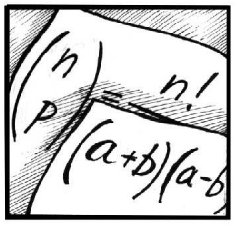

Fermat'n jälkeen

Timo Erkama
Professori
Fysiikan ja matematiikan laitos, Joensuun yliopisto
Timo.Erkama@joensuu.fi

Tieteen popularisointi on joskus vaikeaa, ja matematiikassa se on erityisen vaikeaa. Modernin matematiikan kieli on nimittäin siinä määrin mutkikasta, että alan ammattilaistenkaan ei ole aina helppoa ymmärtää toistensa tutkimustuloksia.

Silloin tällöin pääsevät tiedotusvälineet kuitenkin selostamaan yleisölle sellaista uutta matematiikkaa, jossa ainakin kysymyksenasettelun käsittämiseen riittävät pelkät peruskoulutiedot. Esimerkiksi viime vuosikymmenellä herätti laajaa huomiota ns. Fermat'n suuren lauseen todistus, jonka mukaan yhtälöllä

$$a^n + b^n = c^n \tag{1}$$

voi olla positiivisia kokonaislukuratkaisuja vain jos $n \leq 2$. Tapaus $n = 2$ liittyy Pythagoraan lauseeseen, jonka yhteydessä moni koululainen on tullut tarkastelleeksi suorakulmaista kolmiota, jonka sivujen pituudet ovat kokonaisluvut 3, 4 ja 5; tällöinhän yhtälö (1) toteutuu muodossa $3^2 + 4^2 = 5^2$. Sen sijaan kysymys positiivisten kokonaislukuratkaisujen olemassaolosta arvoilla $n \geq 3$ oli askarruttanut matemaatikkoja yli 300 vuotta, kunnes mm. algebrallisessa geometriassa saavutettujen edistysaskelten ansiosta tämä jo 1600-luvulla esitetty ongelma lopulta ratkesi.

Ongelman esittäjä ranskalainen Pierre de Fermat (1601–1665) oli matemaatikkona oikeastaan harrastelija, koska hän ansaitsi toimeentulonsa laki- ja virkamiehenä. Hänen jälkeensä sadat harrastelijat ovat turhaan yrittäneet keksiä ongelmalle sellaista "ihmeellistä" ratkaisua, jonka jo Fermat kirjoitti löytäneensä mutta jota ei ole säilynyt jälkipolville. Into tällaisen alkeellisen ratkaisun hakemiseen saattaa tosin olla hiipumassa, koska itse ongelmaa pidetään nykyään jo ratkaistuna. Sen vuoksi haluaisin tässä esitellä hypoteesin, joka on edelleen todistamatta mutta joka monessa suhteessa muistuttaa Fermat'n ongelmaa tarjoamalla haasteen myös amatöörille.

Olkoon $P(x) = x^2 + r$ toisen asteen polynomi, missä vakiotermi r on jokin reaaliluku. Merkitään yhdistettyä kuvausta $P \circ P$ symbolilla $P^{(2)}$, kuvausta $P \circ P \circ P$ symbolilla $P^{(3)}$ jne; siis $P^{(2)}(x) = (x^2 + r)^2 + r$ on neljännen asteen, $P^{(3)}(x) = ((x^2 + r)^2 + r)^2 + r$ kahdeksannen asteen polynomi jne.

Lukusuoran piste x on polynomin P *jaksollinen piste*, jos on olemassa positiivinen kokonaisluku n siten, että $P^{(n)}(x) = x$. Pienintä tällaista kokonaislukua n kutsutaan x:n *jaksoksi*, jolloin lukujen x, $P(x)$, $P^{(2)}(x)$,..., $P^{(n-1)}(x)$ joukko on P:n *n-sykli*.

Esimerkiksi luku 0 on polynomin $P(x) = x^2 - 1$ jaksollinen piste, sillä $P(0) = -1$ ja $P(-1) = 0$. Siis luvut 0 ja -1 muodostavat polynomin P 2-syklin. Vastaavasti luvut $\frac{5}{4}$, $-\frac{1}{4}$ ja $-\frac{7}{4}$ muodostavat polynomin

$P(x) = x^2 - \frac{29}{16}$ 3-syklin, sillä $P(\frac{5}{4}) = -\frac{1}{4}$, $P(-\frac{1}{4}) = -\frac{7}{4}$ ja $P(-\frac{7}{4}) = \frac{5}{4}$.

Näissä kahdessa esimerkissä syklin kaikki pisteet olivat rationaalilukuja, siis muotoa $\frac{p}{q}$ missä p ja q ovat kokonaislukuja. Tällaista sykliä kutsutaan *rationaaliseksi* sykliksi. Avoin ongelmamme kuuluu nyt seuraavasti.

Hypoteesi 1. Polynomilla $P(x) = x^2 + r$ ei ole rationaalisia n-syklejä, jos $n \geq 4$.

Tämä hypoteesi on toistaiseksi todistettu vain arvoilla $n = 4$ ja $n = 5$. Todistukset julkaistiin viime vuosikymmenen lopulla, ja varsinkin arvolla $n = 5$ käytetyt menetelmät olivat syvällisiä.

Miten sitten matematiikan harrastelija voisi lähestyä tämänkaltaista ongelmaa? Esimerkin tarjoaa seuraava lause, joka puolestaan on erikoistapaus eräästä lukiolaisten matematiikkaolympialaisten tehtävästä. Lukijamme voi kokeilla matemaattisia kynsiään etsimällä lauseelle omaa todistustaan ennen kuin lukee kirjoitusta eteenpäin.

Lause 1. Polynomilla $P(x) = x^2 + r$ voi olla kokonaisluvuista koostuva n-sykli vain, jos $n \leq 2$.

Todistus. Olkoon $\{x_0, x_1, \ldots, x_{n-1}\}$ polynomin P n-sykli siten, että $P(x_0) = x_1$, $P(x_1) = x_2$, …, $P(x_{n-1}) = x_0$ ovat kokonaislukuja. Voidaan olettaa, että $n \geq 2$, jolloin $x_1 - x_0 \neq 0$. Silloin

$$x_2 - x_1 = x_1^2 + r - (x_0^2 + r) = (x_1 + x_0)(x_1 - x_0) \neq 0,$$
$$x_3 - x_2 = x_2^2 + r - (x_1^2 + r) = (x_2 + x_1)(x_2 - x_1) \neq 0$$

jne. Huomataan siis, että $x_2 - x_1 = m_1(x_1 - x_0)$, missä $m_1 = x_1 + x_0$ on kokonaisluku, $x_3 - x_2 = m_2(x_2 - x_1)$, missä $m_2 = x_2 + x_1$ on kokonaisluku jne. Kertomalla nämä yhtälöt puolittain saadaan

$$(x_2 - x_1)(x_3 - x_2) \cdots (x_0 - x_{n-1})(x_1 - x_0)$$
$$= m_1 m_2 \cdots m_n (x_1 - x_0)(x_2 - x_1) \cdots (x_0 - x_{n-1}),$$

ja supistusten jälkeen $m_1 m_2 \cdots m_n = 1$. Koska $m_1, \ldots, m_n$ ovat kokonaislukuja, tämä on mahdollista vain jos $m_i = \pm 1$ kaikille i. Lisäksi jollakin i:n arvolla tulee olla $m_i = -1$, sillä muuten luvut $x_0, x_1, \ldots, x_{n-1}, x_0$ muodostaisivat *aritmeettisen jonon*, jossa peräkkäisten lukujen erotus on vakio. Tällaisen kasvavan tai vähenevän jonon ensimmäinen ja viimeinen luku eivät tietenkään voi olla samoja. Siis jollakin i:n arvolla $m_i = -1$, josta seuraa $x_{i+1} - x_i = -(x_i - x_{i-1})$ ja edelleen $x_{i+1} = x_{i-1}$. Kysymyksessä on siis 2-sykli. □

Vaativamman haasteen amatöörille tarjoaa seuraava aiemmin julkaisematon lause, jonka todistus on liian pitkä tässä esitettäväksi.

Lause 2. Olkoon $\{x_0, \ldots, x_{n-1}\}$ polynomin $P(x) = x^2 + r$ rationaalinen n-sykli. Silloin on olemassa kokonaisluvut $p_0, \ldots, p_{n-1}$ ja q siten, että millään kahdella näistä kokonaisluvuista ei ole yhteisiä alkutekijöitä ja $x_i = p_i/q$ kaikille $i = 0, \ldots, n-1$.

Mitä yhteistä sitten on hypoteesilla 1 ja Fermat'n probleemalla? *Algebrallisella käyrällä* tarkoitetaan sellaista tason pistejoukkoa, jonka muodostavat jonkin kahden muuttujan polynomin $Q(x, y)$ nollakohdat. Esimerkiksi yksikköympyrä on algebrallinen käyrä, sillä se koostuu polynomin $Q(x, y) = x^2 + y^2 - 1$ nollakohdista. Samoin koulusta tutut ellipsi, paraabeli ja hyperbeli ovat tällaisia algebrallisia käyriä; polynomia $Q(x, y) = x^2 - y$ vastaa paraabeli $y = x^2$ jne. Algebrallisen käyrän pistettä (x, y) sanotaan *rationaaliseksi* pisteeksi, jos sen koordinaatit ovat rationaalilukuja.

Fermat'n ongelmassa on oikeastaan kysymys polynomin $Q(x, y) = x^n + y^n - 1$ määräämän algebrallisen käyrän rationaalisten pisteiden etsimisestä: jokainen yhtälön (1) positiivisista kokonaisluvuista koostuva ratkaisu määrittelee nimittäin tällaisen rationaalisen pisteen $(\frac{a}{c}, \frac{b}{c})$. Tapauksessa $n = 2$ rationaalisia pisteitä löytyy ääretön määrä, ja ne sijaitsevat kaikki yksikköympyrän kehällä. Myös arvoilla $n \geq 3$ löytyy rationaalisia pisteitä x- ja y-akseleilta, mutta niistä ei saada yhtälölle (1) positiivista kokonaislukuratkaisua.

Hypoteesissa 1 puolestaan etsitään rationaalisia pisteitä polynomin $Q(x, r) = P^{(n)}(x) - x$ määräämälle algebralliselle käyrälle, missä muuttujan y paikalla on nyt polynomin P vakiotermi r. Tehtävä näyttää aluksi hankalammalta kuin Fermat'n probleema, sillä suurilla n:n arvoilla polynomin $P^{(n)}(x)$ lauseke on monimutkainen. Ongelman tarkempi analyysi paljastaa kuitenkin rakenteita, joiden systemaattinen tutkiminen on vasta alussa ja saattaa johtaa edistysaskeliin muillakin matematiikan tai sovelletun matematiikan osa-alueilla.

Tulevaisuus näyttää, tarvitaanko hypoteesin 1 ratkaisemiseen vielä 300 vuotta ja osallistuuko siihen kenties joku tämän lehden lukijoista.