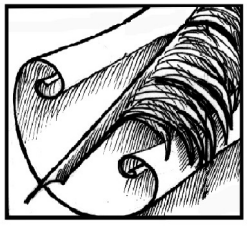

Perustutkimus ja sen merkitys

Pääkirjoitus

Olen lukuteoreetikko. Edustan siis sellaista matematiikan alaa, jota toiset pitävät täysin vanhentuneena. Monet lukuteorian perustuloksista ovatkin hyvin vanhoja – esimerkiksi differentiaali- ja integraalilaskenta on hyvin modernia ja uutta matematiikkaa verrattuna tulokseen siitä, että alkulukuja on ääretön määrä. Todistus sille, että alkulukuja on ääretön määrä, löytyy jo Eukleideen Elementasta. Todistus ei ehkä ole kirjoitettu ihan samoin kuin se kirjoitettaisiin nykyään. Todistuksessa nimittäin osoitetaan, että jos alkuluvut olisivat A, B ja C, niin olisi myös muita alkulukuja. Todistuksen idea on kuitenkin täysin pätevä ja vastaa yleisesti nykyäänkin esitettävää todistusta.

Ei varmaan ole yllätys, että Eukleideen Elementasta löytyy myös esimerkiksi Eukleideen algoritmin periaatteet. Eukleideen algoritmin avulla määritellään suurin yhteinen tekijä. Sen avulla voi määrittää myös murtoluvun ketjumurtoesityksen. Ketjumurtoesitys tuokin minut tämän kirjoituksen varsinaiseen asiaan: se että lukuteoria on vanha ala, ei tee siitä vanhentunutta alaa.

Lukuteoriaa tutkitaan yhä. Itse asiassa monet avoimet tunnetut tutkimusongelmat liittyvät nimenomaan lukuteoriaan. Näistä osa on esitettävissä hyvin alkeellisin (suorastaan antiikkisin) käsittein. Eräs tällainen ongelma on Goldbachin konjektuuri, jonka mukaan jokainen kakkosta suurempi parillinen kokonaisluku voidaan esittää kahden alkuluvun summana. Goldbachin ongelma ei sentään ole antiikista peräisin, mutta vanha sekin on.

Lukuteoriassa on kuitenkin myös paljon muuta tutkimusta, josta suuri osa kuuluu niin sanotun perustutkimuksen piiriin, eli se on nimenomaan matematiikan perusteiden ja teorian tutkimusta, eikä esimerkiksi ajankohtaisten sovellusten katalysoimaa.

Tämä epäilemättä selittää osaltaan sen, miksi jotkut pitävät lukuteoriaa jotenkin vanhana alana. Tämä on kuitenkin suuri harhakäsitys. Ensimmäinen asia on se, että lukuteoriaa itse asiassa käytetään varsin moderneissa sovelluksissa. Esimerkiksi RSA-kryptosysteemi perustuu kongruensseihin ja Fermat'n pikkulauseen (tai Eulerin lauseen) soveltamiseen. Kaikki palikat ovat olleet olemassa jo ties kuinka kauan, mutta vasta vuonna 1977 Rivest, Shamir ja Adleman kuvailivat RSA-järjestelmän MIT:ssa julkaistussa teknisessä raportissa ja vuonna 1978 menetelmä julkaistiin Communications of the ACM -lehdessä. Kummassakin tilannetta on kuvailtu johdannossa näin: "The era of 'electronic mail' may soon be upon us; we must ensure that two important properties of the current 'paper mail' system are preserved: (a) messages are private, and (b) messages can be signed. We demonstrate in this paper how to build these capabilities into an electronic mail system."

Rivest, Shamir ja Adleman siis ottivat hyvin vanhoja työkaluja ja sovelsivat niitä tilanteeseen, joka oli vasta tulevaisuutta. Jos näitä työkaluja ei olisi ollut käytettävissä, olisi soveltaminen ollut vielä paljon haastavampaa.

Mainitsin aiemmin Eukleideen algoritmin, ja miten se on oleellinen esimerkiksi ketjumurtolukujen yhteydessä. Vuonna 1990 Wiener julkaisi IEEE Transactions

on Information Theory -lehdessä artikkelin, jossa hän osoitti, että RSA-järjestelmä murtuu, kun salainen eksponentti on pieni. Tässä tilanteessa ”pieni” tarkoittaa sitä, että se on korkeintaan noin neljäs juuri julkisesta modulista, eli oikeasti kymmenien tai satojen bittien mittainen. Menetelmässä kriittistä on se, että kaikki todella hyvät approksimaatiot luvuille saadaan ketjumurtoesitysten avulla. Ketjumurtoesitys taas voidaan laskea polynomisessa ajassa Eukleideen algoritmin avulla.

Kun halutaan nopeita tuloksia, hienoja moderneja sovelluksia tai ei ymmärretä perustutkimuksen merkitystä, unohdetaan se, että hienot modernit sovellukset nojaavat usein kymmenien, satojen tai tuhansien vuosien takaiseen teoriaan, eli itse asiassa kymmenien, satojen tai tuhansien vuosien takaiseen perustutkimukseen. Jos siis rahan säästämiseksi säästetään perustutkimuksesta, viedään pois tulevaisuudelta. Tämä on käsittämättömän lyhytnäköistä.

Anne-Maria Ernvall-Hytönen