälkeen hänen kootut matemaattiset kirjoituksensa. Juuri tässä teoksessa mainitaan kuuluisa huomautus, jota nykyään kutsutaan Fermat'n suureksi lauseeksi. [**1**, s. 15–18] [**2**, s. 58–60] [**9**, s. 59–60]

Fermat oli koko työuransa ajan tehokas virkamies, joka kaikesta päätellen toteutti velvollisuutensa harkiten ja oikeudentuntoisesti. Hän kohosikin nopeasti virkamiesasteikolla ja pääsi yhteiskunnan eliittiin, minkä myötä hän sai oikeuden käyttää nimessään etuliitettä *de*. Vuonna 1648 hänet ylennettiin kuninkaan neuvosmieheksi Toulousen paikallisessa parlamentissa ja tässä virassa hän toimi aina vuoteen 1665 ja kuolemaansa saakka; Fermat hoiti viimeisen oikeusjuttunsa 10.1.1665 vain kaksi päivää ennen kuolemaansa. Monet historioitsijat ovat ihmetelleet, mistä Fermat'lle riitti aikaa ja energiaa korkealuokkaiseen matemaattiseen tutkimukseen vaativien hallinnollisten tehtävien ohella. Eräs ranskalainen asiantuntija on arvellut, että työ kuninkaan neuvosmiehenä ennemmin auttoi kuin vahingoitti hänen henkistä toimintaansa. Toisin kuin muiden valtion virkailijoiden kohdalla, edellytettiin parlamentin neuvoston jäseniä nimittäin pysymään erillään muista kaupunkilaisista, jottei heitä voitaisi lahjoa tai kiristää. Matematiikasta tuli näin sopiva henkireikä, koska Fermat varmasti halusi harrastaa jotakin virkavelvollisuuksiensa vastapainoksi eikä paikkakunnan seuraelämään osallistuminen tullut kysymykseen. [**1**, s. 17] [**2**, s. 60] [**9**, s. 60]

Vaikka Fermat'ta pidetään yleisesti aikansa yhtenä suurimmista matemaatikoista, ei hänen saavutustensa perustana ollut koulutus, sillä hänen opiskeluaikanaan ei vielä opetettu niitä aloja, joilla hän on tehnyt huomattavimmat työnsä. Matematiikan harrastelijoiden kuninkaan tuotanto onkin vetänyt vastustamattomasti puoleensa matematiikan harrastajia yli kolmen vuosisadan ajan kaikissa sivistyneissä maissa. [**2**, s. 59–60]

Yksi Fermat'n tärkeimpiä saavutuksia oli differentiaali- ja integraalilaskennan pääperiaatteiden hahmotteleminen, sillä vaikka alan varsinaisena kehittäjänä on yleisesti pidetty Isaac Newtonia (1642–1727) ja Gotfried Wilhelm Leibnizia (1646–1716), on Newton itse myöntänyt kehittäneensä differentiaali- ja integraalilaskentaa Fermat'n "tangenttien piirtämisen menetelmän" pohjalta. Analyyttisen geometrian taas Fermat ja René Descartes (1596–1650) keksivät toisistaan riippumatta, mutta Fermat sovelsi tätä ensimmäisenä kolmiulotteiseen avaruuteen. Todennäköisyyslaskennan periaatteet Fermat kehitti yhdessä nuoremman aikalaisensa Blaise Pascalin (1623–1662) kanssa, kun he alkoivat käydä kirjeenvaihtoa ammattipeluri Chevalier de Mérén Pascalille esittämästä rahapeliä koskevasta ongelmasta ja paneutuivat tältä pohjalta myös monimutkaisempiin todennäköisyyteen liittyviin kysymyksiin. [**2**, s. 65] [**9**, s. 65–69]

Pelkästään edellä mainittujen matematiikan alojen kehittäminen olisi riittänyt nostamaan Fermat'n suurten matemaatikkojen joukkoon, mutta hänen yleensä suurimpina pidetyt saavutuksensa koskivat nimenomaan lukuteorian alaa. Fermat yritti intohimoisesti ymmärtää lukujen ominaisuuksia ja niiden välisiä yhteyksiä. Erityisesti hän oli ihastunut kokonaislukujen kauneuteen ja mielekkyyteen. Hän kehitti monia kokonaislukuihin liittyviä teorioita, joista yksi väittää, että muotoa $2^{(2^n)} + 1$ olevat luvut ovat alkulukuja, kun n on luonnollinen luku. Hän ei kuitenkaan väittänyt todistaneensa arvaustaan ja paljon myöhemmin Leonhard Euler (1707–1783) huomasi, ettei tämä väite päde enää, kun $n = 6$. Fermat esitti ilman todistusta myös niin sanotun pienen lauseensa, jonka mukaan $n^p - n$ on jaollinen luvulla p, jos n on mielivaltainen kokonaisluku ja p on mielivaltainen alkuluku. Tälle lauseelle ensimmäisen todistuksen antoi Leibniz 1600-luvun jälkipuoliskolla. [**2**, s. 69–70] [**9**, s. 69]

Fermat keksi myös lauseen, jonka mukaan jokainen alkuluku, joka on muotoa $4n + 1$, voidaan esittää kahden neliön summana yhdellä ja vain yhdellä tavalla, kun taas mikään muotoa $4n - 1$ oleva luku ei ole kahden neliön summa. Kuten tavallista, Fermat ei jättänyt tällekään teoreemalle mitään todistusta. Lopulta tämän tuloksen todisti vasta Euler vuonna 1749 ponnisteltuaan seitsemän vuoden ajan todistuksen keksimiseksi. Fermat kuitenkin kuvaa kirjeessään keksimänsä ns. rajattoman laskeutumisen metodin, jonka avulla hän todisti tämän ja eräitä muitakin ihmeellisistä tuloksistaan. [**2**, s. 70–71]

Fermat väitti todistaneensa myös, että on mahdotonta jakaa kuutiota kahdeksi kuutioksi tai yleisemmin mitään kahta korkeampaa potenssia kahdeksi saman asteen potenssiksi eli että $a^n + b^n \neq c^n$ kun a, b ja c ovat kokonaislukuja ja $n > 2$. Vuosisatojen kuluessa kaikki muut Fermat'n väittämät saatiin osoitettua oikeiksi tai vääriksi, mutta tämä niin sanottu Fermat'n suuri lause jäi lukemattomista todistusyrityksistä huolimatta yhä avoimeksi. [**2**, s. 72]

1.3. Fermat'n jälkeen

Fermat onnistui mitä ilmeisimmin todistamaan suuren lauseensa oikeaksi ainakin tapauksessa, jossa eksponentti n on 4. Hän huomasi myös, että jos hänen väitteensä pitää paikkansa jollakin luvulla n, pitää se paikkansa myös kaikilla luvun n monikerroilla. Kuitenkin vasta Euler onnistui ottamaan seuraavan konkreettisen askeleen kohti lauseen yleisempää todistusta, kun hän pystyi imaginäärilukuja hyödyntäen soveltamaan Fermat'n kehittelemää äärettömän laskeutumisen menetelmää myös tapauksessa $n = 3$. Se oli valtava edistysaskel, mutta tästä huolimatta Euler ei kyennyt soveltamaan havaintoaan lauseen muihin tapauksiin. [**1**, s. 55] [**9**, s. 116]

Sata vuotta Fermat'n kuoleman jälkeen ainoastaan nämä kaksi tapausta oli todistettu hänen suuresta lauseestaan. Vaikka edistyminen oli kiusallisen hidasta, tilanne ei silti ollut niin lohduttoman huono, miltä ensinäkemällä vaikuttaisi. Tapauksen $n = 4$ todistaminen todistaa nimittäin samalla myös tapaukset $n = 8, 12, 16, 20 \ldots$ ja vastaavasti Eulerin todistus tapauksessa $n = 3$ todistaa automaattisesti myös tapaukset $n = 6, 9, 12, 15 \ldots$. Itse asiassa lauseen todistamiseksi riittää, että käsitellään vain kaikki luvun n alkulukuarvot, sillä kaikki muut tapaukset tulevat käsitellyiksi samalla (tämä todetaan sivun 16 Huomautuksessa 2.19). Tutkittavien yhtälöiden määrä väheneekin näin oleellisesti, mutta itse lauseen todistuksen haasteita tämä ei poista,

sillä jo Eukleides oli todistanut, että pelkästään alkulukuja on ääretön määrä. [**9**, s. 118–121]

Seuraavan edistysaskeleen lauseen parissa otti nuori ranskalaisnainen Sophie Germain (1776–1831), joka päätti lähestyä lausetta uudesta näkökulmasta. Hänen ensisijainen tavoitteensa ei ollut todistaa mitään yhtä erityistä tapausta vaan saada tuloksia monista eri tapauksista samanaikaisesti. Germain kehitteli lukuja $2p + 1$ vastaaviin luvun n arvoihin kohdistetun päättelyn, jonka mukaan yhtälöllä $x^n + y^n = z^n$ ei todennäköisesti ole lainkaan ratkaisua. Tällä hän tarkoitti sitä, ettei ratkaisuja luultavasti ollut olemassa, koska muuten joko x, y tai z olisi jaollinen luvulla n, mikä asettaisi hyvin tiukkoja rajoja mahdollisille ratkaisuille. [**9**, s. 128, 137]

Germainin menetelmän merkityksen ymmärsivät ensimmäisinä vuonna 1825 Peter Gustav Lejeune Dirichlet (1805–1859) ja Adrien-Marie Legendre (1752–1833). Nämä kahden täysin eri matemaatikkosukupolven edustajat onnistuivat toisistaan tietämättä todistamaan, ettei tapauksella $n = 5$ ole ratkaisuja, mutta kunnia todistuksesta kuuluu suurelta osin Germainille. Neljätoista vuotta myöhemmin ranskalaisnen matemaatikko Gabriel Lamé (1795–1870) otti seuraavan tärkeän edistysaskeleen todistaessaan tapauksen $n = 7$. [**9**, s.137–138]

Vuonna 1847 Lamé ilmoitti Ranskan tiedeakatemian kokouksessa, että oli aivan Fermat'n suuren lauseen täydellisen todistuksen kynnyksellä. Hän esitteli menetelmänsä pääpiirteet ja epäili, että voi julkaista todistuksen muutaman viikon sisällä tiedeakatemian lehdessä. Heti Lamén puheenvuoron jälkeen myös Augustin Louis Cauchy (1789–1857) ilmoitti, että työstää todistusta samankaltaisten suuntaviivojen mukaan ja että myös hän aikoo julkaista pian oman valmiin todistuksensa. Ranskan tiedeakatemia oli tarjonnut jo Germainin saavuttaman edistyksen jälkeen kultamitalia ja 3000 frangin rahasummaa matemaatikolle, joka onnistuu lopullisesti todistamaan Fermat'n suuren lauseen. Sekä Cauchy että Lamé luovuttivat tasan kolmen viikon kuluttua todistuksensa tiedeakatemialle sinetöidyissä kirjekuorissa ja jäivät odottamaan akatemian vastausta. Noin kahden kuukauden kuluttua julkaistu ilmoitus lopetti vihdoinkin todistuksia koskevat arvailut. Akatemiassa puhunut Joseph Liouville (1809–1882) luki yleisölle otteita Ernst Kummerin (1810–1893) kirjeestä, jossa kyseenalaistettiin molempien todistusyritysten oikeellisuus. Kummerin mukaan perusongelma oli se, että sekä Cauchyn että Lamén todistukset nojasivat ns. yksikäsitteiseen tekijöihinjakoon. Molemmat todistukset kuitenkin edellyttivät imaginaarilukujen käyttöä, kun yksikäsitteinen tekijöihinjako taas sopii sellaisenaan ainoastaan reaaliluvuille. Kummer osoitti, että erään uudenlaisen menetelmän avulla yksikäsitteinen tekijöihinjako oli mahdollista säilyttää monilla luvun n arvoilla. Ongelma saatiinkin näin vältettyä esimerkiksi kaikilla alkuluvuilla n lukuun 31 saakka. Alkulukua $n = 37$ ei kuitenkaan voitu käsitellä enää näin helposti. Lukua 100 pienemmistä alkuluvuista myös $n = 59$ ja $n = 67$ olivat tässä suhteessa hankalia tapauksia. Kummer onnistui kuitenkin todistamaan nämä kolme yksittäistapausta, joten hänen ansiostaan jo 1850-luvulla tiedettiin, että Fermat'n suuri lause pätee, kun $n \leq 100$. [**1**, s. 80] [**9**, s. 143–149]

Nämä niin sanotut epäsäännölliset alkuluvut osoittautuivat ylitsepääsemättömäksi esteeksi niin Cauchyn kuin myös Lamén todistusyrityksille. Kummer totesikin, ettei tätä ongelmaa saada ratkaistua yhdellä kertaa sen aikaisen matematiikan keinoilla. Hän kuitenkin uskoi, että näitä voidaan käsitellä yksi kerrallaan kuhunkin tapaukseen

erillisesti laadituilla menetelmillä. Näiden menetelmien kehittämistyö oli kuitenkin hidasta, eikä asiaa parantanut se, että myös epäsäännöllisiä alkulukuja on äärettömän paljon. [**9**, s. 149–150]

Vuonna 1908 Wolfskehlin säätiö tarjosi 100 000 Saksan markan suuruista palkintoa sille, joka pystyisi todistamaan Fermat'n suuren lauseen. Summa oli aikakauteen suhteutettuna todella suuri, mutta ammattimatemaatikkojen enemmistöä sekään ei saanut enää todistukseen paneutumaan, sillä monet näistä pitivät tehtävää toivottomana. Luvattu palkinto sai kuitenkin aikaan sen, että suuri määrä innokkaita harrastelijoita lähetti säätiölle omia todistusehdotuksiaan. Ratkaisuja virtasikin vuosien saatossa tuhansia, mutta yksikään näistä ei ollut oikea. [**1**, s. 82] [**9**, s. 155–157]

Henri Poincaré (1854–1912) tutki sinin ja kosinin kaltaisia jaksollisia funktioita. Aikalaisistaan poiketen hän kuitenkin käytti reaalitason sijaan kompleksitasoa, jossa reaaliluvut ovat vaaka-akselilla ja imaginaariluvut pystyakselilla. Funktion jaksollisuus voi ilmetä sekä reaaliakselin että imaginaariakselin suunnassa. Poincaré päätteli, että tällä keinolla voidaan löytää funktioita, joilla on hyvin monipuolinen symmetria. Tällaisia olivat ns. automorfifunktiot ja niistä johdetut vielä monimutkaisemmat modulaariset funktiot. Vaikka Poincaré ei jatkanut näiden funktioiden tutkimista vaan siirtyi muille matematiikan aloille, oli hän kuitenkin tietämättään kylvänyt siemeniä, joista olisi myöhemmin paljon apua Fermat'n suuren lauseen todistuksessa. [**1**, s. 94–96]

1900-luvulla alettiin tutkia lähes kahdentuhannen vuoden takaisia Diofantoksen yhtälöitä yhä enemmän elliptisten käyrien ominaisuuksia hyödyntämällä. Nämä käyrät eivät ole ellipsejä eivätkä ne kuvaa elliptisiä funktioitakaan, vaan ne liittyvät kolmannen asteen polynomien ratkaisuihin. Lukuteoreetikoille nämä käyrät tarjosivat tehokkaan tutkimusmenetelmän, sillä niiden avulla saadaan vastauksia moniin yhtälöitä ja niiden ratkaisuja koskeviin kysymyksiin. [**1**, s. 104–105]

Vuonna 1954 kaksi nuorta japanilaista matemaatikkoa, Yutaka Taniyama (1927–1958) ja Goro Shimura (1930–), tutustuivat sattumalta, kun he tarvitsivat omiin tutkimuksiinsa juuri samaan aikaan taustatietoa kompleksisen kertolaskun algebrallisesta teoriasta. Aihetta koskeva julkaisu oli lainassa Taniyamalla ja kun Shimura kysyi, koska tämä aikoi palauttaa sen, päätyivät he vaihtamaan ajatuksia tutkimustuloksistaan. He molemmat tutkivat yhtälöiden modulaarisia muotoja, mitä pidettiin siihen aikaan hyvin epämuodikkaana aiheena. Taniyama oli kuitenkin alkanut pohtia modulaaristen muotojen ja elliptisten yhtälöiden välistä erikoista yhteyttä. Hänen kuoltuaan traagisesti vuonna 1958 Shimura jatkoi tämän aiheen tutkimista. Tutkimustensa tuloksena hän esitti, että jokaisella elliptisellä yhtälöllä on tätä vastaava modulaarinen muoto. Tätä Tanyama–Shimuran otaksumaa epäiltiin aluksi varsin laajalti, sillä elliptisen ja modulaarisen maailman välillä ei aiemmin oltu vakavasti ajateltu olevan pienintäkään yhdistävää lenkkiä. Lopulta Shimuralla oli koossa sen verran todisteita, että kyseinen otaksuma alkoi saada laajempaakin kannatusta. [**9**, s. 211–213, 215, 222, 226 229–230]

Englantilainen matemaatikko Louis J. Mordell (1888–1972) keksi muiden tutkimustensa ohessa vuonna 1922, että Fermat'n suurella lauseella voi olla vain äärellinen määrä ratkaisuja. Tätä havaintoa hän ei kuitenkaan osannut todistaa, mutta vuonna 1983 saksalainen matemaatikko Gerd Faltings (1954–) osoitti tämän Mordellin otaksuman oikeaksi. Fermat'n suuri lause ei Faltingsia sinällään kiinnostanut, sillä

hän piti sitä omana irrallisena lukuteorian ongelmanaan. Hänen löytämänsä todistus osoittautui kuitenkin myöhemmin tärkeäksi Fermat'n ongelman ratkaisussa. Pian tämän jälkeen Andrew Granville (1962–) ja D. R. Heath-Brown (1952–) osoittivat Faltingsin tulokseen nojautuen, että jos Fermat'n suurella lauseella oli ratkaisuja, niitä oli sitä harvemmassa, mitä suuremmaksi luku n kasvaa. Tämä tarkoitti käytännössä sitä, että Fermat'n suuri lause piti "lähes varmasti" paikkansa, koska vuoteen 1983 mennessä lause oli todistettu oikeaksi jo miljoonaan saakka yltäville luvun n arvoille. [**1**, s. 97–100]

Vuonna 1984 Gerhard Frey (1944–) esitti väitteen, jonka mukaan Taniyaman–Shimuran otaksuma ja Fermat'n suuri lause ovat toinen toistensa seurauksia. Tämä väite perustui oletukseen, että hänen Fermat'n yhtälöstä johtamansa elliptinen yhtälö oli niin outo, ettei se voinut olla modulaarinen. Tämän oletuksen todistaminen osoittautui ennakoitua haastavammaksi kunnes Ken Ribet (1948–) vihdoin kesällä 1986 onnistui todistuksessa ja yhdisti samalla Taniyaman–Shimuran otaksuman aukottomasti Fermat'n suureen lauseeseen. Tämä antoi matemaatikoille uuden lähestymistavan lauseen todistukseen, sillä nyt voitiin hyödyntää epäsuoraa todistusta; jos Fermat'n suuren lauseen oletetaan olevan epätosi, niin myös Taniyaman–Shimuran otaksuma on epätosi. Näin ollen, jos Taniyaman–Shimuran otaksuma voidaan todistaa oikeaksi, seuraa tästä, että myös Fermat'n suuren lauseen on oltava tosi. [**9**, s. 236–244]

1.4. Andrew Wilesin lopullinen todistus

Taniyaman–Shimuran otaksumaa oli yritetty todistaa jo kolmekymmentä vuotta ennen kuin sen yhteys Fermat'n suureen lauseeseen selvisi. Tämän myötä heräsi toisaalta uutta uskoa Fermat'n suuren lauseen todistamisen suhteen, mutta toisaalta skeptisimmät epäilivät, että havainnon myötä oli menetetty viimeinenkin toivo kyseisen otaksuman todistamiseen. Andrew Wilesin (1953–) tieto Ribetin todistamasta yhteydestä tavoitti loppukesästä 1986. Heti asiasta kuultuaan Wiles tajusi, että hänen lapsuuden unelmansa Fermat'n suuren lauseen todistamisesta oli muuttunut vakavasti otettavaksi tutkimuskohteeksi, eikä hän voisi päästää tilaisuutta käsistään. [**9**, s. 244–245, 247]

Wiles luopui kaikista töistä, jotka eivät suoranaisesti liittyneet Fermat'n suureen lauseeseen ja pyrki työskentelemään mahdollisimman paljon kotonaan ullakon rauhassa. Päätettyään syventyä lauseen todistamiseen Wiles teki varsin erikoisen ratkaisun ja alkoi työskennellä täysin yksin ja muilta salassa. Tähän Wiles päätyi taatakseen itselleen työrauhan, sillä hän koki kaiken Fermat'n suureen lauseeseen liittyvän herättävän liikaa kiinnostusta, mikä olisi vaikeuttanut täydellistä paneutumista aiheeseen. [**9**, s. 249–251]

Seuraavien vuosien aikana Wiles saavutti useita huomattavia tuloksia, joista ainoakaan ei päässyt julkisuuteen ennen todistuksen lopullista valmistumista. Edes läheiset kollegat eivät tienneet hänen tutkimuksistaan, sillä Wiles johdatti heidän huomionsa toisaalle julkaisemalla säännöllisin väliajoin muutaman vuoden takaisia, mutta vielä julkaisemattomia, elliptisiä käyriä koskevia tutkimustuloksiaan. Ainoastaan hänen vaimonsa Nada tiesi miehensä salaisuudesta ja tutkimuksen edetessä Wiles uskoutui vain ja ainoastaan hänelle. [**9**, s. 251–252]

Jo tutkimustensa ensimmäisinä tuloksina Wiles oli saavuttanut useita edistysaskeleita. Hän oli soveltanut Galois'n ryhmiä elliptisiin yhtälöihin, hajottanut elliptiset yhtälöt äärettömän moneen osaan ja todistanut sen jälkeen, että jokaisen elliptisen yhtälön ensimmäisen osan on oltava modulaarinen. Hän ei kuitenkaan keksinyt keinoa, jolla osoittaa, että jos elliptisen yhtälön yksi osa oli modulaarinen, niin seuraavakin oli. Wiles ryhtyi tutkimaan vielä Iwasawan teoriaa ja pyrki muokkaamaan tästä metodista riittävän tehokkaan seuraavan askeleen ottamiseksi. Kun tämäkään ei onnistunut, Wiles päätti palata ihmisten ilmoille kuullakseen tuoreimmista matemaattisista tutkimuksista. Hän osallistuikin vuonna 1991 Bostonissa järjestettyyn elliptisiä yhtälöitä käsittelevään kongresssiin, jossa kokoontuivat alan kaikki keskeiset asiantuntijat. Täällä Wiles kuuli Matthias Flachin kehittäneen edelleen Kolyvaginin metodia elliptisten yhtälöiden käsittelyssä ja hän päättikin omistautua jatkossa täysin rinnoin tämän Kolyvagin–Flachin metodin laajentamiseen. Pian hänen onnistuikin saada jonkin yksittäisen elliptisen yhtälön tapauksessa induktiotodistus toimimaan. Koska Kolyvaginin–Flachin metodi sopi vain johonkin yksittäiseen yhtälöön, täytyi Wilesin vielä luokitella elliptiset yhtälöt erilaisiin perheisiin ja soveltaa metodia siten, että se sopi kaikkiin kyseisen perheen yhtälöihin. Tätä kautta Wiles lähti käsittelemään metodilla kaikkia elliptisten yhtälöiden perheitä yksi kerrallaan. [**9**, s. 281–285]

Työskenneltyään intensiivisesti kuuden vuoden ajan Wiles alkoi uskoa, että todistuksen valmistuminen häämötti. Hän edistyi työssään tasaisesti ja näytti olevan vain ajan kysymys, milloin viimeisetkin elliptisten käyrien perheet olisi käsitelty. Koska Wilesin työ perustui valtaosin varsin tuoreeseen ja monimutkaiseen metodiin, päätti hän viimein tammikuussa 1993 uskoutua pitkään tuntemalleen kollegalleen Nick Katzille. Wiles tahtoi varmuuden siitä, ettei hänen todistuksensa tekniseen osaan jää aukkoja ja miehet katsoivat, että paras tapa Wilesin tutkimustuloksien läpikäymiseen oli säännöllinen jatko-opiskelijoille suunnattu luentosarja, jolla Katz olisi yleisön joukossa. Aiheen hankaluuden vuoksi opiskelijat jäivät luennoilta pois yksi toisensa jälkeen, eikä kukaan koko laitoksella voinut edelleenkään aavistaa Wilesin olevan lähellä alan vuosisadan suurinta läpimurtoa. Lopulta jäljellä olikin enää Katz, joka luentosarjan päätyttyä arvioi Kolyvaginin–Flachin metodin toimivan täydellisesti. [**9**, s. 285–289]

Seuraavina kuukausina Wiles omistautui todistuksen täydentämiselle. Hän onnistui toukokuussa 1993 soveltamaan Kolyvaginin–Flachin metodia vihdoin viimeiseenkin elliptisten käyrien perheeseen. Tässä vaiheessa hän oli vakuuttunut, että Fermat'n suuren lauseen todistus oli hänen hallussaan. Vaikka Wiles olisi halunnut vielä tarkastaa todistustaan, hän päätyi julkistamaan todistuksensa vanhassa koti- ja opiskelukaupungissaan Cambridgessa Isaac Newtonin instituutissa pidetyn kongressin luentosarjansa huipennuksena 23.6.1993. [**9**, s. 290–295]

Todistuksen tarkastuksessa löytyi kuitenkin aukko, joka aiheutti sen, ettei käytettyä metodia voitukaan soveltaa Wilesin haluamalla tavalla. Kun Wiles ei yrityksistä huolimatta saanut todistustaan paikattua, alkoivat huhut ongelmasta levitä ja matemaatikkopiirit vaativat Wilesia julkaisemaan todistuksensa, jotta muutkin pääsevät yrittämään virheen korjaamista ja lauseen lopullista todistamista. Joulukuussa 1993 Wiles julkaisi lyhyen tilanneselostuksen ja myönsi, ettei todistus ole täydellinen nykyisessä muodossaan. [**9**, s. 304–313]

Kun Wiles ei päässyt todistuksessaan eteenpäin seuraavan talven kuluessa, hän harkitsi jo tappionsa tunnustamista. Kollegansa kehotuksesta hän päätti ottaa vielä työparikseen entisen oppilaansa Richard Taylorin, joka oli yksi Wilesin todistuksen tarkastamisesta vastaavista asiantuntijoista. Miehet jatkoivat tutkimusta läpi kevään ja kesän, mutta mainittavaa edistystä ei tapahtunut ja todistuksen lopullinen kaatuminen näytti väistämättömältä. Wiles päätti kuitenkin vielä kerran syventyä Kolyvaginin–Flachin metodin rakenteeseen, sillä hän halusi vähintään ymmärtää, miksi oli epäonnistunut todistuksessa. Äkkiä hän oivalsi, että vaikka kyseinen metodi ei toimi täydellisesti, tämä oli juuri se, mitä hän tarvitsi alkuperäisen Iwasawan teorian täydentämiseen. Wiles palasikin kolmen vuoden takaiseen lähestymistapaansa ja laati syksyn aikana yhdessä Taylorin kanssa alkuperäiseen todistukseensa täydennysosan, jossa yhdistettiin Iwasawan teoria Kolyvaginin–Flachin metodiin. Tämän myötä matemaatikoita vuosisatojen ajan vaivannut arvoitus oli saatu viimein ratkaistua. [**9**, s. 319–328]

LUKU 2

Fermat'n suuren lauseen erikoistapauksia

Tässä työssä todistetaan Fermat'n suuri lause tapauksissa $n = 3$ ja $n = 4$. Aluksi kuitenkin käydään läpi hieman näissä tarvittavia perustietoja.

2.1. Perustietoja

MÄÄRITELMÄ 2.1. Olkoot luvut $a, b \in \mathbb{Z}$. Sanotaan, että luku a *jakaa luvun* b, merkitään $a|b$, jos on olemassa luku $c \in \mathbb{Z}$ siten, että $b = ac$.

HUOMAUTUS 2.2. Määritelmästä 2.1 seuraa, että $a|0$ ja $1|a$ kaikilla $a \in \mathbb{Z}$ ja että luku nolla jakaa kaikista kokonaisluvuista ainoastaan itsensä. Lisäksi jos $a|b$ ja $b \neq 0$, niin $|a| \leq |b|$.

MÄÄRITELMÄ 2.3. Kokonaislukua $p > 1$ kutsutaan *alkuluvuksi*, jos se on jaollinen ainoastaan luvulla 1 ja itse luvulla p.

LEMMA 2.4. *Olkoot* $x, a, b, c \in \mathbb{Z}$. *Jos* $x|a$, $x|b$ *ja* $x|c$, *niin* $x|(ka+lb+mc)$ *kaikille* $k, l, m \in \mathbb{Z}$.

TODISTUS. Oletetaan, että $x|a$, $x|b$ ja $x|c$. Nyt on olemassa sellaiset d,e,$f \in \mathbb{Z}$, että $a = xd$, $b = xe$ ja $c = xf$. Näin ollen $ka+lb+mc = kxd+lxe+mxf = x(kd+le+mf)$ eli $x|(ka + lb + mc)$ kaikilla $k, l, m \in \mathbb{Z}$.

□

MÄÄRITELMÄ 2.5. Olkoot luvut $a, b \in \mathbb{Z}$ siten, että ainakin toinen näistä on nollasta poikkeava. Luku $c \in \mathbb{Z}$ on lukujen a ja b *suurin yhteinen tekijä*, merkitään $c = \text{syt}(a, b)$, jos

(1) $c|a$, $c|b$, ja
(2) jos $d|a$, $d|b$, niin $d \leq c$.

HUOMAUTUS 2.6. Määritelmästä 2.5 seuraa, että
(1) kokonaislukujen a ja b, joista toinen on nollasta poikkeava, suurin yhteinen tekijä on aina olemassa ja sille pätee $\text{syt}(a, b) \geq 1$, sillä $1|a$ ja $1|b$ kaikilla $a, b \in \mathbb{Z}$. Tällöin $\text{syt}(a, b)$ saadaan huomautuksen 2.2 nojalla maksimina äärellisestä joukosta kokonaislukuja. Jos olisi $a = 0$ ja $b = 0$, lukujen suurinta yhteistä tekijää ei tällöin olisi, sillä kaikki luvut $c \in \mathbb{Z}$ jakavat nollan.
(2) $\text{syt}(a, b)$ on yksikäsitteinen, sillä jos olisi voimassa $\text{syt}(a, b) = c$ ja $\text{syt}(a, b) = d$, niin olisi $c \leq d$ ja $d \leq c$ eli $c = d$.
(3) $\text{syt}(a, b) = 1$ on yhtäpitävää sen kanssa, ettei luvuilla a ja b ole yhteisiä *alkulukutekijöitä*.
(4) Jos $a = p_1^{r_1} \cdots p_n^{r_n}$ ja $b = p_1^{s_1} \cdots p_n^{s_n}$, $r_i, s_i \geq 0$ ovat lukujen a ja b alkulukuesityksiä, niin alkulukuesityksen olemassaolon ja yksikäsitteisyyden nojalla selvästi $\text{syt}(a, b) = p_1^{t_1} \cdots p_n^{t_n}$, missä $t_i = \min(r_i, s_i)$.

MÄÄRITELMÄ 2.7. Olkoot luvut $a, b, c \in \mathbb{Z}$ siten, että ainakin kaksi näistä on nollasta poikkeavia. Luku $d \in \mathbb{Z}$ on lukujen a, b ja c *suurin yhteinen tekijä*, merkitään $\text{syt}(a, b, c)$, jos

(1) $d|a$, $d|b$, $d|c$ ja
(2) jos $e|a$, $e|b$, $e|c$ niin $e \leq d$.

Huomautuksen 2.6 kohdasta (1) seuraa, että $\text{syt}(a, b, c)$ on aina olemassa ja sille pätee $\text{syt}(a, b, c) \geq 1$. Vastaavasti huomautuksen kohdasta (2) seuraa, että myös $\text{syt}(a, b, c)$ on yksikäsitteinen.

MÄÄRITELMÄ 2.8. Määritellään *kongruenssirelaatio* $\equiv \pmod p$:

$$a \equiv b \pmod p \iff a = b + kp \text{ jollakin } k \in \mathbb{Z}.$$

Kongruenssirealaatiolle käytetään myös merkintää $\equiv_p$. Jos p on selvä asiayhteydestä, voidaan $(\text{mod } p)$ jättää merkitsemättä.

LEMMA 2.9. *Kongruenssirelaatio* $\equiv_p$ *on ekvivalenssirelaatio joukossa* $\mathbb{Z}$.

TODISTUS. Todistetaan seuraavat kohdat:

(i) Refleksiivisyys: $a \equiv_p a$ kaikilla $a \in \mathbb{Z}$.
$a = a + 0 \cdot p$ kaikilla $p \in \mathbb{Z}$, siis $a \equiv_p a$.
(ii) Symmetrisyys: jos $a \equiv_p b$, niin $b \equiv_p a$ kaikilla $a, b \in \mathbb{Z}$.
Jos $a \equiv_p b$, niin $a = b + kp$ jollakin $k \in \mathbb{Z}$. Siispä $b = a - kp$ eli $b \equiv_p a$.
(iii) Transitiivisuus: jos $a \equiv_p b$ ja $b \equiv_p c$, niin $a \equiv_p c$ kaikilla $a, b, c \in \mathbb{Z}$.
Jos $a \equiv_p b$, niin $a = b + kp$ jollakin $k \in \mathbb{Z}$ ja jos $b \equiv_p c$, niin $b = c + lp$ jollakin $l \in \mathbb{Z}$. Siten $a = c + lp + kp = c + (k + l)p$ eli $a \equiv_p c$.

□

MÄÄRITELMÄ 2.10 (Pariteetti). Luvun a *pariteetti* on lukuun a liitettävä binääriarvo. Sanotaan, että luku $a \in \mathbb{Z}$ on *parillinen* ja että sen pariteetti on 0, jos $a \equiv_2 0$. Vastaavasti sanotaan, että luku a on *pariton* ja sen pariteetti on 1, jos $a \equiv_2 1$.

2.2. Tapaus $n = 4$

Todistetaan ensin Fermat'n suuri lause tapauksessa $n = 4$. Tätä tapausta pidetään yleisesti kaikista helpoimpana ja sille on olemassa lukuisia vaihtoehtoisia todistuksia, joista esitetty todistus pohjautuu jo Fermat'n aikana tiedossa olleisiin ideoihin.

LEMMA 2.11. *Olkoot* $x, y \in \mathbb{N}$. *Jos* $\text{syt}(x, y) = 1$ *ja* $xy = z^2$ *jollakin* $z \in \mathbb{N}$, *niin on olemassa luvut* $u, v \in \mathbb{N}$ *siten, että* $x = u^2$ *ja* $y = v^2$.

TODISTUS. Olkoot $x = x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n}$, $y = y_1^{j_1} \cdot y_2^{j_2} \cdots y_m^{j_m}$ ja $z = z_1^{l_1} \cdot z_2^{l_2} \cdots z_h^{l_h}$ lukujen x, y ja z alkulukuesitykset.

Koska $\text{syt}(x, y) = 1$, niin luvuilla x ja y ei ole huomautuksen 2.6 kohdan (3) nojalla yhteisiä alkulukutekijöitä. Koska alkulukuesitys on järjestystä lukuunottamatta yksikäsitteinen, on luvun xy alkulukuesitys muotoa $xy = x_1^{i_1} \cdot x_2^{i_2} \cdots x_n^{i_n} \cdot y_1^{j_1} \cdot y_2^{j_2} \cdots y_m^{j_m}$.

Nyt toisaalta $xy = z^2 = z_1^{2l_1} \cdot z_2^{2l_2} \cdots z_h^{2l_h}$ on neliöiden tulo. Alkulukuesityksen yksikäsitteisyyden nojalla tulee lukujen $x_r^{i_r}$ ja $y_s^{j_s}$ olla neliöitä, joten on olemassa luvut $u, v \in \mathbb{N}$ siten, että $x = u^2$ ja $y = v^2$.

□

LEMMA 2.12. *Olkoot* $x, y \in \mathbb{N}$. *Tällöin* $\operatorname{syt}(x, y) = 1$ *jos ja vain jos* $\operatorname{syt}(x^2, y) = 1$.

TODISTUS. Olkoot $x = x_1^{p_1} \cdot x_2^{p_2} \cdots x_n^{p_n}$ ja $y = y_1^{q_1} \cdot y_2^{q_2} \cdots y_m^{q_m}$ lukujen x ja y alkulukuesitykset. Huomautuksen 2.6 kohdan (3) nojalla $\operatorname{syt}(x, y) = 1$ on yhtäpitävää sen kanssa, ettei luvuilla x ja y ole yhteisiä alkulukutekijöitä. Kun huomataan, että luvun $x^2 = x_1^{2p_1} \cdot x_2^{2p_2} \cdots x_n^{2p_n}$ alkulukutekijät ovat samat kuin luvulla x, ei luvuilla x^2 ja y ole yhteisiä alkulukutekijöitä. Tämä on yhtäpitävää sen kanssa, että $\operatorname{syt}(x^2, y) = 1$.
□

LEMMA 2.13. *Jos* $\operatorname{syt}(x, y) = 1$, *niin* $\operatorname{syt}(x^2 + y^2, x^2 - y^2)$ *on* 1 *tai* 2.

TODISTUS. Voidaan rajoittua tutkimaan kahta tapausta:

1) x ja y ovat molemmat parittomia tai
2) luvuilla x ja y on eri pariteetti.

Tapaus 1): Havaitaan, että nyt $x^2 + y^2$ ja $x^2 - y^2$ ovat molemmat parillisia. Näin ollen $2 | \operatorname{syt}(x^2 + y^2, x^2 - y^2)$. Jos olisi $\operatorname{syt}(x^2 + y^2, x^2 - y^2) = k$, missä $k > 2$ on parillinen, niin olisi $m, n \in \mathbb{Z}$ siten, että $x^2 + y^2 = mk$ ja $x^2 - y^2 = nk$. Laskemalla nämä yhtälöt yhteen saadaan $2x^2 = (m + n)k$, josta jakamalla puolittain saadaan $x^2 = (m + n)\left(\frac{k}{2}\right)$, missä $\left(\frac{k}{2}\right) \in \mathbb{Z}$. Vastaavasti laskemalla saadaan $y^2 = (m - n)\left(\frac{k}{2}\right)$. Siispä $\operatorname{syt}(x^2, y^2) \geq \left(\frac{k}{2}\right) \geq 2$, mikä on oletuksen ja lemman 2.12 nojalla ristiriita. Tässä tapauksessa $\operatorname{syt}(x^2 + y^2, x^2 - y^2) = 2$.

Tapaus 2): Nyt havaitaan, että $x^2 + y^2$ ja $x^2 - y^2$ ovat molemmat parittomia. Toisin sanoen, $2 \nmid \operatorname{syt}(x^2 + y^2, x^2 - y^2)$. Jos olisi $\operatorname{syt}(x^2 + y^2, x^2 - y^2) = k$, missä $k > 1$ on pariton, niin olisi parittomat luvut $m, n \in \mathbb{Z}$ siten, että $x^2 + y^2 = mk$ ja $x^2 - y^2 = nk$. Edellisen kohdan laskutapaa noudattaen saadaan $x^2 = \frac{(m+n)}{2}k$, missä $\frac{(m+n)}{2} \in \mathbb{Z}$ ja vastaavasti $y^2 = \frac{(m-n)}{2}k$, missä $\frac{(m-n)}{2} \in \mathbb{Z}$. Tällöin $\operatorname{syt}(x^2, y^2) = k$, mikä on ristiriita kuten edellä. Tässä tapauksessa $\operatorname{syt}(x^2 + y^2, x^2 - y^2) = 1$.

□

MÄÄRITELMÄ 2.14. Lukukolmikko $(a, b, c) \in \mathbb{N}^3$ on *Pythagoraan kolmikko*, jos se toteuttaa *Pythagoraan ehdon*

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

$\operatorname{syt}(a, b, c) = 1$ ja b on parillinen.

LAUSE 2.15. *Jokainen Pythagoraan kolmikko voidaan esittää lukukolmikkona* $(d^2 - e^2, 2de, d^2 + e^2)$, *jossa* $d, e \in \mathbb{N}$ *siten, että* $d > e$, $\operatorname{syt}(d, e) = 1$ *ja toinen luvuista d,e on parillinen.*

TODISTUS. Olkoon $(a,b,c) \in \mathbb{N}^3$ Pythagoraan kolmikko. Koska kolmikon jäsenet a ja c ovat parittomia ja $c > a$, ovat $c-a$ ja $c+a$ parillisia ja aidosti positiivisia. Näin ollen on voimassa

$$f := \frac{c+a}{2} \in \mathbb{N} \quad \text{ja} \quad g := \frac{c-a}{2} \in \mathbb{N}.$$

Jos valitaan luku $p \in \mathbb{N}$ siten, että $p|f$ ja $p|g$, niin $p|(f+g)$ ja $p|(f-g)$. Tästä seuraa, että $p|a$ ja $p|c$. Koska $\text{syt}(a,b,c) = 1$ ja $a^2+b^2 = c^2$, niin on oltava $\text{syt}(a,c) = 1$. Jos näet olisi $\text{syt}(a,c) = k > 1$, niin olisi $b^2 = (nk)^2 - (mk)^2 = (n^2-m^2)k^2$, missä k on lukujen a ja c tekijä ja $m,n \in \mathbb{N}$. Tällöin olisi $\text{syt}(a,b,c) = k$. Niinpä täytyy olla $p = 1$, mistä seuraa, että $\text{syt}(f,g) = 1$. Huomataan myös, että $fg = \frac{c-a}{2} \cdot \frac{c+a}{2} = \frac{c^2-a^2}{4} = \frac{b^2}{4} = (\frac{b}{2})^2$. Koska b on parillinen, niin $\frac{b}{2} \in \mathbb{N}$. Siten luku fg on neliö ja koska $\text{syt}(f,g) = 1$, ovat luvut f ja g lemman 2.11 nojalla neliöitä. On siis olemassa luvut $d,e \in \mathbb{N}$ siten, että $d^2 = f = \frac{c+a}{2}$ ja $e^2 = g = \frac{c-a}{2}$. Näille luvuille d ja e pätee

(1) $d^2 - e^2 = \frac{c+a}{2} - \frac{c-a}{2} = a$,
(2) $2de = 2\sqrt{fg} = 2\sqrt{\frac{c+a}{2} \cdot \frac{c-a}{2}} = 2\sqrt{\frac{b^2}{4}} = b$ ja
(3) $d^2 + e^2 = \frac{c+a}{2} + \frac{c-a}{2} = c$.

Nyt toinen luvuista d, e on parillinen, koska luku c on pariton ja sille pätee $c = d^2 + e^2$. Myös ehto $d > e$ pätee, sillä $f > g$. Koska $\text{syt}(f,g) = \text{syt}(d^2,e^2) = 1$, niin lemman 2.12 mukaan $\text{syt}(d,e^2) = 1$ ja tämän myötä myös $\text{syt}(d,e) = 1$. Siten ehtojen (1)-(3) perusteella d ja e ovat haluttua muotoa.

□

LAUSE 2.16. *Yhtälöllä $x^4 - y^4 = z^2$ ei ole nollasta poikkeavia kokonaislukuratkaisuja.*

TODISTUS. Antiteesi: Olkoon (x,y,z) kolmikko positiivisia kokonaislukuja, joille $x^4 - y^4 = z^2$ ja jossa x on pienin mahdollinen. Nyt $\text{syt}(x,y) = 1$, sillä jos alkuluku p jakaisi luvut x,y, tällöin $p^4|z^2$, joten $p^2|z$. Valitsemalla $x = px'$, $y = py'$, $z = p^2z'$ saadaan $(x')^4 - (y')^4 = (z')^2$, jolloin $0 < x' < x$, mikä on ristiriidassa antiteesin kanssa.

Nyt on voimassa $z^2 = x^4 - y^4 = (x^2+y^2)(x^2-y^2)$ ja koska $\text{syt}(x,y) = 1$, niin $\text{syt}(x^2+y^2, x^2-y^2)$ on Lemman 2.12 nojalla joko 1 tai 2. Tarkastellaan erikseen näitä kahta tapausta.

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

Koska lukujen x^2+y^2 ja x^2-y^2 tulo on neliö, ovat molemmat luvuista x^2+y^2, x^2-y^2 neliöitä Lemman 2.11 nojalla. Tarkemmin sanottuna on olemassa $s,t \in \mathbb{N}$, joille $\text{syt}(s,t) = 1$, siten että $x^2+y^2 = s^2$ ja $x^2-y^2 = t^2$. Tästä seuraa, että lukujen s ja t täytyy olla parittomia; koska on voimassa $2x^2 = s^2+t^2$, luvuilla s,t on sama pariteetti ja koska $\text{syt}(s,t) = 1$ ne eivät voi molemmat olla parillisia.

Niinpä on olemassa $u,v \in \mathbb{N}$, joille $u = (s+t)/2$ ja $v = (s-t)/2$ ja välttämättä $\text{syt}(u,v) = 1$, sillä s ja t ovat parittomia ja $\text{syt}(s,t) = 1$ (todistus vastaavasti kuin lemmalle 2.13). Nyt $uv = (s^2-t^2)/4 = y^2/2$, joten $y^2 = 2uv$. Koska $\text{syt}(u,v) = 1$, on

olemassa $l, m \in \mathbb{N}$ siten, että $u = 2l^2$ ja $v = m^2$ tai $u = l^2$ ja $v = 2m^2$. Tarkastellaan näistä ainoastaan ensimmäistä vaihtoehtoa, sillä tapaukset vastaavat toisiaan.

Nyt siis u on parillinen, $\text{syt}(u, v, x) = 1$ ja $u^2 + v^2 = \frac{(s+t)^2+(s-t)^2}{4} = \frac{s^2+t^2}{2} = x^2$. Lauseesta 2.15 seuraa, että on olemassa $a, b \in \mathbb{N}$, $0 < b < a$, $\text{syt}(a, b) = 1$ siten, että $2l^2 = u = 2ab$, $m^2 = v = a^2 - b^2$ ja $x = a^2 + b^2$. Tästä seuraa, että $l^2 = ab$. Siispä löydetään $c, d \in \mathbb{N}$, $\text{syt}(c, d) = 1$ siten, että $a = c^2$ ja $b = d^2$, joten $m^2 = c^4 - d^4$. Nyt havaitaan, että on voimassa $0 < c < a < x$ ja lukukolmikko (c, d, m) on yhtälön ratkaisu, mikä on ristiriita sen kanssa, että x on pienin mahdollinen.

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

Nyt x, y ovat parittomia ja z on parillinen. Lauseen 2.15 perusteella löydetään luvut $a, b \in \mathbb{N}$ siten, että $0 < b < a$, $\text{syt}(a, b) = 1$ ja näille luvuille on voimassa $x^2 = a^2 + b^2$, $y^2 = a^2 - b^2$ sekä $z = 2ab$.

Siispä $x^2y^2 = a^4 - b^4$ ja $0 < a < x$, mikä on ristiriita sen kanssa, että x on pienin mahdollinen.

□

Esimerkki 2.17. Olkoon A suorakulmainen kolmio, jonka kateetit ovat pituudeltaan a, b ja hypotenuusa c siten, että $a, b, c \in \mathbb{N}$. Tällöin kolmion A pinta-ala ei ole kokonaisluvun neliö.

Todistus. Olkoot a, b, c suorakulmaisen kolmion sivuja, joista c on hypotenuusa. Pythagoraan lause on siis voimassa eli kolmion sivuille pätee yhtälö $c^2 = a^2 + b^2$. Muodostetaan antiteesi, jonka mukaan kolmion pinta-ala on kokonaisluvun s neliö eli on voimassa yhtälö $ab/2 = s^2$. Nyt siis

$$\begin{cases} (a+b)^2 = c^2 + 4s^2, \\ (a-b)^2 = c^2 - 4s^2. \end{cases}$$

Edellisten yhtälöiden tuloa tarkastellessa huomataan, että

$$\begin{aligned} (a+b)^2(a-b)^2 &= (c^2 + 4s^2)(c^2 - 4s^2) \\ a^4 - 2a^2b^2 + b^4 &= c^4 - 16s^4 \\ (a^2 - b^2)^2 &= c^4 - (2s)^4. \end{aligned}$$

Koska tämä yhtälö on muotoa $x^4 - y^4 = z^2$, ei sillä lauseen 2.16 nojalla ole kokonaislukuratkaisuja. Tämä on ristiriita antiteesin kanssa, joten alkuperäinen väite pätee.

□

Lause 2.18. *Yhtälöllä $x^4 + y^4 = z^4$ ei ole nollasta eroavia kokonaislukuratkaisuja.*

TODISTUS. Jos x, y, z ovat nollasta eroavia kokonaislukuja, joille on voimassa $x^4 + y^4 = z^4$, niin $z^4 - y^4 = (x^2)^2$, mikä on ristiriita lauseen 2.16 kanssa. □

HUOMAUTUS 2.19. Myöskään muotoa $x^{4n} + y^{4n} = z^{4n}$ olevalla yhtälöllä ei ole nollasta eroavia kokonaislukuratkaisuja, sillä jos olisi, niin valitsemalla kokonaisluvut $s = x^n$, $t = y^n$ ja $u = z^n$ edellinen yhtälö on yhtäpitävää yhtälön $s^4 + t^4 = u^4$ kanssa. Tämä on ristiriita lauseen 2.18 kanssa.

Yleisemmin, jos yhtälöllä $x^n + y^n = z^n$ ei ole nollasta poikkeavia kokonaislukuratkaisuja jollakin luvulla n, niin myöskään yhtälöllä $x^{kn} + y^{kn} = z^{kn}$ ei ole ratkaisuja millään luonnollisella luvulla k. Jos nimittäin valitaan kokonaisluvut $s = x^k$, $t = y^k$ ja $u = z^k$ vastaavaan tapaan kuin edellä, on edellinen yhtälö yhtäpitävää yhtälön $s^n + t^n + u^n$ kanssa, eikä tätä muotoa olevalle yhtälölle ole oletuksen mukaan ratkaisua.

2.3. Tapaus $n = 3$

Fermat'n suuri lause saadaan todistettua myös tapauksessa $n = 3$ pääpiirteittäin melko vaivattomasti. Yksi todistuksessa otettava askel vaatii kuitenkin myöhemmin todistettavan Lemman 2.35 käyttämistä, mikä tekee tapauksesta lopulta huomattavasti edellistä monimutkaisemman.

LEMMA 2.20. *Olkoot $a, b \in \mathbb{Z}$ siten, että* $\operatorname{syt}(a+b, a-b) = 1$. *Tällöin* $\operatorname{syt}(a, b) = 1$.

TODISTUS. Tehdään antiteesi: $\operatorname{syt}(a, b) = k \geq 2$ jollakin $k \in \mathbb{Z}$. Tällöin $a = mk$ ja $b = nk$ joillakin $m, n \in \mathbb{Z}$. Nyt

$$\begin{cases} a + b &= mk + nk &= (m + n)k \\ a - b &= mk - nk &= (m - n)k, \end{cases}$$

mikä on ristiriita oletuksen kanssa. □

LAUSE 2.21. *Yhtälöllä $x^3 + y^3 + z^3 = 0$ ei ole nollasta poikkeavia kokonaislukuratkaisuja.*

TODISTUS. Olkoot luvut x, y, z nollasta eroavia siten, että näistä luvuista muodostetut lukuparit (x, y), (x, z) sekä (y, z) ovat jokainen keskenään jaottomia ja että luvuille on voimassa yhtälö $x^3 + y^3 + z^3 = 0$. Luvut eivät voi olla samoja, koska muuten olisi $2x^3 = z^3$, mikä on mahdotonta, koska luku 2 ei ole kuutio. Lisäksi täsmälleen yhden luvuista on oltava parillinen. Valitaan luvut siten, että x, y ovat parittomia ja z on parillinen. Valitaan nyt yhtälön kaikista edellämainitut ominaisuudet omaavista ratkaisuista sellainen, jossa $|z|$ on pienin.

Pyritään seuraavaksi löytämään nollasta poikkeavat ja kaikkien lukuparien osalta keskenään jaottomat kokonaisluvut l, m, n, joille $l^3 + m^3 + n^3 = 0$, n on parillinen ja $|z| > |n|$, mikä olisi ristiriita luvun $|z|$ valinnan kanssa. Koska luvut $x + y$ ja $x - y$ ovat parittomien lukujen erotuksina parillisia, on olemassa kokonaisluvut $a, b \neq 0$ siten, että $2a = x + y$ ja $2b = x - y$. Kun jaetaan edellä mainitut yhtälöt kahdella ja muodostetaan näiden summa sekä erotus, saadaan yhtälöt muotoihin $x = a + b$ ja $y = a - b$. Koska luvut x ja y ovat keskenään jaottomia, on myös luvuilla a, b eri

pariteetti ja lemman 2.20 nojalla $\text{syt}(a, b) = 1$.

Edellisen perusteella on siis voimassa yhtälö

$$-z^3 = x^3 + y^3 = (a + b)^3 + (a - b)^3 = 2a(a^2 + 3b^2).$$

Kuitenkin $a^2 + 3b^2$ on pariton, koska luvuilla a, b on eri pariteetti, ja z on oletuksen nojalla parillinen. Niinpä on voimassa $8|z^3$ ja koska tämän seurauksena myös $8|2a$, täytyy luvun b olla pariton. Nyt $\text{syt}(2a, a^2 + 3b^2)$ voi olla joko 1 tai 3, sillä jos p on alkuluku, $k \geq 1$ ja p^k jakaa luvut $2a$ ja $a^2 + 3b^2$, niin $p \neq 2$. Siis p^k jakaa luvut a ja $3b^2$, mutta p ei jaa lukua b, joten täytyy olla $k = 1$ ja $p = 3$.

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

Nyt luku 3 ei jaa lukua a. Koska luvuilla a, b on eri pariteetti, seuraa yhtälöstä $-z^3 = 2a(a^2 + 3b^2)$, että luvut $2a$ ja $a^2 + 3b^2$ ovat kuutioita. On siis olemassa luvut s, r siten, että

$$\begin{cases} 2a = r^3, \\ a^2 + 3b^2 = s^3, \end{cases}$$

missä s on pariton ja s ei ole luvun 3 monikerta. Tässä vaiheessa hyödynnetään myöhemmin todistettavaa tulosta (Lemma 2.35): jos s on pariton, $s^3 = a^2 + 3b^2$ ja $\text{syt}(a, b) = 1$, niin luvun s täytyy myös olla muotoa $s = u^2 + 3v^2$ joillakin $u, v \in \mathbb{Z}$, joille

$$\begin{cases} a = u(u^2 - 9v^2), \\ b = 3v(u^2 - v^2). \end{cases}$$

Nyt v on pariton ja u on parillinen, koska b on pariton, $u \neq 0$, luku 3 ei jaa lukua u, koska 3 ei jaa lukua a ja $\text{syt}(u, v) = 1$. Näin ollen $2u, u + 3v, u - 3v$ ovat keskenään jaottomia lukupareittain ja koska $r^3 = 2a = 2u(u - 3v)(u + 3v)$, niin $2u$, $u - 3v$ ja $u + 3v$ ovat kuutioita:

$$\begin{cases} 2u = -n^3, \\ u - 3v = l^3, \\ u + 3v = m^3, \end{cases}$$

missä l, m, n ovat nollasta eroavia, koska 3 ei jaa lukua u, ja lukupareittain keskenään jaottomia.

Edellisen perusteella siis $l^3 + m^3 + n^3 = 0$ ja n on parillinen. Näytetään seuraavaksi, että $|z| > |n|$. Itse asiassa nyt on voimassa

$$|z|^3 = |2a(a^2 + 3b^2)| = |n^3(u^2 - 9v^2)(a^2 + 3b^2)| \geq 3|n^3| > |n^3|,$$

koska $u^2 - 9v^2 = l^3m^3 \neq 0$ ja $b \neq 0$ (koska b on pariton). Tämä on ristiriita, sillä luvun $|z|$ piti olla pienin mahdollinen parillinen luku ratkaisukolmikossa.

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

Merkitään $a = 3c$. Näin ollen c on parillinen ja $4 \mid c$, kun taas $3 \nmid b$ (koska a, b ovat keskenään jaottomia). Nyt $-z^3 = 6c(9c^2 + 3b^2) = 18c(3c^2 + b^2)$, missä $\text{syt}(18c, 3c^2 + b^2) = 1$. Niinpä c on parillinen ja b on pariton, minkä vuoksi $3c^2 + b^2$ on pariton, $3 \nmid 3c^2 + b^2$ ja $\text{syt}(b, c) = 1$. Koska näillä luvuilla on eri pariteetti, ovat $18c$ ja $3c^2 + b^2$ kuutioita. On siis olemassa luvut s, r siten, että

$$\begin{cases} 18c = r^3, \\ 3c^2 + b^2 = s^3, \end{cases}$$

missä s on pariton ja $3 \mid r$. Koska s on pariton, $s^3 = b^2 + 3c^2$ ja $\text{syt}(b, c) = 1$, voidaan hyödyntää samaa tulosta kuin aiemmin (Lemma 2.35) ja täten luvun s täytyy olla muotoa $s = u^2 + 3v^2$ joillakin $u, v \in \mathbb{Z}$, joille

$$\begin{cases} b = u(u^2 - 9v^2), \\ c = 3v(u^2 - v^2). \end{cases}$$

Nyt u on pariton, v on parillinen, koska b on pariton, $v \neq 0$ ja $\text{syt}(u, v) = 1$. Havaitaan myös, että $2v, u+v, u-v$ ovat keskenään jaottomia lukupareittain. Yhtälöstä $r^3 = 18c = 54v(u + v)(u - v)$ voidaan huomata, että $(r/3)^3 = 2v(u + v)(u - v)$ ja niinpä $2v, u + v, u - v$ ovat kolmansia potensseja:

$$\begin{cases} 2v = -n^3 \\ u + v = l^3 \\ u - v = -m^3 \end{cases}$$

Siispä $l^3 + m^3 + n^3 = 0$, $l, m, n \neq 0$ ja n on parillinen. Näytetään seuraavaksi, että $|z| > |n|$. Itse asiassa nyt on voimassa

$$\begin{aligned} |z|^3 &= 18|c|(3c^2 + b^2) \\ &= 54|v(u^2 - v^2)|(3c^2 + b^2) \\ &= 27|n|^3|u^2 - v^2|(3c^2 + b^2) \\ &> |n|^3 \end{aligned}$$

koska $u^2 - v^2 = -l^3m^3 \neq 0$ ja $|3c^2 + b^2| \geq 1$. Tämä on ristiriita, sillä luvun $|z|$ piti olla pienin mahdollinen parillinen luku ratkaisukolmikossa. □

Perustellaan vielä lauseketta $s = u^2 + 3v^2$ koskeva askel edellisestä todistuksesta. Käytetään tähän tarkoitukseen jo Fermat'n aikaan tiedossa olleita tuloksia, jotka koskevat muotoa $u^2 + v^2$ olevia kokonaislukuja. Olkoon $\mathbb{S}$ muotoa $a^2 + 3b^2$, $a, b \in \mathbb{Z}$ olevien kokonaislukujen joukko. Joukko $\mathbb{S}$ on kertolaskun suhteen suljettu, koska

$(a^2 + 3b^2)(c^2 + 3d^2) = a^2c^2 + 3a^2d^2 + 3b^2c^2 + 9b^2d^2 = (ac \pm 3bd)^2 + 3(ad \mp bc)^2$ (merkit vastaavassa järjestyksessä).

MÄÄRITELMÄ 2.22 (Neliönjäännös). Olkoon p pariton alkuluku ja $a \in \mathbb{Z}$ siten, että p ei jaa lukua a. Sanotaan, että luku a on *neliönjäännös modulo p*, jos on olemassa kokonaisluku x, jolle

$$x^2 \equiv a \pmod{p}.$$

Muussa tapauksessa lukua a sanotaan *neliönepäjäännökseksi*.

ESIMERKKI 2.23. Tutkitaan tapauksia $p = 5$ ja $p = 7$.

x	1	2	3	4	5	6
x^2	1	4	9	16	25	36
$x^2 \equiv_5$	1	4	4	1	0	1
$x^2 \equiv_7$	1	4	2	2	4	1

Tästä huomataan, että 1 ja 4 ovat neliönjäännöksiä (mod 5) ja vastaavasti 1, 4, 2 ovat neliönjäännöksiä (mod 7).

MÄÄRITELMÄ 2.24 (Legendren symboli). Olkoon p pariton alkuluku ja olkoon $a \in \mathbb{Z}$ siten, että p ei jaa lukua a. Määritellään *Legendren symboli* asettamalla:

$$\left(\frac{a}{p}\right) = \begin{cases} 1, & \text{jos } a \text{ on neliönjäännös mod } p \\ -1, & \text{jos } a \text{ on neliönepäjäännös mod } p. \end{cases}$$

ESIMERKKI 2.25. Tutkitaan edelleen tapauksia $p = 5$ ja $p = 7$. Edellisen esimerkin mukaisesti

x	1	2	3	4	5	6
$\left(\frac{x}{5}\right)$	1	-1	-1	1	-1	1
$\left(\frac{x}{7}\right)$	1	1	-1	1	-1	-1

.

LAUSE 2.26 (Gaussin resiprookkilaki). *Olkoot p ja q erisuuria parittomia alkulukuja. Tällöin*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

TODISTUS. Todistus luvussa 2.4. □

LEMMA 2.27. *Olkoon p alkuluku siten, että $p > 3$. Seuraavat ehdot ovat tällöin ekvivalentteja:*

(1) $p \equiv 1 \pmod{6}$.
(2) -3 *on neliö modulo* p.

TODISTUS. Osoitetaan, että kohdat (1) ja (2) ovat ekvivalentteja määrittämällä Legendren symboli Gaussin resiprookkilakia hyödyntämällä:

$$\left(\frac{p}{3}\right)\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}(-1)^{\frac{3-1}{2}} = (-1)^{\frac{p-1}{2}},$$

joten

$$\left(\frac{3}{p}\right) = \frac{(-1)^{\frac{p-1}{2}}}{\left(\frac{p}{3}\right)}.$$

Tästä saadaan

$$\left(\frac{3}{p}\right) = (-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right),$$

kun huomataan, että $\left(\frac{p}{3}\right) = \pm 1$.

Eulerin kriteeriä 2.40 (todistus luvussa 2.4) sekä edellistä yhtälöä hyödyntämällä saadaan

$$\begin{aligned}\left(\frac{-3}{p}\right) &\equiv (-3)^{\frac{p-1}{2}} \\ &\equiv (-1)^{\frac{p-1}{2}} \cdot 3^{\frac{p-1}{2}} \\ &\equiv \left(\frac{-1}{p}\right)\left(\frac{3}{p}\right) \\ &\equiv (-1)^{\frac{p-1}{2}}(-1)^{\frac{p-1}{2}}\left(\frac{p}{3}\right) \\ &\equiv \left(\frac{p}{3}\right) \pmod p.\end{aligned}$$

Siispä $\left(\frac{-3}{p}\right) = +1$, jos ja vain jos $p \equiv 1 \pmod 3$. Tämä on yhtäpitävää sen kanssa, että $p \equiv 1 \pmod 6$, sillä

$$p \equiv 1 \pmod 3 \quad \Leftrightarrow \quad p = 3 \cdot k + 1$$

jollakin $k \in \mathbb{N}$. Kun huomataan, että p on pariton ja $p > 3$, niin on oltava $k = 2l$ jollakin $l \in \mathbb{N}$, jolloin

$$\begin{aligned}p \equiv 1 \pmod 3 &\Leftrightarrow p = 3 \cdot k + 1 \\ &\Leftrightarrow p = 3 \cdot 2 \cdot l + 1 \\ &\Leftrightarrow p \equiv 1 \pmod 6.\end{aligned}$$

□

Lemma 2.28. *Jos k on nollasta eroava kokonaisluku, p on alkuluku siten, että $p = c^2 + 3d^2 \in \mathbb{S}$ ja $pk = a^2 + 3b^2 \in \mathbb{S}$, niin $p \mid ac \pm 3bd$ ja $p \mid ad \mp bc$ (merkit vastaavassa järjestyksessä) ja*

$$k = \left(\frac{ac \pm 3bd}{p}\right)^2 + 3\left(\frac{ad \mp bc}{p}\right)^2 \in \mathbb{S}.$$

Todistus. Olkoon

$$k = \frac{(a^2 + 3b^2)(c^2 + 3d^2)}{(c^2 + 3d^2)^2} = \left(\frac{ac \pm 3bd}{c^2 + 3d^2}\right)^2 + 3\left(\frac{ad \mp bc}{c^2 + 3d^2}\right)^2.$$

Tiedetään, että $k \in \mathbb{Z}$. Lisäksi havaitaan, että

$$\begin{aligned}(ac + 3bd)(ac - 3bd) &= a^2c^2 - 9b^2d^2 \\ &= a^2(c^2 + 3d^2) - 3(a^2 + 3b^2)d^2 \\ &= a^2p - 3pkd^2 \\ &= p(a^2 - 3kd^2) \\ &= (c^2 + 3d^2)(a^2 - 3kd^2) \\ &= (a^2 - 3kd^2)(c^2 + 3d^2).\end{aligned}$$

Koska $p = c^2 + 3d^2$ on alkuluku, on voimassa joko $p|ac + 3bd$ tai $p|ac - 3bd$. Tarkastellaan tapausta $p|ac+3bd$ (tapaus $p|ac-3bd$ vastaavasti): Tällöin $(ac+3bd)/p \in \mathbb{Z}$. Koska $k \in \mathbb{Z}$, niin on oltava myös $3((ad - bc)/p)^2 \in \mathbb{Z}$ ja siten $(ad - bc)/p \in \mathbb{Z}$, joten $k \in \mathbb{S}$.

□

LEMMA 2.29. *Jos p on alkuluku, niin $p \in \mathbb{S}$, jos ja vain jos $p = 3$ tai $p \equiv 1 \pmod 3$.*

TODISTUS. Jos $p = a^2 + 3b^2$, $p \neq 3$, niin $b \neq 0$, joten $p \equiv a^2 \pmod 3$. Koska p on alkuluku, täytyy olla $2 \nmid a$ ja $3 \nmid a$ ja Siispä $p \equiv a^2 \equiv 1 \pmod 3$.

Selvästi $3 \in \mathbb{S}$. Olkoon nyt $p \equiv 1 \pmod 3$. Tällöin Lemman 2.27 mukaan $\left(\frac{-3}{p}\right) = 1$, joten on olemassa $t \in \mathbb{Z}$ siten, että $0 < t < p/2$ ja $-3 \equiv t^2 \pmod p$. Niinpä on olemassa $m \in \mathbb{Z}$ siten, että $mp = t^2 + 3 < (p/2)^2 + 3 < p^2$ eli täytyy olla $0 < m < p$. Havaitaan, että jokaiselle $t \geq 1$ on olemassa enintään yksi alkuluku $p \neq 2, 3$ siten, että $p \mid t^2 + 3$, mutta $p \nmid u^2 + 3$ kaikille u, joille $1 \leq u < t$. Osoitetaan tämä kääntei-sellä todistuksella eli väitetään, että on olemassa toisistaan eroavat alkuluvut p ja p' kuten yllä siten, että $p < p'$. Edeltävän huomion mukaan nyt täytyy olla $0 < t < p/2$ ja $t^2 + 3 = pm$ siten, että $0 < m < p$. Koska $p' \mid t^2 + 3$, niin $p' \mid m$. Tästä seuraa, että $p' \leq m < p$, mikä on ristiriita.

Nyt olemme valmiita todistamaan itse väittämän. Oletetaan, että on olemassa alkuluku p, $p \equiv 1 \pmod 3$ siten, että $p \notin \mathbb{S}$ ja valitaan näistä alkuluvuista pienin. Olkoon $t \geq 1$ pienin kokonaisluku, jolle pätee $p \mid t^2 + 3$, siten, että $0 < t < p/2$, $t^2 + 3 = mp$ ja $0 < m < p$. Jos p' olisi mikä tahansa luvun m jakava alkuluku, olisi $m = p'm'$, joten $p' \leq m' < p$ eli $p' \in \mathbb{S}$. Nyt $p'(pm') = pm = t^2 + 3 \in \mathbb{S}$ ja tämän myötä Lemman 2.28 perusteella $pm' \in \mathbb{S}$. Jos $m' = 1$, niin $p \in \mathbb{S}$, mitä pyritäänkin osoittamaan. Jos p'' on luvun m' jakava alkuluku ja $m' = p''m''$, niin $p'' \leq m' < p$, joten $p'' \in \mathbb{S}$. Näin ollen $p''(pm'') = pm' \in \mathbb{S}$ ja Lemman 2.28 nojalla $pm'' \in \mathbb{S}$, missä $m'' < m'$. Toistamalla tätä perustelua päädytään siihen, että $p \in \mathbb{S}$.

□

LEMMA 2.30. *Olkoon $m = u^2 + 3v^2$, $u, v \neq 0$ ja $\operatorname{syt}(u, v) = 1$. Jos p on pariton luvun m jakava alkuluku, niin $p \in \mathbb{S}$.*

TODISTUS. Koska $3 \in \mathbb{S}$, voidaan olettaa, että $p \neq 3$. Jos $p \mid m$, niin $p \nmid v$, sillä muuten p jakaisi myös luvun u, mikä olisi vastoin oletuksia. Olkoon v' siten, että $vv' \equiv 1 \pmod p$. Tällöin on voimassa

$$(uv')^2 \equiv u^2v'^2 \equiv (m-3v^2)v'^2 \equiv mv'^2 - 3v^2v'^2 \equiv -3 \pmod{p},$$

sillä $p \mid m$. Siispä $(uv')^2 \equiv -3 \pmod{p}$ ja siten $\left(\frac{-3}{p}\right) = 1$, joten Lemman 2.27 nojalla $p \equiv 1 \pmod 3$. Niinpä Lemman 2.29 nojalla $p \in \mathbb{S}$.

□

LEMMA 2.31. *Jos p on alkuluku ja $p \in \mathbb{S}$, niin sen esitysmuoto $p = a^2+3b^2$, missä $a \geq 0$, $b \geq 0$, on yksikäsitteinen.*

TODISTUS. Sovelletaan Lemman 2.28 tapausta $k = 1$, jolloin $p = a^2 + 3b^2 = c^2 + 3d^2$, missä $a, c \geq 0$ ja $b, d > 0$. Näin ollen

$$1 = \left(\frac{ac \pm 3bd}{p}\right)^2 + 3\left(\frac{ad \mp bc}{p}\right)^2,$$

joten $p = ac \pm 3bd, ad = \pm bc$. Nyt on siis voimassa

$$pd = acd \pm 3bd^2 = \pm bc^2 \pm 3bd^2 = \pm b(c^2 + 3d^2) = \pm bp.$$

Näin ollen $d = \pm b$, joten $b = d$ ja tämän myötä $a = c$.

□

SOPIMUS 2.32. Merkitään löysästi $\sqrt{-3}$ kun tarkoitetaan imaginäärilukua $i\sqrt{3}$.

MÄÄRITELMÄ 2.33 (Kompleksikonjugaatti). Imaginääriluvun $u + iv$ *kompleksikonjugaatti* on luku $u - iv$.

LEMMA 2.34. *Olkoon $m = 3$ tai $m = u^2 + 3v^2$, $u, v \neq 0$ ja $\operatorname{syt}(u, v) = 1$. Jos m on pariton ja $m = \prod_{i=1}^{n} p_i^{e_i}$, jossa $p_1, ..., p_n$ ovat alkulukuja ja $e_i \geq 1$, niin on olemassa kokonaisluvut a_i ja b_i, joissa $i = 1, ..., n$ siten, että $p_i = a_i^2 + 3b_i^2$ ja*

$$u + v\sqrt{-3} = \prod_{i=1}^{n}(a_i + b_i\sqrt{-3})^{e_i}.$$

TODISTUS. Todistetaan väite induktiolla luvun m suhteen. Väite on selvä, kun $m = 3$. Olkoon $m > 3$, $m = u^2 + 3v^2$, $u, v \neq 0$ ja $\operatorname{syt}(u, v) = 1$. Olkoon p luvun m jakava alkuluku, jolloin $m = pk$. Lemman 2.30 mukaan $p = a^2 + 3b^2$ ja Lemman 2.28 nojalla $k = c^2 + 3d^2$, missä $c = (ua \pm 3vb)/p$, $d = ub \mp va)/p$ vastaavin merkein. Lisäksi $(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = (ac + 3bd) \pm (bc - ad)\sqrt{-3}$, missä

$$\begin{aligned} ac + 3bd &= \tfrac{1}{p}(ua^2 \pm 3vab + 3ub^2 \mp 3vab) = u, \\ \pm(bc - ad) &= \pm\tfrac{1}{p}(ab \pm 3vb^2 - uab \pm va^2) = v, \end{aligned}$$

joten

$$(a \pm b\sqrt{-3})(c \mp d\sqrt{-3}) = u + v\sqrt{-3}.$$

Jos $k = 1$, väite on selvä. Jos $k \neq 1$, niin joko $k = 3$ tai $k \neq 3$. Jälkimmäisessä tapauksessa $c \neq 0$ (muuten $c = 0$, jolloin d jakaisi luvut u, v, jolloin $d = 1$ ja $k = 3$, mikä on vastoin oletusta); vastaavasti $d \neq 0$ (muuten $d = 0$, jolloin c jakaisi luvut u, v, jolloin $c = 1$ ja $k = 1$, mikä on vastoin oletusta). Lisäksi $\operatorname{syt}(c, d) = 1$, koska

$\text{syt}(u, v) = 1$. Siispä väite pätee luvulle k, sillä $c \mp d\sqrt{-3}$ voidaan esittää vaaditussa muodossa. Koska $(a \pm b\sqrt{3})(c \mp d\sqrt{-3}) = u + v\sqrt{-3}$, pätee väite kaikille luvuille m. □

LEMMA 2.35. *Olkoon E kaikkien sellaisten lukukolmikoiden (u, v, s) joukko, joilla s on pariton,* $\text{syt}(u, v) = 1$ *ja $s^3 = u^2 + 3v^2$. Olkoon F kaikkien sellaisten lukuparien (t, w) joukko, joilla* $\text{syt}(t, w) = 1$ *ja $t \not\equiv w \pmod 2$. Kuvaus $\Phi : F \to E$, $\Phi(t, w) = (u, v, s)$, jossa*

$$\begin{cases} u = t(t^2 - 9w^2), \\ v = 3w(t^2 - w^2), \\ s = t^2 + 3w^2, \end{cases}$$

on bijektio.

TODISTUS. Edellisen perusteella on voimassa

$$\begin{cases} u^2 = t^6 - 18t^4w^2 + 81t^2w^4, \\ 3v^2 = 27t^4w^2 - 54t^2w^4 + 27w^6, \\ s^3 = t^6 + 9t^4w^2 + 27t^2w^4 + 27w^6. \end{cases}$$

Nyt havaitaan, että

$$u^2 + 3v^2 = t^6 + 9t^4w^2 + 27t^2w^4 + 27w^6 = s^3,$$

Koska luvuilla t ja w on eri pariteetti, luku s on pariton. Näytetään seuraavaksi, että $\text{syt}(u, v) = 1$. Huomataan ensin, että $\text{syt}(t^2 - 9w^2, t^2 - w^2) = 1$, koska jos alkuluku p jakaa luvut $t^2 - 9w^2$ ja $t^2 - w^2$, se jakaa myös luvun $9t^2 - 9w^2$ ja täten myös luvun $8t^2$. Tästä seuraa, että $p = 2$, koska p ei voi jakaa lukua t, sillä $\text{syt}(t, w) = 1$. Koska luvuilla t ja w on eri pariteetti, tämä on kuitenkin mahdotonta. Oletetaan nyt, että p on alkuluku, $e \geq 1$ ja p^e jakaa luvut u, v. Tällöin luku p jakaa joko luvun t tai luvun $t^2 - 9w^2$. Jos olisi voimassa $p \mid t^2 - 9w^2$, niin tästä seuraisi, että $p \mid 3w$, sillä edellä todettiin, että p ei tällöin voi jakaa lukua $t^2 - w^2$. Siispä luku p jakaisi myös luvun $9w^2$, minkä seurauksena täytyisi luvun p joka tapauksessa jakaa luku t. Niinpä $p \nmid w(t^2 - w^2)$, joten $p = 3$. Koska $3^e \mid v$ ja $3 \mid t$, täytyy olla $e = 1$, sillä $\text{syt}(u, v) = 1$ tai 3. Jos $3 \mid u$ ja $3 \mid v$, niin $3 \mid t$, $3 \nmid w$, joten $3 \mid s$, mutta $3^2 \nmid s$. Kuitenkin $s^3 = u^2 + 3v^2$, joten $3^2 \mid s^3$, sillä $3^2 \mid s$, mikä on ristiriita. Tämä osoittaa, että $\Phi(t, w) = (u, v, s) \in E$.

Toisaalta, jos $(u, v, s) \in E$, olkoon $s^3 = \prod_{i=1}^{n} p_i^{e_i}$ alkulukuhajotelma, jossa $p_1, \ldots, p_n$ ovat erillisiä ja $e_i \geq 1$. Nyt $e_i = 3e_i'$ kaikilla i. Lemman 2.34 mukaan on olemassa $a_i, b_i \in \mathbb{Z}, i = 1, \ldots, n$ siten, että $p_i = a_i^2 + 3b_i^2$ ja

$$u + v\sqrt{-3} = \prod_{i=1}^{n} (a_i + b_i\sqrt{-3})^{e_i}.$$

Olkoot $t, w \in \mathbb{Z}$ siten, että ne toteuttavat yhtälön

$$\prod_{i=1}^{n} (a_i + b_i\sqrt{-3})^{e_i'} = t + w\sqrt{-3}$$

eli

$$u + v\sqrt{-3} = (t + w\sqrt{-3})^3.$$

Laskemalla kuutio auki saadaan

$$\begin{aligned} u + v\sqrt{-3} &= (t + w\sqrt{-3})^3 \\ &= (t^2 + 2tw\sqrt{-3} - 3w^2)(t + w\sqrt{-3}) \\ &= t^3 + 2t^2w\sqrt{-3} - 3tw^2 + t^2w\sqrt{-3} - 6tw^2 - 3w^3\sqrt{-3} \\ &= t(t^2 - 9w^2) + 3w(t^2 - w^2)\sqrt{-3} \end{aligned}$$

eli $u = t(t^2 - 9w^2)$ ja $v = 3w(t^2 - w^2)$. Vastaavasti kompleksikonjugaatille pätee $u - v\sqrt{-3} = (t - w\sqrt{-3})^3$. Nyt kertomalla $u + v\sqrt{-3}$ konjugaatillaan saadaan $s^3 = u^2 + 3v^2 = (t^2 + 3w^2)^3$, joten $s = t^2 + 3w^2$. Tästä seuraa, että luvuilla t ja w on eri pariteetti, $\text{syt}(t, w) = 1$ ja $\Phi(t, w) = (u, v, s)$.

□

Nyt kaikki vaiheet Eulerin todistuksesta (Lause 2.21) on vahvistettu lukuunottamatta Gaussin resiprookkilain todistusta, joka käsitellään erikseen seuraavassa luvussa.

2.4. Gaussin resiprookkilain todistus

MÄÄRITELMÄ 2.36. Jos kongruenssi on muotoa $ax \equiv b \pmod m$, missä x on tuntematon kokonaisluku, kutsutaan tätä *lineaariseksi kongruenssiksi yhdellä muuttujalla.*

LAUSE 2.37 (Wilsonin lause). *Jos p on alkuluku, niin* $(p-1)! \equiv -1 (\text{mod } p)$.

TODISTUS. [**8**, Lause 6.2, s. 218].

□

LAUSE 2.38 (Fermat'n pieni lause). *Jos p on alkuluku ja $p \nmid a$, niin*

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

TODISTUS. [**8**, Lause 6.3, s. 219].

□

LEMMA 2.39. *Olkoot a ja m kokonaislukuja siten, että* $\text{syt}(a, m) = 1$ *ja $m > 0$ ja olkoon b kokonaisluku. Tällöin lineaarisella kongruenssilla $ax \equiv b \pmod m$ on vain yksi ratkaisu modulo m.*

TODISTUS. [**8**, Seuraus 4.11.1, s. 158].

□

LEMMA 2.40 (Eulerin kriteeri). *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että* $\text{syt}(p, a) = 1$. *Tällöin*

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

TODISTUS. Oletetaan ensin, että

$$\left(\frac{a}{p}\right) = 1.$$

Nyt kongruenssilla $x^2 \equiv a \pmod{p}$ on ratkaisu, olkoon tämä $x = x_0$. Lauseen 2.38 mukaan

$$a^{(p-1)/2} \equiv (x_0^2)^{(p-1)/2} = x_0^{(p-1)} \equiv 1 \pmod{p}.$$

Näin ollen, jos $\left(\frac{a}{p}\right) = 1$, niin täytyy olla $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

Käydään vielä läpi tilanne, jossa

$$\left(\frac{a}{p}\right) = -1.$$

Nyt kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole ratkaisuja. Lemman 2.39 mukaan, jokaiselle kokonaisluvulle i, jolle $\text{syt}(i, p) = 1$, voidaan löytää kokonaisluku j siten, että $ij \equiv a \pmod{p}$. Koska kongruenssilla $x^2 \equiv a \pmod{p}$ ei ole ratkaisuja, tiedämme, että $i \neq j$. Täten voimme ryhmitellä kokonaisluvut $1, 2, ..., p-1$ pareihin, joita on $(p-1)/2$ kappaletta ja joiden kaikkien tulona on a. Kertomalla nämä parit keskenään huomataan, että

$$(p-1)! \equiv a^{(p-1)/2} \pmod{p}.$$

Koska Lause 2.37 sanoo, että $(p-1)! \equiv -1 \pmod{p}$, niin

$$-1 \equiv a^{(p-1)/2} \pmod{p}.$$

Siispä myös tässä tapauksessa pätee $\left(\frac{a}{p}\right) \equiv a^{(p-1)/2} \pmod{p}$.

□

LEMMA 2.41 (Gaussin lemma). *Olkoon p pariton alkuluku ja olkoon a sellainen kokonaisluku, että* $\text{syt}(a, p) = 1$. *Olkoon s joukon $a, 2a, 3a, ..., \frac{p-1}{2}a$ sellaisten alkioiden lukumäärä, joiden jakojäännös modulo p on suurempi kuin $\frac{p}{2}$. Silloin $\left(\frac{a}{p}\right) = (-1)^s$*

TODISTUS. Tarkastellaan kokonaislukuja $a, 2a, ..., ((p-1)/2)a$. Olkoot $u_1, u_2, ..., u_s$ pienimmät positiiviset lukua $p/2$ suuremmat jakojäännökset ja olkoot $v_1, v_2, ..., v_t$ pienimmät positiviiset lukua $p/2$ pienemmät jakojäännökset. Koska $\text{syt}(ja, p) = 1$ kaikille kokonaisluvuille j, joille $1 \leq j \leq (p-1)/2$, nämä pienimmät positiiviset jakojäännökset ovat joukossa $1, 2, ..., p-1$.

Osoitetaan nyt, että $p-u_1, p-u_2, ...p-u_s, v_1, v_2, ..., v_t$ sisältyvät joukkoon $1, 2, ...(p-1)/2$ jossakin järjestyksessä. Tämän nähdäksemme riittää osoittaa, että mitkään kaksi näistä kokonaisluvuista eivät ole kongruentteja modulo p, sillä joukossa on täsmälleen $(p-1)/2$ jäsentä ja kaikki näistä ovat lukua $(p-1)/2$ pienempiä positiivisia kokonaislukuja.

Selvästi mitkään kaksi lukua u_i eivät ole kongurentteja modulo p ja mitkään kaksi lukua v_j eivät ole kongruentteja modulo p; jos tällaiset luvut u_i tai v_i olisivat olemassa, löydettäisiin myös lukua $(p-1)/2$ pienemmät positiiviset kokonaisluvut m ja n siten, että $ma \equiv na \pmod{p}$. Koska $p \nmid a$, seuraisi tästä, että $m \equiv n \pmod{p}$, mikä on mahdotonta.

Myöskään mikään kokonaisluvuista $p - u_i$ ei voi olla kongruentti luvulle v_j, sillä muuten olisi $ma \equiv p - na \pmod{p}$ eli $ma \equiv -na \pmod{p}$. Koska $p \nmid a$, seuraisi tästä, että $m \equiv -n \pmod{p}$. Tämä on kuitenkin mahdotonta, sillä sekä m että n kuuluvat joukkoon $1, 2, ..., (p-1)/2$.

Nyt kun tiedetään, että $p - u_1, p - u_2, \ldots, p - u_s, v_1, v_2, ..., v_t$ ovat kokonaisluvut $1, 2, ..., (p-1)/2$ jossakin järjestyksessä voidaan päätellä, että

$$(p - u_1)(p - u_2) \cdots (p - u_s)v_1v_2 \cdots v_t = (\tfrac{p-1}{2})!,$$

minkä seurauksena

$$(-1)^s u_1u_2 \cdots u_sv_1v_2 \cdots v_t \equiv (\tfrac{p-1}{2})! \pmod{p}.$$

Koska $u_1, u_2, ...u_s, v_1, v_2, ...v_t$ ovat pienimmät positiiviset jakojäännökset luvuille $a, 2a, ...((p-1)/2)a$, niin voidaan havaita myös seuraavaa

$$u_1u_2 \cdots u_sv_1v_2 \cdots v_t \equiv a \cdot 2a \cdots ((p-1)/2))a = a^{\frac{p-1}{2}}(\tfrac{p-1}{2})! \pmod{p}.$$

Nyt edellisten kohtien pohjalta saadaan

$$(-1)^s a^{\frac{p-1}{2}}(\tfrac{p-1}{2})! \equiv (\tfrac{p-1}{2})! \pmod{p}.$$

Koska $\text{syt}(p, ((p-1)/2)!) = 1$, niin edellisestä kongruenssista seuraa, että

$$(-1)^s a^{\frac{p-1}{2}} \equiv 1 \pmod{p}.$$

Kertomalla yhtälön molemmat puolet luvulla $(-1)^s$ saadaan

$$a^{\frac{p-1}{2}} \equiv (-1)^s \pmod{p}.$$

Lauseen 2.40 mukaan $a^{\frac{p-1}{2}} \equiv \left(\frac{a}{p}\right) \pmod{p}$, joten

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

minkä myötä todistus on valmis.

□

MÄÄRITELMÄ 2.42. Määritellään luvun $x \in \mathbb{R}$ *kokonaisosa* $[x]$ asettamalla

$$[x] = \max\{z : z \leq x, z \in \mathbb{Z}\}.$$

LEMMA 2.43. *Jos p on pariton alkuluku ja a on pariton kokonaisluku, jolle $p \nmid a$, niin*

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)},$$

missä

$$T(a,p) = \sum_{j=1}^{(p-1)/2} [ja/p].$$

TODISTUS. Tarkastellaan pienintä positiivista jakojäännöstä kokonaisluvuista a, $2a$, ..., $((p-1)/2)a$. Olkoon u_1, u_2 , ..., u_s suurempia kuin $p/2$ ja olkoon v_1, v_2 , ..., v_t pienempiä kuin $p/2$. Jakoalgoritmin mukaan

$$ja = p[ja/p] + \text{jakojäännös},$$

missä jakojäännös on yksi luvuista u_j tai luvuista v_j. Tätä käyttämällä voidaan muodostaa $(p-1)/2$ kappaletta yhtälöitä. Laskemalla näiden yhtälöiden summa, huomataan, että

$$\sum_{j=1}^{(p-1)/2} ja = \sum_{j=1}^{(p-1)/2} p[ja/p] + \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{2.1}$$

Kuten Gaussin lemman todistuksessa näytettiin, kattavat kokonaisluvut $p-u_1$, ..., $p-u_s$, v_1, ...v_t täsmälleen kokonaisluvut 1, 2, ..., $(p-1)/2$ jossakin järjestyksessä. Näin ollen laskemalla kaikkien näiden kokonaislukujen summa, saadaan

$$\sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{s}(p-u_j) + \sum_{j=1}^{t} v_j = ps - \sum_{j=1}^{s} u_j + \sum_{j=1}^{t} v_j. \tag{2.2}$$

Vähentämällä yhtälöstä (2.1) yhtälö (2.2) saadaan

$$\sum_{j=1}^{(p-1)/2} ja - \sum_{j=1}^{(p-1)/2} j = \sum_{j=1}^{(p-1)/2} p[ja/p] - ps + 2\sum_{j=1}^{s} u_j.$$

Toisaalta koska

$$T(a,p) = \sum_{j=1}^{(p-1)/2} [ja/p],$$

niin

$$(a-1)\sum_{j=1}^{(p-1)/2} j = pT(a,p) - ps + 2\sum_{j=1}^{s} u_j.$$

Koska a on pariton, voidaan rajoittua tarkastelemaan erotuksen $pT(a,p) - ps$ pariteettia. Edelleen, koska p on pariton, voidaan rajoittua tarkastelemaan erotusta $T(a,p) - s$. Edellisestä yhtälöstä saadaan näin

$$0 \equiv T(a,p) - s \pmod 2.$$

Siispä

$$T(a,p) \equiv s \pmod 2.$$

Nyt huomataan Gaussin lemman avulla, että

$$\left(\frac{a}{p}\right) = (-1)^s.$$

Koska $(-1)^s = (-1)^{T(a,p)}$, seuraa tästä, että

$$\left(\frac{a}{p}\right) = (-1)^{T(a,p)}.$$

□

Lemmaa 2.43 käytetään etupäässä työkaluna Gaussin resiprookkilain todistamiseen, mutta sen avulla voidaan myös laskea arvoja Legendren symboleille:

Esimerkki 2.44. Laskeaksemme $\left(\frac{7}{13}\right)$ lemmaa 2.43 käyttäen muodostetaan summa

$$\begin{aligned}\sum_{j=1}^{6}[7j/13] &= [7/13] + [14/13] + [21/13] + [28/13] + [35/13] + [42/13] \\ &= 0 + 1 + 1 + 2 + 2 + 3 = 9.\end{aligned}$$

Siispä $\left(\frac{7}{13}\right) = (-1)^9 = -1$.

Vastaavasti selvittääksemme $\left(\frac{13}{7}\right)$ muodostetaan summa

$$\begin{aligned}\sum_{j=1}^{3}[13j/7] &= [13/7] + [26/7] + [39/7] \\ &= 1 + 3 + 5 = 9.\end{aligned}$$

Näin ollen myös $\left(\frac{13}{7}\right) = (-1)^9 = -1$.

Ennen Gaussin resiprookkilain todistamista käydään läpi vielä yksi esimerkki, jossa havainnollistetaan todistuksessa käytettävää metodia:

Esimerkki 2.45. Olkoot $p = 7$ ja $q = 13$. Tutkitaan kokonaislukupareja (x, y), joille $1 \leq x \leq (7-1)/2 = 3$ ja $1 \leq y \leq (13-1)/2 = 6$. Näitä pareja on yhteensä 18 kappaletta. Huomataan, ettei mikään näistä kokonaislukupareista toteuta yhtälöä $13x = 7y$, sillä jos näin olisi, niin $13 \mid 7y$, mutta selvästi $13 \nmid 7$ ja toisaalta $13 \nmid y$, koska $1 \leq y \leq 6$.

Jaetaan nyt nämä 18 kokonaislukuparia kahteen ryhmään riippujen lukujen $13x$ ja $7y$ suhteellisesta koosta kuvan 2.1 mukaisesti.

Kokonaislukuparit (x, y), joille $1 \leq x \leq 3$, $1 \leq y \leq 6$ ja $13x > 7y$ ovat täsmälleen ne parit, joille $1 \leq x \leq 3$ ja $1 \leq y \leq 13x/7$. Kiinteälle kokonaisluvulle x, jolle $1 \leq x \leq 3$, on siis olemassa $[13x/7]$ mahdollista luvun y arvoa. Näin ollen ehdot $1 \leq x \leq 3$, $1 \leq y \leq 6$ ja $13x > 7y$ täyttäviä kokonaislukupareja on täsmälleen

$$\begin{aligned}\sum_{j=1}^{3}[13j/7] &= [13/7]+[26/7]+[39/7]\\ &= 1+3+5=9 \text{ kappaletta.}\end{aligned}$$

Nämä yhdeksän paria ovat $(1,1)$, $(2,1)$, $(2,2)$, $(2,3)$, $(3,1)$, $(3,2)$, $(3,3)$, $(3,4)$ ja $(3,5)$.

Vastaavasti kokonaislukuparit (x,y), joille $1\le x\le 3$, $1\le y\le 6$ ja $13x<7y$ ovat täsmälleen ne parit, joille $1\le y\le 6$ ja $1\le x\le 7y/13$. Kiinteälle kokonaisluvulle y, jolle $1\le y\le 6$, on siis olemassa $[7y/13]$ mahdollista luvun x arvoa. Näin ollen ehdot $1\le x\le 3$, $1\le y\le 6$ ja $13x<7y$ täyttäviä kokonaislukupareja on täsmälleen

$$\begin{aligned}\sum_{j=1}^{6}[7j/13] &= [7/13]+[14/13]+[21/13]+[28/13]+[35/13]+[42/13]\\ &= 0+1+1+2+2+3=9 \text{ kappaletta.}\end{aligned}$$

Nämä yhdeksän paria ovat $(1,2)$, $(1,3)$, $(1,4)$, $(1,5)$, $(1,6)$, $(2,4)$, $(2,5)$, $(2,6)$ ja $(3,6)$.

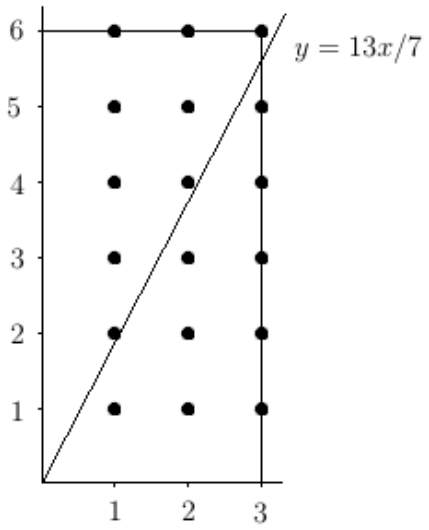
Edellisten myötä havaitaan, että

$$\frac{13-1}{2}\cdot\frac{7-1}{2}=6\cdot 3=\sum_{j=1}^{3}[13j/7]+\sum_{j=1}^{6}[7j/13]=9+9.$$

Siispä

$$(-1)^{\frac{13-1}{2}\cdot\frac{7-1}{2}}=(-1)^{\sum_{j=1}^{3}[13j/7]+\sum_{j=1}^{6}[7j/13]}=(-1)^{\sum_{j=1}^{3}[13j/7]}(-1)^{\sum_{j=1}^{6}[7j/13]}.$$

Koska lemman 2.43 mukaan



KUVA 2.1. Lasketaan hilapisteet tulon $\left(\frac{7}{13}\right)\left(\frac{13}{7}\right)$ selvittämiseksi.

$$\left(\frac{13}{7}\right) = (-1)^{\sum_{j=1}^{3}[13j/7]} \text{ ja } \left(\frac{7}{13}\right) = (-1)^{\sum_{j=1}^{6}[7j/13]},$$

niin huomataan, että

$$\left(\frac{7}{13}\right)\left(\frac{13}{7}\right) = (-1)^{\frac{7-1}{2}\cdot\frac{13-1}{2}}.$$

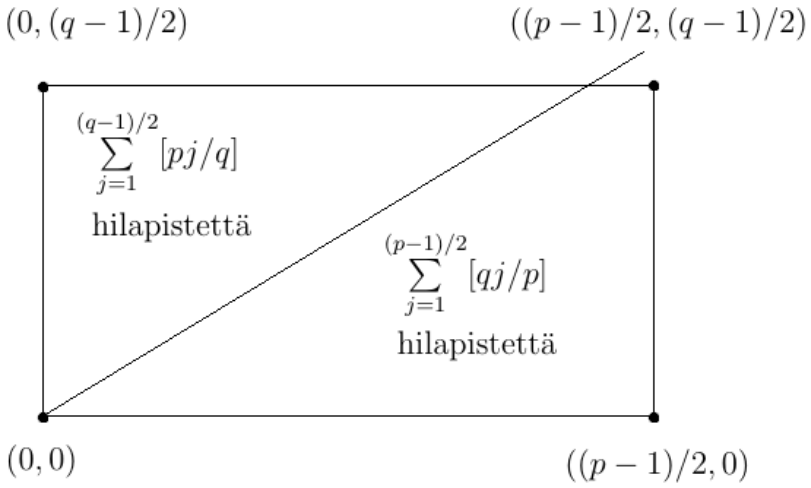
Tämä vahvistaa Gaussin resiprookkilain erikoistapauksen, jossa $p = 7$ ja $q = 13$.

Todistetaan nyt vastaavaan tapaan lause 2.26 eli:

LAUSE (Gaussin resiprookkilaki). *Olkoot p ja q erisuuria parittomia alkulukuja. Tällöin*

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2}\cdot\frac{q-1}{2}}.$$

TODISTUS. Tutkitaan kokonaislukupareja (x, y), joille $1 \leq x \leq (p-1)/2$ ja $1 \leq y \leq (q-1)/2$. Näitä pareja on olemassa yhteensä $\frac{p-1}{2} \cdot \frac{q-1}{2}$. Jaetaan nämä parit kahteen ryhmään kuten kuvassa 2.2.



KUVA 2.2. Lasketaan hilapisteet tulon $\left(\frac{p}{q}\right)\left(\frac{q}{p}\right)$ selvittämiseksi.

Huomataan, että $qx \neq py$ kaikille näille pareille, sillä jos olisi $qx = py$, niin $q \mid py$ eli joko $q \mid p$ tai $q \mid y$. Joka tapauksessa, koska luvut q ja p ovat toisistaan eroavia alkulukuja, niin $q \nmid p$ ja koska $1 \leq y \leq (q-1)/2$, niin $q \nmid y$.

Listatessamme kokonaislukupareja (x, y), joille $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$ ja $qx > py$, voidaan huomata, että nämä parit ovat täsmälleen niitä, joille $1 \leq x \leq (p-1)/2$ ja $1 \leq y \leq qx/p$. Jokaiselle määrätylle kokonaisluvun x arvolle, jolle $1 \leq x \leq (p-1)/2$, on olemassa täsmälleen $[qx/p]$ kokonaislukua, joille $1 \leq y \leq qx/p$.

Näinpä kokonaislukuparien (x, y), joille $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$ ja $qx > py$, lukumäärä on yhteensä $\sum_{j=1}^{(p-1)/2} [qj/p]$.

Tutkitaan nyt kokonaislukupareja (x, y), joille $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2$ ja $qx < py$. Nämä parit ovat täsmälleen kokonaislukuparit (x, y), joille $1 \leq y \leq (q-1)/2$ ja $1 \leq x \leq py/q$. Näin ollen, jokaiselle määritetylle kokonaisluvun y arvolle, jolle $1 \leq y \leq (q-1)/2$, on olemassa täsmälleen $[py/q]$ kokonaislukua, joille $1 \leq x \leq py/q$. Näinpä kokonaislukuparien (x, y), joille $1 \leq x \leq (p-1)/2$, $1 \leq y \leq (q-1)/2)$ ja $qx < py$ lukumäärä on yhteensä $\sum_{j=1}^{(q-1)/2} [pj/q]$.

Summaamalla näiden ryhmien kokonaislukuparien lukumäärät huomaten samalla, että näitä pareja on yhteensä $\frac{p-1}{2} \cdot \frac{q-1}{2}$, nähdään, että

$$\sum_{j=1}^{(p-1)/2} [qj/p] + \sum_{j=1}^{(q-1)/2} [pj/q] = \frac{p-1}{2} \cdot \frac{q-1}{2}$$

tai Lemman 2.43 merkinnöillä

$$T(q, p) + T(p, q) = \frac{p-1}{2} \cdot \frac{q-1}{2}.$$

Nyt on siis voimassa

$$\begin{aligned} (-1)^{T(q,p)+T(p,q)} &= (-1)^{T(q,p)}(-1)^{T(p,q)} \\ &= (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}}. \end{aligned}$$

Lemman 2.43 mukaan

$$(-1)^{T(q,p)} = \left(\frac{q}{p}\right) \text{ ja } (-1)^{T(p,q)} = \left(\frac{p}{q}\right).$$

Näin ollen

$$\left(\frac{p}{q}\right)\left(\frac{q}{p}\right) = (-1)^{\frac{p-1}{2} \cdot \frac{q-1}{2}},$$

mikä täydentää Gaussin resiprookkilain todistuksen.

□

Kirjallisuutta

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

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

[3] Coppel, W. A.: *Number Theory: An Introduction for Mathematics.* Springer, 2009.

[4] Everest, G.,Ward, T.: *An Introduction to Number Theory.* Springer, 2005.

[5] Hardy, G. H. and Wright, E. M.: *An Introduction to theory of numbers.* 6th edition, Oxford University Press, Great Britain, 2008.

[6] Hintikka, P: *Fermat'n suuri lause, salaisuus kolmen vuosisadan takaa.* Gummerus 2003

[7] Ribenhoim, P.: *Fermat's last theorem for amateurs.* toinen laitos, Springer, 1999.

[8] Rosen, K. H.: *Elementary number theory and its applications.* kuudes laitos, Pearson, 2005.

[9] Singh, S.: *Fermat'n viimeinen teoreema. (Englanninkielinen alkuteos: Fermat's Enigma. The Epic Quest to Solve the World's Greatest Mathematical Problem) Suomentanut Katriina Savolainen.* Tammi, 1998.