Miljoonan dollarin ongelmat

Osmo Pekonen

"Kukapa ei olisi iloinen, jos voisi kohottaa tulevaisuuden verhoa ja luoda silmäyksen tieteen edistysaskeliin ja sen tulevan kehityksen salaisuuksiin tulevina vuosisatoina?" Näin aloitti David Hilbert (1862–1943) luentonsa Pariisin kansainvälisessä matemaatikkokongressissa 8. elokuuta 1900. Hilbert oli matematiikan viimeisiä universalisteja. Hänellä oli tieteenalastaan niin laaja näkemys, että historiallisessa luennossaan hän uskalsi ennustaa matematiikan kehityksen 1900-luvun suuntaviivat – ja osui monissa kohdissa hämmästyttävän hyvin oikeaan.

Hilbert kiteytti visionsa luettelemalla joukon ongelmia, joita hän piti matematiikan keskeisimpinä. Hilbertin ongelmista, joita oli alunperin 23 kappaletta, tuli sittemmin käsite. Menneen 1900-luvun matematiikasta iso osa on ollut Hilbertin ongelmien tutkimusta ja tulkintaa. Matematiikka on toki laajentunut moniin sellaisiinkin suuntiin, joista Hilbertillä ei ollut aavistustakaan, mutta edelleen pidetään erityisenä saavutuksena, jos joku onnistuu ratkaisemaan jonkin hänen ongelmistaan. Suomalaisista matemaatikoista tämä kunnia on osunut Sören Illmanille, joka vuonna 1994 ratkaisi osan Hilbertin viidennestä ongelmasta. Illman osoitti, että sileällä monistolla ankarasti ja sileästi toimiva Lien ryhmä saadaan toimimaan myös reaalianalyyttisesti.

Hilbertin julistusta sävytti tieteellinen edistysusko. Filosofina Hilbert oli formalisti, jonka mukaan kaikki matemaattinen tieto oli ihmisjärjen loogisen päättelykyvyn saavutettavissa, kunhan vain matematiikan kulmakivet eli aksioomat asetettaisiin kyllin huolellisesti paikoilleen. "Vakaumus jokaisen matemaattisen ongelman ratkeavuudesta on tutkijalle valtava kannustin. Kuulemme sisällämme äänen sanovan: Tässä on ongelma. Etsi sen ratkaisu. Voit löytää sen puhtaan järjen avulla, sillä matematiikassa emme koskaan joudu sanomaan *ignorabimus*." Filosofisesti Hilbert oli kuitenkin väärässä, kuten Kurt Gödelin epätäydellisyyslause (1931) sittemmin osoitti: Jokaisesta aksioomajärjestelmästä löytyy myös lauseita, joiden totuusarvoa ei voida ratkaista.

Hilbertin rajatonta luottamusta matematiikan selittävään voimaan kuvaa hänen kuudes ongelmansa, jossa tehtäväksi annetaan fysiikan aksiomatisoiminen. Jälkiviisaasti ajateltuna näin suurisuuntainen projekti tuntuu haihattelulta -- ottaen huomioon, ettei vuonna 1900 vielä tunnettu sen enempää suhteellisuusteoriaa kuin kvanttimekaniikkaa! Vuoden 1900 fysiikassa itse asiassa vallitsi hieman samantapainen tilanne kuin nykyisin: Oli alettu uskoa, että fysiikan suuret ongelmat oli jo pääosin ratkaistu ja että "Kaikenselittävä Kaiken Teoria" oli käden ulottuvilla. Hilbert itse kirjoitti fysiikan aksiomatisoimisesta visionäärisen teoksen *Grundlagen der Physik* (1915), mutta Einstein kommentoi sitä ironisesti: "Hilbertin teos materiasta vaikuttaa minusta lapselliselta siinä mielessä, ettei lapsi tunne ulkomaailman petollisuutta."

Hilbertin ongelmien nykytilanne on sellainen, että 23 alkuperäisestä ongelmasta 12 on ratkaistu, 3 on avoinna ja loput 8 (kuten em. kuudes ongelma) ovat luonteeltaan niin laajoja, ettei niiden voi odottaa pikaisesti ratkeavan.

Uuden vuosisadan ongelmat

Sata vuotta myöhemmin, 24. toukokuuta 2000, matematiikan historian lehdet havisivat, kun joukko maailman eturivin matemaatikoita kokoontui Pariisissa Collège de Francessa esittämään uuden vuosisadan "uudet Hilbertin ongelmat". Tällä kertaa ongelmia oli vain seitsemän; niistä yksi periytyi Hilbertin listalta. Uutta Hilbertiä ei kuitenkaan esittänyt kukaan. Matematiikka on paisunut niin valtavaksi tiedon alueeksi, ettei kaiken hallitsevia uusia universaalineroja enää ole, vaan ongelmat valitsi komitea. Siihen kuuluivat ainakin ranskalainen Alain Connes, amerikkalainen Arthur Jaffe, amerikkalainen Edward Witten ja englantilainen Andrew Wiles, mutta varmaan monia muitakin oli konsultoitu. Kunkin ongelman ratkaisemisesta luvattiin miljoonan dollarin palkintosumma, jonka maksaa amerikkalaisen miljonääripariskunnan Landon ja Lavinia Clayn perustama uusi matematiikan rahoitusjärjestö Clay Mathematics Institute.

Clayn säätiö jakaa myös tunnustuspalkintoja, jollaisen ovat tähän mennessä saaneet Andrew Wiles Fermat'n suuren ongelman ratkaisemisesta, Alain Connes epäkommutatiivisen geometrian kehittämisestä ja nuoremman sukupolven edustajana ranskalainen normaalikoululainen Laurent Lafforgue kontribuutioistaan ns.

Langlandsin vastaavuuden todistamiseksi.

Hilbert oli hengessä mukana Collège de Francen tilaisuudessa, sillä äänilevyltä kuultiin hänen Königsbergissä vuonna 1930 taltioitu paatoksellinen julistuksensa, joka päättyi sanoihin: *Wir müssen wissen. Wir werden wissen.* Sama teksti on kaiverrettu hänen hautapaateensa.

Nykyinen luonnontieteellinen tutkimus on enimmäkseen ryhmätyötä. Biologiassa tai fysiikassa tieteellisen julkaisun allekirjoittajia saattaa olla kymmenittäin. Matemaattinen työskentely sen sijaan on edelleen suurelta osin yksinäistä puurtamista. Kukaan ei toki työskentele tyhjiössä, mutta jos matemaattiset käsitteet eivät ala elää tutkijan omissa aivoissa, ei työryhmästäkään ole apua. Kuuluisia esimerkkejä huipputason yhteistyöstä löytyy paljon matematiikastakin (veljekset Rolf ja Frithiof Nevanlinna, Hardy ja Littlewood, Atiyah ja Singer...), mutta myös yksinäisen tutkijan huippusaavutukset ovat edelleen mahdollisia, kuten Andrew Wilesin tapaus osoittaa.

Matematiikan suurista palkinnoista Suomeen on saatu yksi Fieldsin mitali (Lars Ahlfors 1936) ja yksi Salemin palkinto (Kari Astala 1994). Kultaa ja kunniaa halajaville tieteen sankareille on tästedes tarjolla myös Clayn palkinto. Miljoonan dollarin taskurahan lisäksi sen voittajat saavat kaupanpäälliseksi myös topologisesti mielenkiintoisen pronssiveistoksen olohuoneensa nurkkaa somistamaan. Koska Clayn palkintokilpailu on avoin kenelle tahansa, esittelen seuraavassa lyhyesti uuden vuosisadan -- vaiko peräti vuosituhannen? -- seitsemän suurinta matemaattista ongelmaa.

Ongelma 1: P versus NP -ongelma

Tämän ongelman esitti kanadalainen Stephen Cook vuonna 1971. Lyhenne **P** tarkoittaa "polynomista aikaa" ja **NP** "ei-determinististä polynomista aikaa". Näiden käsitteiden tarkka määritteleminen on tapauskohtaista ja itse asiassa osa ongelmaa, mutta kysymys on

formalisoidun tietokoneen (esimerkiksi ns. Turingin koneen) vaatimasta laskenta-ajasta tietyn ongelman ratkaisemiseksi. Tehtävänä on selvittää, ovatko **P** ja **NP** sama asia.

P versus **NP** -ongelman juuret ovat kryptografiassa eli salakirjoitustieteessä. Epämääräisesti puhuen jokin ongelma, vaikkapa salakirjoituksen avaaminen, on luokassa **P**, jos se voidaan ratkaista käyttäen algoritmia, jonka koko kasvaa korkeintaan polynomiaalisesti suhteessa annetun datan pituuteen. Jos tehtävänä on esimerkiksi ratkaista, onko annettu kokonaisluku *n* toisen kokonaisluvun neliö, kyseessä on selvästi luokan **P** ongelma, sillä riittää laskea \sqrt *n*. Jos taas tehtävänä on jakaa annettu

(suuri) kokonaisluku *n* alkutekijöihinsä, kyseessä on luokan **NP** ongelma, mutta ei tiedetä, olisiko se sopivaa algoritmia käyttäen myös luokassa **P.**

Käytännössä tämä merkitsee, että annetun tarpeeksi suuren kokonaisluvun jakaminen alkutekijöihinsä on mahdoton (so. liiaksi aikaa vievä) tehtävä tuntemiemme kaltaisilla tietokoneilla ja ohjelmilla. Tähän perustuu kuuluisa RSA-koodi, jonka kehittivät Ronald Rivest, Adi Shamir ja Leonard Adleman vuonna 1978. Kyseessä on ns. julkisen avaimen koodi, joka perustuu siihen, että kahden suuren, vaikkapa 100-numeroisen, alkuluvun kertominen keskenään on hyvin helppoa, kun taas tulokseksi saadun enintään 200-numeroisen luvun jakaminen takaisin tekijöihinsä on hyvin vaikeaa. Jos voitaisiin osoittaa, että annetun luvun *n* jakaminen tekijöihinsä onkin tyypin **P** ongelma, seuraukset olisivat dramaattiset, sillä sähköisen viesti- ja rahaliikenteen yleisimmin käytetty suojausmenetelmä olisi silloin murrettu. Suurvaltojenkin turvallisuus riippuu siis muutaman ison alkuluvun tuntemisesta!

Tämäntapaista matematiikkaa pitäisi harrastaa Suomessa enemmän, koska meillä on merkittäviä tietosuoja-alan yrityksiä, jotka tarvitsevat uusinta tutkimustietoa. Aihepiiristä kiinnostuneen kannattaa tulla kuuntelemaan teoreettisen tietojenkäsittelytieteen "nobelilla" eli Rolf Nevanlinna -mitalilla palkittuja huippututkijoita, jotka Kansainvälisen Matematiikan Vuoden 2000 merkeissä kokoontuvat Helsingin yliopiston matematiikan laitoksella 5.--6. syyskuuta. Rolf Nevanlinna -palkinnon vuonna 1998 saanut amerikkalainen Peter Shor on osoittanut teoreettisesti, että RSA-koodi voitaisiin murtaa polynomiaalisessa ajassa käyttäen kvanttitietokonetta. Sitkeä huhu on tietävinään, että amerikkalainen National Security Agency (NSA) olisi jo rakentanut kvanttitietokoneen ja murtanut RSA-koodin -- ja voisi siis lukea koko maailman sähköpostit. Siinä sivussa NSA voisi myös kuitata Clayn palkinnon, mikäli olisi pikkurahan tarpeessa. Mene ja tiedä.

Ongelma 2: Hodgen konjektuuri

Ongelman esitti englantilainen W. V. D. Hodge vuonna 1950. Tämä ongelma on valitettavasti kovin tekninen ja avautuu vain asiantuntijalle. On todistettava seuraava väite: "Projektiivisella ei-singulaarisella algebrallisella varistolla yli kompleksilukujen kunnan pätee, että jokainen rationaalinen (p,p)-kohomologialuokka on rationaalinen lineaarikombinaatio kodimensiota p olevien algebrallisten syklien määräämistä kompleksisista $2p$-kohomologialuokista".

Ongelma 3: Poincarén konjektuuri

Ongelman esitti ranskalainen Henri Poincaré vuonna 1904. Kyseessä on yksinkertaiselta kuulostava topologian ongelma: On osoitettava, että *jokainen suljettu yhdesti yhtenäinen 3-ulotteinen monisto on homeomorfinen 3-ulotteisen pallonkuoren kanssa.*

Kysymys voidaan yleistää seuraavasti: On osoitettava, että jokainen suljettu yhdesti yhtenäinen n-ulotteinen monisto on homeomorfinen n-ulotteisen pallonkuoren kanssa. Poincaré oli tietoinen yleistyksestä, mutta hän luuli todistaneensa sen jo vuonna 1900,

mistä syystä ongelma ei esiinny Hilbertin listassa. Vuonna 1904 Poincaré tajusi erehtyneensä ja esitti konjektuurin avoimena ongelmana.

Tapauksissa n=1 ja n=2 väite on triviaali. Tapauksessa n>4 ongelman ratkaisi Stephen Smale vuonna 1960. Hänet palkittiin Fieldsin mitalilla 1966. Michael Freedman puolestaan ratkaisi tapauksen n=4 vuonna 1983 ja sai Fieldsin mitalin 1986. Avoinna on siis enää tapaus n=3.

Tapauksessa n=2 ongelmaa on mahdollista havainnollistaa arkikielen käsitteitä käyttäen: Kuvitellaan taikinasta tehtyjä leivoksia kuten pullia, munkkeja ja viipurinrinkeleitä, jolloin niiden pinnat X ovat erilaisia "suljettuja 2-ulotteisia monistoja". Yhdesti yhtenäisyys tarkoittaa seuraavaa: Piirretään pinnalle X silmukka, joka ei leikkaa itseään. Silloin tavallisen pyöreän pullan pinta jakautuu aina kahteen osaan, jotka voidaan vaikkapa värittää kahdella eri värillä. Sanomme, että pullan pinta on "yhdesti yhtenäinen". Sen sijaan munkkirinkilän pinnalle on mahdollista piirtää silmukka (tutki millainen!), joka ei jaa munkin pintaa kahteen osaan, so. väritys kahdella värillä ei onnistu. Munkkirinkilän pinta ei ole yhdesti yhtenäinen. Sama pätee *a fortiori* viipurinrinkelin tapauksessa.

Poincarén konjektuuri tapauksessa n=2 sanoo, että kaikki suljetut "kahvattomat" pinnat ovat keskenään homeomorfisia, toisin sanoen ne voidaan muovailla toinen toisikseen pelkällä venyttelyllä *repimättä tai liimaamatta pullataikinaa.* Asia on intuitiivisesti selvä, kuten jokainen voi itse todeta taikinapalloa pyörittelemällä. Vasta rinkelin tekeminen pyöreästä pullasta (tai päinvastoin) edellyttää "kahvan" luomista tai poistamista ja siis taikinan liimaamista tai repimistä.

Saman asian kuvitteleminen tapauksessa n=3 on vaikeampaa, koska 3-ulotteinen monisto on 4-ulotteisen moniston "pinta" (esimerkiksi 3-ulotteinen pallonkuori S^3 on 4-ulotteisen "umpipallon" B^4 pinta), mutta emme kykene kuvittelemaan 4-ulotteisia objekteja.

Poincarén konjektuurin yleistys on Thurstonin konjektuuri: "Jokainen suljettu 3-ulotteinen monisto X, jolla on äärellinen perusryhmä, voidaan varustaa vakiokaarevalla positiivisen kaarevuuden metriikalla, ja tällöin X on homeomorfinen S_3/\Gamma:n kanssa, missä \Gamma on S^3:lla vapaasti toimiva kiertoryhmän SO(4) äärellinen aliryhmä."

Poincarén konjektuuri seuraa Thurstonin konjektuurista, kun \Gamma:ksi (eli perusryhmäksi) valitaan triviaali ryhmä.

Poincarén konjektuuri on täynnä sudenkuoppia. Se on tullut kuuluisaksi lukemattomista vääristä ratkaisuista, joita sille on aikojen kuluessa esitetty.

Ongelma 4: Riemannin hypoteesi

Ongelman esitti saksalainen Bernhard Riemann vuonna 1859. Kyseessä on epäilemättä puhtaan matematiikan kuuluisin avoin ongelma, joka oli mukana myös Hilbertin listassa vuonna 1900, ongelmana n:o 8. Kokonaiset matemaatikkosukupolvet ovat menneet hautaan yrittäessään ratkaista tätä ongelmaa. Kuuluisaksi on tullut postikortti, jonka G. H. Hardy kerran lähetti lähtiessään laivalla Tanskasta Englantiin. Paatti oli pieni, ja Hardy pelkäsi sen uppoavan nousevassa myrskyssä. Niinpä hän raapusti jäähyväisiksi matemaatikko Harald Bohrille osoittamaansa postikorttiin: "I proved the Riemann Hypothesis. G. H. Hardy". Puolitoista vuosisataa jatkunut työ Riemannin hypoteesin todistamiseksi ei kuitenkaan ole ollut turhaa, sillä hypoteesi on syvällisessä yhteydessä moniin muihin matematiikan aloihin.

Riemannin hypoteesi kuuluu funktioteoriaan, suomalaisten matemaatikkojen vanhaan leipälajiin. Riemannin zeta-funktio on yhden kompleksisen muuttujan *s* funktio, joka on määritelty puolitasossa $\Re(s)>1$ absoluuttisesti suppenevana sarjana

$$\zeta (s) = \sum_{n=1}^{\infty}\frac{1}{n^s}.$$

Koko kompleksitasoon analyyttisesti jatkaen saadaan meromorfifunktio, jonka ainoa, yksinkertainen napa on pisteessä $s=1$. Nollakohtia on kahdenlaisia: Triviaalit nollakohdat ovat negatiivisissa parillisissa kokonaislukupisteissä -2,-4,-6,... ja epätriviaalit nollakohdat jossain muualla.

Riemannin hypoteesi sanoo, että zeta-funktion epätriviaalien nollakohtien reaaliosa on aina $=\frac{1}{2}$. Kaikki epätriviaalit nollakohdat siis sijaitsevat samalla kompleksitason *kriittisellä suoralla* $\Re (s)=\frac{1}{2}$.

Ensi silmäyksellä moinen lausahdus ei kuulosta erityisen syvälliseltä. Kyseessä näyttäisi olevan vain erään erikoisfunktion mielenkiintoinen ominaisuus, jonka todistuksen luulisi ennen pitkää löytyvän. Riemann itse sanoo alkuperäisessä artikkelissaan "Über die Anzahl der Primzahlen unter einer gegebenen Grösse":

"Epäilemättä tälle tulokselle löytyisi täsmällinen todistus; olen kuitenkin jättänyt sen toistaiseksi sivuun, koska se ei ollut välttämätön tutkimukseni välittömälle päämäärälle."

Riemannin hypoteesi on kuitenkin uhmannut tutkijoita jo puolitoista vuosisataa. Se on vähitellen paljastunut nykyisen lukuteorian suurimmaksi avoimeksi ongelmaksi, joka on syvällisesti yhteydessä alkulukujen jakautumiseen, kuten Riemann itsekin hyvin tiesi.

Alkulukuja 2,3,5,7,11,... on ääretön määrä, kuten jo Eukleides todisti. Alkuluvut näyttävät kuitenkin harvenevan mitä pitemmälle jonossa mennään. Ei kuitenkaan tiedetä, millä tavoin tämä harveneminen täsmällisesti tapahtuu. Ei esimerkiksi tiedetä, onko olemassa äärettömän monta alkulukuparia muotoa *p*, *p*+2 (kuten esimerkiksi 3 ja 5, 5 ja 7, 11 ja 13 jne.)

Alkulukujen lukumäärää positiiviseen lukuun *x* asti on tapana merkitä symbolilla $\pi(x)$. Gauss tiesi jo vuonna 1849, että $\pi(x)$:ää voidaan approksimoida eksplisiittisellä funktiolla

$$\text{Li}(x)=\int_{0}^{x}\frac{\text{d}t}{\log t}\,.$$

Riemannin hypoteesi puolestaan on yhtäpitävää sen kanssa, että

$$\pi(x)=\text{Li}(x)+{\cal O}(\sqrt x \log x),$$

missä $\cal O$ on Landaun symboli.

Näin tulkittuna Riemannin hypoteesi kouraisee lukuteorian perusteita todella syvältä. On paljon mahdollista, että Riemannin hypoteesin ratkaisija joutuu käyttämään niin syvällisiä menetelmiä, että hän siinä sivussa tulee murtaneeksi myös RSA-koodin (vrt.

ongelma 1).

Koska teoreettista ratkaisua Riemannin hypoteesille ei ole löytynyt, on ongelmaa testattu kokeellisesti. Numeronmurskaimet ovat jauhaneet tuloksen, että ainakin zeta-funktion 1,5 miljardia ensimmäistä epätriviaalia nollakohtaa todella ovat kriittisellä suoralla.

Myös suomalainen Ernst Lindelöf (1870--1946) esitti vuonna 1908 Riemannin zeta-funktion käyttäytymistä koskevan tärkeän hypoteesin, jonka mukaan kaikilla $\epsilon>0$ pätee

$$\vert \zeta (\frac{1}{2}+it) \vert = {\cal O}({\vert t \vert}^{\epsilon}).$$

Lindelöfin hypoteesi seuraa Riemannin hypoteesista, mutta on edelleen avoinna. Paras eksponentti, jolla em. arvio on saatu todistetuksi (Martin N. Huxley), on

$\epsilon = \frac{89}{570} \approx 0,16.$

Ongelma 5: Kaikenselittävä Kaiken Teoria

Tämä ongelma on hieman epämääräisesti muotoiltu (kuten Hilbertin kuudes ongelma). Tehtävänä on selittää "kvarkkien vankeus" analysoimalla standardimallia kuvaavia Yangin-Millsin yhtälöitä (1954). Palkinnon saantia ei haittaa, jos samantien löytää lopullisen ratkaisun koko hiukkasfysiikalle.

Ongelman esitellyt Royal Societyn entinen presidentti Sir Michael Atiyah ei salaillut

matemaatikkojen ironista suhtautumista fysiikkaan. Vakaumuksellinen platonisti Alain Connes puolestaan kommentoi, ettei fysikaalista todellisuutta kannata ottaa kovin vakavasti, koska se on vain matemaattisen todellisuuden vähäpätöinen osa; illuusio, jonka

kaltaisemme massiiviset havainnoitsijat kokevat.

Ongelma 6: Navierin-Stokesin yhtälöt

Navierin-Stokesin (ja Eulerin) yhtälöt ovat virtausdynamiikan perusyhtälöt. Tarkastelkaamme kokoonpuristumatonta nestettä avaruudessa ${\Bbb R}^{n}$ (tavallisesti n=2 tai n=3).

Pisteessä $x\in {\Bbb R}^{n}$ hetkellä t>0 olevan nestehiukkasen nopeusvektori olkoon $u(x,t)=(u_{i}(x,t))_{1\leq i\leq n}\in {\Bbb R}^{n}$ ja paine $p(x,t)\in {\Bbb R}$. Navierin-Stokesin yhtälöt kuuluvat seuraavasti:

$$\begin{align}
\frac{\partial}{\partial t}u_{i}+\sum_{j=1}^{n}u_{j}\frac{\partial u_{i}}{\partial x_{j}}=\nu \Delta u_{i} -\frac{\partial p}{\partial x_{i}} +f_{i}(x,t) \qquad & (x\in {\Bbb R}^{n}, t \geq 0) \\
\text{div}\, u = \sum_{i=1}^{n}\frac{\partial u_{i}}{\partial x_{i}}=0 \qquad & (x\in {\Bbb R}^{n}, t \geq 0),
\end{align}$$

minkä lisäksi tarvitaan alkuehto

$$u(x,0)=u^{0}(x).$$

Yllä olevassa $u^{0}(x)$ on sileä lähteetön vektorikenttä ${\Bbb R}^{n}$:ssä, $f_{i}(x,t)$:t ovat annetun ulkoisen voiman (esimerkiksi painovoiman) komponentit, ν on positiivinen vakio eli viskositeetti ja $\Delta = \sum_{i=1}^{n}\frac{\partial^2}{\partial x_{i}^{2}}.$ Jos viskositeetti $\nu = 0$, samoista kaavoista saadaan erikoistapauksena Eulerin yhtälöt.

Leonhard Euler eli 1707--1783, Claude Navier 1785--1836 ja George Gabriel Stokes 1819--1903. Kaksiulotteisessa tapauksessa heidän muotoilemansa virtausdynamiikka hallitaan nykyisin suurin piirtein. Sen sijaan kolmiulotteinen tapaus on ollut vuosisatoja avoinna. Ei tiedetä tarkkaan, millä ehdoilla em. yhtälöillä on olemassa fysikaalisesti realistinen sileä ratkaisu. Kysymys on hyvin konkreettisista asioista kuten aina virtausdynamiikassa: nesteen virtauksesta joessa, meressä tai vaikkapa kahvipannussa. Tuntuu omituiselta, ettei vuosisatojen yrittämisen jälkeen ymmärretä, mitä yhtälöiden tasolla täsmällisesti tapahtuu, kun kaadan kahvia kuppiin! On tyydyttävä klassiseen toteamukseen: Minä juon nyt kahvia.

Ongelma 7: Birchin ja Swinnerton-Dyerin konjektuuri

Kokonaislukuyhtälöt eli Diofantoksen yhtälöt ovat olleet matemaatikkojen erityisen kiinnostuksen kohteena antiikista asti.

Kuuluisin niistä on

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

jonka jo Eukleides osasi ratkaista Pythagoraan lausetta vastaavassa tapauksessa n=2. Yleisesti tunnettu ratkaisu on esimerkiksi x=3, y=4 ja z=5, jonka avulla rakennusmiehet ovat jo vuosituhansia sitten osanneet muodostaa suoran kulman pelkän nuoranpätkän avulla. Fermat'n suuri lause, jonka Andrew Wiles äskettäin todisti, sanoo ettei em. yhtälöllä sen sijaan ole kokonaislukuratkaisuja, kun n>2.

Hilbertin kymmenes ongelma kysyy, onko diofanttisten yhtälöiden ratkaisemiseksi olemassa yleispätevää menetelmää. Vuonna 1970 venäläinen Juri Matijasevit{\v s} osoitti, ettei näin ole. Erikoistapauksissa voidaan kuitenkin sanoa jotain. Genuksen yksi elliptisten käyrien tärkeässä erikoistapauksessa Birchin ja Swinnerton-Dyerin konjektuuri vuodelta 1965 sanoo, että rationaalisten ratkaisujen muodostaman ryhmän koko riippuu kyseiseen käyrään liittyvän Riemannin zeta-funktion yleistyksen käyttäytymisestä lähellä arvoa s=1.

Tällaiset asiat ovat erittäin teknisiä eikä niitä ole mahdollista popularisoida lyhyesti. Osoituksena siitä, että viisaskin voi mennä vipuun, mainittakoon Leonhard Eulerin konjektuuri vuodelta 1769. Hän arveli, ettei diofanttisella yhtälöllä

$x^4+y^4+z^4=t^4$

voi olla ratkaisuja. Vuonna 1988 Harvardin yliopiston matematiikan professori Noam D. Elkies kuitenkin löysi seuraavan vastaesimerkin:

2682440^4 + 15365639^4 + 18796760^4 = 20615673^4.

Elkies on hämmästyttävä tapaus, sillä hän on niittänyt mainetta myös säveltäjänä. Juuri hänen käsialaansa on muun muassa laulu Harvard Alma Mater, joka alkaa sanoin:

Fair Harvard, thy sons to thy jubilee throng...

Lasikuution vankina

Miljoonan dollarin ansaitsemiseksi löytyy helpompiakin keinoja kuin edellä mainittujen ongelmien ratkaiseminen! Yksi mahdollisuus on kirjoittaa kansainväliseksi bestselleriksi nouseva romaani. Esimerkiksi slummissa syntynyt intialainen Arundhati Roy sai miljoona dollaria läpimurtoteoksensa *Joutavuuksien jumala* pelkistä julkaisuoikeuksista.

Collège de Francen tilaisuudessa oli viitisensataa osallistujaa. Nuorimmille heistä järjestäjät antoivat kannustimeksi harvinaislaatuisen lahjan: lasikuution, johon "uudet Hilbertin ongelmat" on upotettu. Minä sain sellaisen, mutta Sören Illman ei saanut. Teksti tosin on niin pientä söherrystä, että sen lukemiseksi tarvitaan suurennuslasi.

Matematiikassa tunnetaan myös käsite Hilbertin kuutio, joka on varsin kunnianarvoisa matemaattisen mietiskelyn kohde. Minulla lienee nyt siis hallussani Suomen ainoa Hilbertin kuutio!

Kirjoittaja on Helsingin ja Jyväskylän yliopistojen matematiikan dosentti.