Fareyn luvut ja Mathematica

Matti K. Sinisalo, FL
Oulun yliopisto

1996

Abstract: By the Farey sequence F_m of order m we mean the positive fractional numbers, whose denominators do not exceed m, arranged in ascending order of magnitude. In this paper we give explicit expressions to the immediately following and to the immediately preceding numbers to a given number in some Farey sequence. The method is based on the modular arithmetics and the Euclidean algorithm. This method works probably quite well even with the numbers with 1000-10000 digits.

As a byproduct of the proof of the main result we get the Farey-Cauchy theorem and the mediant theorem. As an application of the Farey numbers we give a solution to the problem of Egyptian fractions. Theoretically interesting is the connection between the distribution of the Farey numbers and the Riemann hypothesis.

The Farey sequences have applications in a very wide area of mathematics. Anyway, our computationally important explicit results have not in general been presented in the litterature of the elementary number theory, computational number theory and the theory of mathematical algorithms.

This talk is based on the lecture cource "Mathematics with microcomputer" given by the author for the students of the department of the mathematical sciences in the university of Oulu in the autumn 1995. The treatment of the subject is elementary.

Johdanto

Fareyn luvuilla tarkoitetaan positiivisia rationaalilukuja, joiden nimittäjän arvo on ylhäältä rajoitettu ts. pienempi kuin jokin annettu positiivinen kokonaisluku m. Tällaiset luvut voidaan hyvin järjestää. Esimerkiksi parametrin m arvolla 6 saadaan jono (F_6)

$$\frac{1}{6} < \frac{1}{5} < \frac{1}{4} < \frac{1}{3} < \frac{2}{5} < \frac{1}{2} < \frac{3}{5} < \frac{2}{3} < \frac{3}{4} < \frac{4}{5} < \frac{5}{6} < 1 < \frac{7}{6} < ...$$

Yleensä Fareyn jonoilla tarkoitetaan välillä $(0, 1]$ olevia yo. tyyppisiä lukuja.

Tämä on kuitenkin tarpeeton rajoitus mm. tarkasteltaessa rationaalilukujen approksimoimista toisilla rationaaliluvuilla.

Merkintöjä

Jos x on jokin reaaliluku, niin merkinnällä $\lfloor x \rfloor$ tarkoitamme suurinta sellaista kokonaislukua, joka on pienempi tai yhtäsuuri kuin x. Edelleen määrittelemme jakojäännösfunktion $\mathrm{Mod} : \mathbf{Z} \times \mathbf{Z}^+ \to \mathbf{Z}$ asettamalla $m = \lfloor \frac{m}{n} \rfloor n + \mathrm{Mod}(m, n)$ kaikilla $m \in \mathbf{Z}$, $n \in \mathbf{Z}^+$.

Jos m ja n ovat kokonaislukuja, $n \neq 0$ ja $\mathrm{syt}(m, n) = 1$, niin (laajennettua) Eukleideen algoritmia käyttäen voidaan löytää sellaiset kokonaisluvut a ja b, että $am + bn = 1$. Tällöin $am \equiv 1 \pmod{n}$. Kongruenssilla $mx \equiv 1 \pmod{n}$ on siis tehokkaasti laskettavissa oleva ratkaisu. Tätä ratkaisua sanotaan luvun m *modulaariseksi käänteisluvuksi* (inverssiksi) modulo n.

Päätulokset

Fareyn lukuja käsiteltäessä seuraava lause on keskeinen.

Lause 1: Olkoot p, q, m positiivisia kokonaislukuja, $q \leq m$ ja $\mathrm{syt}(p, q) = 1$. Olkoon r jokin luvun p käänteisluku modulo q ja

$$q' = \lfloor \frac{m+r}{q} \rfloor q - r = m - \mathrm{Mod}(m + r, q) \quad \textbf{ja} \quad p' = \frac{pq' + 1}{q}.$$

Tällöin $0 < q' \leq m$, $\mathrm{syt}(p', q') = 1$ ja luku p'/q' on lukua p/q lähinnä seuraava sellainen rationaaliluku, jonka nimittäjä $\leq m$.

Todistus. 1) Selvästi q' on kokonaisluku. Edelleen $pq'+1 = p\lfloor \frac{m+r}{q} \rfloor q - pr + 1 \equiv 0 \pmod{q}$. Siten myös p' on kokonaisluku.

2) Koska $p'q - pq' = 1$, niin $\mathrm{syt}(p', q') = 1$. Luku p'/q' on siis supistetussa muodossa.

3) Kertomalla epäyhtälöt

$$0 \leq \frac{m+r}{q} - \lfloor \frac{m+r}{q} \rfloor \leq \frac{q-1}{q}$$

puolittain luvulla q ja lisäämällä luku r saadaan $r \leq m + r - q' \leq q - 1 + r$, josta saadaan edelleen $m + 1 - q \leq q' \leq m$.

4) Osoitamme, että lukujen p/q ja p'/q' välissä ei ole sellaista rationaalilukua, jonka nimittäjä olisi $\leq m$. Oletetaan, että $\frac{p}{q} < \frac{s}{t} < \frac{p'}{q'}$, $0 < t \leq m$. Tällöin $sq - pt \geq 1$, $p't - sq' \geq 1$ ja edelleen

$$1 = p'q - pq' = qq'(\frac{p'}{q'} - \frac{p}{q}) = qq' \left((\frac{p'}{q'} - \frac{s}{t}) + (\frac{s}{t} - \frac{p}{q}) \right)$$

$$= qq' \left(\frac{p't - sq'}{tq'} + \frac{sq - pt}{tq} \right) \geq qq' \left(\frac{1}{tq'} + \frac{1}{tq} \right) = \frac{q + q'}{t} > \frac{m}{t} \geq 1.$$

Tämä on ristiriita. Siten $\frac{p}{q}$ ja $\frac{p'}{q'}$ ovat peräkkäiset sellaiset rationaaliluvut, joiden nimittäjät $\leq m$. QED

Todistuksen oleelliset vaiheet löytyvät Hardyn ja Wrightin lukuteorian kirjasta vuodelta 1938 [4]. Kirjassa ei kuitenkaan esitetä kyseistä tulosta yllä esitetyssä laskennallisesti käyttökelpoisessa muodossa.

Samalla tavalla kuin lause 1 voidaan todistaa myös seuraava tulos:

Lause 2: Olkoot p, q, m **positiivisia kokonaislukuja,** $q \leq m$ **ja** $\mathrm{syt}(p, q) = 1$**. Olkoon** r **jokin luvun** p **käänteisluku modulo** q **ja**

$$q'' = \lfloor \frac{m-r}{q} \rfloor q + r = m - \mathrm{Mod}(m-r, q) \quad \textbf{ja} \quad p'' = \frac{pq''-1}{q}.$$

Tällöin $0 < q'' < m$**,** $\mathrm{syt}(q'', p'') = 1$ **ja luku** p''/q'' **on lukua** p/q **lähinnä edeltävä sellainen rationaaliluku, jonka nimittäjä** $\leq m$**.**

Lauseen 1 todistuksen yhteydessä olemme todistaneet erityisesti seuraavan lauseen.

Lause 3: (Fareyn-Cauchyn lause) Jos p/q **ja** p'/q'**, missä** $0 < q$**,** $0 < q'$ **ja** $\mathrm{syt}(p, q) = \mathrm{syt}(p', q') = 1$**, ovat minkä tahansa Fareyn jonon** F_m **kaksi peräkkäistä murtolukua, niin** $p'q - pq' = 1$**.**

Veikko Nevanlinna [3] toteaa tästä lauseesta seuraavaa: "Farey ei todistanut väitettään. Tämä onkin ymmärrettävää, sillä todistuksen vaikeus on sitä luokkaa, että sen keksimiseen tarvittiin CAUCHYn (Augustin Cauchy 1789-1857, ranskalainen matemaatikko) kaltainen huippumatemaatikko. Todistus ei edellytä peruskoulukurssin ylittäviä tietoja; kuitenkin, joka sen omintakeisesti keksii, voi hyvällä syyllä väittää olevansa matemaattinen kyky!" Nevanlinna esittää tämän jälkeen yleisesti käytetyn Cauchyltä lähtöisin olevan standarditodistuksen, jonka esittämiseen tarvitaan lähes neljä konekirjoitettua sivua. Edellä esitettyä todistusta voitaneen kuitenkin pitää parempana sekä pedagogisista, että käytännöllisistä, laskennallisista syistä. Antaahan se lähinnä seuraavalle (ja lähinnä edeltävälle) Fareyn luvulle eksplisiittisen, tehokkaasti laskettavan esityksen.

Lause 4: (Medianttikaava) Olkoot $p_1/q_1 < p_2/q_2 < p_3/q_3$**, missä** $q_i > 0$ **ja** $\mathrm{syt}(p_i, q_i) = 1$ **kaikilla** $i = 1, 2, 3$**, kolme peräkkäistä murtolukua jossain Fareyn jonossa** F_m**. Tällöin** $p_2/q_2 = (p_1 + p_3)/(q_1 + q_3)$**.**

Todistus. Lauseiden 1 ja 2 mukaan $p_1 = (p_2 q_1 - 1)/q_2$ ja $p_3 = (p_2 q_3 + 1)/q_2$ ja näinollen suoralla sijoituksella saadaan $(p_1 + p_3)/(q_1 + q_3) = p_2/q_2$. QED

Egyptiläisten murtolukujen probleema

Muinaiset egyptiläiset tutkivat positiivisten rationaalilukujen esitettävyyttä erisuurten *yksikkömurtolukujen* (ts. muotoa $1/m$, missä m on positiivinen kokonaisluku) summana. Tätä ongelmaa kutsutaan *egyptiläisten murtolukujen probleemaksi.*

Eräs ratkaisutapa egyptiläisten murtolukujen ongelmaan on ns. *ahne algoritmi* (greedy algorithm). Tässä menettelyssä toimitaan seuraavasti. Olkoon r_1, $0 < r_1 < 1$, tarkasteltava rationaaliluku. Valitaan mahdollisimman pieni sellainen positiivinen kokonaisluku m_1, että $1/m_1 \leq r_1$. Jos $r_1 = 1/m_1$, niin prosessi päättyy. Muussa tapauksessa asetetaan $r_2 = r_1 - 1/m_1$. Tämän jälkeen valitaan jälleen mahdollisimman pieni sellainen positiivinen kokonaisluku m_2, että $1/m_2 \leq r_2$. Näin jatkaen lasketaan positiivisten kokonaislukujen jonoa $m_1, m_2, ...$, kunnes jollakin indeksin arvolla s toteutuu ehto $1/m_s = r_s$. Suhteellisen helposti voidaan osoittaa, että 1) näin määritelty prosessi päättyy, 2) lukujono $m_1, m_2, ..., m_s$ on aidosti kasvava ja että 3) $r_1 = 1/m_1 + 1/m_2 + ... + 1/m_s$.

Ahneen algoritmin etuna on se, että se päättyy yleensä nopeasti. Algoritmia kokeilemalla todetaan kuitenkin helposti sen keskeinen ongelma, nimittäin se, että osanimittäjät m_i kasvavat usein hirvittävän suuriksi.

Fareyn luvuista saadaan tämän probleeman ratkaisemiseen erittäin käyttökelpoinen menetelmä. Richard Guyn [3] mukaan tämän mahdollisuuden on esittänyt Bleicher vuonna 1969 [1]. Bleicherin esitystä minulla ei kuitenkaan ole ollut käytettävissäni.

Lause 5: Olkoon $0 < p < q$ **ja** $\text{syt}(p, q) = 1$**. Muodostetaan rationaalilukujono** p_i/q_i**,** $i = 0, 1, ...$ **asettamalla**
1) $p_0 = q - p$**,** $q_0 = q$ **ja**
2) jos $q_i > 1$ **jollakin** $i \geq 0$**, niin valitaan rationaaliluku** p_{i+1}/q_{i+1} **lukua** p_i/q_i **lähinnä seuraavaksi supistetussa muodossa olevaksi rationaaliluvuksi Fareyn jonossa parametrilla** q_i**. Muuten jono päättyy.**
Tällöin
(i) on olemassa sellainen kokonaisluku $s \geq 1$**, että** $p_s = q_s = 1$ **ja**
(ii)

$$\frac{p}{q} = \frac{1}{q_s q_{s-1}} + \frac{1}{q_{s-1} q_{s-2}} + ... + \frac{1}{q_1 q_0}.$$

Todistus. Selvästi $p_0/q_0 < p_1/q_1 < p_2/q_2 < ...$ ts. jono on aidosti kasvava.

Jos $0 < p_i/q_i < 1$ ja $q_i > 1$ (ts. p_{i+1}/q_{i+1} on määritelty) jollakin $i \geq 0$, ja r_i on luvun p_i pienin ei-negatiivinen käänteisluku modulo q_i, niin $1 \leq r_i < q_i$ ja

$$q_{i+1} = \lfloor \frac{q_i + r_i}{q_i} \rfloor q_i - r_i = q_i - r_i \leq q_i - 1 < q_i.$$

Nimittäjien q_i jono on siis aidosti vähenevä positiivisten kokonaislukujen jono, joten se välttämättä päättyy. Toisin sanoen on olemassa sellainen $s \geq 0$, että $q_s = 1$.

Väitämme, että myös $p_s = 1$. Olkoon $0 < p_i/q_i < 1$ jollakin $i < s$. Tällöin $p_{i+1} = (p_i q_{i+1} + 1)/q_i$, joten

$$\frac{p_{i+1}}{q_{i+1}} = \frac{p_i}{q_i} + \frac{1}{q_i q_{i+1}} \leq \frac{p_i}{q_i} + \frac{1}{q_i} = \frac{p_i + 1}{q_i} \leq 1.$$

Induktiolla indeksin i suhteen päättelemme, että $0 < p_i/q_i \leq 1$ kaikilla $i = 0, 1, ..., s$. Erityisesti $0 < p_s/q_s \leq 1$ ja koska $q_s = 1$, niin $p_s = 1$. Siis kohta (i) on todistettu.

Fareyn-Cauchyn lausetta käyttäen toteamme nyt, että

$$\frac{p}{q} = 1 - \frac{q-p}{q} = \frac{p_s}{q_s} - \frac{p_0}{q_0} = (\frac{p_s}{q_s} - \frac{p_{s-1}}{q_{s-1}}) + (\frac{p_{s-1}}{q_{s-1}} - \frac{p_{s-2}}{q_{s-2}}) + ...(\frac{p_1}{q_1} - \frac{p_0}{q_0}) =$$

$$\frac{1}{q_s q_{s-1}} + \frac{1}{q_{s-1} q_{s-2}} + ... + \frac{1}{q_1 q_0}.$$

Kohta (ii) on siten todistettu. QED

Lause 5 antaa siis käyttökelpoisen menetelmän egyptiläisten murtolukujen probleeman ratkaisemiseen. Jos p/q on tarkasteltava rationaaliluku, niin menetelmän antaman ratkaisun osanimittäjät ovat $\leq q(q-1)$. Termien lukumäärä voi kuitenkin olla melko suuri, mutta ainakin $\leq q$.

Yhteys Riemannin hypoteesiin

Fermat'n lauseen tultua todistetuksi on *Riemannin hypoteesi* (ks. [2],[5]) tällä hetkellä matematiikan tunnetuin ratkaisematon ongelma. Toisin kuin Fermat'n lause, jota voidaan pitää jonkinlaisena kuriositeettina, tarjoaa Riemannin hypoteesi erittäin käyttökelpoisen työkalun eräiden matematiikan alojen, erityisesti analyyttisen lukuteorian, tulosten todistamiseen. Vaikka Riemannin hypoteesia ei siihen uhratuista työvuosista huolimatta olekaan pystytty todistamaan, erittäin laajamittaiset numeeriset tarkastelut tukevat sen paikkansapitävyyttä. Riemannin hypoteesin käyttökelpoisuuden ansiosta sitä käytetään varsin yleisesti analyyttisen lukuteorian tulosten todistamiseen. Kuitenkin todistuksen yhteydessä on tullut tavaksi mainita erikseen hypoteesin käytöstä.

Fareyn luvut tekee mielenkiintoisiksi myös niiden yhteys Riemannin hypoteesiin. Voidaan nimittäin osoittaa, että Riemannin hypoteesi pitää paikkansa jos ja vain jos välillä $(0, 1]$ olevat Fareyn luvut ovat tietyssä mielessä riittävän tasaisesti jakautuneita.

Olkoon $m > 0$ ja $0 < f_1 < f_2 < ... < f_M = 1$ parametria m vastaavan Fareyn jonon välillä $(0, 1]$ olevat rationaaliluvut. Määritellään positiivisten kokonaislukujen joukossa rationaalilukuarvoinen funktio D asettamalla $D(m) = \sum_{i=1}^{M} |f_i - i/M|$.

Tarkastellaan seuraavaa väitettä:

V1: Jokaista reaalilukua $e > 1/2$ kohti on olemassa sellainen reaaliluku $C = C(e)$, että jokaisella positiivisella kokonaisluvulla m on $D(m) < Cm^e$.

Tunnetut matemaatikot J. Franel ja E. Landau osoittivat vuonna 1924, että väite V1 on yhtäpitävä Riemannin hypoteesin kanssa.

Lopuksi

Tässä kirjoitelmassa esitellyt asiat pohjautuvat Oulun yliopiston matematiikan laitoksella syksyllä 1995 pitämäni kurssin "Matematiikkaa mikrolla" teoriaosuuteen. Kurssilla käytettiin Mathematica-ohjelmistoa. Tällä ohjelmistolla yllä esitetyt Fareyn lukujen tarkastelut ovat helposti ohjelmoitavissa. Ohjelmisto sisältää mm. tarvittavat modulaarisen käänteisluvun ja kokonaislukujen jakoalgoritmin valmiiksi ohjelmoituina. Kurssilla tutustuttiin tosin myös näiden algoritmien rekursiiviseen ohjelmointiin.

Lähteet

[**1**] Beck A., Bleicher M. N., Crowe D. W.: Excursions into mathematics, Worth Publishers, New York, 1969.

[**2**] Edwards H. M.: Riemann's zeta function, Academic Press, 1974.

[**3**] Guy Richard: Unsolved Problems in Number Theory, Springer-Verlag, 1981.

[**4**] Hardy G. H., Wright E. M.: An Introduction to the Theory of Numbers, Oxford Science Publications, Clarendon Press, Oxford 1938 (Fifth edition, reprinted 1995).

[**5**] Matematiikan käsikirja, toinen painos, Tammi 1994.

[**6**] Nevanlinna Veikko: Lukuteorian alkeet, Jyväskylän yliopiston matematiikan laitoksen luentomoniste 8, Jyväskylä 1988.