UNIVERZA V LJUBLJANI
FAKULTETA ZA MATEMATIKO IN FIZIKO

Matematika – 1. stopnja

Tjaša Vrhovnik

Fareyevo zaporedje in Riemannova hipoteza

Delo diplomskega seminarja

Mentor: izr. prof. dr. Aleš Vavpetič

Ljubljana, 2019

Kazalo

Fareyevo zaporedje in Riemannova hipoteza

Povzetek

The Farey Sequence and The Riemann Hypothesis

Abstract

Math. Subj. Class. (2010):
Ključne besede:
Keywords:

1. Uvod

Zgodovina Fareyevega zaporedja sega v London 18. stoletja. Med letoma 1704 in 1841 je izhajal letni zbornik "The Ladies Diary: or, the Woman's Almanack", ki je povezoval ljubitelje matematičnih ugank. Bralce so namreč nagovarjali k pošiljanju in reševanju aritmetičnih problemov, ki so bili v zborniku objavljeni. Leta 1747 se je pojavilo naslednje vprašanje: Najti je potrebno število ulomkov različnih vrednosti, manjših od 1, katerih imenovalec ni večji od 100.

2. Fareyevo zaporedje

2.1. **Zgodovina Fareyevega zaporedja.** Vrnimo se k v uvodu omenjeni nalogi o številu ulomkov različnih vrednosti, manjših od 1, z imenovalci kvečjemu 100. Prvi odgovor na članek je bila tabela ulomkov z imenovalci manjšimi od 10, nato pa še dve tabeli z rezultatoma 3055 in 4851. Leta 1751 je R. Flitcon objavil pravilni odgovor 3003, kateremu je dodal tudi opis postopka. Preden ga razložimo, si oglejmo Eulerjevo funkcijo in njene lastnosti, ki nas bo pripeljala do rešitve.

Definicija 2.1. Preslikava $\varphi\colon \mathbb{N} \to \mathbb{N}$, ki za vsako naravno število n prešteje števila, manjša od n, ki so n tuja, se imenuje Eulerjeva funkcija φ.

Trditev 2.2. *Če sta k in l tuji si števili, velja $\varphi(kl) = \varphi(k)\varphi(l)$, torej je Eulerjeva funkcija multiplikativna.*

Dokaz. V dokazu multiplikativnosti si bomo pomagali z lastnostmi grup. Naj $\mathbb{Z}_k^*$ označuje grupo vseh obrnljivih elementov grupe $\mathbb{Z}_k$. Vemo, da so obrnljivi elementi grupe $\mathbb{Z}_k$ tista števila iz množice $\{0, 1, \ldots, k-1\}$, ki so tuja k, zato je $|\mathbb{Z}_k^*| = \varphi(k)$. Dobimo zvezi

$$|\mathbb{Z}_{kl}^*| = \varphi(kl)$$

$$|\mathbb{Z}_k^*||\mathbb{Z}_l^*| = \varphi(k)\varphi(l)$$

Ker je preslikava $\psi\colon \mathbb{Z}_{kl}^* \to \mathbb{Z}_k^* \times \mathbb{Z}_l^*$ za tuji števili k in l izomorfizem grup in je moč kartezičnega produkta dveh množic enaka produktu njunih moči, sledi

$$\varphi(kl) = |\mathbb{Z}_{kl}^*| = |\mathbb{Z}_k^*||\mathbb{Z}_l^*| = \varphi(k)\varphi(l),$$

s čimer je multiplikativnost dokazana. □

Trditev 2.3.

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right),$$

kjer so p prafaktorji števila n.

Dokaz. Zapišimo n kot produkt prafaktorjev, $n = \prod_{i=1}^{m} p_i^{r_i}, r_i \in \mathbb{N}, p_i \in \mathbb{P}\ \forall i$. $\varphi(p^r)$ prešteje vsa števila, manjša od p^r, ki so tuja p^r. To so natanko tista, ki niso deljiva s praštevilom p. Večkratnikov p med števili $1, 2, \ldots, p^r - 1$ je toliko kot večkratnikov p med števili $1, 2, \ldots, p^r$, teh pa je $\frac{p^r}{p} = p^{r-1}$. Torej je

$$\varphi(p^r) = (p^r - 1) - (p^{r-1} - 1) = p^r - p^{r-1} = p^r \left(1 - \frac{1}{p}\right).$$

Z upoštevanjem multiplikativnosti funkcije φ dobimo

$$\varphi(n) = \varphi\left(\prod_{i=1}^{m} p_i^{r_i}\right) = \prod_{i=1}^{m} \varphi(p_i^{r_i}) = \prod_{i=1}^{m} p_i^{r_i}\left(1 - \frac{1}{p_i}\right)$$
$$= \prod_{i=1}^{m} p_i^{r_i} \times \prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right) = n\prod_{i=1}^{m}\left(1 - \frac{1}{p_i}\right) = n\prod_{p|n}\left(1 - \frac{1}{p}\right).$$

□

Trditev 2.4. *Obstajajo 3003 racionalna števila* $\frac{p}{q}, 0 < \frac{p}{q} < 1$ *s* $q \leq 100$.

Namesto formalnega dokaza trditve bomo predstavili Flitconovo rešitev. Naredimo tabelo s tremi stolpci in 99 vrsticami. V prvi stolpec vsake vrstice napišemo po eno izmed naravnih števil od 2 do 100. V drugi stolpec posamezne vrstice zapišemo naravno število iz prvega stolpca kot produkt prafaktorjev, v tretji stolpec pa vrednost $\varphi(n)$. Pomagamo si s trditvama 2.2 in 2.3. Vsota vrednosti v tretjem stolpcu nam da število iskanih ulomkov. Res, vsak $\varphi(n)$ nam pove število okrajšanih ulomkov med 0 in 1 z imenovalcem n, vsota Eulerjevih funkcij pa število vseh okrajšanih ulomkov med 0 in 1 z imenovalci med 2 in 100. [1]

Neodvisno od Flitconove rešitve je francoski matematik Charles Haros leta 1802 sestavil enak seznam ulomkov, vendar na precej zaneslivejši način. Haros se dela ni lotil z željo po reševanju aritmetične naloge, pač pa je pisal tabele za pretvarjanje med ulomki in decimalnim zapisom ter obratno. V Franciji so namreč v času revolucije konec 18. stoletja uvajali nov metrični sistem, ki je med drugim zahteval uporabo decimalnega zapisa. Tabele so bile objavljene v *Journal de l'Ecole Polytechnique*, primerom ter algoritmom za pretvarjanje pa so bile dodane skice dokazov in nekatere lastnosti zaporedja ulomkov, ki so kasneje postali znani pod imenom Fareyevo zaporedje.

Posebej zanimiva je zgodba o pivovarju in ljubiteljskemu matematiku Henryju Goodwynu. Čeprav ni imel formalne izobrazbe, se je navduševal nad zanostjo in tehniko, sestavljal različne tabele in računal, kako izboljšati svoje poslovanje. Po upokojitvi se je vse bolj posvečal matematiki – tako je med letoma 1816 in 1823 objavil več člankov s tabelami okrajšanih ulomkov. Njegovo delo sta opazila znameniti francoski matematik Augustin Louis Cauchy in John Farey, geolog, po komer se obravnavano zaporedje okrajšanih ulomkov imenuje. Vemo, da je Cauchy prispeval nekaj dokazov lastnosti Fareyevega zaporedja, v nasprotju pa ostaja neznano, ali sta Goodwyn in Farey zaporedje in nekatere njegove lastnosti odkrila neodvisno od Harosa, bodisi sta vedela za njegove ugotovitve. Farey je najverjetneje na podlagi Goodwynovih tabel maja 1816 v pismu časopisu *The Philosophical Magazine and Journal* z naslovom *On a curious Property of vulgar Fractions* predstavil medianto, najpomembnejšo lastnost zaporedja. Čeprav zaporedje morda neupravičeno nosi ime Johna Fareya, pa ne smemo spregledati njegovega prispevka k raziskovanju matematike v glasbi, vzorcev, astronomije in seveda geologije.

2.2. O Fareyevem zaporedju.

Definicija 2.5. Fareyevo zaporedje reda n oz. n-to Fareyevo zaporedje je množica racionalnih števil $\frac{p}{q}$ urejenih po velikosti, kjer sta p in q tuji si števili, ter velja $0 \leq p \leq g \leq n$. Označimo ga z F_n.

[1] Čeprav Flitcon ne omenja Eulerjeve funkcije $\varphi(n)$, je uporabil njene lastnosti v svoji matematično manj formalni metodi.

Ekvivalentno, F_n vsebuje vse okrajšane ulomke med 0 in 1 z imenovalci, kvečjemu enakimi n.

Primer 2.6. $F_1 = \left\{\frac{0}{1}, \frac{1}{1}\right\}$
$F_2 = \left\{\frac{0}{1}, \frac{1}{2}, \frac{1}{1}\right\}$
$F_3 = \left\{\frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1}\right\}$
$F_4 = \left\{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\right\}$
$F_5 = \left\{\frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1}\right\}$ ♢

V zgornjih primerih opazimo, da za vsaka sosednja člena v Fareyevem zaporedju velja, da je križni produkt obeh števcev in imenovalcev po absolutni vrednosti enak 1. To se bo izkazalo za pomembno opazko, zato definiramo naslednji pojem.

Definicija 2.7. Sosednja člena v Fareyevem zaporedju imenujemo Fareyeva soseda.

Definicija 2.8. Naj bosta $\frac{a}{b}$ in $\frac{c}{d}$ sosednja člena nekega Fareyevega zaporedja. Člen

$$\frac{a+c}{b+d}$$

imenujemo medianta.

Trditev 2.9. *Za medianto okrajšanih ulomkov $\frac{a}{b} < \frac{c}{d}$ velja $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$.*

Dokaz. Poračunajmo razliko med členoma

$$\frac{a+c}{b+d} - \frac{a}{b} = \frac{ab+bc-ab-ad}{b(b+d)} = \frac{bc-ad}{b(b+d)} = \frac{1}{b(b+d)} > 0$$

in

$$\frac{c}{d} - \frac{a+c}{b+d} = \frac{bc+cd-ad-cd}{d(b+d)} = \frac{bc-ad}{d(b+d)} = \frac{1}{d(b+d)} > 0.$$

Zveza torej velja. □

Trditev 2.10. *Naj velja $0 \leq \frac{a}{b} < \frac{c}{d} \leq 1$. $\frac{a}{b}$ in $\frac{c}{d}$ sta Fareyeva soseda v F_n natanko tedaj, ko velja $bc - ad = 1$.*

Dokaz. ($\Rightarrow$) Denimo, da sta $\frac{a}{b}$ in $\frac{p}{q}$ ter $\frac{p}{q}$ in $\frac{c}{d}$ Fareyeva soseda. Dokaz bo potekal z indukcijo na n. Za $n = 1$ je $F_n = \{\frac{0}{1}, \frac{1}{1}\}$, $bc-ad = 1*1-0*1 = 1$, zato osnovni korak velja. Po indukcijski predpostavki za zaporedje $F_n = \{\ldots \frac{a}{b}, \frac{c}{d} \ldots\}$ velja $bc-ad = 1$. Dokažimo, da velja tudi za $n+1$. Če je $b+d \leq n+1$, je $F_{n+1} = \{\ldots \frac{a}{b}, \frac{a+c}{b+d}, \frac{c}{d} \ldots\}$ in $b(a+c)-a(b+d) = ba+bc-ab-ad = bc-ad = 1$, kjer smo v zadnji enakosti uporabili indukcijsko predpostavko. Podobno je $(b+d)c - (a+c)d = bc + dc - ad - cd = bc-ad = 1$. Sicer je $b+d \geq n+1$ in $F_n = \{\ldots \frac{a}{b}, \frac{c}{d} \ldots\}$ ter po indukcijski predpostavki $bc - ad = 1$. Indukcijski korak je s tem končan. Torej sklep velja za vsa Fareyeva zaporedja.

($\Leftarrow$) Obratno, naj bodo $\frac{a}{b}$, $\frac{p}{q}$ in $\frac{c}{d}$ členi poljubnega Fareyevega zaporedja, za katere velja $\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$ in $bp - aq = qc - pd = 1$. S preureditvijo zgornje enakosti dobimo

$$bp + pd = aq + qc$$
$$p(b+d) = q(a+c)$$
$$\frac{p}{q} = \frac{a+c}{b+d}$$

od koder sledi, da sta $\frac{a}{b}$ in $\frac{p}{q}$ ter $\frac{p}{q}$ in $\frac{c}{d}$ Fareyeva soseda. □

Lema 2.11. *Medianta je okrajšan ulomek.*

Dokaz. Naj za $\frac{a}{b} < \frac{c}{d}$ velja $bc - ad = 1$. Dokazati želimo, da je $\frac{a+c}{b+d}$ okrajšan ulomek, torej sta si števili $a + c$ in $b + d$ tuji.

$$1 = bc - ad = ba + bc - ab - ad = b(a + c) - a(b + d)$$

To pomeni, da $b+d$ in $a+c$ nimata skupnega faktorja, zato je ulomek $\frac{a+c}{b+d}$ okrajšan. □

Flitconova metoda za izračun števila okrajšanih ulomkov nas pripelje do naslednje rekurzivne definicije dolžine Fareyeva zaporedja.

Trditev 2.12. *Naj bo $\varphi(n)$ Eulerjeva funkcija. Dolžina Fareyevega zaporedja reda n je*

$$|F_n| = |F_{n-1}| + \varphi(n).$$

Opomba 2.13. Z upoštevanjem vrednosti $|F_1| = 2$ iz trditve 2.12 sledi

$$|F_n| = \sum_{i=1}^{n} \varphi(i) + 1.$$

Trditev 2.14. *Asimptotično se dolžina Fareyevega zaporedja obnaša kot*

$$|F_n| \sim \frac{3n^2}{\pi^2}.$$

Preden dokažemo zgornjo trditev, definirajmo naslednjo oznako, ki jo bomo v dokazu uporabljali.

Definicija 2.15. Notacija veliki O predstavlja množico funkcij, ki so po absolutni vrednosti do multiplikativne konstante manjše od dane funkcije.

Natančneje, funkcja f pripada razredu $O(g)$, če obstajata konstanta M in x_0, tako da za vsak $x > x_0$ velja $|f(x)| \leq M \cdot |g(x)|$.

Pišemo $f \in O(g)$ oziroma $f = O(g)$.

Sedaj lahko dokažemo trditev 2.14.

Dokaz. Asimptotično obnašanje bomo izračunali s pomočjo ocene vrednosti vsote $\sum_{i=1}^{n} \varphi(i)$. Spomnimo se, da je

$$\varphi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right) = n - \sum \frac{n}{p} + \sum \frac{n}{pp'} - \cdots,$$

kjer so p, p' praštevilski delitelji števila n. Z upoštevanjem Möbiusove funkcije je zadnja vsota enaka

$$\varphi(n) = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Sedaj računajmo vsoto

$$\begin{aligned}
\sum_{i=1}^{n}\varphi(i) &= \sum_{i=1}^{n} i\sum_{d\mid i}\frac{\mu(d)}{d} = \sum_{dd'\le n} d'\mu(d) = \sum_{d=1}^{n}\mu(d)\sum_{d'=1}^{\left\lfloor \frac{n}{d}\right\rfloor} d' \\
&= \frac{1}{2}\sum_{d=1}^{n}\mu(d)\left(\left\lfloor\frac{n}{d}\right\rfloor^2 + \left\lfloor\frac{n}{d}\right\rfloor\right) = \frac{1}{2}\sum_{d=1}^{n}\mu(d)\left(\frac{n^2}{d^2} + O\left(\frac{n}{d}\right)\right) \\
&= \frac{1}{2}n^2\sum_{d=1}^{n}\frac{\mu(d)}{d^2} + O\left(n\sum_{d=1}^{n}\frac{1}{d}\right) \\
&\overset{(1)}{=} \frac{1}{2}n^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} - \frac{1}{2}n^2\sum_{d=n+1}^{\infty}\frac{\mu(d)}{d^2} + O(n\ln n) \\
&= \frac{1}{2}n^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + O\left(n^2\sum_{d=n+1}^{\infty}\frac{1}{d^2}\right) + O(n\ln n) \\
&\overset{(2)}{=} \frac{n^2}{2\zeta(2)} + O(n) + O(n\ln n) \overset{(3)}{=} \frac{3n^2}{\pi^2} + O(n\ln n).
\end{aligned}$$

V enakosti (1) smo zadnji sumand ocenili navzgor s pomočjo Taylorjevega razvoja funkcije ln

$$\ln(1+x) = \sum_{n=1}^{\infty}(-1)^{n+1}\frac{x^n}{n}.$$

V enakosti (2) smo uporabili naslednjo oceno:

$$n^2\sum_{d=n+1}^{\infty}\frac{1}{d^2} \le n^2\sum_{d=n+1}^{\infty}\frac{1}{d(d-1)} = n^2\sum_{d=n+1}^{\infty}\left(-\frac{1}{d}+\frac{1}{d-1}\right) = n^2\frac{1}{n} = n.$$

V enakosti (3) smo za izračun funkcije $\zeta(2)$ uporabili znano vrednost

$$\zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}.$$

Po opombi 2.13 sledi, da je $|F_n| = \frac{3n^2}{\pi^2} + O(n\ln n) \sim \frac{3n^2}{\pi^2}$.

□

Slovar strokovnih izrazov

Literatura

[1] J. Ainsworth, M. Dawson, J. Pianta in J. Warwick, *The Farey sequence*, diplomsko delo, School of Mathematics, University of Edinburgh, 2012; dostopno tudi na `https://www.maths.ed.ac.uk/~v1ranick/fareyproject.pdf`.

[2] S. B. Guthery, *A motif of mathematics*, Docent Press, Boston, 2011; dostopno tudi na `https://www.maths.ed.ac.uk/~v1ranick/papers/farey.pdf`.

[3] G. H. Hardy in E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford University Press, Oxford, 1960.

[4] A. Hatcher, *Topology of numbers*, verzija junij 2018, [ogled 31. 10. 2018], dostopno na `https://pi.math.cornell.edu/~hatcher/TN/TNpage.html`.