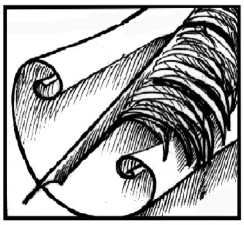

Hyvin hankalat, mahdottomat ja hyvin työläät ongelmat

Pääkirjoitus

Matematiikassa on ongelmia, joiden tiedetään olevan äärimmäisen hankalia, ja joita on yritetty ratkaista jo hyvin pitkään. Näihin kuuluu esimerkiksi Riemannin hypoteesin todistaminen. Hypoteesin mukaan Riemannin zeta-funktion kaikki epätriviaalit nollakohdat ovat ns. kriittisellä suoralla, eli kompleksitason suoralla, jolla luvun reaaliosa on $\frac{1}{2}$. Riemannin hypoteesi on oleellinen, koska sillä on valtavia implikaatioita muihin tuloksiin. Lukuteoriassa on merkittävä määrä tuloksia, jotka on todistettu olettaen Riemannin hypoteesi. Näin saadaan toisinaan parempia tuloksia kuin olettamatta hypoteesia. Riemannin zeta-funktiolla on yhteys esimerkiksi alkulukujen jakaumaan. Kaikkien epätriviaalien nollakohtien sijaitseminen kriittisellä suoralla on yhtäpitävää alkulukujen tasaisemman jakautumisen kanssa (eli alkulukulauseen virhetermin pienuuden kanssa).

Eräät ongelmat ovat äärimmäisen työläitä. Näihin kuuluu esimerkiksi tekijöihinjako. Siinä missä pienen luvun tekijöihin jakaminen on toisinaan ehkä mukava harjoitustehtävä, ison luvun jakaminen tekijöihin on pahimmillaan todella hidasta. Mille tahansa annetulle luvulle voidaan kyllä löytää tekijät, kyse on lähinnä siitä, kuinka kauan aikaa kuluu. Tämän ongelman työläyteen perustuu esimerkiksi RSA-kryptosysteemi. RSA murtuu, jos tekijöihinjako saadaan nopeaksi. Toisaalta, jos RSA murtuu, niin tekijöihinjako onnistuu myös nopeasti. Kvanttikoneelle on olemassa nopea algoritmi tekijöihinjakoa varten, mutta ilman kvanttikonetta tällaista ei tunneta, vaikka kysymystä on pohdittu jo kauan. Toinen vastaava ongelma on hilan lyhimmän nollasta poikkeavan vektorin löytäminen. Siihenkään ei ole nopeaa menetelmää, joka toimisi aina. Myös tämän kysymyksen työläyttä voidaan hyödyntää kryptografiassa.

Jotkut ongelmat on todistettu mahdottomiksi. Näihin kuuluu esimerkiksi yleisen ratkaisukaavan johtaminen vähintään 5. asteen yhtälölle ja kulman kolmiajako harppia ja viivoitinta käyttäen. Tämä ei tarkoita sitä, etteikö joitakin esimerkiksi 5. asteen yhtälöitä voisi ratkaista helposti tai etteikö joitakin kulmia voisi jakaa siististi kolmeen osaan harpilla ja viivaimella. Esimerkiksi yhtälö $x^5 + 1 = 0$ on helppo ratkaista. Myös 90 asteen kulma on mukava jakaa harpilla ja viivaimella kolmeen osaan käyttäen tämän nimenomaisen kulman erityisominaisuuksia. Kyse on siitä, että yleinen tilanne ei ole mahdollinen, eli löytyy vähintään joku tapaus, joka ei onnistu. Yhtälöitä voi lähestyä erilaisin numeerisin menetelmin. Myös kulmien kolmiajakoa voi lähestyä approksimoiden. Tässä lehdessä on juttu, jossa kerrotaan, kuinka kulman voi jakaa kolmeen osaan saaden melko hyvän tuloksen ja käyttäen vain harppia ja viivainta.

Lisäksi on todistettu, että on olemassa lauseita, joiden totuusarvoa ei pystytä todistamaan. Tätä käsitellään seuraavassa numerossa Antti Valmarin kirjoituksessa.

Monet hankalat ongelmat ovat kiehtovia. Ennen kuin Fermat’n suuri lause todistettiin, yritti moni todistaa sitä, mahdollisesti yrittäen toistaa Fermat’n itse väittämän erinomaisen todistuksen. Fermat’n suuri lause oli muotoiltavissa niin yksinkertaisesti, että hyvin moni ymmärsi väitteen, vaikka todistus oli lopulta äärimmäisen pitkä, tekninen ja syvällinen.

Nykypäivänä ehkä vastaava kysymys voisi olla ns. $3x+1$-konjektuuri, eli jos aloitetaan mistä tahansa positiivisesta kokonaisluvusta, ja jos luku on parillinen, niin jaetaan kahdella, muulloin kerrotaan kolmella ja lisätään yksi, niin väite on, että jos tätä operaatiota jatketaan, ennen pitkää päästään ykköseen. Kysymys kuulostaa alkeelliselta. Millä tahansa helpolla esimerkillä todellakin ennen pitkää päästään ykköseen. Konjektuuria on numeerisesti tarkistettu varsin suuriin lukuihin asti. Kysymys on kuitenkin yhä auki. Maineikas lukuteoreetikko Alf van der Poorten arvioi, että kysymys on niin perustavanlaatuisesti lukujen ominaisuuksiin liittyvä, että sitä ei saada koskaan todistettua.

Osa hankalista tai työläistä ongelmista on relevantteja, koska niillä on selkeitä implikaatioita joko teoriaan (kuten zeta-funktion tapauksessa) tai käytäntöön (kuten tekijöihinjaon yhteydessä). Osa kysymyksistä ei ole merkittäviä samalla tavalla. Tämä ei kuitenkaan tarkoita sitä, etteikö niiden merkitys matematiikan tutkimukselle ja kehitykselle voisi olla valtava. Vaikka Fermat'n suuren lauseen suorat implikaatiot olivat selvästi vähäisempiä kuin vaikkapa Riemannin hypoteesin implikaatiot olisivat, Fermat'n suuren lauseen todistusyritysten merkitys oli valtava. Kun sitä yritettiin todistaa, kehitettiin valtava määrä muuta teoriaa.

Työntekoa arvostavana kansana suomalaiset varmaan osaavatkin arvostaa ajatusta siitä, että (ongelman) työläyden tai hankaluuden merkitystä ei pidä aliarvioida, vaan olla siitä tyytyväinen.

Anne-Maria Ernvall-Hytönen