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

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

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

Znano je, da je preslikava $\psi\colon \mathbb{Z}_{kl}^* \to \mathbb{Z}_k^* \times \mathbb{Z}_l^*$ za tuji naravni števili k in l izomorfizem grup. Ker 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. *Vrednost Eulerjeve funkcije je enaka*

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

kjer so p prafaktorji števila n.

Dokaz. Zapišimo n kot produkt prafaktorjev, $n = \prod_{i=1}^{m} p_i^{r_i}$, kjer so $r_i \in \mathbb{N}$ in p_i praštevila. Funkcija $\varphi(p^r)$ 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

$$\begin{aligned}\varphi(n) &= \varphi\left(\prod_{i=1}^{m} p_i^{r_i}\right) = \prod_{i=1}^{m} \varphi(p_i^{r_i}) = \prod_{i=1}^{m} p_i^{r_i}\left(1-\frac{1}{p_i}\right) \\ &= \prod_{i=1}^{m} p_i^{r_i} \times \prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right) = n\prod_{i=1}^{m}\left(1-\frac{1}{p_i}\right) = n\prod_{p|n}\left(1-\frac{1}{p}\right),\end{aligned}$$

kar smo želeli dokazati. □

Trditev 2.4. *Obstajajo* 3003 *racionalna števila* $\frac{p}{q}$*, za katera velja* $0 < \frac{p}{q} < 1$ *ter je* $q \leq 100$*.*

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 vrednosti Eulerjeve funkcije $\varphi(n)$ za vsa števila n med 2 in 100 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 bolj zanesljiv 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 časniku *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 znanostjo 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.**

[1] Čeprav Flitcon ne omenja Eulerjeve funkcije φ, je uporabil njene lastnosti v svoji matematično manj formalni metodi.

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 $0 \leq p \leq q \leq n$. Označimo ga z F_n.

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

Primer 2.6. Poglejmo si prvih nekaj Fareyevih zapredij.

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

Opomba 2.7. Če pogoj $0 \leq p \leq q \leq n$ v definiciji 2.5 omilimo v pogoj $0 \leq p, q \leq n$, okrajšane ulomke z intervala $[0, 1]$ razširimo na interval $[0, \infty)$. V primeru, ko za p in q dovoljujemo tudi negativna cela števila, dobimo okrajšane ulomke na celotni realni osi.

V zgornjih primerih opazimo, da za vsaka sosednja člena Fareyevega zaporedja velja naslednje. Če števec prvega ulomka množimo z imenovalcem drugega in nato vlogi ulomkov zamenjamo, je razlika obeh produktov po absolutni vrednosti enaka 1. To se bo izkazalo za pomembno opazko, zato vpeljemo pojem, ki sledi.

Definicija 2.8. Sosednja člena v Fareyevem zaporedju imenujemo *Fareyeva soseda*.

Definicija 2.9. Naj bosta $\frac{a}{b}$ in $\frac{c}{d}$ sosednja člena nekega Fareyevega zaporedja. Člen

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

imenujemo *medianta*.

Trditev 2.10. *Za medianto okrajšanih ulomkov $\frac{a}{b} < \frac{c}{d}$ velja $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$.*

Dokaz. Poračunajmo razliki med členoma

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

in

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

Obe neenakosti sledita iz dejstva, da je $\frac{a}{b} < \frac{c}{d}$, kjer so $a, b, c, d \in \mathbb{N}$, zato je $ad < bc$. Zveza torej velja. □

Kako dobimo člen Fareyevega zaporedja reda $(n+1)$? Označimo iskani okrajšan ulomek s $\frac{k}{n+1}$. Seveda sta $k, n \in \mathbb{N}, k < n+1$ tuji si števili. Zato obstajata enolično določeni naravni števili $a < b$, da velja $a(n+1) - bk = 1$. S preoblikovanjem zadnje enakosti dobimo zvezo $a(n+1-b) - b(k-a) = 1$, kar pomeni, da sta si tudi naravni števili $k-a$ in $n+1-b$ tuji. Brez škode za splošnost naj bo $k-a < n+1-b$. Zato lahko tvorimo okrajšan ulomek $\frac{k-a}{n+1-b}$, ki pripada nekemu Fareyevemu zaporedju. Prav tako je okrajšan ulomek $\frac{a}{b}$ element nekega Fareyevega zaporedja. Sedaj prepišimo ulomek $\frac{k}{n+1}$ v $\frac{a+(k-a)}{b+(n+1-b)}$, kar pa je medianta ulomkov $\frac{a}{b}$ in $\frac{k-a}{n+1-b}$. Dokazali smo, da iz danega Fareyevega zaporedja člene zaporedja višjega reda dobimo z računanjem mediant.

Trditev 2.11. *Naj velja* $0 \leq \frac{a}{b} < \frac{c}{d} \leq 1$. *Ulomka* $\frac{a}{b}$ *in* $\frac{c}{d}$ *sta Fareyeva soseda v nekem Fareyevem zaporeju natanko tedaj, ko velja* $bc - ad = 1$.

Dokaz. ($\Rightarrow$) Dokaz bo potekal z indukcijo na n. Za $n = 1$ je $F_n = \{\frac{0}{1}, \frac{1}{1}\}$, $bc - ad = 1 \cdot 1 - 0 \cdot 1 = 1$, 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 F_{n+1}. Vemo, da nove člene zaporedja dobimo z računanjem mediant. Če je $b + d > n + 1$, $\frac{a+c}{b+d} \notin F_{n+1}$ in $F_{n+1} = \{\ldots \frac{a}{b}, \frac{c}{d} \ldots\}$ ter po indukcijski predpostavki $bc - ad = 1$. Če je $b + d < n + 1$, je $\frac{a+c}{b+d}$ že nek člen v zaporedju F_n in uporabimo indukcijsko predpostavko. Če je $b + d = n + 1$, 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 $(b + d)c - (a + c)d = bc + dc - ad - cd = bc - ad = 1$. 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 te 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 2.12. *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, z drugimi besedami, da sta si števili $a + c$ in $b + d$ tuji. Če preoblikujemo zgornjo enakost, dobimo

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

kar pomeni, da $b + d$ in $a + c$ nimata skupnega faktorja. Ulomek $\frac{a+c}{b+d}$ je torej okrajšan. □

Flitconova metoda za izračun števila okrajšanih ulomkov nas pripelje do naslednje rekurzivne formule dolžine Fareyevega zaporedja.

Trditev 2.13. *Naj bo* φ *Eulerjeva funkcija. Dolžina Fareyevega zaporedja reda* n *je*

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

Opomba 2.14. Z upoštevanjem vrednosti $|F_1| = 2$ iz trditve 2.13 sledi

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

Trditev 2.15. *Asimptotično se dolžina Fareyevega zaporedja obnaša kot*

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

Opomba 2.16. Simbol $\sim$ v trditvi 2.15 označuje asimptotično ekvivalentno obnašanje dveh funkcij. Po definiciji za funkciji $f(x)$ in $g(x)$ velja $f(x) \sim g(x)$ natanko tedaj, ko je $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$.

Preden dokažemo zgornjo trditev, definirajmo naslednjo oznako in dve funkciji, ki jih bomo v dokazu potrebovali.

Definicija 2.17. *Notacija veliki O* predstavlja množico funkcij, ki so po absolutni vrednosti do multiplikativne konstante manjše od dane funkcije.

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

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

Definicija 2.18. Preslikava $\mu\colon \mathbb{N} \to \mathbb{N}$, definirana kot

$$\mu(n) = \begin{cases} 0 & ;\ n \text{ je deljiv s kvadratom praštevila} \\ (-1)^p & ;\ n \text{ je produkt } p \text{ različnih praštevil,} \end{cases}$$

se imenuje *Möbiusova funkcija.*

Primer 2.19. Izračunajmo vrednosti Möbiusove funkcije za nekaj naravnih števil.
$\mu(1) = 1$
$\mu(2) = (-1)^1 = -1 = \mu(3)$
$\mu(4) = \mu(2^2) = 0$
$\mu(6) = \mu(2 \cdot 3) = (-1)^2 = 1$
$\mu(8) = \mu(2 \cdot 2^2) = 0$
$\mu(18) = \mu(2 \cdot 3^2) = 0$ ♢

Definicija 2.20. *Riemannova funkcija zeta* je za $s \in \mathbb{C}\backslash\{1\}$ definirana kot

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Sedaj lahko dokažemo trditev 2.15.

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

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

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

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

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

3. Fordovi krogi

Definicija 3.1. *Fordov krog* $\mathrm{C}(\frac{p}{q})$ je krog v zgornji polravnini, ki se abscisne osi dotika v točki $\frac{p}{q}$ in ima polmer $\frac{1}{2q^2}$. Pri tem sta p in q tuji si števili.

Fordovi krogi so definirani za vsak okrajšan ulomek, torej lahko vsakemu racionalnemu številu enolično priredimo Fordov krog. Zaradi simetrije jih je dovolj obravnavati na intervalu $[0,1]$, obenem pa se zavedati, da jih lahko induktivno razširimo na celotno realno os.

Z izbiro polmera dolžine $\frac{1}{2q^2}$ dosežemo, da sta poljubna Fordova kroga bodisi tangentna bodisi disjunktna. Za tangentne Fordove kroge veljata naslednji lastnosti, ki lastnosti Fareyevih sosedov preneseta v jezik geometrije.

Trditev 3.2. *Fordova kroga* $C(\frac{a}{b})$ *in* $C(\frac{c}{d})$ *sta tangentna natanko tedaj, ko velja* $|bc-ad| = 1$.

Dokaz. Trditev bomo dokazali tako, da bomo dokazali implikaciji v desno in levo. Naj za Fordova kroga $C(\frac{a}{b})$ in $C(\frac{c}{d})$ velja $\frac{a}{b} < \frac{c}{d}$. Naj bodo D središče kroga $C(\frac{a}{b})$, E središče kroga $C(\frac{c}{d})$ in F presečišče navpične premice skozi točko D z vodoravno premico skozi točko E.

($\Rightarrow$) Denimo, da sta Fordova kroga $C(\frac{a}{b})$ in $C(\frac{c}{d})$ tangentna. Vemo, da se dotikata abscisne osi zaporedoma v točkah $\frac{a}{b}$ in $\frac{c}{d}$, njuna polmera pa merita $\frac{1}{2b^2}$ in $\frac{1}{2d^2}$. Od tod lahko izračunamo razdalje $|DF|$, $|EF|$ in $|DE|$. Po konstrukciji je trikotnik DFE pravokoten s pravim kotom v oglišču F, zato velja Pitagorov izrek

$$|EF|^2 + |DF|^2 = |DE|^2.$$

Če dolžine izrazimo z a, b, c in d, dobimo enakost

$$\left(\frac{c}{d} - \frac{a}{b}\right)^2 + \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 = \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2.$$

Ko odpravimo oklepaje, opazimo, da se nekateri členi odštejejo. Nato odpravimo ulomke in dobljeno enakost poenostavimo.

$$\frac{c^2}{d^2} - \frac{2ac}{bd} + \frac{a^2}{b^2} + \frac{1}{4b^4} - \frac{1}{2b^2d^2} + \frac{1}{4d^4} = \frac{1}{4b^4} + \frac{1}{2b^2d^2} + \frac{1}{4d^4}$$

$$b^2c^2 - 2abcd + a^2d^2 - 1 = 0$$

$$(bc - ad)^2 = 1$$

$$|bc - ad| = 1$$

Implikacija v desno je s tem dokazana.

($\Leftarrow$) Sedaj naj velja $|bc - ad| = 1$. To je ekvivalentno enakosti $(bc - ad)^2 = 1$, kar lahko po obratnem postopku kot zgoraj prepišemo v obliko

$$\left(\frac{c}{d} - \frac{a}{b}\right)^2 + \left(\frac{1}{2b^2} - \frac{1}{2d^2}\right)^2 = \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2.$$

To pomeni, da je dolžina hipotenuze pravokotnega trikotnika DFE enaka vsoti dolžin polmerov Fordovih krogov $C(\frac{a}{b})$ in $C(\frac{c}{d})$, torej sta kroga tangentna. □

Definicija 3.3. Tangentna Fordova kroga imenujemo *Fordova soseda.*

Trditev 3.4. *Naj bosta $C(\frac{a}{b})$ in $C(\frac{c}{d})$ Fordova soseda. Tedaj obstaja enolično določen Fordov krog $C(\frac{a+c}{b+d})$ in je tangenten na izbrana kroga.*

Dokaz. Po definiciji Fordovih krogov vemo, da sta $\frac{a}{b}$ in $\frac{c}{d}$ okrajšana ulomka in zaradi tangentnosti Fareyeva soseda v nekem Fareyevem zaporedju (razširjenem na celotno realno os). Po lemi 2.12 je njuna medianta $\frac{a+c}{b+d}$ tudi okrajšan ulomek, torej obstaja natanko en Fordov krog $C(\frac{a+c}{b+d})$.

Dokažimo še, da je $C(\frac{a+c}{b+d})$ tangenten na izbrana kroga. Ker sta $C(\frac{a}{b})$ in $C(\frac{c}{d})$ Fordova soseda, velja zveza $|bc - ad| = 1$. Če jo nekoliko preoblikujemo, dobimo

$$|bc - ad| = |bc - ad + cd - cd| = |(b + d)c - (a + c)d| = 1,$$

od koder sledi, da sta Fordova kroga $C(\frac{a+c}{b+d})$ in $C(\frac{c}{d})$ tangentna. Podobno

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

pomeni, da sta Fordova kroga $C(\frac{a}{b})$ in $C(\frac{a+c}{b+d})$ tangentna. □

V dokazu trditve 3.2 smo konstruirali pravokotni trikotnik, določen s središčema tangentnih Fordovih krogov in presečiščem premic skozi središči. Spomnimo se znane definicije iz teorije števil, ki izhaja iz evklidske geometrije.

Definicija 3.5. Trojica naravnih števil (a, b, c), za katero velja $a^2 + b^2 = c^2$, se imenuje *pitagorejska trojica*. Pitagorejska trojica je *primitivna*, če števila a, b, in c nimajo skupnega faktorja.

Trditev 3.6. *Pravokotna trikotnika, ki pripadata poljubnima paroma Fordovih sosedov, določata različni primitivni pitagorejski trojici.*

Dokaz. Naj bosta $\mathrm{C}(\frac{a}{b})$ in $\mathrm{C}(\frac{c}{d})$ ter $\mathrm{C}(\frac{a'}{b'})$ in $\mathrm{C}(\frac{c'}{d'})$ poljubna različna para Fordovih sosedov. Brez škode za splošnost naj velja $\frac{a}{b} < \frac{c}{d}$ in $\frac{a'}{b'} < \frac{c'}{d'}$. Naj prvemu paru Fordovih sosedov pripada pravokotni trikotnik DFE, drugemu paru pa pravokotni trikotnik $D'F'E'$. Dokazati želimo, da si trikotnika nista podobna.

Pa denimo, da sta si trikotnika DFE in $D'F'E'$ podobna. Tedaj obstaja tako naravno število $\lambda \neq 1$, da za dolžine stranic obeh pravokotnih trikotnikov veljajo naslednje zveze:

$$\frac{1}{2b^2} - \frac{1}{2d^2} = \lambda \left(\frac{1}{2b'^2} - \frac{1}{2d'^2} \right) \tag{1}$$

$$\frac{1}{2b^2} + \frac{1}{2d^2} = \lambda \left(\frac{1}{2b'^2} + \frac{1}{2d'^2} \right) \tag{2}$$

$$\frac{c}{d} - \frac{a}{b} = \lambda \left(\frac{c'}{d'} - \frac{a'}{b'} \right). \tag{3}$$

Če seštejemo prvi dve enačbi, dobimo

$$\begin{aligned} \frac{1}{b^2} &= \lambda \frac{1}{b'^2} \\ b'^2 &= \lambda b^2 \\ b' &= \sqrt{\lambda} b. \end{aligned} \tag{4}$$

Enačbo (3) lahko poenostavimo, saj gre za para Fordovih sosedov. Velja

$$\frac{1}{bd} = \frac{bc - ad}{bd} = \frac{c}{d} - \frac{a}{b} = \lambda \left(\frac{c'}{d'} - \frac{a'}{b'} \right) = \lambda \frac{b'c' - a'd'}{b'd'} = \lambda \frac{1}{b'd'}. \tag{5}$$

Iz (4) in (5) sledi

$$\begin{aligned} \frac{1}{bd} &= \lambda \frac{1}{\sqrt{\lambda} b d'} \\ \frac{1}{d} &= \frac{\sqrt{\lambda}}{d'} \\ d' &= \sqrt{\lambda} d. \end{aligned} \tag{6}$$

Nazadnje še v pogoj za tangentnost Fordovih krogov $\mathrm{C}(\frac{a'}{b'})$ in $\mathrm{C}(\frac{c'}{d'})$ vstavimo zvezi (4) in (6):

$$\begin{aligned} b'c' - a'd' &= 1 \\ \sqrt{\lambda} b c' - a' \sqrt{\lambda} d &= 1 \\ \sqrt{\lambda}(bc' - a'd) &= 1. \end{aligned} \tag{7}$$

To pa je možno le tedaj, ko je $\lambda = 1$. Prispeli smo do protislovja, kar pomeni, da si trikotnika nista podobna. □

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`.

[5] M. Strnad, *Pitagorov izrek pred Pitagorom*, Presek **17** (1989) 8–11; dostopno tudi na `http://www.presek.si/17/966-Strnad.pdf`.