TAMPEREEN YLIOPISTO

Luonnontieteiden kandidaatin tutkielma

Jori Mäntysalo

Pythagoraan kolmikot ja Fermat'n suuri lause eksponentille 4

Informaatiotieteiden yksikkö

Matematiikka

Lokakuu 2011

Sisältö

1 Johdanto **3**

2 Todistuksen kulku pääpiirteittäin **3**

3 Pythagoraan kolmikot **4**

3.1 Määritelmät 4

3.2 Jakamattomien kolmikoiden ominaisuuksista 4

3.3 Eukleideen kaava 5

4 Päätodistus **6**

5 Hieman historiaa **7**

5.1 Erikoistapausten todistaminen 8

5.2 Yleinen todistus 9

Viitteet **10**

1 Johdanto

On olemassa äärettömän monta positiivisten kokonaislukujen kolmikkoa (a, b, c), joille pätee $a^2 + b^2 = c^2$; esimerkiksi $(12, 5, 13)$. Luonteva jatkokysymys kuuluu, onko vastaavia kolmikkoja, jos eksponentti ei ole 2 vaan jokin suurempi luku. Fermat'n suuri lause väittää, että sellaisia ei ole.

Fermat itse väitti keksineensä todistuksen vuonna 1637, mutta sellaista ei hänen jäämistöstään löydetty. Lauseen todisti lopulta Andrew Wiles vuonna 1995, siis yli 350 vuotta sen esittämisen jälkeen.

Ennen yleistä todistusta useille eksponentin arvoille oli laadittu erikoistapausta koskevia todistuksia. Helpoin ja ainoa aivan alkeellisin menetelmin käsiteltävissä oleva koskee eksponentin arvoa 4. Tämä erikoistapaus käydään läpi tässä tutkielmassa.

Formaalisti sanoen tässä työssä siis todistetaan seuraava:

$$\nexists a, b, c \in \mathbb{Z}_+ : a^4 + b^4 = c^4.$$

Tässä esitettävä todistus noudattaa Gottfried Leibnizin todistusta vuodelta 1678. Päälähteenä on L.J. Mordellin Three Lectures on Fermat's Last Theorem.

Matemaattisen sisällön jälkeen tutkielmassa kerrotaan hieman Fermat'n suuren lauseen historiaa.

2 Todistuksen kulku pääpiirteittäin

Päätodistus käyttää *äärettömän laskeutumisen periaatetta*. Aputulokset koskevat *jaottomia Pythagoraan kolmikkoja* ja niiden generointia.

Oletetaan, että jokaisella luonnollisella luvulla n_0 on ominaisuus P. Oletetaan edelleen, että voidaan todistaa $P(n_0) \Rightarrow P(n_1)$, jossa n_1 on jokin lukua n_0 pienempi luonnollinen luku.

Tällöin menettelyä voidaan toistaa: $P(n_i) \Rightarrow P(n_{i+1})$ ja kukin n_{i+1} on pienempi kuin n_i. Luonnolliset luvut eivät voi loputtomasti pienentyä. Näin

päädytään ristiriitaan, ja ominaisuutta P ei voi olla millään luonnollisella luvulla. Tämä on äärettömän laskeutumisen periaate.

Todistuksessa määritellään ensin *jaoton Pythagoraan kolmikko*. Tämän jälkeen todistetaan kaava, joka tuottaa kaikki tällaiset kolmikot.

Varsinainen todistus perustuu yllä kuvattuun äärettömän laskeutumisen periaatteeseen. Oletamme, että ratkaisukolmikko on olemassa ja osoitamme, että tällöin on olemassa toinen, pienempi kolmikko.

3 Pythagoraan kolmikot

3.1 Määritelmät

Määritelmä 3.1. Olkoot a, b ja c positiivisia kokonaislukuja siten, että

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

Tällöin lukukolmikko (a, b, c) on *Pythagoraan kolmikko*.

Esimerkiksi $(3, 4, 5)$, $(6, 8, 10)$ ja $(20, 99, 101)$ ovat Pythagoraan kolmikkoja, koska $3^2 + 4^2 = 5^2$, $6^2 + 8^2 = 10^2$ ja $20^2 + 99^2 = 101^2$.

Jos (a, b, c) on Pythagoraan kolmikko ja k ykköstä suurempi kokonaisluku, niin myös (ka, kb, kc) on Pythagoraan kolmikko. Edellä $(6, 8, 10)$ on tällainen esimerkki, se saadaan kertomalla $(3, 4, 5)$ kahdella.

Määritelmä 3.2. Olkoon (a, b, c) Pythagoraan kolmikko. Jos a ja b ovat keskenään jaottomia, niin (a, b, c) on *jaoton Pythagoraan kolmikko*.

3.2 Jakamattomien kolmikoiden ominaisuuksista

Helposti nähdään, että jos (a, b, c) on jaoton Pythagoraan kolmikko, myös a ja c sekä b ja c ovat keskenään jaottomia. Jos olisi jokin k siten, että $a = ka'$ ja $c = kc'$, olisi myös $b^2 = c^2 - a^2 = (kc')^2 - (ka')^2 = k^2(c'^2 - a'^2)$ ja k siis b:n ja c:n yhteinen tekijä.

Parillisuus ja parittomuus säilyvät, kun luku neliöidään. Summa on parillinen, jos yhteenlaskettavista molemmat tai ei kumpikaan on parillinen. Näistä seuraa, että kolmikossa (a, b, c) parillisia lukuja on yksi tai kolme.

Kolmikon kaikki luvut eivät voi olla parillisia; jos ne olisivat, kolmikko ei olisi jaoton vaan jaettavissa kahdella. Siis parillisia lukuja on yksi.

Jos a ja b olisivat parittomia, ne voitaisiin esittää muodossa $2u+1$ ja $2v+1$. Neliöden summa olisi tällöin $4(u^2+u+v^2+v)+2$, joka ei ole jaollinen neljällä. Jokaisen parillisen luvun neliö puolestaan on jaollinen neljällä. Näin kolmikossa (a, b, c) ei c voi olla parillinen.

Johtopäätöksenä jokaisessa jaottomassa Pythagoraan kolmikossa (a, b, c) on joko a parillinen ja b pariton tai toisinpäin. Luku c on aina pariton. Yleisyyttä menettämättä voidaan päättää, että a on parillinen.

3.3 Eukleideen kaava

Eukleideen kaava tuottaa osan Pythagoraan kolmikoista.

Valitaan mielivaltaiset $m, n \in \mathbb{Z}_+$ siten, että $m > n$. Tällöin $(2mn, m^2 - n^2, m^2 + n^2)$ on Pythagoraan kolmikko.

Esimerkiksi $m = 10, n = 1$ tuottaa kolmikon $(2 \cdot 10 \cdot 1, 10^2 - 1^2, 10^2 + 1^2) = (20, 99, 101)$ ja $m = 2, n = 1$ tuottaa kolmikon $(4, 3, 5)$.

Eukleideen kaava *ei* tuota kaikkia Pythagoraan kolmikkoja; esimerkiksi $(9, 12, 15)$ ei löydy tällä kaavalla. Koska $4^2 > 15$, ovat ainoat mahdollisuudet neliöiden summaksi $1^2 + 2^2$, $1^2 + 3^2$ ja $2^2 + 3^2$ eli 5, 10 ja 13, eikä mikään niistä ole 15.

Seuraavaksi todistamme, että Eukleideen kaava tuottaa kuitenkin *kaikki jaottomat* kolmikot; lähteenä todistuksen suuntaviivoille on ollut [3]. Muokataan ensin alkuperäistä yhtälöä:

$a^2 + b^2 = c^2 \Leftrightarrow a^2 = (c + b)(c - b)$.

Koska b ja c ovat parittomia, ovat niiden erotus ja summa parillisia. Ne voidaan siis esittää muodossa $2u = c - b$, $2v = c + b$. Laskemalla nämä puolittain yhteen saadaan $c = u + v$, ja tämä sijoittamalla edelleen $b = v - u$.

Luvuilla u ja v ei voi olla yhteisiä tekijöitä. Jos nimittäin olisi olemassa $k > 1$ siten, että $u = ku', v = kv'$, niin olisi $c = u + v = k(u' + v')$ ja $b = v - u = k(v' - u')$, ja siis k myös b:n ja c:n yhteinen tekijä.

Koska $a^2 = c^2 - b^2 = (c-b)(c+b) = 4uv$ ja u:lla ja v:llä ei ole yhtä suurempaa yhteistä tekijää, on niiden oltava kokonaislukujen neliötä; muutoinhan niiden tulo ei olisi kokonaisluvun neliö.

On siis olemassa kokonaisluvut m ja n siten, että $v = n^2$ ja $u = m^2$, joille $\text{syt}(m, n) = 1$.

Jokainen jaoton Pythagoraan kolmikko siis löydetään tällä Eukleideen kaavalla. Sillä, että kaava löytää joukon muitakin Pythagoraan kolmikkoja, ei ole jatkon kannalta merkitystä.

Käytännössä parin m, n laskeminen on helppoa. Esimerkiksi kolmikossa $(168, 95, 193)$ täytyy olla $m^2 - n^2 = 95$ ja $m^2 + n^2 = 193$. Laskemalla puolittain yhteen saadaan $m^2 = \frac{193-95}{2} = 49$, siis $m = 7$, ja tämä sijoittamalla saadaan $n = 12$.

4 Päätodistus

Toteamme ensin, että riittää tutkia sellaisia kolmikoita, joissa luvut ovat keskenään jaottomia.

Jos kolmikko (a, b, c) toteuttaa yhtälön $a^4 + b^4 = c^4$, ja k on jokin ykköstä suurempi luku, niin selvästi myös (ka, kb, kc) toteuttaa yhtälön. Siksi voidaan rajoittua tutkimaan vain jaottomia kolmikkoja. Jos niille ei löydy ratkaisua, ei sitä löydy niiden monikerroillekaan.

Edellä todistettiin, että jaottomassa Pythagoraan kolmikossa (a, b, c) on c aina pariton ja joko a parillinen ja b pariton tai toisinpäin. Samalla päättelyllä saadaan myös yhtälön $a^4 + b^4 = c^4$ mahdolliselle jaottomalle ratkaisulle samat parillisuussäännöt. Valitaan a parilliseksi ja b parittomaksi.

Merkitään $c^2 = d$ ja muokataan potenssimerkintää, jolloin yhtälöksi tulee $(a^2)^2 + (b^2)^2 = d^2$.

Aiemmin esitetyn perusteella on tällöin olemassa luvut m ja n, $m > n$ siten, että $\text{syt}(m, n) = 1, a^2 = 2mn, b^2 = m^2 - n^2, d = m^2 + n^2$.

Seuraavaksi osoitetaan, että m on pariton.

Jokaisen luvun neliön jakojäännös neljällä jaettaessa on 0 tai 1. Tämä nähdään siitä, että $(2t)^2$ on selvästi neljällä jaollinen, ja $(2t+1)^2 = 4(t^2+t)+1$, siis jakojäännös on 1.

Jos m olisi parillinen eli muotoa $2t_0$, niin n olisi pariton eli muotoa $2t_1+1$. Tällöin m^2-n^2 olisi $(2t_0)^2-(2t_1+1)^2 = 4({t_0}^2-{t_1}^2-t_1-1)+3$ eli muotoa $4t+3$. Mutta piti olla $b^2 = m^2-n^2$ eli siis m^2-n^2 jonkin luvun neliö, mikä on mahdotonta. Siis m on pariton ja n parillinen.

Lauseke $b^2 = m^2-n^2$ voidaan kirjoittaa $n^2+b^2 = m^2$, jossa siis m pariton.

Nyt on oltava olemassa luvut u ja v, $u > v$ siten, että $\text{syt}(u,v) = 1, n = 2uv, b = u^2-v^2, m = u^2+v^2$.

Sijoittamalla aiempaan yhtälöön $a^2 = 2mn$ edeltä $n = 2uv$ saadaan $a^2 = 4muv$. Koska $\text{syt}(u,v) = 1$ ja $\text{syt}(2uv,m) = \text{syt}(n,m) = 1$, on $\text{syt}(m,u) = 1$ ja $\text{syt}(m,v) = 1$. Tässä käytettiin tietoa siitä, että m on pariton; siksi $\text{syt}(2uv,m)$ ei voi olla 2.

Selvästi m, u ja v ovat kokonaislukujen neliöitä.

Voidaan päätellä, että on olemassa luonnolliset luvut a_1, b_1 ja d_1, joilla $u = {a_1}^2$, $v = {b_1}^2$ ja $m = {d_1}^2$. Luvut a_1, b_1 ja d_1 toteuttavat alkuperäisen yhtälön, koska $u^2+v^2 = m$.

Nyt voitaisiin edelleen vastaavalla tavalla todistaa olevan olemassa vielä pienemmät luvut a_2, b_2 ja d_2, joille yhtälö pätisi. Koska luonnollisia lukuja ei voida rajattomasti pienentää, päädytään ristiriitaan. Yhtälöllä $a^4+b^4 = d^2$ ei siis ole kokonaislukuratkaisuja, eikä näin ollen myöskään alkuperäisellä yhtälöllä $a^4+b^4 = c^4$.

5 Hieman historiaa

Monet tunnetut matematiikan ratkaisemattomat ongelmat vaativat jo tehtävän ymmärtämiseksi laajaa taustatietoa. Esimerkiksi Riemannin hypoteesi käsittelee kompleksilukuja, jotka Suomessa tulevat opiskelijalle tutuksi vasta

lukiossa. Kysymystä siitä, onko P=NP, ei käytännössä voi ymmärtää ilman yliopistotasoista laskennan teorian kurssia.

Poikkeuksiakin on. Goldbachin vahva konjektuuri kuuluu ”Jokainen kahta suurempi parillinen luku on kahden alkuluvun summa.” Vaikka alkulukuja ei juurikaan peruskoulussa käsitellä, on käsite selitettävissä jo ennen ala-asteen päättymistä.

Fermat’n suuri lause on silti yksinkertaisuudessaan ylivoimainen. Purkamalla potenssit kertolaskuiksi on ongelma ymmärrettävissä jokaiselle, joka osaa yhteen- ja kertolaskun. Se on myös helppo kokeiltava laskimella tai jopa käsin laskien, ja tietokoneella vaatii vain vähän ohjelmointitaitoa testata tuhansia lukukolmikoita.

Helposti ymmärrettävä ongelma on siis ollut ratkaisematta satoja vuosia. Ei liene siksi ihme, että monet harrastelijatkin ovat tutkineet kysymystä. Myös tämän kirjoittaja on aikanaan testannut Commodore 64 -tietokoneella lukukolmikoita pienillä eksponenteilla.

5.1 Erikoistapausten todistaminen

Ongelmaa on lähestytty osatodistuksin, lähinnä tietyillä eksponentin arvoilla. Päälähteenä koko tälle osiolle on [5].

Mordell kertoo kirjassaan, että Fermat itse todisti hyvin lähellä tapausta $n = 4$ olevan toisen lauseen, ja pitää ilmeisesti uskottavana, että Fermat olisi voinut todistaa tapauksen $n = 4$ [4, s. 5]. Viimeistään 1678 Leibniz todisti lauseen eksponentilla 4 edellä kuvatulla tavalla.

Euler laati todistusta tapaukselle $n = 3$ vuonna 1753. Todistuksessa oli aukko, mutta Euler itse todisti myöhemmin muussa yhteydessä lauseen, jolla aukko olisi sulkeutunut. Näin Euleria voidaan pitää tapauksen $n = 3$ ratkaisijana.

Tapauksen $n = 5$ ratkaisivat toisistaan riippumatta Legendre ja Dirichlet vuonna 1825; Dirichlet ratkaisi vielä tapauksen $n = 14$ vuonna 1832. Tapauksen $n = 7$ ratkaisi Gabriel Lamé vuonna 1839.

Tapaus $n = 7$ ratkaisee samalla tapauksen $n = 14$. Jos olisi olemassa (a, b, c) siten, että $a^{14} + b^{14} = c^{14}$, niin (a^2, b^2, c^2) olisi ratkaisu eksponentille 7; mutta kuten yllä todetaan, $n = 14$ ratkaistiin ensin.

Alkuperäisten todistusten lisäksi on sekä laadittu toisia todistuksia että yksinkertaistettu ensimmäisiä todistuksia. Eksponentit 6 ja 10 on lisäksi todistettu erillisinä todistuksina, mutta niiden osalta todistus seuraa jo siitä, että tapaukset 3 ja 5 oli ratkaistu aiemmin; ratkaisulogiikka on sama kuin edellisessä kappaleessa.

5.2 Yleinen todistus

Lauseen todisti lopulta englantilainen matemaatikko Andrew Wiles – todistuksen johdosta nykyään *sir* Andrew Wiles. Wiles aloitti työnsä vuonna 1986 kertomatta juuri kenellekään mitä on tutkimassa. Hän julkaisi yrityksen todistukseksi lopulta vuonna 1993. Yrityksestä löytyi kuitenkin aukko.

Wiles kertoo saaneensa 14.9.1994 idean, jolla todistuksen aukko pystyttiin kiertämään. Lopullinen todistus julkaistiin vuonna 1995. Aikaa Fermat'n kirjan sivumarginaaliin kirjoittamista sanoista oli kulunut 358 vuotta.

Yleinen todistus on yli sata sivua pitkä ja rakentuu useiden matematiikan alojen päälle. Todistuksen julkaisemisen jälkeen Andrew Granville kuvasi The Guardian -lehdessä sitä sanoin "- - koko maailmassa ei ole ehkä enempää kuin puolisen tusinaa ihmistä, jotka voivat kokonaisuudessaan ymmärtää kaikki Wilesin käyttämät yksityiskohdat." [2] (Suomennos tekijän)

Oliko Fermat'lla itsellään yleinen todistus lauseelleen? Lauseen lopulta todistanut Wiles vastaa kysymykseen siitä, oliko Fermat keksinyt hänen todistuksensa, näin:

"Se on mahdotonta. - - Se on 20. vuosisadan todistus. - - Tässä todistuksessa käytettyjä keinoja ei ollut olemassa Fermat'n aikana." [1] (Suomennos tekijän)

Viitteet

[1] [Anon.] *Andrew Wiles on Solving Fermat.* http://www.pbs.org/wgbh/nova/physics/andrew-wiles-fermat.html, viitattu 22.10.2011.

[2] Grandville, Andrew. *History of Fermat's Last Theorem.* http://math.albany.edu:8010/g/Math/topics/fermat/granville.hist, viitattu 22.10.2011.

[3] Halmetoja, Markku. *Fermat'n lause tapauksessa n = 4.* http://www.mantta.fi/ hamlet/math/fermat/, viitattu 23.10.2011.

[4] Mordell, L. J. *Three Lectures on Fermat's Last Theorem.* Cambridge: Cambridge University Press, 1921.

[5] Wikipedia, "Proof of Fermat's Last Theorem for specific exponents", viitattu 22.10.2011.