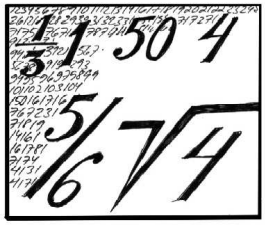

Lukujen uusi maailma: p-adiset luvut

Tauno Metsänkylä
Matematiikan laitos, Turun yliopisto

Kun kokonaislukujen 0,1,2,... joukkoa laajennetaan vaiheittain ottamalla mukaan negatiiviset kokonaisluvut, murtoluvut, irrationaaliluvut ja lopulta imaginaariluvut, saadaan rakennetuksi kompleksilukujen joukko $\mathbf{C}$. Tämä on laajin mahdollinen "lukujen maailma", kuten Solmussakin hiljattain [2] kerrottiin: sitä ei voida enää laajentaa, jos sen halutaan säilyttävän totutut yhteen-, vähennys-, kerto- ja jakolaskusäännöt. Joukkoa, jossa nämä säännöt pätevät, sanotaan matematiikan kielellä *kunnaksi*, ja erityisesti $\mathbf{C}$ on *algebrallisesti suljettu kunta*.

Mutta tässä ei ole koko tarina lukualueiden laajentamisesta ja "hyvistä" lukumaailmoista. Lähtemällä liikkeelle rationaalilukujen joukosta ja käyttämällä toisenlaista laajentamistapaa päädytään uudenlaisiin joukkoihin, joiden alkioita voidaan hyvästä syystä myös nimittää luvuiksi. Myös niistä muodostuu nimittäin kunta, jolla on monia samanlaisia ominaisuuksia kuin reaalilukukunnalla $\mathbf{R}$ ja kompleksilukukunnalla $\mathbf{C}$. Lisäksi sillä on useita jännittävällä tavalla erilaisia ominaisuuksia.

Kyseessä ovat *p-adiset luvut*. Tässä p tarkoittaa mitä tahansa alkulukua eli jaotonta lukua, joka on valittu kiinteäksi. Tapauksissa $p = 2$ ja $p = 3$ puhutaan myös *dyadisista* ja *triadisista* luvuista, mikä ehkä saa oudonnäköisen "adinen"-päätteen (englanniksi *adic*) kuulostamaan luontevammalta.

Tällaiset p-adiset luvut eivät ole mikään pelkkä kuriositeetti. Ne ovat päin vastoin osoittautuneet hyvin käytökelpoisiksi usealla matematiikan alalla, erityisesti lukuteoriassa.

Etäisyyksiä ja itseisarvoja

Ajatellaan ensin reaalilukujoukkoa $\mathbf{R}$. Sen alkioiden kesken voidaan paitsi suorittaa tavallisia laskutoimituksia myös ajatella *etäisyyksiä*: kahden luvun a ja b etäisyys on $|a - b|$. Tämä ns. *euklidinen* etäisyys vastaa arkielämän etäisyyskäsitettä, kun reaalilukuja kuvataan lukusuoran pisteinä.

Etäisyys näyttelee keskeistä osaa monissa matematiikan tarkasteluissa. Siksi on luonnollista kysyä, olisiko euklidisella etäisyydellä vaihtoehtoja ja mitä seurauksia sellaisesta olisi.

Ensiksi on syytä miettiä, mitä ominaisuuksia etäisyydellä pitää olla. Ilmeisesti ainakin kahden eri luvun etäisyyden on oltava positiivinen ja luvun etäisyyden itsestään on oltava 0. Lisäksi etäisyyden täytyy suhtautua lukujen laskutoimituksiin "oikealla" tavalla. Euklidisen etäisyyden tapauksessa nämä etäisyyden ominaisuudet palautuvat seuraaviin itseisarvon ominaisuuksiin: aina kun $a,b \in \mathbf{R}$,

E1. $|a| > 0$, jos $a \neq 0$; $|0|=0$,

E2. $|ab| = |a| \cdot |b|$,

E3. $|a + b| \leq |a| + |b|$.

Viimeksi mainittu ominaisuus on tärkeä *kolmioepäyhtälö*. Tämän nimityksen voi ymmärtää ajattelemalla hetkeksi a ja b kompleksilukuina ja esittämällä ne kompleksitason pisteinä (tai vektoreina); silloin ehto E3 sanoo, että kolmion sivu on pienempi (tai yhtäsuuri) kuin kahden muun sivun summa.

Kysymystä uudenlaisesta etäisyydestä voidaan nyt pohtia kysymällä, voitaisiinko luvuille ensin määritellä jokin toinen ehdot E1–E3 täyttävä "itseisarvo". Tällaisia mahdollisuuksia kyllä onkin, mutta ne eivät johda mihinkään mielenkiintoiseen etäisyyskäsitteeseen. Tilanne muuttuu paremmaksi, kun hylätään ajatus, että lukualueena on koko $\mathbf{R}$. Sen takia muutetaan lähtötilannetta siten, että otetaan $\mathbf{R}$:n tilalle sen osajoukko $\mathbf{Q}$, pelkät rationaaliluvut. Ajatellaan siis lähtökohtana vain rationaalilukujen välistä euklidista etäisyyttä sekä tätä etäisyyttä luonnehtivia ehtoja E1–E3, missä nyt $a,b \in \mathbf{Q}$.

Osoittautuu, että tässä tapauksessa ehdot E1–E3 pysyvät voimassa, kun tavallinen itseisarvo $|a|$ korvataan *p-adisella itseisarvolla* $|a|_p$. Tämä määritellään seuraavasti. Kiinnitetään alkuluku p ja kirjoitetaan rationaaliluku $a = \frac{t}{u}$ supistettuna murtolukuna, missä siis t ja u ovat kokonaislukuja, joilla ei ole yhteisiä tekijöitä. Tässä on tietysti oletettava, että $a \neq 0$. Katsotaan, onko jompikumpi luvuista t,u jaollinen p:llä, ja kirjoitetaan a muotoon

$$a = p^k \frac{t_1}{u_1},$$

missä t_1 ja u_1 ovat p:llä jaottomia. Eksponenttia k, joka siis on positiivinen, negatiivinen tai 0, sanotaan luvun a *p-eksponentiksi*. Otetaan sille käyttöön merkintä $k = v_p(a)$. Voidaan sanoa, että a on *jaollinen* alkuluvun p potenssilla $p^{v_p(a)}$ (sillä siitähän on kysymys, jos a sattuu itse olemaan kokonaisluku). Nyt asetetaan määritelmä

$$|a|_p = (\tfrac{1}{2})^{v_p(a)} \qquad (a \neq 0) \tag{1}$$

ja lisäksi $|0|_p = 0$. Silloin ehdot E1–E3 ovat voimassa, kun $|.|$:n tilalla on $|.|_p$. Ensimmäinen ehtohan nähdään suoraan määritelmästä ja E2 ja E3 seuraavat (tapauksessa $a \neq 0, b \neq 0$) siitä, että

$$v_p(ab) = v_p(a) + v_p(b),$$
$$v_p(a+b) \geq \min(v_p(a), v_p(b)). \tag{2}$$

Tässä jälkimmäinen ehto siis lausuu, että summasta $a+b$ voidaan ottaa yhteiseksi tekijäksi vähintään se p:n potenssi, jolla molemmat yhteenlaskettavat ovat jaollisia. Voit myös varmistua näistä kirjoittamalla

$$a = p^{v_p(a)} \frac{t_1}{u_1}, \quad b = p^{v_p(b)} \frac{t_2}{u_2}$$

ja muodostamalla näiden lukujen tulon ja summan.

Summan tapauksessa ehdosta (2) seuraa edelleen, että

$$|a+b|_p \leq \max(|a|_p, |b|_p) \leq |a|_p + |b|_p. \tag{3}$$

Täydellisyyden vuoksi ehdot E2 ja E3 on tarkistettava myös tapauksessa, jossa esim. $a = 0$. Silloin näiden ehtojen paikkansapitävyys nähdään välittömästi.

Luvun $\frac{1}{2}$ valinta kaavassa (1) on pitkälti mielivaltainen; mikä tahansa luku r väliltä $0 < r < 1$ kelpaisi. Tämän luvun vaihteleminen merkitsisi vain eräänlaista mittakaavan vaihtelua. Usein tehdään mittakaavan normalisointi valitsemalla $r = \frac{1}{p}$.

Esimerkiksi alkuluvulla $p = 5$ saadaan

$$|\tfrac{75}{88}|_5 = |5^2 \cdot \tfrac{3}{88}|_5 = (\tfrac{1}{2})^2 = \tfrac{1}{4},$$
$$|\tfrac{11}{15}|_5 = |5^{-1} \cdot \tfrac{11}{3}|_5 = (\tfrac{1}{2})^{-1} = 2,$$
$$|1250|_5 = |5^4 \cdot 2|_5 = (\tfrac{1}{2})^4 = \tfrac{1}{16},$$
$$|\tfrac{261}{13}|_5 = (\tfrac{1}{2})^0 = 1.$$

Näin määritelty p-adinen itseisarvo $|.|_p$ antaa rationaalilukujen a ja b *p-adisen etäisyyden* $|a-b|_p$. Sanotaan myös, että $|.|_p$ määrittelee rationaalilukujen joukossa *p-adisen metriikan*. Huomaa, että a ja b ovat "lähekkäin", kun $a-b$ on jaollinen korkealla p:n potenssilla. Tämä on p-adisen metriikan tyypillinen piirre, joka kannattaa muotoilla erityisesti näkyville:

Kahden rationaaliluvun p-adinen etäisyys on sitä pienempi, mitä korkeammalla p:n potenssilla niiden erotus on jaollinen.

Erityisesti siis p:n kasvavien potenssien jonossa $p,p^2,p^3,\ldots$ lukujen etäisyys nollasta pienenee eli tässä metriikassa nämä luvut lähestyvät nollaa.

On myös tärkeä huomata, että (3):n nojalla kolmioepäyhtälölle saadaan nyt vahvempi muoto

$$|a+b|_p \leq \max(|a|_p, |b|_p). \tag{4}$$

Katsomalla tarkemmin sitä, miten (3) edellä pääteltiin oikeaksi, havaitaan lisäksi, että

$$|a+b|_p = \max(|a|_p, |b|_p), \qquad \text{jos } |a|_p \neq |b|_p. \tag{5}$$

Näillä kahdella kaavalla on kauaskantoiset seuraukset p-adisten lukujen maailmassa. Kaavan (4) perusteella p-adista metriikkaa sanotaan myös *epäarkhimediseksi*; siltä nimittäin puuttuu eräs euklidisen metriikan yksinkertainen ominaisuus, jota matemaatikot sanovat "Arkhimedeen ominaisuudeksi".

Käytetään myös nimitystä *ultrametriikka*. Tämä johtuu siitä, että tällä metriikalla on oudontuntuisia ominaisuuksia. Esimerkiksi kun $|a|_p, |b|_p$ ja $|a+b|_p$ tulkitaan vastaavasti kuin edellä kolmion sivujen pituuksiksi, niin (5):stä nähdään, että jokainen kolmio p-adisessa metriikassa on tasakylkinen! Kolmiossa nimittäin joko $|a|_p = |b|_p$ tai muussa tapauksessa $|a+b|_p = |a|_p$ tai $|b|_p$.

Uusia lukuja

Tähän mennessä olemme siis löytäneet rationaalilukujen joukossa uuden metriikan mutta toistaiseksi ei ole saatu vielä aikaan yhtään uutta "lukua". Nyt on niiden vuoro.

Jos "tavallisessa" matematiikassa halutaan selvittää annetun murtoluvun suuruus, niin luku kannattaa yleensä muuttaa desimaaliluvuksi: esim. $\frac{109}{8} = 13{,}625$ eli

$$\frac{109}{8} = 1 \cdot 10^1 + 3 \cdot 10^0 + 6 \cdot 10^{-1} + 2 \cdot 10^{-2} + 5 \cdot 10^{-3}.$$

Tässä desimaalien vaikutus luvun suuruuteen vähenee oikealle mentäessä, koska potenssit $10^{-1}, 10^{-2}, 10^{-3}$ pienenevät. Näin siis euklidisessa metriikassa.

Vastaavasti p-adisessa metriikassa kannattaa lausua annettu luku p:n *kasvavien* potenssien mukaan, esim. (kun $p = 5$)

$$199 = 4 + 4 \cdot 5 + 2 \cdot 5^2 + 1 \cdot 5^3,$$

sillä potenssit $p, p^2, p^3, \ldots$ lähenevät nollaa p-adisessa metriikassa. (Käytännössä edellisen kehitelmän määrittäminen kannattaa tosin tehdä "takaperin", aloittamalla siitä, että 5^3 on korkein 5:n potenssi, joka ei ylitä lukua 199.)

Edellisten esimerkkien luvut oli valittu siten, että kehitelmät ovat päättyviä. Mutta rationaaliluvun desimaaliesitys voi tietysti myös olla päättymätön (jolloin se on jostain kohdasta alkaen jaksollinen), esim.

$$\frac{249}{110} = 2{,}2363636\ldots.$$

Samoin rationaaliluvun p-adinen kehitelmä, esim.

$$\frac{29}{40} = 3 \cdot 5^{-1} + 2 \cdot 5^0 + 4 \cdot 5 + 1 \cdot 5^2 + 4 \cdot 5^3 + 1 \cdot 5^4 + \cdots.$$

Tämä kirjoitelma luonnollisesti tarkoittaa, että oikealla puolella oleva summa on sitä lähempänä (p-adisessa metriikassa) lukua $\frac{29}{40}$, mitä enemmän siihen on otettu mukaan termejä, toisin sanoen mitä kauempaa se on katkaistu. Tarkemmin sanottuna: jos katkaisu on tehty potenssin p^n jälkeen, niin summan etäisyys ko. rationaaliluvusta on $\leq (\frac{1}{2})^{n+1}$. Esimerkiksi

$$\left|\frac{29}{40} - 3 \cdot 5^{-1} - 2 - 4 \cdot 5 - 1 \cdot 5^2\right|_5 = \left|-\frac{375}{8}\right|_5 = \left|-5^3 \cdot \frac{3}{8}\right|_5 = (\tfrac{1}{2})^3 = \tfrac{1}{8}.$$

(Eri asia on, miten kehitelmä saadaan määritetyksi. Siihen palataan tuonnempana.)

Rationaalilukujen joukon $\mathbf{Q}$ laajentaminen perinteiseksi reaalilukujoukoksi $\mathbf{R}$ on matemaattisesti melko monimutkainen prosessi, mutta prosessin tulos on yksinkertaista kuvailla lukusuoran avulla: uudet luvut, irrationaaliluvut, täyttävät rationaalilukujen väliset "aukot", niin että alkujaan erillisistä pisteistä muodostunut rationaalilukujen joukko on täydentynyt yhtenäiseksi suoraksi. Reaalilukuja esittävät *kaikki mahdolliset desimaaliluvut*; irrationaalisia näistä ovat ne, jotka ovat päättymättömiä ja jaksottomia. Avainasemassa tässä laajentamisprosessissa on ilmeisesti euklidinen metriikka.

Analoginen laajentaminen voidaan suorittaa p-adista metriikkaa käyttäen. Tällöin tulosta ei voida havainnollistaa lukusuoraa käyttäen, mutta joka tapauksessa tuloksena on rationaalilukujen joukkoa $\mathbf{Q}$ paljon laajempi joukko, *p-adisten lukujen joukko* $\mathbf{Q}_p$, jonka muodostavat *kaikki mahdolliset p-adiset kehitelmät*. Uusia, ei-rationaalisia lukuja näistä ovat jälleen ne, jotka ovat päättymättömiä ja jaksottomia. Yleisessä muodossa tällainen kehitelmä on muotoa

$$a_{-k}p^{-k} + a_{-k+1}p^{-k+1} + \cdots + a_0p^0 + a_1p^1 + a_2p^2 + \cdots, \quad (6)$$

missä kertoimet siis ovat kokonaislukuja välillä $0 \leq a_i \leq p-1$ ja summa jatkuu oikealle äärettömiin (joskin rationaaliluvun tapauksessa kertoimet a_i voivat jostain kohdasta alkaen kaikki olla $= 0$). Tässä voi k tietysti olla myös negatiivinen, jolloin kehitelmä alkaa p:n positiivisella potenssilla. Tavallista desimaalilukuesitystä jäljitellen lukua (6) voidaan merkitä

$$a_{-k}a_{-k+1}\ldots a_0{,}a_1a_2\ldots$$

ja siinä tapauksessa, että k on negatiivinen, $k = -h$,

$$0{,}00\ldots0a_ha_{h+1}\ldots.$$

Kertoimia a_i voidaan sanoa luvun "numeroiksi". Siis esimerkiksi

$$\frac{29}{40} = 32{,}4141\ldots$$

5-adisesti.

Näin saatuja lukuja voidaan laskea yhteen, vähentää, kertoa ja jakaa aivan samoin kuin tavallisia desimaalilukuja. Tätä valaistaan seuraavassa pykälässä muutamin esimerkein. Tuloksena oleva joukko $\mathbf{Q}_p$ onkin kunta aivan kuten $\mathbf{R}$. Lisäksi se on *täydellinen*, toisin sanoen se täyttää ehdon, joka on analoginen $\mathbf{R}$:n täydellisyysaksioman kanssa (ks. [2]).

Edellä määritelty p-adinen itseisarvo joukossa $\mathbf{Q}$ laajenee luonnollisella tavalla myös joukkoon $\mathbf{Q}_p$:

$$|a_{-k}a_{-k+1}\ldots a_0{,}a_1a_2\ldots|_p = (\tfrac{1}{2})^{-k},$$

jos $a_{-k} \neq 0$. Tarkista tämän kaavan paikkansapitävyys edellisen luvun $\frac{29}{40}$ tapauksessa. Itseisarvo $|.|_p$ antaa joukkoon $\mathbf{Q}_p$ p-adisen etäisyyden, jolla on samat ominaisuudet kuin edellä. Erityisesti voimassa ovat ehdot (4) ja (5) eli metriikka on ultrametriikka.

Niiden p-adisten lukujen x joukkoa, jotka täyttävät ehdon $|x-a|_p = r$ (missä a on annettu p-adinen luku ja r jokin $|.|_p$:n arvo), on luonnollista sanoa a-keskiseksi r-säteiseksi ympyräksi. Jos b on tämän ympyrän sisällä, toisin sanoen jos $|b-a|_p < r$, niin ehtoa (5) käyttäen saadaan

$$|x-b|_p = |x-a+a-b|_p = \max(|x-a|_p, |a-b|_p) = r$$

aina, kun x on ympyrällä. Tämä merkitsee, että myös b on ympyrän keskipiste. Siis jokainen ympyrän sisällä oleva piste on ympyrän keskipiste!

Samoin kuin reaalilukujen kunnassa $\mathbf{R}$ myös p-adisten lukujen kunnassa $\mathbf{Q}_p$ voidaan ratkaista sellaisia yhtälöitä, joilla ei ole rationaalilukuratkaisuja. Esimerkiksi yhtälöllä $x^2 = 6$ on ratkaisut $x = \pm 1{,}3042\ldots$ (päättymätön) kunnassa $\mathbf{Q}_5$. Yhtälöllä $x^4 = 1$ on tässä kunnassa maksimimäärä eli neljä ratkaisua. Kunta $\mathbf{Q}_5$ on siis tässä suhteessa parempi kuin kunta $\mathbf{R}$; tämähän on laajennettava kompleksilukukunnaksi $\mathbf{C}$ ennen kuin saadaan yhtälölle $x^4 = 1$ kaikki neljä ratkaisua ± 1, $\pm i$.

Kunta $\mathbf{Q}_p$ voidaan algebran yleisten periaatteiden mukaan laajentaa sellaiseksi kunnaksi, joka on algebrallisesti suljettu. Siinä jokaisella n:nnen asteen yhtälöllä on n ratkaisua. Lisäksi tämä kunta voidaan valita siten, että se on täydellinen yllä mainitussa mielessä. Siinä voidaan kehittää samanlaista funktioiden teoriaa kuin $\mathbf{R}$:ssä ja $\mathbf{C}$:ssä, alkaen derivoinnista ja integroinnista. Hyvän yleiskuvan asiasta saa selailemalla esim. kirjaa [1]. Näin muodostettua kuntaa, josta usein käytetään merkintää $\mathbf{C}_p$, on luonnollista pitää kompleksilukukunnan p-adisena analogiana.

Laskutoimituksia

Palataan takaisin p-adisten lukujen kuntaan $\mathbf{Q}_p$. Yksinkertaiset numerolaskut p-adisilla luvuilla sujuvat aivan vastaavasti kuin tavallisilla desimaaliluvuilla. Seuraavissa esimerkeissä aina $p = 5$.

Yhteenlasku voidaan tehdä kirjoittamalla luvut tavalliseen tapaan alakkain, mutta laskujen suunta on nyt vasemmalta oikealle, koska ”muistinumero” siirretään aina korkeamman potenssin kohdalle eli oikealle, siis esimerkiksi

$$\begin{array}{r} {\scriptstyle 1} \\ 1\,,\,2\,1 \\ 2\,,\,4\,2 \\ \hline 3\,,\,1\,4 \end{array} \quad + \qquad \begin{array}{r} {\scriptstyle 1\ 1} \\ 3\,3\,,\,2\,2 \\ 2\,,\,4\,2 \\ \hline 3\,0\,,\,2\,0\,1 \end{array} \quad +$$

Vähennyslaskussa on samoin edettävä vasemmalta oikealle, koska ”lainaaminen” tapahtuu korkeamman potenssin kohdalta. Vähennyslaskun voi myös muuttaa yhteenlaskuksi vaihtamalla vähentäjän ensin vastaluvukseen. Luvun vastaluku saadaan korvaamalla ensimmäinen numero $a_{-k} (\neq 0)$ numerolla $p - a_{-k}$ ja jokainen seuraava numero a_i numerolla $p-1-a_i$. Tämä on helppo perustella laskemalla, että näiden lukujen summaksi tulee 0. Esimerkiksi

$$-3{,}421 = 2{,}02344\ldots, \quad -0{,}01134 = -0{,}04331044\ldots$$

(kehitelmät ovat päättymättömiä). Tässä vähennyslasku molemmilla tavoilla:

$$\begin{array}{r} 4\,,\,1\,\cancel{1}\,\cancel{3} \\ 3\,,\,4\,2\,1 \\ \hline 1\,,\,2\,3\,1 \end{array} \quad - \qquad \begin{array}{r} {\scriptstyle 1\ 1\ 1} \\ 4\,,\,1\,1\,3 \\ 2\,,\,0\,2\,3\,4\,4\ldots \\ \hline 1\,,\,2\,3\,1\,0\,0\ldots \end{array} \quad +$$

Myös lukujen kertominen alakkain (tämäkin vasemmalta oikealle) on helppoa. Laskuja helpottaa, jos välituloksissa (eli kerrottaessa yksittäisellä numerolla) jätetään numerot redusoimatta välille $0,\ldots,4$, siis kirjoitetaan esimerkiksi tulo $3 \cdot 1{,}32$ muodossa 3,96. Redusoitunahan, eli ns. *kanonisessa* muodossa, se olisi 3,421. Redusointi tehdään sitten näiden lukujen yhteenlaskussa.

Tehtävä. Tarkista, että 5-adinen luku 2,1213 kerrottuna itsellään antaa tulokseksi luvun -1 viiden numeron tarkkuudella (siis 5-adisessa muodossa 4,4444). Kyseessä on kompleksilukujen kunnan imaginaariyksikköä $i = \sqrt{-1}$ vastaavan 5-adisen luvun likiarvo eli samalla myös yhtälön $x^4 = 1$ yhden ratkaisun likiarvo (vrt. edellisen pykälän loppuun).

Jos edellisessä pykälässä annettu yhtälön $x^2 = 6$ ratkaisun likiarvo 1,3042 kunnassa $\mathbf{Q}_5$ on oikea, niin 1,3042 korotettuna neliöön antaa viiden numeron tarkkuudella luvun 6 (eli 5-adisessa muodossa 1,1). Tarkista tämä.

Jakolasku (jakokulmassa) on vähän vaativampaa, koska siinä tavallaan ratkaistaan *kongruensseja* modulo p. Jos lasketaan esim. $\frac{4{,}01}{0{,}31}$, on aloitettava selvittämällä, montako kertaa 3 (jakajan ensimmäinen nollasta eroava numero) ”menee” 4:ään. Vastaus on 3, koska $3 \cdot 3$ antaa välille $0,\ldots,4$ redusoituna tulokseksi 4. Tällöin on tosiasiassa ratkaistu kongruenssi $3x \equiv 4 \pmod 5$. Helpointa on luonnollisesti laatia ensin valmiiksi pieni taulukko tuloista $3x$ laskettuna modulo 5, kun $x = 0,\ldots,4$.

Tehtävä. Suorita edellistä jakolaskua jakokulmassa pitemmälle. Kyseessä on edellisessä pykälässä esiintynyt luku 29/40, jossa osoittaja ja nimittäjä on vain kirjoitettu 5-adiseen muotoon. Sille pitää siis tulla kehitelmä $32{,}4141\ldots$.

Vähän historiaa – ja muutakin

Kunnia p-adisten lukujen keksimisestä kuuluu matemaatikko *Kurt Henselille* (1861–1941), joka toimi professorina Saksassa Marburgin yliopistossa. Hensel ei

päätynyt keksintöönsä yllä esitetyllä ajattelutavalla, vaan otti lähtökohdakseen funktioiden sarjakehitelmät (kompleksialueessa). Ajatuksena oli, että samoin kuin sarjakehitelmä tietyssä kompleksitason pisteessä kuvaa funktion käyttäytymistä tämän pisteen läheisyydessä, eli funktion *lokaalia* (paikallista) käyttäytymistä, myös luvun p-adinen kehitelmä kertoo luvusta lokaalista tietoa "paikassa p". Kuntia $\mathbf{Q}_p$ sanotaankin *lokaaleiksi kunniksi*.

Hensel julkaisi p-adisia lukuja koskevan teoriansa vuoden 1900 paikkeilla, mutta sen merkitystä ei aluksi oikein ymmärretty. Teorian varsinainen läpimurto tapahtui noin 20 vuotta myöhemmin, kun Henselin oppilas Helmut Hasse ratkaisi kuuluisan neliömuotoja koskevan probleeman p-adisia lukuja käyttäen.

Koska p-adisten lukujen varsinaiset sovellukset vaativat melko syvällistä matematiikkaa, näistä luvuista ei yleensä puhuta lukuteorian alkeiden kirjoissa. Joitakin helppolukuisia esityksiä voi löytää esim. Googlen avulla, yksinkertaisesti haulla *p-adic numbers*.

Lukijalle, joka on kiinnostunut matematiikan ja musiikin yhteyksistä ja/tai naisten aseman historiallisesta kehityksestä, vielä pieni lisäys. Kurt Henselin isoäiti oli *Fanny Hensel*, tyttönimeltään Mendelssohn, säveltäjä *Felix Mendelssohnin* sisar. Fanny oli itsekin säveltäjä, mutta tuohon aikaan sellaista pidettiin sopimattomana naiselle. Niinpä Fanny sävelsi pääasiassa pöytälaatikkoon, tai joissakin tapauksissa julkaisi sävellyksensä veljensä nimissä. Mutta nyttemmin hänen sävellyksensä on löydetty ja tunnistettu, ja ne ovat päässeet julkisuuteen. Monet niistä ovat erinomaisia – pankaapa vain merkille, jos satutte kuulemaan niitä esim. radiossa.

Viitteet

[1] Schikhof, W.H.: *Ultrametric Calculus: An Introduction to p-Adic Analysis*. Cambridge University Press, 1982.

[2] Valmari, Antti: *Onko* $\sqrt{-1}$ *olemassa?*, 1. osa, Solmu 1/2008, 18–24; 2. osa, Solmu 2/2008, 13–20.