Zermelo ja aritmetiikan peruslause

Esa V. Vesalainen
Matematiikan ja tilastotieteen laitos, Helsingin yliopisto

Lukuteorian alkeita opiskellessa ensimmäinen iso merkkipaalu lienee aritmetiikan peruslause, joka sanoo, että jokainen luonnollinen luku $n > 1$ on tekijöiden järjestystä vaille yksikäsitteisellä tavalla alkulukujen tulo. Tavallisesti tämä todistetaan niin, että ensin jakoyhtälöstä lähtien esitellään Eukleideen algoritmi, jolla vuorostaan ratkaistaan lineaariset Diofantoksen yhtälöt. Lineaaristen Diofantoksen yhtälöiden ratkaisuiden olemassaolosta sitten seuraa, että jos alkuluku jakaa tulon, niin se jakaa myös jonkin tulontekijöistä. Tämän jälkeen alkutekijöihin jaon yksikäsitteisyys seuraa helpohkosti.

Koska Eukleideen algoritmi on hyvin tärkeä, ja siksi esiteltävä lukuteorian alkeiden yhteydessä, yllä kuvattu tie aritmetiikan peruslauseeseen on varsin taloudellinen, ja näin asiat esitetään useimmissa suomalaisissa lukion oppikirjoissakin.

Toisaalta, tämän klassisen lähestymistavan perusteella arvaisi, että aritmetiikan peruslause on jollakin tapaa vaikea lause todistaa, mutta osoittautuu, että näin ei olekaan. Nimittäin, joukko-opillisista ansioistaan kuuluisa saksalainen matemaatikko E. Zermelo keksi vaihtoehtoisen todistuksen 1912, joka perustuu lähinnä jaollisuuden helpoimpiin perusominaisuuksiin, ja suoraviivaiseen induktioon luvun n yli. Seuraavassa tarkoituksena on esittää hänen kaunis todistuksensa.

Kertausta: jaollisuus ja alkuluvut

Muistin virkistämisen nimissä ja nähdäksemme, kuinka vähän koneistoa myöhemmin esitettävän todistuksen taakse oikeastaan kätkeytyykään, aloitamme aivan alusta, eli jaollisuuden määritelmästä: Olkoot a ja n kokonaislukuja. Jos on olemassa kokonaisluku k, jolle $a = nk$, niin merkitsemme $n \mid a$ ja sanomme, että a on jaollinen luvulla n, tai että n jakaa luvun a.

Määritelmästä seuraa suoraan monia asioita, mutta jaollisuuden perusominaisuuksista ei oikeastaan tarvita seuraavassa kuin sellaisia helppoja havaintoja, kuin että

- jos kokonaisluvuille a, b ja n pätee $n \mid a$ ja $n \mid b$, niin myös $n \mid (a + b)$ ja $n \mid (a - b)$, tai että
- jos kokonaisluvuilla a, b ja n pätee $n \mid a$, niin myös $n \mid ab$.

Lukua $p > 1$ sanotaan alkuluvuksi, jos sitä ei voi kirjoittaa itseään pienempien luonnollisten lukujen tulona. Luku 2 on varmasti alkuluku, koska ainoa sitä pienempi luonnollinen luku on 1.

Tunnetusti alkuluvut ovat eräänlaisia multiplikatiivisia ”atomeita”, joista kaikki luonnolliset luvut koostuvat:

Havainto. *Jokainen luonnollinen luku $n > 1$ on alkulukujen tulo.*

Tässä ”tulo” tosin sisältää vain yhden tulontekijän, jos n on alkuluku.

Todistus. Tehdään induktio luvun n suhteen. Tapaus $n = 2$ on selvä, koska 2 on alkuluku. Oletetaan sitten, että $n > 1$ ja kaikki luonnolliset luvut m, joilla $1 < m < n$, ovat alkulukujen tuloja.

Nyt, jos n on alkuluku, asia on selvä. Muutoin luku n on pienempien luonnollisten lukujen tulo, ja induktio-oletuksen nojalla nämä pienemmät luvut ovat alkulukujen tuloja, ja siis myös n on, ja todistus on valmis.

Todettakoon, että tämän argumentin voisi luontevasti integroida Zermelon todistuksessa tehtävään induktiopäättelyyn.

Vaikka se ei olisikaan tarpeen, seuraava tulos on hyvä mainita jo ihan täydellisyydenkin vuoksi. Vaikka tätä tulosta ei aritmetiikan peruslauseen todistuksessa tarvitakaan, se on peruslauseen kannalta ilmeisen oleellinen tulos. Lisäksi se on kenties Zermelon todistustakin kauniimpi esimerkki siitä, miten paljon joskus pystyy sanomaan niin vähin työkaluin.

Lause. *Alkulukuja on äärettömän monta.*

Eukleideen todistus. Tehdään vastaoletus: oletetaan, että alkulukuja on vain äärellinen määrä. Olkoot $p_1 < p_2 < \ldots < p_k$ kaikki alkuluvut, missä tietenkin $k \in \mathbb{Z}_+$.

Tarkastellaan lukua $N = p_1 p_2 \cdots p_k + 1$. Koska on olemassa ainakin yksi alkuluku, nimittäin 2, on $N > 1$. Luku N on siis alkulukujen tulo, ja sen on oltava jaollinen ainakin yhdellä alkuluvulla, jonka vastaoletuksen nojalla täytyy olla jokin luvuista p_1, p_2, …, p_k, sanokaamme p_ℓ. Nyt $p_\ell \mid N$ ja varmasti $p_\ell \mid p_1 p_2 \cdots p_k$, eli

$$p_\ell \mid (N - p_1 p_2 \cdots p_k) = 1,$$

mikä on selvästi mahdotonta.

Aritmetiikan peruslause ja ”vastaesimerkkejä”

Nyt voimme keskittyä tekijöihinjaon yksikäsitteisyyteen. Mielenkiinnon kohteena oleva tulos on siis seuraava.

Aritmetiikan peruslause. *Jokainen luonnollinen luku $n > 1$ on alkulukujen tulo tekijöiden järjestystä vaille yksikäsitteisellä tavalla.*

Vaikka tämä tulos onkin luonnollisen tuntuinen, mitenkään itsestäänselvä se ei ole. Kuitenkaan lukuteorian perusesityksissä ei aina pohdita kysymystä siitä, miten alkulukujen tekijöihinjako oikeastaan voisi mennä pieleen. Joka tapauksessa lienee ainakin mielenkiintoista ennen todistusta tutustua analogisiin tilanteisiin, jossa tulos ei päde.

Hilbert esitti aikoinaan yksinkertaisen esimerkin epäyksikäsitteisestä tekijöihinjaosta. Luonnollisesti esimerkki ei voi koskea kokonaislukujen tekijöihinjakoa, koska niille yksikäsitteinen tekijöihinjako pätee, kuten tulemme näkemään. Hilbertin esimerkki koskee lukuja, jotka ovat muotoa $4k + 1$ jollakin ei-negatiivisella kokonaisluvulla k:

$$1, \quad 5, \quad 9, \quad 13, \quad 17, \quad 21, \quad 25, \quad 29, \quad 33 \quad \ldots$$

On helppo nähdä, että kahden tämän listan luvun tulo on myös tämän listan luku: Nimittäin lukujen $4k + 1$ ja $4k' + 1$ tulo on muotoa

$$(4k + 1)(4k' + 1) = 4(4kk' + k + k') + 1.$$

Samoin, näille luvuille löytyy ilmeinen ”alkuluvun” käsite; esimerkiksi luvut 5, 21, 9 ja 49 ovat ”alkulukuja”, koska ne eivät ole pienempien saman listan lukujen tuloja. Kolme viimeksi mainittua siksi, että niiden ainoat oikeat alkulukutekijät 3 ja 7 eivät ole muotoa $4k + 1$. Nyt luvulle 441 saadaan kaksi oleellisesti erilaista ”tekijöihinjakoa”

$$441 = 21 \cdot 21 = 9 \cdot 49.$$

Muita, vakavampia esimerkkejä saadaan, kun tarkastellaan kokonaislukujen renkaan laajennoksia, mitkä lukuteoriassa ovat erittäin tärkeitä. Esimerkiksi jos kokonaislukujen sekaan lisää luvun $i\sqrt{5}$, jolloin siis tarkastellaan lukuja $a + bi\sqrt{5}$, missä $a, b \in \mathbb{Z}$, niin osoittautuu, että luvulla 21 on kaksi oleellisesti erilaista tekijöihinjakoa:

$$21 = 3 \cdot 7 = \left(1 + 2i\sqrt{5}\right)\left(1 - 2i\sqrt{5}\right).$$

Osoittautuu, että eräässä mielessä tällaiset esimerkit ovat luonteeltaan Hilbertin esimerkin kaltaisia; alkulukuja on niissä ikään kuin liian vähän. 1800-luvulla tälle ongelmalle löydettiin suurenmoinen osittaisratkaisu tarkastelemalla lukujen sijasta ns. ideaaleita.

Zermelon todistus

Todistamme aritmetiikan peruslauseen induktiolla luvun n suhteen. Todetaan ensin, että väite pätee, kun n on alkuluku. Erityisesti, väite on selvä, kun $n = 2$.

Oletetaan sitten, että $n > 1$, ja että väite on jo todistettu kaikille lukua n pienemmille positiivisille kokonaisluvuille. Meidän on osoitettava, että jos luvun n kirjoittaa kahdella eri tavalla alkulukujen tulona, niin itse asiassa molemmissa tuloissa esiintyvät täsmälleen samat alkuluvut, tosin mahdollisesti eri järjestyksessä.

Jos luku n sattuu olemaan alkuluku, olemme valmiit. Muutoin on olemassa pienin epätriviaali luvun n tekijä p, siis pienin $p \in \mathbb{Z}_+$, jolle $p \mid n$ ja $1 < p < n$. Tämä luku p on itse asiassa alkuluku, sillä luvun p epätriviaali tekijä olisi lukua p pienempi luvun n epätriviaali tekijä.

Kirjoitetaan $n = pb$, missä $b \in \mathbb{Z}_+$ on tietenkin pienempi kuin n. Nyt induktio-oletuksen nojalla luku b on alkulukujen tulo yksikäsitteisellä tavalla. Tästä seuraa, että luvulla n on vain yksi alkutekijöihinjako, jossa esiintyy luku p.

Seuraavaksi on osoitettava, että luvulla n ei voi olla muita alkutekijöihinjakoja. Tehdään se vastaoletus, että luvulla n olisi jokin muukin alkutekijöihinjako. Olkoon sen pienin alkutekijä q. Nyt siis $p < q$ ja $n = qc$ jollakin $c \in \mathbb{Z}_+$, jolle $c < n$ ja $p \nmid c$.

Seuraavaksi tarkastellaan lukua

$$n_0 = n - pc = \begin{cases} pb - pc = p\,(b - c)\,, \\ qc - pc = (q - p)\,c. \end{cases}$$

Tämä luku on positiivinen kokonaisluku ja varmasti pienempi kuin n. Koska $p \mid n_0$, on induktio-oletuksen nojalla alkuluvun p esiinnyttävä tulon $(q - p)\,c$ alkutekijähajotelmassa, ja siis ainakin toisen luvuista $q - p$ ja c alkutekijähajotelmassa. Mutta olemme jo todenneet, että $p \nmid c$, eli on oltava $p \mid (q - p)$. Mutta nyt olisi myös $p \mid (q - p + p) = q$, ja koska p ja q ovat molemmat alkulukuja, olisi $p = q$, vastoin sitä seikkaa, että $p < q$. Olemme päätyneet ristiriitaan, ja siksi luvulla n on oltava vain yksi alkutekijöihinjako, ja olemme valmiit.

Lähteet

Klassisesta jaollisuusteoriasta suomenkielellä löytyy esimerkiksi hyvä lukiotason esitys oppikirjasta [3], ja Väisälän oppikirjasta [7] yliopistollisempi esitys, joka on tiiviimpi, mutta luonnollisesti etenee aiheeseen syvemmälle.

Alkulukujen äärettömyyden todistus on peräisin Eukleideen Alkeista [2], missä se on 9. kirjan 20. propositio.

Kirjoittaja oppi Zermelon todistuksesta ensimmäisen kerran Hassen klassikkoteoksesta [5]. Vaikka todistus on peräisin jo vuodelta 1912, jolloin Zermelo keskusteli siitä mm. Hurwitzin ja Landaun kanssa, se julkaistiin ensimmäisen kerran vasta 1934 hänen ainoassa puhtaasti lukuteoreettisessa paperissaan [8], joka löytyy myös hänen kootuista teoksistaan [9] Volken lyhyen mutta kiintoisan historiallisen johdannon [6] kanssa.

On mielenkiintoista, että ennen Gaussia ja hänen monumentaalista teostaan [4], kukaan ei ollut muotoillut aritmetiikan peruslausetta, vaikka siihen riittävä koneisto oikeastaan löytyykin jo Eukleideen Alkeista [2].

Hilbertin esimerkki on esitelty esimerkiksi Cohnin oppikirjan [1] pykälässä III.5. Esimerkki luvun 21 tekijöihinjaosta on saman teoksen pykälästä VI.6. Kokonaislukujen renkaan laajentamiseen ja ideaaliteoriaan voi tutustua suomeksikin esimerkiksi Väisälän kirjasta [7].

Viitteet

[1] Cohn, H.: *Advanced Number Theory*, Dover Publications, 1980.

[2] Eukleides: *Alkeet*, n. 300 eKr. Tämän teoksen eri käännöksiä löytyy Internetistä runsaasti. Linkkejä näihin löytyy helposti esimerkiksi Wikipedia-sivulta `http://en.wikipedia.org/wiki/Euclid's_Elements`.

[3] Ernvall-Hytönen, A.-M., K. Luosto, ja T. Pokela: *Pyramidi 11: Lukuteoria ja logiikka*, Tammi, 2006.

[4] Gauss, C. F.: *Disquisitiones Arithmeticae*, 1801. Alkuperäinen latinankielinen teksti on myöhemmin käännetty monille kielille, englanniksi löytyy A. A. Clarken käännös (Yale University Press, 1966, tai Springer, 1986).

[5] Hasse, H.: *Number Theory*, Classics in Mathematics, Springer, 2002.

[6] Volke, D.: *Introductory note to 1934*, johdanto Zermelon artikkeliin [8] kokoomateoksessa [9], 574–575.

[7] Väisälä, K.: *Lukuteorian ja korkeamman algebran alkeet*, Otava, 1961.

[8] Zermelo, E.: *Elementary considerations concerning the theory of prime numbers*, kokoomateoksessa [9], 576–581, mistä löytyy myös alkuperäinen *Elementare Betrachtungen zur Theorie der Primzahlen*, Wissenschaftliche Gesellschaft zu Göttingen, 2.11.1934.

[9] Zermelo, E. (kirj.), sekä H.-D. Ebbinghaus, ja A. Kanamori (toim.): *Ernst Zermelo. Collected Works. Volume I. Set Theory, Miscellanea*, Springer, 2010.