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

Matti Lehtinen

FERMAT'N VÄITTÄMÄ : ENTINEN HYPOTEESI VAI TULEVA TEOREEMA?

Matematiikan merkitys maailman muuttajana ja edistyksen tukipilarina on kiistaton, ja käytännön tarpeiden sanelemat matematiikan ongelmat ovat kiinnostavia ja moninaisia. Kuitenkin monen matemaatikon elämän todellisena käyttövoimana toimivat sellaiset ongelmat, joiden merkitys sisältyy niihin itseensä. Tällaisista ongelmista kiehtovimpia on jo pitkään ollut Fermat'n hypoteesi. Uutisvälineet kertoivat viime vuoden kesäkuun 23:ntena, että englantilainen matemaatikko *Andrew Wiles* on ilmeisesti todella ratkaissut Fermat'n ongelman eli todistanut, että jos x, y ja z ovat kokonaislukuja ja $n > 2$, niin yhtälöstä

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

seuraa välttämättä $xyz = 0$. Uutinen oli monelle tavallaan surullinen: yksi matemaatikon tavoite otettiin pois. Samalla tuntui hävinneen mahdollisuus esittää maallikollekin helposti selitettävä esimerkki todella vaikeasta matemaattisesta ongelmasta – esimerkiksi kuuluisan Riemannin hypoteesin ymmärtäminen vaatii paljon enemmän taustatietoa, ja neliväriongelma on jo selvitetty.

Fermat'n ongelman historia on melkein yhtä pitkä kuin itse matematiikan. Toisen ajanlaskumme alkua edeltävän vuosituhannen alkupuolella nuolenpääkirjoituksella piirretty babylonialainen savitaulu, joka nykyään tunnetaan nimellä *Plimpton 322*, sisältää systemaattisen taulukon ehdon $x^2 + y^2 = z^2$ toteuttavista kokonaisluvuista, Pythagoraan kolmikoista. Hellenistisen antiikin ajan suurin babylonialaisen aritmeettis-algebrallisen perinteen jatkaja *Diofantos* käsitteli noin v. 250 kirjoittamassaan *Arithmetica* -teoksessa mm. kokonaisluvun neliön jakamista kahdeksi rationaaliluvun neliöksi samoin kuin neliön jakamista kolmeksi neljänneksi potenssiksi.

Matematiikan kehitys ei ole ollut jatkuvaa eikä aina edistystä. Antiikin monessa suhteessa loistavat matemaattiset saavutukset unohtuivat Rooman valtakunnan ja hellenistisen kulttuurin sorruttua keskiajan alussa, ja vasta keskiajan lopulla ja renessanssin aikaan länsimainen matematiikan harrastus alkoi elpyä. Antiikin matematiikka tuli uudelleen tunnetuksi, kun klassikoiden yleensä kreikankielisiä, usein vain arabiankielisinä käännöksinä säilyneitä tekstejä käännettiin latinaksi. Suurista antiikin matemaatikoista juuri Diofantos oli viimeisiä, joita käännettiin. Ensimmäinen Diofantos-latinannos on vuodelta 1575, ja vuonna 1621 painettiin ranskalaisen *Bachet'n* laitos, jossa alkuperäisen kreikkalaisen tekstin lisäksi oli latinankielinen käännös ja kommentteja. Juuri tämä kirja on inspiroinut Fermat'n ongelman.

Pieni kirjoitus marginaalissa, suuri harppaus ihmiskunnalle

Pierre de Fermat (1601-65) ei ollut matemaatikko koulutukseltaan tai ammatiltaan – harvat noina vuosina olivatkaan. Hän oli juristi ja ilmeisen pätevä sellainen, ja matematiikka oli hänen vapaa-ajan harrastuksensa. Tunnetun kirjan *The Mathematics of Great Amateurs* tekijä *Julian Lowell Coolidge* ei kuitenkaan suostunut sisällyttämään Fermat'ta teokseensa, "koska hän on niin suuri, että häntä täytyy pitää ammattilaisena". Matemaatikkona Fermat oli todella ensi luokan nero: hän on *Descartesin* ohella analyyttisen geometrian keksijä ja hänen panoksensa matemaattisen analyysin syntyvaiheissa on merkittävä. Mutta legendan Fermat'sta tekevät hänen lukuteoreettiset havaintonsa, joista käytetyin on *Fermat'n pieni lause:* jos p on alkuluku ja a jaoton p:llä, niin $a^{p-1} - 1$ on jaollinen p:llä.

Fermat ei julkaissut tuloksiaan samoin kuin nykyajan matemaatikot. Hän kirjoitti kirjeitä ja kommentteja lukemiinsa kirjoihin. Fermat'n kommentein varustetun Bachet'n Diofantos-käännöksen julkaisi Fermat'n poika v. 1670. Sen myötä tuli julki koko joukko Fermat'n tuloksia ja myös Fermat'n hypoteesi kokonaislukujen n:nsien potenssien summista. Fermat ilmoitti löytäneensä väittämälle "ihmeellisen todistuksen, joka kuitenkin on liian pitkä kirjan marginaaliin merkittäväksi".

Ensimmäinen Fermat'n tuloksia todistellut matemaatikko oli *Euler*. Hän löysi Fermat'lta virheen: muotoa $2^{2^n} + 1$ olevat luvut eivät olekaan kaikki alkulukuja, toisin kuin Fermat oli esittänyt. Kaikki muut Fermat'n väittämät ovat osoittautuneet aikaa myöten tosiksi, paitsi kokonaislukujen *n*:nsien potenssien summaa koskeva väite. Tästä johtuu, että kyseistä hypoteesia usein nimitetään Fermat'n *viimeiseksi lauseeksi*. Nimitys on tuonut yleiseen käyttöön myös lyhenteen *FLT - Fermat's Last Theorem*.

Fermat itse todisti väittämänsä varmasti tapauksessa $n = 4$; koska todistus tapauksessa $n = 3$ on samanlainen ja Fermat kirjeissään ilmoittaa osaavansa todistaa asian, on uskominen, että tapaukset $n = 3$ ja $n = 4$ selvitti jo Fermat. Täydellisemmin nämä tapaukset käsitteli Euler.

1800-alkuun mennessä Fermat'n perintö alkoi olla perattua: vain suuri lause, nyt oikeutetusti viimeinen lause, oli avoin. Vuonna 1816 Ranskan akatemia julisti hypoteesin todistuksesta palkintokilpailun; kilpailu uusittiin vuona 1850. Ensimmäisiä yleisiä tuloksia Fermat'n ongelmasta sai eräs kaikkein ensimmäisistä naispuolisista matemaatikoista, ranskalainen *Sophie Germain*, joka todisti 1820-luvulla, että jos sekä n että $2n + 1$ ovat alkulukuja ja $x^n + y^n = z^n$, niin n on tekijänä ainakin yhdessä luvuista x, y ja z. (Sen mukaan, sallitaanko *n*:n jakaa tulo xyz vai ei, puhutaan Fermat'n hypoteesin *toisesta* ja *ensimmäisestä* tapauksesta; Germainin todistus selvitti siis osan ensimmäisestä tapauksesta.)

1800-luvun alkupuolella Fermat'n hypoteesi todistettiin tapauksissa $n = 5$ (*Peter Lejeune Dirichlet* ja *Adrien Marie Legendre*), $n = 14$ (Dirichlet), $n = 7$ (*Gustav Lamé*). Vuosina 1844-47 *Ernst Eduard Kummer* teki perustavaa tutkimusta lukukuntien parissa, tavoitteenaan ennen muuta Gaussin ja Legendren neliöiden jakojäännöksiä koskevan teorian yleistäminen. Tämän työn seurauksena Fermat'n hypoteesi tuli todistetuksi kaikille alkulukueksponenteille, jotka ovat säännöllisiä; säännöllisyys puolestaan voitiin tarkistaa ns. *Bernoullin lukujen* avulla. Osoittautui, että sataa pienemmistä alkuluvuista vain 37, 59 ja 67 ovat epäsäännöllisiä; kaikille muille Fermat'n hypoteesi on voimassa. Myöhemmin Kummer esitti mutkikkaita menetelmiä hypoteesin käsittelemiseksimyös epäsäännöllisten eksponenttien tapauksessa; hänen tulostensa perusteella Fermat'n hypoteesi tuli todistetuksi kaikilla 100:aa pienemmillä alkulukueksponenteilla. Kummer sai Ranskan Akatemian palkinnon.

Lause toteen – satatonnia käteen

Fermat'n hypoteesi on synnyttänyt toisenkin palkintokilpailun, yhä voimassa olevan. Rahat, alkuaan 100000 Saksan markkaa, palkintoon lahjoitti saksalainen lääkäri *Paul Wolfskehl* vuonna 1908, ja kilpailu jatkuu 13:nteen syyskuuta 2007, ellei todistusta sitä ennen löydy. Saksan inflaatio ja maailman mullistukset ovat syöneet Wolfskehlin palkinnon pääomaa, mutta se on edelleen 10000 Saksan markan suuruusluokkaa. Palkinnosta päättää Göttingenin tiedeakatemia. Se on vuosien mittaan joutunut ottamaan vastaan tuhansia yleensä melko alkeellisia todistusyritelmiä.

Fermat'n hypoteesin tiimoilta on myös Suomessa, Turun Yliopistossa, tehty erittäin merkittävää työtä. *Kustaa Inkerin* tulos vuodelta 1953 kertoo eksponentista riippuvan rajan, jonka yläpuolelta yhtälön mahdolliset ratkaisut löytyvät. Uusimpiin kuuluva arvio, jonka mukaan Fermat'n hypoteesi on tosi kaikilla alkulukueksponenteilla $p < 4000000$, on tutkijaryhmältä, johon kuuluvat turkulaiset *Reijo Ernvall* ja *Tauno Metsänkylä*. Yhdistettynä Inkerin arvioihin tämä merkitsee, että Fermat'n hypoteesin mahdolliset vastaesimerkit tulisivat olemaan lukuja, jotka ylittäisivät kaikki käsittelymahdollisuudet. Silti tällaisia lukuja saattaa olla olemassa.

1980-luvulta alkaen on runsaammin tutkittu Fermat'n hypoteesin yhteyksiä erilaisiin geometrisluonteisiin olettamuksiin. Merkittävä edistysaskel oli saksalaisen *Gerd Faltingsin* vuonna 1983 antama todistus ns. *Mordellin hypoteesille*, jonka mukaan varsin yleisen ehdon täyttävän rationaalikertoimisen polynomin $Q(x, y)$ määrittelemällä käyrällä $Q(x, y) = 0$ on vain äärellinen määrä rationaalilukukoordinaattisia pisteitä. Yhteys Fermat'n ongelmaan nähdään, kun tarkastellaan polynomia $Q(x, y) = x^n + y^n - 1$. Faltingsin tulos on johtanut lukuisiin tarkennuksiin, jotka ovat puristaneet mahdolliset vastaesimerkit yhä ahtaammalle. Fermat'n väittämän todistukseen ei silti tätäkään tietä ole päästy.

Wilesin todisyrityksen lähtökohta on japanilaisen *Yutaka Taniyaman* 1955 esittämä olettamus rationaalikertoimisten elliptisten käyrien ominaisuudesta, jonka yksityiskohtaisempi kuvaus on jätettävä eksperteille. Saksalainen *Gerhard Frey* havaitsi 1982, että jos $a^p + b^p = c^p$, niin elliptisellä käyrällä $y^2 = x(x - a^p)(x + b^p)$ ei ole Taniyaman oletuksen mukaista ominaisuutta. Jos siis Taniyaman olettamus on tosi, myös Fermat'n hypoteesi on tosi. Freyn alkuperäinen todistus oli aukkoinen, mutta *Jean-Pierre Serre* ja *Kenneth Ribet* täydensivät sen. Useimmat ekspertit uskovat, että Taniyaman hypoteesi on tosi. Sen todistaminen tuntui kuitenkin erittäin vaativaltatehtävältä. Andrew Wiles teki ongelman kanssa työtä kuusi vuotta, ennen kuin oli valmis ilmoittamaan onnistumisestaan. Mutta Fermat'n ongelma ei vieläkään ole luovuttanut. Wilesin todistuksesssa on puute, jota ei tätä kirjoitettaessa - tasan vuosi Wilesin ilmoituksen jälkeen - vielä ole saatu korjatuksi. Jännitys ikivanhan ongelman ympärillä jatkuu. Ja yleinen menetelmä kokonaislukuyhtälöiden ratkaisemiseksi odottaa keksimistään. Vuosisatamme lukuteorian suurmiehen, *André Weilin* sanoin: "Fermat'n hypoteesin todistaminen muistuttaa Mount Everestille kiipeämistä. Mies, joka yrittää Everestille mutta jää sadan metrin päähän huipusta, ei ole kiivennyt Everestille."