

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

1. Uvod	4
2. Fareyevo zaporedje	4
2.1. Zgodovina Fareyevega zaporedja	4
2.2. O Fareyevem zaporedju	5
2.3. Dolžina Fareyevega zaporedja	7
3. Fordovi krogi	9
3.1. Fordovi sosedi	10
3.2. Posplošeni Fordovi krogi	13
3.3. Fordove krogle	14
3.4. Möbiusove transformacije na Fordovih krogih	15
4. Riemannova hipoteza	17
4.1. Praštevila in Riemannova zeta funkcija	18
4.2. Riemannova hipoteza	19
Slovar strokovnih izrazov	24
Literatura	24

# Fareyevo zaporedje in Riemannova hipoteza

POVZETEK

# The Farey Sequence and The Riemann Hypothesis

ABSTRACT

Math. Subj. Class. (2010):

Ključne besede:

Keywords:

## 1. UVOD

Zgodovina Fareyvega 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 Fareyvega 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  $\varphi: \mathbb{N} \rightarrow \mathbb{N}$ , ki za vsako naravno število  $n$  prešteje števila, manjša od  $n$ , ki so  $n$  tuja, se imenuje *Eulerjeva funkcija*  $\varphi$ .

**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  $\{0, 1, \dots, k-1\}$ , 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  $\psi: \mathbb{Z}_{kl}^* \rightarrow \mathbb{Z}_k^* \times \mathbb{Z}_l^*$  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  $1, 2, \dots, p^r - 1$  je toliko kot večkratnikov  $p$  med števili  $1, 2, \dots, p^r$ , 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  $\varphi$  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.  $\square$

**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.<sup>1</sup>

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 Fareyvega 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.

<sup>1</sup>Čeprav Flitcon ne omenja Eulerjeve funkcije  $\varphi$ , 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 zaporedij.

$$\begin{aligned} F_1 &= \left\{ \frac{0}{1}, \frac{1}{1} \right\} \\ F_2 &= \left\{ \frac{0}{1}, \frac{1}{2}, \frac{1}{1} \right\} \\ F_3 &= \left\{ \frac{0}{1}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{1}{1} \right\} \\ F_4 &= \left\{ \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1} \right\} \\ F_5 &= \left\{ \frac{0}{1}, \frac{1}{5}, \frac{1}{4}, \frac{1}{3}, \frac{2}{5}, \frac{1}{2}, \frac{3}{5}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \frac{1}{1} \right\} \end{aligned} \quad \diamond$$

**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 Fareyvega 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 Fareyvega 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.  $\square$

Kako dobimo člen Fareyvega 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 Fareyvega 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 naslednjo lema.

**Lema 2.11.** Dano naj bo Fareyeva zaporedje. Elemente zaporedja višjega reda dobimo z računanjem mediant elementov danega zaporedja.

**Trditev 2.12** (Lastnost Fareyevih sosedov). 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 induksijski predpostavki za zaporedje  $F_n = \{\dots, \frac{a}{b}, \frac{c}{d}, \dots\}$  velja  $bc - ad = 1$ . Dokažimo, da velja tudi za  $F_{n+1}$ . Vemo, da nove člene zaporedja dobimo z računanjem mediant. Če je  $b + d > n + 1$ , potem  $\frac{a+c}{b+d} \notin F_{n+1}$  in je  $F_{n+1} = \{\dots, \frac{a}{b}, \frac{c}{d}, \dots\}$  ter po induksijski predpostavki  $bc - ad = 1$ . Če je  $b + d \leq n + 1$ , je  $\frac{a+c}{b+d}$  že nek člen v zaporedju  $F_n$  in uporabimo induksijsko predpostavko. Preostane še možnost  $b + d = n + 1$ . Po Lema 2.11 je edina možnost za člen med elementoma  $\frac{a}{b}$  in  $\frac{c}{d}$  njuna medianta  $\frac{a+c}{b+d}$ , ki pa je tudi edini nov člen v opazovanem delu zaporedja. To je zato oblike  $F_{n+1} = \{\dots, \frac{a}{b}, \frac{a+c}{b+d}, \frac{c}{d}, \dots\}$  in  $b(a + c) - a(b + d) = ba + bc - ab - ad = bc - ad = 1$ , kjer smo v zadnji enakosti uporabili induksijsko predpostavko. Podobno je  $(b + d)c - (a + c)d = bc + dc - ad - cd = bc - ad = 1$ . Induksijski 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 Fareyvega zaporedja, za katere velja  $\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$  in  $bp - aq = qc - pd = 1$ . S preureditvijo te enakosti dobimo

$$\begin{aligned} bp + pd &= aq + qc, \\ p(b + d) &= q(a + c), \\ \frac{p}{q} &= \frac{a + c}{b + d}. \end{aligned}$$

Vidimo, da je  $\frac{p}{q}$  medianta ulomkov  $\frac{a}{b}$  in  $\frac{c}{d}$ , od tod pa sledi, da sta  $\frac{a}{b}$  in  $\frac{p}{q}$  ter  $\frac{p}{q}$  in  $\frac{c}{d}$  Fareyeva soseda.  $\square$

**Lema 2.13.** 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.  $\square$

**Opomba 2.14.** Medianta  $\frac{a+c}{b+d}$  je enolično določena z ulomkoma  $\frac{a}{b}$  in  $\frac{c}{d}$ . To imenujemo *lastnost medianta*.

**2.3. Dolžina Fareyvega zaporedja.** Flitconova metoda za izračun števila okrajšanih ulomkov nas pripelje do naslednje rekurzivne formule dolžine Fareyvega zaporedja.

**Trditev 2.15.** Naj bo  $\varphi$  Eulerjeva funkcija. Dolžina Fareyvega zaporedja reda  $n$  je

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

**Opomba 2.16.** Z upoštevanjem vrednosti  $|F_1| = 2$  iz Trditve 2.15 sledi

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

**Trditev 2.17.** *Asimptotično se dolžina Fareyvega zaporedja obnaša kot*

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

**Opomba 2.18.** Simbol  $\sim$  v Trditvi 2.17 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  $\lim_{x \rightarrow \infty} \frac{f(x)}{g(x)} = 1$ .

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

**Definicija 2.19.** *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 2.20.** Preslikava  $\mu: \mathbb{N} \rightarrow \mathbb{N}$ , 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<sup>2</sup> funkcija*.

**Primer 2.21.** 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 2.22.** *Riemannova funkcija zeta* je za  $s \in \mathbb{C} \setminus \{1\}$  definirana kot

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

Sedaj lahko dokažemo Trditev 2.17.

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

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

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

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

---

<sup>2</sup>August Ferdinand Möbius, 17. 11. 1790 – 26. 9. 1868, nemški matematik in astronom.



Sedaj računajmo vsoto

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

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:

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

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 2.16 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.** Naj bosta  $p$  in  $q$  tuji si števili v množici celih števil. *Fordov<sup>3</sup> krog*  $C(\frac{p}{q})$  je krog v zgornji polravnini, ki se abscisne osi dotika v točki  $\frac{p}{q}$ , njegov polmer pa meri  $\frac{1}{2q^2}$ .

Ker so Fordovi krogi definirani za vsak okrajšan ulomek, lahko poljubnemu racionalnemu številu enolično priredimo Fordov krog. Iz analize vemo, da je množica racionalnih števil gosta podmnožica množice realnih števil, abscisna os pa je geometrijska predstavitev le-te. Zato poljubno majhen interval na abscisni osi vsebuje neskončno mnogo dotikališč Fordovih krogov.

Zaradi simetrije je Fordove kroge dovolj obravnavati na intervalu  $[0, 1]$ , obenem pa se zavedati, da jih lahko induktivno razširimo na celotno realno os.

---

<sup>3</sup>Lester Randolph Ford Sr., 25. 10. 1886 – 11. 11. 1967, ameriški matematik.

**Opomba 3.2.** Iz definicije zaradi pogoja o tujosti števil  $p$  in  $q$  neposredno sledi, da je množica Fordovih krogov v bijekciji s Fareyevim zapredjem.

Oglejmo si konstrukcijo pravokotnega trikotnika, določenega s parom Fordovih krogov, ki bo ključna pri dokazovanju trditev v tem poglavju. Izberimo okrajšana ulomka  $\frac{a}{b}$  in  $\frac{c}{d}$ , za katera velja  $\frac{a}{b} < \frac{c}{d}$ , ter jima priredimo ustrezna Fordova kroga. Naj bosta  $A$  središče Fordovega kroga  $C(\frac{a}{b})$  in  $B$  središče Fordovega kroga  $C(\frac{c}{d})$ . Če je  $b < d$ , kar pomeni, da je polmer kroga  $C(\frac{a}{b})$  večji od polmera  $C(\frac{c}{d})$ , točko  $C$  določimo kot presečišče navpične premice skozi točko  $A$  z vodoravno premico skozi točko  $B$ . Sicer je  $b > d$ , točka  $C$  pa presečišče navpične premice skozi točko  $B$  z vodoravno premico skozi točko  $A$ . Povežimo središči obeh krogov. Točki  $D$  in  $E$  naj bosta presečišči daljice  $AB$  s Fordovima krogoma  $C(\frac{a}{b})$  in  $C(\frac{c}{d})$ .

Vemo, da se kroga 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  $|AB|$ ,  $|AC|$  in  $|BC|$ . Po konstrukciji je trikotnik  $ABC$  pravokoten s pravim kotom v oglišču  $C$ , zato velja Pitagorov izrek

$$|AB|^2 = |AC|^2 + |BC|^2.$$

**Opomba 3.3.** V konstrukciji smo brez škode za splošnost predpostavili zvezo  $\frac{a}{b} < \frac{c}{d}$ . Če v splošnem primeru ta ne velja, zamenjamo vlogi ulomkov in postopamo na enak način kot v zgoraj opisanem primeru.

**Trditev 3.4.** *Fordova kroga, ki pripadata različnima okrajšanima ulomkoma, sta bodisi tangentna bodisi disjunktna.*

*Dokaz.* Konstruirajmo pravokotni trikotnik, kot je opisano zgoraj in zapišimo Pitagorov izrek

$$|AB|^2 = |AC|^2 + |BC|^2.$$

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

$$\begin{aligned} |AB|^2 &= \left( \left| \frac{1}{2b^2} - \frac{1}{2d^2} \right| \right)^2 + \left( \left| \frac{c}{d} - \frac{a}{b} \right| \right)^2 \\ &= \frac{1}{4b^4} - \frac{1}{2b^2d^2} + \frac{1}{4d^4} + \left( \frac{bc - ad}{bd} \right)^2 \\ &= \left( \frac{1}{2b^2} + \frac{1}{2d^2} \right)^2 - \frac{1}{b^2d^2} + \frac{(bc - ad)^2}{b^2d^2} \\ &= (|AD| + |EB|)^2 + \frac{(bc - ad)^2 - 1}{b^2d^2}. \end{aligned}$$

Če je  $|bc - ad| > 1$ , je  $|AB|^2 > (|AD| + |EB|)^2$ , zato je  $|AB| > |AD| + |EB|$  in Fordova kroga  $C(\frac{a}{b})$  in  $C(\frac{c}{d})$  sta disjunktna.

Če je  $|bc - ad| = 1$ , je  $|AB|^2 = (|AD| + |EB|)^2$ , zato je  $|AB| = |AD| + |EB|$  in Fordova kroga  $C(\frac{a}{b})$  in  $C(\frac{c}{d})$  sta tangentna.

Če je  $|bc - ad| < 1$ , je  $|bc - ad| = 0$ , saj smo v množici celih števil. Sledi  $\frac{a}{b} = \frac{c}{d}$ , kar vodi v protislovje s predpostavko trditve.  $\square$

**3.1. Fordovi sosedi.** Za tangentne Fordove kroge veljata naslednji lastnosti, ki lastnosti Fareyevih sosedov preneseta v jezik geometrije.

**Trditev 3.5** (Lastnost Fordovih sosedov). *Fordova kroga  $C(\frac{a}{b})$  in  $C(\frac{c}{d})$  sta tangenta natanko tedaj, ko velja  $|bc - ad| = 1$ .*

*Dokaz.* Ponovno konstruirajmo pravokotni trikotnik kot v prejšnjem razdelku. Implikacijo v levo smo že izpeljali, zato si oglejmo še implikacijo v desno.

Denimo, da sta Fordova kroga  $C(\frac{a}{b})$  in  $C(\frac{c}{d})$  tangentna. Potem za pravokotni trikotnik, ki ga določata, velja Pitagorov izrek

$$|AC|^2 + |BC|^2 = |AB|^2$$

oziroma

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

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

$$\begin{aligned} \frac{1}{4b^4} - \frac{1}{2b^2d^2} + \frac{1}{4d^4} + \frac{c^2}{d^2} - \frac{2ac}{bd} + \frac{a^2}{b^2} &= \frac{1}{4b^4} + \frac{1}{2b^2d^2} + \frac{1}{4d^4}, \\ b^2c^2 - 2abcd + a^2d^2 &= 1, \\ (bc - ad)^2 &= 1, \\ |bc - ad| &= 1. \end{aligned}$$

Trditev je s tem dokazana. □

**Definicija 3.6.** Tangentna Fordova kroga imenujemo *Fordova soseda*.

**Trditev 3.7** (Lastnost medianta za Fordove kroge). *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 tangenta na izbrana kroga. Imenujemo ga medianta Fordovih krogov.*

*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 Lema 2.13 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  $C(\frac{a+c}{b+d})$  tangenta 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. □

Naslednji izrek pove, kako konstruiramo množico vseh Fordovih sosedov danega Fordovega kroga.

**Izrek 3.8.** *Naj bosta kroga  $C(\frac{p}{q})$  in  $C(\frac{P}{Q})$  Fordova soseda. Vse Fordove sosede Fordovega kroga  $C(\frac{p}{q})$  lahko zapišemo v obliki  $C(\frac{P_n}{Q_n})$ , kjer je  $\frac{P_n}{Q_n} = \frac{P+np}{Q+nq}$  in  $n$  preteče vsa cela števila.*

*Dokaz.* Najprej dokažimo, da sta Fordova kroga  $C(\frac{p}{q})$  in  $C(\frac{P}{Q})$  res Fordova soseda. Računajmo

$$|qP_n - pQ_n| = |q(P+np) - p(Q+nq)| = |qP + qnp - pQ - pnq| = |qP - pQ| = 1.$$

Zadnja enakost velja po predpostavki, da sta  $C(\frac{p}{q})$  in  $C(\frac{P}{Q})$  Fordova soseda.

Sedaj preverimo, če obstajajo še Fordovi sosedi, ki niso zgornje oblike. Opazovali bomo zaporedje Fordovih krogov  $\mathcal{M} = \{C(\frac{P_n}{Q_n}); n \in \mathbb{Z}\}$ . Iz računa

$$\begin{aligned} |Q_n P_{n+1} - P_n Q_{n+1}| &= |(Q + nq)(P + (n+1)p) - (P + np)(Q + (n+1)q)| \\ &= |QP + (n+1)Qp + nPq + n(n+1)pq \\ &\quad - PQ - (n+1)Pq - npQ - n(n+1)pq| \\ &= |Qp - pQ| \\ &= 1 \end{aligned}$$

sledi, da sta zaporedna elementa zaporedja  $\mathcal{M}$  Fordova soseda. Ulomek  $\frac{P_n}{Q_n}$ , ki predstavlja Fordov krog  $C(\frac{P_n}{Q_n})$ , lahko zapišemo kot

$$\begin{aligned} \frac{P_n}{Q_n} &= \frac{P + np}{Q + nq} = \frac{Pq + npq}{q(Q + nq)} = \frac{Pq + npq + pQ - pQ}{q(Q + nq)} = \frac{p(Q + nq) + (Pq - pQ)}{q(Q + nq)} \\ &= \frac{p}{q} + \frac{Pq - pQ}{q(Q + nq)} = \frac{p}{q} \pm \frac{1}{q(Q + nq)} = \frac{p}{q} \pm \frac{1}{q^2 \left(n + \frac{Q}{q}\right)}. \end{aligned}$$

V limiti, ko gre  $n$  preko vseh meja, gre  $\frac{P_n}{Q_n}$  proti  $\frac{p}{q}$ . Ugotovili smo, da Fordovi krogi oblike  $C(\frac{P_n}{Q_n})$  geometrijsko tvorijo obroč okroli Fordovega kroga  $C(\frac{p}{q})$ . Z njim so namreč vsi tangentni, prav tako pa so tangentni tudi na svojega predhodnika in naslednika v zaporedju  $\mathcal{M}$ . Njihova dotikališča z abscisno osjo konvergirajo proti točki  $\frac{p}{q}$ , ki je dotikališče danega Fordovega kroga  $C(\frac{p}{q})$ , zaradi medsebojne tangentnosti pa so njihovi polmeri vse manjši. Zato ne obstaja Fordov krog, tangen na  $C(\frac{p}{q})$ , ki ni zgornje oblike in ne seka katerega izmed krogov iz zaporedja  $\mathcal{M}$ .  $\square$

V prejšnjem razdelku 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 3.9.** Trojica naravnih števil  $(a, b, c)$ , za katero velja  $a^2 + b^2 = c^2$ , se imenuje *pitagorejska trojica*<sup>4</sup>. Pitagorejska trojica je *primitivna*, če števila  $a$ ,  $b$ , in  $c$  nimajo skupnega faktorja.

**Trditev 3.10.** *Pravokotna trikotnika, ki pripadata poljubnima paroma Fordovih sosedov, določata različni primitivni pitagorejski trojici.*

*Dokaz.* Naj bosta  $C(\frac{a}{b})$  in  $C(\frac{c}{d})$  ter  $C(\frac{a'}{b'})$  in  $C(\frac{c'}{d'})$  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  $ABC$ , drugemu paru pa pravokotni trikotnik  $A'B'C'$ . Dokazati želimo, da si trikotnika nista podobna.

Pa denimo, da sta si trikotnika  $ABC$  in  $A'B'C'$  podobna. Tedaj obstaja tako naravno število  $\lambda \neq 1$ , da za dolžine stranic obeh pravokotnih trikotnikov veljajo

<sup>4</sup>Pojem pitagorejska trojica nosi ime slavnega starogrškega matematika Pitagore (okoli 570 pr. n. št. – 495 pr. n. št.), ki ga poznamo predvsem po Pitagorovem izreku.

naslednje zveze:

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

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

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

Če seštejemo prvi dve enačbi, dobimo

$$(4) \quad \begin{aligned} \frac{1}{b^2} &= \lambda \frac{1}{b'^2}, \\ b'^2 &= \lambda b^2, \\ b' &= \sqrt{\lambda} b. \end{aligned}$$

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

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

Iz (4) in (5) sledi

$$(6) \quad \begin{aligned} \frac{1}{bd} &= \lambda \frac{1}{\sqrt{\lambda} b d'}, \\ \frac{1}{d} &= \frac{\sqrt{\lambda}}{d'}, \\ d' &= \sqrt{\lambda} d. \end{aligned}$$

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

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

To pa je možno le tedaj, ko je  $\lambda = 1$ . Prispeli smo do protislovja, kar pomeni, da si trikotnika nista podobna. Zakaj so pitagorejske trojice primitivne? Če so dolžine stranic posameznega pravokotnega trikotnika paroma tuja si cela števila, že določajo primitivno pitagorejsko trojico. Če imajo ta cela števila skupni celoštevilski faktor, jih z njim delimo (to geometrijsko pomeni, da konstruiramo podobni trikotnik), kar nam da primitivno pitagorejsko trojico. Če pa so dolžine stranic racionalna števila, jih pomnožimo z najmanjšim skupnim večkratnikom njihovih imenovalcev in dobimo enega izmed zgornjih primerov.  $\square$

**3.2. Posplošeni Fordovi krogi.** V prejšnjem razdelku smo se ukvarjali s Fordovimi krogi, ki so bili enolično določeni z racionalnim številom. Natančneje, za dan okrajšan ulomek  $\frac{p}{q}$  smo konstruirali Fordov krog na zgornji polravnini evklidske ravnine, ki se abscisne osi dotika v točki  $\frac{p}{q}$ , njegov polmer pa meri  $\frac{1}{2q^2}$ . Nadaljujemo lahko s splošnejšimi Fordovimi krogi, ki so definirani na povsem enak način, le da

imajo polmer enak  $\frac{1}{2hq^2}$ , pri čemer je  $h$  poljubno realno število. Imenujemo jih tudi Speiserjevi<sup>5</sup> krogi. Če izberemo  $h = 1$ , dobimo običajne Fordove kroge.

**3.3. Fordove krogle.** Tokrat naj bosta števili  $p$  in  $q$  elementa množice Gaussovih celih števil, ki je definirana kot  $\mathbb{Z}[i] = \{a + bi; a, b \in \mathbb{Z}\}$ . Zapišimo  $p = p' + ip''$  in  $q = q' + iq''$ , kjer so  $p', p'', q', q'' \in \mathbb{Z}$ . Definirajmo ulomek

$$\frac{p}{q} = \frac{p' + ip''}{q' + iq''} = \frac{(p' + ip'')(q' - iq'')}{(q' + iq'')(q' - iq'')} = \frac{p'q' + p''q''}{q'^2 + q''^2} + i \frac{p''q' - p'q''}{q'^2 + q''^2},$$

ki pripada kompleksnim številom, in ga okrajšajmo. Geometrijsko predstavlja točko v Gaussovi  $xy$ -ravnini z realno in imaginarno komponento. Gaussovo ravnino postavimo v prostor, določen z osjo  $z$ , pravokotno na Gaussovo ravnino, in opazujemo podprostor, ki pripada pozitivnim vrednostim na  $z$ -osi. Analogno Fordovim krogom v ravnini pridemo do naslednjega pojma.

**Definicija 3.11.** *Fordova krogla*  $S(\frac{p}{q})$ , kjer je  $\frac{p}{q}$  okrajšan ulomek v množici kompleksnih števil, je krogla v zgornjem polprostoru, definiranem kot zgoraj, ki se  $xy$ -ravnine dotika v točki, določeni s  $\frac{p}{q}$ , njen polmer pa meri  $\frac{1}{2|q|^2}$ .

Na analogen način trditvam, ki opisujejo lastnosti Fordovih krogov, lahko izpeljemo in dokažemo lastnosti Fordovih krogel. Omenimo le nekatere izmed njih.

Poljubno majhen zaprt pravokotnik v  $xy$ -ravnini vsebuje neskončno mnogo dotikališč Fordovih krogel.

Spomnimo se konstrukcije pravokotnega trikotnika, določenega z dvema Fordovima krogoma. Naj točki  $\frac{p}{Q}$  in  $\frac{P}{Q}$  določata Fordovi krogi ter konstruirajmo pravokotni trikotnik  $ABC$  kot prej. Iz zveze

$$|AB|^2 = \left| \frac{P}{Q} - \frac{p}{q} \right|^2 + \left| \frac{1}{2|Q|^2} - \frac{1}{2|q|^2} \right|^2 = \frac{|Pq - pQ|^2 - 1}{|Q|^2|q|^2} + (|AD| + |EB|)^2$$

sledi: če je  $|Pq - pQ| > 1$ , je  $|AB| > |AD| + |EB|$  in krogi sta disjunktni; sicer je  $|Pq - pQ| = 1$ , zato je  $|AB| = |AD| + |EB|$  in krogi sta tangentni.

Naj bosta  $S(\frac{p}{Q})$  in  $S(\frac{P}{Q})$  tangentni Fordovi krogi. Kot prej tangentne Fordove krogle na kroglo  $S(\frac{p}{q})$  konstruiramo s pomočjo formule

$$\frac{P_n}{Q_n} = \frac{P + np}{Q + nq},$$

le da tokrat  $n$  pripada množici Gaussovih celih števil. Nadalje nas zanima, koliko Fordovih krogel je tangentnih na kroglo  $S(\frac{P_n}{Q_n})$ . Uporabimo pogoj za tangentnost, ki smo ga izpeljali. Računajmo

$$\begin{aligned} |P_n Q_m - P_m Q_n| &= |(P + np)(Q + mq) - (P + mp)(Q + nq)| \\ &= |PQ + mPq + npQ + mnnpq - PQ - nqP - mpQ - mnmpq| \\ &= |Pq - pQ||m - n| = 1. \end{aligned}$$

Sledi, da je  $|m - n| = 1$ , torej je razlika  $m - n \in \{1, -1, i, -i\}$ . Ugotovili smo, da je vsaka Fordova krogla, ki je tangentna na dano Fordovo kroglo, tangentna še na štiri druge Fordove krogle. Velja, da so te edine tangentne krogle.

<sup>5</sup>Andreas Speiser, 10. 6. 1885 – 12. 10. 1970, švicarski matematik, ki se je ukvarjal s teorijo števil in teorijo grup.

**3.4. Möbiusove transformacije na Fordovih krogih.** Do sedaj smo Fordove kroge obravnavali s pomočjo geometrijskih sredstev. V tem poglavju si bomo z algebro pomagali do nekaterih že znanih rezultatov o Fordovih krogih. Geometrijske objekte si bomo predstavljali v kompleksni ravnini, torej bo točka s koordinatama  $(x, y)$  opisana s kompleksnim številom  $z = x + iy$ .

Najprej se spomnimo naslednjega pojma iz kompleksne analize.

**Definicija 3.12.** Preslikava  $f: \mathbb{CP}^1 \rightarrow \mathbb{CP}^1$ , definirana s predpisom  $f(z) = \frac{az+c}{bz+d}$ , kjer so  $a, b, c, d \in \mathbb{C}$  in  $ad - bc \neq 0$ , se imenuje *Möbiusova transformacija*.

**Opomba 3.13.** Simbol  $\mathbb{CP}^1$  označuje *Riemannovo sfero*, to je kompaktifikacijo kompleksne ravnine z eno točko, kar zapišemo kot  $\mathbb{CP}^1 = \mathbb{C} \cup \{\infty\}$ .

**Opomba 3.14.** Števila  $a, b, c, d$  lahko pomnožimo s poljubnim neničelnim kompleksnim številom, zato lahko predpostavimo, da je  $ad - bc = 1$ .

V našem primeru bo dovolj obravnavati le  $a, b, c, d \in \mathbb{Z}$ .

Möbiusova transformacija je meromorfna in bijektivna preslikava z inverzom, ki je spet take oblike, identična preslikava  $id(z) = z$  je Möbiusova transformacija, prav tako je kompozitum Möbiusovih transformacij Möbiusova transformacija. Množica takih preslikav tako tvori grupo za kompozitum. Preslikavo  $f$  lahko zapišemo v matrični obliki

$$\mathbf{A} = \begin{bmatrix} a & c \\ b & d \end{bmatrix},$$

kjer so  $a, b, c, d \in \mathbb{Z}$ . Ker velja  $ad - bc = 1$ , je matrika  $A \in SL_2(\mathbb{Z})$ . Zato bomo Möbiusove transformacije predstavljali s splošno linearno grupo  $SL_2(\mathbb{Z})$ .

Ključen pri izpeljavi rezultatov o Fordovih krogih je pojem, ki ga v algebri pogosto uporabljamo.

**Definicija 3.15.** *Delovanje grupe  $G$  na množico  $M$*  je taka preslikava  $\circ: G \times M \rightarrow M$ , za katero velja:

- (1)  $e \circ \alpha = \alpha$  za vsak  $\alpha \in M$ , kjer je  $e$  enota grupe  $G$ ,
- (2)  $g \circ (h \circ \alpha) = (gh) \circ \alpha$  za vsak  $\alpha \in M$  in vsaka  $g, h \in G$ .

Ekvivalentno, delovanje grupe  $G$  na množico  $M$  je homomorfizem iz grupe  $G$  v grupo permutacij množice  $M$ .

**Primer 3.16.** Naj bo  $G$  grupa permutacij  $n$  elementov, torej  $G = S_n$ ,  $M$  pa naj bo množica  $M = \{1, 2, \dots, n\}$ . Delovanje grupe  $G$  na množico  $M$  je preslikava  $\circ: G \times M \rightarrow M$  s predpisom  $(\pi, \alpha) \mapsto \pi(\alpha) = \pi \circ \alpha$ .  $\diamond$

**Definicija 3.17.** Fordov krog  $C(\frac{1}{0})$ , katerega polmer je neskončen, je premica  $\mathbb{R} + i$ .

**Izrek 3.18.** *Möbiusova transformacija slika Fordove kroge v Fordove kroge.*

*Dokaz.* Naj bo Möbiusova transformacija dana z matriko

$$\mathbf{A} = \begin{bmatrix} a & c \\ b & d \end{bmatrix} \in SL_2(\mathbb{Z}).$$

Vemo, da tovrstna preslikava slika premice in krožnice v premice in krožnice. Ideja dokaza je pokazati, da grupa  $SL_2(\mathbb{Z})$  deluje na množico Fordovih krogov.

S krajšim računom se lahko prepričamo, da je grupa  $SL_2(\mathbb{Z})$  generirana z matrikama  $\begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}$  in  $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$ . To pomeni, da je vsako Möbiusovo transformacijo

moč zapisati kot kompozitum preslikav  $z \mapsto z + 1$  in  $z \mapsto -\frac{1}{z}$ , ki ustrezata generatorjema. Trdimo, da Möbiusova transformacija preslika Fordov krog z intervala  $[0, 1]$  v Fordov krog z intervala  $[n, n + 1]$ , kjer  $n$  pripada množici celih števil.

Preslikava  $z \mapsto z + 1$  je translacija, zato zgornje očitno velja.

Kaj pa preslikava  $z \mapsto -\frac{1}{z}$ ? Najprej si oglejmo splošen primer. Naj bo original Fordov krog s polmerom  $r$  in središčem v  $\alpha$ , predstavljen z enačbo  $|z - \alpha| = r$ . Prepišimo enačbo v

$$(8) \quad \begin{aligned} (z - \alpha)(\bar{z} - \bar{\alpha}) &= r^2, \\ z\bar{z} - \alpha\bar{z} - \bar{\alpha}z + \alpha\bar{\alpha} - r^2 &= 0 \end{aligned}$$

in označimo  $R = \alpha\bar{\alpha} - r^2$ . Polmer lahko izrazimo kot  $r = \sqrt{|\alpha|^2 - R}$ . Preslikajmo original s preslikavo  $z \mapsto -\frac{1}{z}$ . Enačba slike se glasi

$$(9) \quad \begin{aligned} \left(-\frac{1}{z}\right)\left(-\frac{1}{\bar{z}}\right) + \alpha\frac{1}{\bar{z}} + \bar{\alpha}\frac{1}{z} + R &= 0, \\ 1 + \alpha z + \bar{\alpha}\bar{z} + Rz\bar{z} &= 0, \\ z\bar{z} + \frac{\bar{\alpha}}{R}\bar{z} + \frac{\alpha}{R}z + \frac{1}{R} &= 0. \end{aligned}$$

Sedaj vzemimo Fordov krog  $C(\frac{p}{q})$ . Njegov polmer meri  $\frac{1}{2q^2}$ , središče pa je v točki  $\frac{p}{q} + i\frac{1}{2q^2}$ . Izračunajmo

$$R = \alpha\bar{\alpha} - r^2 = \left(\frac{p}{q} + i\frac{1}{2q^2}\right)\left(\frac{p}{q} - i\frac{1}{2q^2}\right) - \frac{1}{4q^4} = \frac{p^2}{q^2} + \frac{1}{4q^4} - \frac{1}{4q^4} = \frac{p^2}{q^2}$$

in preverimo, da je slika izbranega Fordovega kroga tudi Fordov krog. Res, središče slike je po enačbi (9) v točki

$$-\frac{\bar{\alpha}}{R} = -\frac{\frac{p}{q} - i\frac{1}{2q^2}}{\frac{p^2}{q^2}} = -\frac{q}{p} + i\frac{1}{2p^2},$$

polmer pa meri

$$\sqrt{\left|-\frac{\bar{\alpha}}{R}\right|^2 - \frac{1}{R}} = \sqrt{\frac{\bar{\alpha}\alpha}{R} - \frac{1}{R}} = \frac{1}{R}\sqrt{|\alpha|^2 - R} = \frac{1}{R}\frac{1}{2q^2} = \frac{q^2}{2p^2q^2} = \frac{1}{2p^2}.$$

Dokazali smo, da preslikavi, ki generirata grupo Möbiusovih transformacij, Fordov krog preslikata v Fordov krog z intervala  $[n, n + 1]$  za  $n \in \mathbb{Z}$ . Da dobimo Fordov krog z intervala  $[0, 1]$ , moramo prvotno preslikavo komponirati z  $n$  translacijami v levo (za  $-1$ ). Ker identiteta slika Fordov krog vase in je kompozitum Möbiusovih transformacij dobro definiran, grupa  $SL_2(\mathbb{Z})$  res deluje na množico Fordovih krogov.  $\square$

**Lema 3.19.** *Dana naj bosta Fordova kroga  $C(\frac{e}{f})$  in  $C(\frac{g}{h})$ . Möbiusova transformacija, ki deluje na množico Fordovih krogov, ohranja  $|eh - fg|$ .*

*Dokaz.* Kot v Definiciji 3.12 zapišimo Möbiusovo transformacijo v obliki  $f(z) = \frac{az+c}{bz+d}$ , kjer so  $a, b, c, d \in \mathbb{Z}$  in velja  $ad - bc = 1$ . Vzemimo Fordova kroga  $C(\frac{e}{f})$  in  $C(\frac{g}{h})$  in pogledajmo, kam se preslikata. Ker velja Izrek 3.18 in je Fordov krog enolično določen s točko, v kateri se dotika realne osi v kompleksni ravnini, je dovolj poznati sliko te točke. Izračunajmo

$$f\left(\frac{e}{f}\right) = \frac{a\frac{e}{f} + c}{b\frac{e}{f} + d} = \frac{ae + cf}{be + df},$$



od koder sledi, da se Fordov krog  $C(\frac{e}{f})$  preslika v Fordov krog  $C(\frac{ae+cf}{be+df})$ . Podobno,

$$f\left(\frac{g}{h}\right) = \frac{a\frac{g}{h} + c}{b\frac{g}{h} + d} = \frac{ag + ch}{bg + dh},$$

in  $C(\frac{g}{h})$  se preslika v  $C(\frac{ag+ch}{bg+dh})$ . Označimo  $e' = ae + cf$ ,  $f' = be + df$ ,  $g' = ag + ch$  in  $h' = bg + dh$ . Računajmo

$$e'h' - f'g' = (ae + cf)(bg + dh) - (be + df)(ag + ch) = (ad - bc)(eh - fg),$$

katerega absolutna vrednost je enaka

$$|e'h' - f'g'| = |ad - bc||eh - fg| = |eh - fg|,$$

s čimer smo dokazali želeno enakost.  $\square$

Iz zgornjega neposredno sledi naslednja ugotovitev.

**Posledica 3.20.** Dana naj bosta Fordova kroga  $C(\frac{e}{f})$  in  $C(\frac{g}{h})$ . Möbiusova transformacija, ki deluje na množico Fordovih krogov, ohranja  $|eh - fg| = 1$ .

Sedaj bomo s pomočjo orodij, ki smo jih obravnavali v tem razdelku, ponovno dokazali že znano lastnost medianta za Fordove kroge.

*Dokaz lastnosti medianta za Fordove kroge z Möbiusovimi transformacijami.* Kroga  $C(\frac{r}{s})$  in  $C(\frac{p}{q})$  naj bosta Fordova soseda. Trdimo, da je kandidat  $C(\frac{r+p}{s+q})$  medianta izbranih Fordovih krogov.

Vzemimo točke v presečiščih teh treh krogov. Vemo, da za točke  $\alpha, \beta, \gamma$  obstaja Möbiusova transformacija, ki jih preslika v poljubne točke  $\lambda, \mu, \nu$ . Torej obstaja Möbiusova transformacija  $M_1$ , ki izbrane točke v presečiščih preslika v točke  $i, \frac{1}{2} + \frac{1}{2}i, 1 + i$ . Ker Möbiusova transformacija slika Fordove kroge v Fordove kroge, mi pa poznamo slike dveh točk na vsakem izmed krogov  $C(\frac{r}{s})$ ,  $C(\frac{p}{q})$  in  $C(\frac{r+p}{s+q})$ , poznamo slike vseh treh Fordovih krogov. Te pa so točno  $C(\frac{1}{0})$ ,  $C(\frac{0}{1})$  in  $C(\frac{1}{1})$ .

Sedaj bomo konstruirali zaporedje Möbiusovih transformacij (ki je prav tako Möbiusova transformacija). Začnimo s Fordovima sosedoma  $C(\frac{r}{s})$  in  $C(\frac{p}{q})$ . Preslikava  $M_1$  ju preslika v Fordova kroga  $C(\frac{1}{0})$  in  $C(\frac{0}{1})$  z medianto, Fordovim krogom,  $C(\frac{1}{1})$ . Kot v prvem delu dokaza izberimo tri točke v presečiščih in jih preslikajmo. Obstaja Möbiusova transformacija  $M_2$ , ki Fordove kroge  $C(\frac{1}{0})$ ,  $C(\frac{0}{1})$  in  $C(\frac{1}{1})$  zaporedoma preslika v Fordove kroge  $C(\frac{a}{b})$  in  $C(\frac{c}{d})$  in  $C(\frac{a+c}{b+d})$ . Nadaljujemo s transformacijo  $M_3$ , ki slednje preslika po vrsti v Fordove kroge  $C(\frac{1}{0})$ ,  $C(\frac{0}{1})$  in  $C(\frac{1}{1})$ , in končajmo s transformacijo  $M_4$ , ki le-te preslika v Fordove kroge  $C(\frac{r}{s})$ ,  $C(\frac{p}{q})$  in  $C(\frac{r+p}{s+q})$ .

Vse zgornje preslikave so Möbiusove transformacije, ki ohranjajo medianto Fordovih krogov (saj velja Posledica 3.20 ter je  $C(\frac{1}{1})$  medianta  $C(\frac{1}{0})$  in  $C(\frac{0}{1})$ ), zato tudi kompozitum  $M_4 \circ M_3 \circ M_2 \circ M_1$  ohranja medianto. Sledi, da je naš kandidat  $C(\frac{r+p}{s+q})$  res medianta. Z drugimi besedami, za poljubna Fordova soseda obstaja enolično določen Fordov krog, ki je tangen na oba.  $\square$

#### 4. RIEMANNOVA HIPOTEZA

Riemannova hipoteza, znana tudi kot 8. Hilbertov problem, je eno najbolj slavnih, še vedno nerešenih matematičnih vprašanj. Ime je dobila po nemškem matematiku Bernhardu Riemannu, ki jo je formuliral med preučevanjem lastnosti velikih praštevil.

**4.1. Praštevila in Riemannova zeta funkcija.** Praštevila so poznali že v Stari Grčiji, od koder prihaja tudi naslednji izrek.

**Izrek 4.1** (Evklid). *Praštevilo je neskončno mnogo.*

Dokazov tega fundamentalnega izreka je veliko, velja pa omeniti Evklidovo idejo dokazovanja s protislovjem, ki jo pogosto uporabljamo še danes.

V 1. polovici 18. stoletja je Euler definiriral realno funkcijo zeta s predpisom

$$(10) \quad \zeta: \mathbb{R} \rightarrow \mathbb{R},$$

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

Za  $n = 1$  je enaka harmonični vrsti, ki divergira; za  $n > 1$  pa dobimo konvergentno vrsto. Funkcija zeta je povezana s praštevili preko naslednje formule, ki jo je Euler objavil leta 1737 v knjigi *Variae observationes circa series infinitas*.

**Izrek 4.2** (Eulerjeva produktna formula). *Naj bo  $n \in \mathbb{N}$  in  $p \in \mathbb{P}$ . Tedaj velja*

$$(11) \quad \sum_n \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}.$$

*Dokaz.* Zapišimo predpis za funkcijo zeta. V naslednjem koraku funkcijo zeta pomnožimo z  $\frac{1}{2^s}$  ter dobljeno enakost odštejemo od prve enakosti. S tem odpadejo vsi členi s faktorjem 2. Ta dva koraka ponavljamo: enakost na trenutnem koraku pomnožimo z drugim sumandom na desni strani enakosti, nato pa predzadnji vrstici odštejemo zadnjo vrstico.

$$\begin{aligned} \zeta(s) &= 1 + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots, \\ \frac{1}{2^s} \zeta(s) &= \frac{1}{2^s} + \frac{1}{4^s} + \frac{1}{6^s} + \frac{1}{8^s} + \frac{1}{10^s} + \dots, \\ \left(1 - \frac{1}{2^s}\right) \zeta(s) &= 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \dots, \\ \frac{1}{3^s} \left(1 - \frac{1}{2^s}\right) \zeta(s) &= \frac{1}{3^s} + \frac{1}{9^s} + \frac{1}{15^s} + \frac{1}{21^s} + \frac{1}{27^s} \dots, \\ \left(1 - \frac{1}{3^s}\right) \left(1 - \frac{1}{2^s}\right) \zeta(s) &= 1 + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \dots \end{aligned}$$

Opazimo, da smo vselej množili z ulomki oblike  $\frac{1}{p^s}$ , kjer  $p$  pripada množici praštevil. Dobimo enakost

$$\dots \left(1 - \frac{1}{13^s}\right) \left(1 - \frac{1}{11^s}\right) \left(1 - \frac{1}{7^s}\right) \left(1 - \frac{1}{5^s}\right) \left(1 - \frac{1}{3^s}\right) \left(1 - \frac{1}{2^s}\right) \zeta(s) = 1,$$

od koder lahko izrazimo

$$\zeta(s) = \frac{1}{1 - \frac{1}{2^s}} \frac{1}{1 - \frac{1}{3^s}} \frac{1}{1 - \frac{1}{5^s}} \frac{1}{1 - \frac{1}{7^s}} \frac{1}{1 - \frac{1}{11^s}} \dots = \prod_p \frac{1}{1 - p^{-s}},$$

kar smo želeli pokazati. □

V 19. stoletju so začeli računati s kompleksnimi števili, tako je Riemann leta 1859 razširil Eulerjevo definicijo funkcije zeta. Riemannova funkcija zeta množico  $\mathbb{C} \setminus \{1\}$  preslika na množico  $\mathbb{C}$  in je definirana v Definiciji 2.22.

**Opomba 4.3.** V Izreku 4.2 nismo povedali, kateri množici pripada spremenljivka  $s$ . Euler je formulo namreč formuliral za celoštevilске  $s$ , Riemann pa je z razširitvijo funkcije zeta dokazal, da enakost velja za vse  $s$ , za katere velja  $\operatorname{Re}(s) > 1$ .

Zanimajo nas ničle Riemannove funkcije zeta. Na polravnini  $\operatorname{Re}(s) > 1$  se funkcija ujema s  $\prod_p \frac{1}{1-p^{-s}}$ . Ker so vsi faktorji  $\frac{1}{1-p^{-s}} \neq 0$  in je  $\lim_{p \rightarrow \infty} \frac{1}{1-p^{-s}} = 1$ , je na tej polravnini  $\prod_p \frac{1}{1-p^{-s}} \neq 0$ . To pomeni, da Riemannova funkcija zeta nima ničel za  $\operatorname{Re}(s) > 1$ .

Kako je z ničlami na polravnini  $\operatorname{Re}(s) < 0$ ? Pomagali si bomo z Bernoullijevimi števili. Naj bo  $|z| < 2\pi$ . Bernoullijeva<sup>6</sup> števila  $B_k$  definiramo preko funkcije

$$(12) \quad G(z) = \frac{z}{e^z - 1} = \sum_{k=0}^{\infty} B_k \frac{z^k}{k!}.$$

Z razvojem v Taylorjevo vrsto dobimo

$$G(z) = \left(1 + \frac{z}{2!} + \frac{z^2}{3!} + \frac{z^3}{4!} + \dots\right)^{-1} = 1 - \frac{z}{2} + \frac{z^2}{12} - \frac{z^4}{720} + \dots,$$

od koder preberemo prvih nekaj Bernoullijevih števil:  $B_0 = 1$ ,  $B_1 = -\frac{1}{2}$ ,  $B_2 = \frac{1}{6}$ ,  $B_3 = 0$ ,  $B_4 = -\frac{1}{30}$ . Za vse lihe  $n$ , kjer je  $n \geq 3$ , velja  $B_n = 0$ . Za nas je pomembna naslednja povezava Bernoullijevih števil z Riemannovo funkcijo zeta. Naj bo  $n \in \{0, 1, 2, \dots\}$ . Velja

$$(13) \quad \zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}.$$

Ker so za sode  $n$  vrednosti  $B_{n+1} = 0$ , je  $\zeta(s) = 0$  za  $s \in \{-2, -4, -6, \dots\}$ . To pa so tudi edine ničle na opazovani polravnini. Imenujemo jih *trivialne ničle* Riemannove funkcije zeta. Ostal je še pas  $0 < \operatorname{Re}(s) < 1$ , o ničlah na njem pa govori naslednji izrek.

**Izrek 4.4** (Riemannova hipoteza). *Vse netrivialne ničle Riemannove funkcije zeta ležijo na premici  $s = \frac{1}{2} + it$ .*

**4.2. Riemannova hipoteza.** Obstaja več ekvivalentnih formulacij Riemannove hipoteze. Dokazali bomo eno izmed njih, ki vključuje Fareyjevo zaporedje. Pred tem se spomnimo Möbiusove funkcije, definirane v Definiciji 2.20.

**Definicija 4.5.** Za  $n \in \mathbb{N}$  je Mertensova<sup>7</sup> funkcija definirana s predpisom

$$M(n) = \sum_{k \leq n} \mu(k).$$

**Primer 4.6.** Izračunajmo nekaj vrednosti Mertensove funkcije.

$$M(2) = \mu(1) + \mu(2) = 1 - 1 = 0$$

$$M(3) = \mu(1) + \mu(2) + \mu(3) = 1 - 1 - 1 = -1$$

$$M(6) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(5) + \mu(6) = 1 - 1 - 1 + 0 - 1 + 1 = -1 \quad \diamond$$

<sup>6</sup>Jacob Bernoulli, 27. 12. 1654 – 16. 8. 1705, rojen v družini znamenitih švicarskih matematikov. Med drugim mu pripisujemo odkritje konstante  $e$ .

<sup>7</sup>Franz Mertens, 20. 3. 1840 – 5. 3. 1927, poljski matematik.

Naslednjo trditev, ki jo bomo navedli brez dokaza, je leta 1912 dokazal Littlewood. Njeno bistvo je, da Riemannovo hipotezo lahko prevedemo na ekvivalentno trditev, ki opisuje rast Mertensove funkcije.

**Trditev 4.7.** *Za vsak  $\epsilon > 0$  velja  $M(n) = o(n^{1/2+\epsilon})$  natanko tedaj, ko velja Riemannova hipoteza.*

Pred drugo ekvivalenco Riemannove hipoteze potrebujemo definicijo, ki sledi.

**Definicija 4.8.** Naj bosta  $L(n)$  dolžina Fareyvega zaporedja  $F_n$  in  $r_v$  njegov  $v$ -ti element. Definiramo razliko

$$\delta_v = r_v - v/L(n).$$

**Primer 4.9.** Vzemimo Fareyvo zaporedje reda 4 in pogledimo nekaj razlik.

$$\begin{aligned} F_4 &= \left\{ \frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1} \right\}, \\ L(4) &= 7, \\ \delta_1 &= \frac{0}{1} - \frac{1}{7} = -\frac{1}{7}, \\ \delta_2 &= \frac{1}{4} - \frac{2}{7} = -\frac{1}{28}, \\ \delta_7 &= \frac{1}{1} - \frac{7}{7} = 0. \end{aligned}$$

◇

**Trditev 4.10** (Franel – Landau, 1924). *Za vsak  $\epsilon > 0$  velja  $\sum_{v=1}^{L(n)} |\delta_v| = o(n^{1/2+\epsilon})$  natanko tedaj, ko velja Riemannova hipoteza.*

Dokaz zgornje trditve izpustimo. Pač pa bomo v nadaljevanju dokazali povezavo med navedenima ekvivalenčnima formulacijama Riemannove hipoteze, ki jo lahko združimo v izrek.

**Izrek 4.11.** *Naj bo  $\epsilon > 0$ .  $\sum_{v=1}^{L(n)} |\delta_v| = o(n^{1/2+\epsilon})$  velja tedaj in le tedaj, ko velja  $M(n) = o(n^{1/2+\epsilon})$ .*

Naslednja lema bo ključ do dokaza zgornjega izreka.

**Lema 4.12.** *Realna funkcija  $f$  naj bo definirana na intervalu  $[0, 1]$ . Naj bodo  $r_v$  elementi Fareyvega zaporedja reda  $n$ ,  $r_0 = 0$  in  $r_{L(n)} = 1$ <sup>8</sup>. Tedaj velja enakost*

$$(14) \quad \sum_{v=1}^{L(n)} f(r_v) = \sum_{k=1}^{\infty} \sum_{j=1}^k f\left(\frac{j}{k}\right) M\left(\frac{n}{k}\right).$$

4.2.1. *Dokaz implikacije v desno.* Naj bo  $\epsilon > 0$ . Naj bo  $u \in [0, 1]$  in definirajmo funkcijo  $f(u) = e^{2\pi i u}$ . Uporabimo lema 4.12 in funkcijo vstavimo v enakost (14); dobimo

$$(15) \quad \sum_{v=1}^{L(n)} e^{2\pi i r_v} = \sum_{k=1}^{\infty} \sum_{j=1}^k e^{2\pi i \frac{j}{k}} M\left(\frac{n}{k}\right).$$

Vemo, da je  $\sum_{j=1}^k e^{2\pi i \frac{j}{k}} = 0$  za  $k \geq 2$ , za  $k = 1$  pa se vsota poenostavi v  $e^{2\pi i} = 1$ . Enakost (15) zato prepišemo v

$$M(n) = \sum_{v=1}^{L(n)} e^{2\pi i r_v} = \sum_{v=1}^{L(n)} e^{2\pi i \left(\frac{v}{L(n)} + \delta_v\right)} = \sum_{v=1}^{L(n)} e^{\frac{2\pi i v}{L(n)}} (e^{2\pi i \delta_v} - 1) + \sum_{v=1}^{L(n)} e^{\frac{2\pi i v}{L(n)}}.$$

<sup>8</sup>Zgolj zaradi preglednejšega zapisa bomo za potrebe dokaza Fareyvo zaporedje opazovali od neničelnega člena dalje. Tako bo element  $r_v$  zdaj predstavljal element  $r_{v+1}$  v običajni notaciji, vrednost  $L(n)$  pa se bo zmanjšala za 1.

Ker je  $L(n) > 1$ , je zadnji sumand enak 0. Sedaj ocenimo absolutno vrednost zgornjega izraza:

$$\begin{aligned}
|M(n)| &\leq \sum_{v=1}^{L(n)} \left| e^{\frac{2\pi i v}{L(n)}} \right| |e^{2\pi i \delta_v} - 1| = \sum_{v=1}^{L(n)} |e^{2\pi i \delta_v} - 1| = \sum_{v=1}^{L(n)} |e^{\pi i \delta_v}| |e^{\pi i \delta_v} - e^{-\pi i \delta_v}| \\
&= 2 \sum_{v=1}^{L(n)} |\sin(\pi \delta_v)| \leq 2 \sum_{v=1}^{L(n)} |\delta_v| \pi = 2\pi \sum_{v=1}^{L(n)} |\delta_v| \\
&\leq 2\pi K(\varepsilon) n^{1/2+\varepsilon} = K'(\varepsilon) n^{1/2+\varepsilon}.
\end{aligned}$$

V zadnji neenakosti smo uporabili predpostavko  $\sum_{v=1}^{L(n)} |\delta_v| = o(n^{1/2+\varepsilon})$ , kar je ekvivalentno  $\sum_{v=1}^{L(n)} |\delta_v| \leq K(\varepsilon) n^{1/2+\varepsilon}$  za neko konstanto  $K$ , ki je odvisna od  $\varepsilon$ . Od tod sledi, da je  $M(n) = o(n^{1/2+\varepsilon})$ .

**4.2.2. Pomožne definicije.** Preden se lotimo dokazovanja obratne implikacije, potrebujemo nekaj novih pojmov. Navedli bomo le najpomembnejše rezultate, ki jih bomo v dokazu potrebovali. Izpeljave niso pretežke, vendar jih bomo tokrat izpustili, saj bi precej povečale obseg dela. Povzeti so po [2, poglavje 6.2].

**Definicija 4.13.** Naj bo  $n \in \mathbb{N} \cup \{0\}$ .  $n$ -ti Bernoullijev polinom  $B_n$  je polinom stopnje  $n$ , ki ustreza zvezi

$$(16) \quad \int_x^{x+1} B_n(t) dt = x^n.$$

**Primer 4.14.** Zapišimo nekaj Bernoullijevih polinomov najnižjih stopenj.

$$\begin{aligned}
B_0(x) &= 1, \\
B_1(x) &= x - \frac{1}{2}, \\
B_2(x) &= x^2 - x + \frac{1}{6}, \\
B_3(x) &= x^3 - \frac{3}{2}x^2 + \frac{1}{2}x.
\end{aligned}$$

◇

**Definicija 4.15.** Naj bo  $B_n$   $n$ -ti Bernoullijev polinom. Pripadajoča funkcija  $\bar{B}_n$  je definirana kot  $\bar{B}_n(x) = B_n(x - \lfloor x \rfloor)$ .

**Opomba 4.16.** Iz definicije sledi, da je  $\bar{B}_n$  periodična funkcija.

**Primer 4.17.** Funkcijo  $\bar{B}_1(x) = x - \lfloor x \rfloor - \frac{1}{2}$  bomo potrebovali v dokazu.

◇

**Trditev 4.18.** Naj bo  $k \in \mathbb{N}$ . Tedaj je

$$(17) \quad B_n(ku) = k^{n-1} \left( B_n(u) + B_n\left(u + \frac{1}{k}\right) + \cdots + B_n\left(u + \frac{k-1}{k}\right) \right).$$

*Dokaz.* Dokaz za  $k = 2$  se nahaja v [2, poglavje 6.2, str. 102 – 103]. Za splošen  $k$  je dokaz analogen. □

**4.2.3. Dokaz implikacije v levo.** Spomnimo se funkcije  $\bar{B}_1(x) = x - \lfloor x \rfloor - \frac{1}{2}$  in enačbe 17. Izberimo  $n = 1$ . Funkcija  $\bar{B}_1$  je periodična s periodo 1, zato je za  $x = ku$  dovolj obravnavati vrednosti  $0 \leq u \leq \frac{1}{k}$ . Za te vrednosti pa se  $\bar{B}_1$  ujema s funkcijo  $B_1$ . Enačba 17 zato dobi obliko

$$\begin{aligned}
\bar{B}_1(ku) &= \bar{B}_1(u) + \bar{B}_1\left(u + \frac{1}{k}\right) + \cdots + \bar{B}_1\left(u + \frac{k-1}{k}\right) \\
(18) \quad &= \bar{B}_1\left(u + \frac{1}{k}\right) + \bar{B}_1\left(u + \frac{2}{k}\right) + \cdots + \bar{B}_1(u + 1).
\end{aligned}$$

Ključni korak dokaza je, da v enakost iz leme 4.12 vstavimo funkcijo  $\bar{B}_1$ , pri čemer uporabimo zvezo 18. Označimo

$$(19) \quad G(u) = \sum_{v=1}^{L(n)} \bar{B}_1(u + r_v) = \sum_{k=1}^{\infty} \sum_{j=1}^k \bar{B}_1\left(u + \frac{j}{k}\right) M\left(\frac{n}{k}\right) = \sum_{k=1}^{\infty} \bar{B}_1(ku) M\left(\frac{n}{k}\right)$$

in dobimo dva izraza za funkcijo  $G$ . Izračunali bomo integral

$$(20) \quad I = \int_0^1 G(u)^2 du.$$

1. primer:  $G(u) = \sum_{v=1}^{L(n)} \bar{B}_1(u + r_v)$ . Oglejmo si, kakšna je funkcija  $G$ . Razpišimo zgornjo zvezo:

$$(21) \quad \begin{aligned} G(u) &= \sum_{v=1}^{L(n)} \bar{B}_1(u + r_v) = \sum_{v=1}^{L(n)} \left( u + r_v - \lfloor u + r_v \rfloor - \frac{1}{2} \right) \\ &= L(n)u + \sum_{v=1}^{L(n)} r_v - \sum_{v=1}^{L(n)} \lfloor u + r_v \rfloor - \frac{L(n)}{2}, \end{aligned}$$

in opazujemo člen s spodnjim celim delom. Ker so členi Fareyvega zaporedja razen  $r_{L(n)} = 1$  simetrično razporejeni okrog vrednosti  $\frac{1}{2}$ , lahko zapišemo  $\sum_{v=1}^{L(n)} \lfloor u + r_v \rfloor = \sum_{v=1}^{L(n)} \lfloor u + 1 - r_v \rfloor$ . Za  $u \in [0, 1]$  zavzame  $\lfloor u + 1 - r_v \rfloor$  le celi števili 0 in 1, slednje je le v primeru, ko je  $u = r_v$ . Zato je

$$\sum_{v=1}^{L(n)} \lfloor u + 1 - r_v \rfloor = \begin{cases} 1 & \text{če } u = r_v \\ 0 & \text{sicer} \end{cases},$$

kar pomeni, da ima funkcija  $G$ , evaluirana v elementih Fareyvega zaporedja, skok za  $-1$ . Med Fareyevima sosedoma, torej na intervalu  $[r_{v-1}, r_v]$ , je  $G$  linearna funkcija spremenljivke  $u$  s koeficientom  $L(n)$ . Zaradi simetrije členov Fareyvega zaporedja velja še  $\sum_{v=1}^{L(n)-1} \bar{B}_1(r_v) = 0$ . Od tod izračunamo desno limito funkcije  $G$  v točki 0,

$$\lim_{u \rightarrow 0} G(u) = \lim_{u \rightarrow 0} \bar{B}_1(u + 1) = -\frac{1}{2}.$$

Funkcija  $G$  se na intervalu  $[r_{v-1}, r_v]$  izraža s predpisom

$$G(u) = L(n)u - v - \frac{1}{2}.$$

Izrazimo še

$$L(n)r_v = L(n) \left( r_v - \frac{v}{L(n)} + \frac{v}{L(n)} \right) = L(n)\delta_v + v,$$

$$L(n)r_v - v + \frac{1}{2} = L(n)\delta_v + \frac{1}{2}, \quad L(n)r_{v-1} - v + \frac{1}{2} = L(n)\delta_{v-1} - \frac{1}{2}.$$

Sedaj lahko izračunamo integral

$$\begin{aligned}
I &\stackrel{(1)}{=} \sum_{v=1}^{L(n)} \int_{r_{v-1}}^{r_v} \left( L(n)u - v - \frac{1}{2} + 1 \right)^2 du \\
&= \sum_{v=1}^{L(n)} \frac{(L(n)u - v + \frac{1}{2})^3}{3L(n)} \Big|_{r_{v-1}}^{r_v} \\
&= \frac{1}{3L(n)} \sum_{v=1}^{L(n)} \left( \left( L(n)\delta_v + \frac{1}{2} \right)^3 - \left( L(n)\delta_{v-1} - \frac{1}{2} \right)^3 \right) \\
&\stackrel{(2)}{=} \frac{1}{3L(n)} \sum_{v=1}^{L(n)} \left( \left( L(n)\delta_v + \frac{1}{2} \right)^3 - \left( L(n)\delta_v - \frac{1}{2} \right)^3 \right) \\
&= \frac{1}{3L(n)} \sum_{v=1}^{L(n)} \left( 3(L(n)\delta_v)^2 + \frac{1}{4} \right) \\
&= L(n) \sum_{v=1}^{L(n)} \delta_v^2 + \frac{1}{12L(n)} L(n) \\
(22) \quad &= L(n) \sum_{v=1}^{L(n)} \delta_v^2 + \frac{1}{12}.
\end{aligned}$$

Zaradi privzetka, da je  $r_0 = 0$  in  $r_{L(n)} = 1$ , enakost (1) res drži. V enakosti (2) smo upoštevali, da je  $\delta_{L(n)} = 0$  in  $L(n)\delta_0 - \frac{1}{2} = L(n)\delta_{L(n)} - \frac{1}{2}$ .

2. primer:  $G(u) = \sum_{k=1}^{\infty} \bar{B}_1(ku) M\left(\frac{n}{k}\right)$ . Računajmo integral

$$\begin{aligned}
I &= \int_0^1 \sum_{k=1}^{\infty} \left( \bar{B}_1(ku) M\left(\frac{n}{k}\right) \right)^2 du \\
&= \int_0^1 \sum_{a=1}^{\infty} \sum_{b=1}^{\infty} \bar{B}_1(au) \bar{B}_1(bu) M\left(\frac{n}{a}\right) M\left(\frac{n}{b}\right) du \\
(23) \quad &= \sum_{a=1}^{\infty} \sum_{b=1}^{\infty} M\left(\frac{n}{a}\right) M\left(\frac{n}{b}\right) \int_0^1 \bar{B}_1(au) \bar{B}_1(bu) du
\end{aligned}$$

Označimo  $I_{ab} = \int_0^1 \bar{B}_1(au) \bar{B}_1(bu) du$ . Vrednost integrala bomo izračunali v treh korakih.

Naj bo  $b = 1$ . Tedaj je

$$\begin{aligned}
I_{a1} &= \int_0^1 \bar{B}_1(au) \bar{B}_1(u) du \stackrel{(1)}{=} \frac{1}{a} \int_0^a \bar{B}_1(v) \bar{B}_1\left(\frac{v}{a}\right) dv \\
&\stackrel{(2)}{=} \frac{1}{a} \sum_{k=0}^{a-1} \int_0^1 \bar{B}_1(k+t) \bar{B}_1\left(\frac{k}{a} + \frac{t}{a}\right) dt \\
&\stackrel{(3)}{=} \frac{1}{a} \int_0^1 \bar{B}_1(t) \bar{B}_1\left(\frac{t}{a}\right) dt \stackrel{(4)}{=} \frac{1}{a} \int_0^1 \left(t - \frac{1}{2}\right)^2 dt \\
(24) \quad &= \frac{1}{3a} \left(t - \frac{1}{2}\right)^3 \Big|_0^1 = \frac{1}{12a}.
\end{aligned}$$

V enakostih (1) in (2) smo zaporedoma uvedli novi spremenljivki  $v = au$  in  $v = k+t$ . V enakosti (3) smo upoštevali periodičnost funkcije  $\bar{B}_1$  in zvezo 18. V enakosti (4) smo upoštevali, da na intervalu  $[0, 1]$  velja  $\bar{B}_1(t) = t - \frac{1}{2}$ .

Oglejmo si primer, ko sta  $a$  in  $b$  tuji si števili.

$$\begin{aligned}
 I_{ab} &= \int_0^1 \bar{B}_1(au) \bar{B}_1(bu) du = \frac{1}{a} \int_0^a \bar{B}_1(v) \bar{B}_1\left(\frac{bv}{a}\right) dv \\
 &= \frac{1}{a} \sum_{k=0}^{a-1} \int_0^1 \bar{B}_1(k+t) \bar{B}_1\left(\frac{bk}{a} + \frac{bt}{a}\right) dt \\
 (25) \quad &\stackrel{(5)}{=} \frac{1}{a} \int_0^1 \bar{B}_1(t) \bar{B}_1\left(a \frac{bt}{a}\right) dt = \frac{1}{a} I_{1b} = \frac{1}{12ab}
 \end{aligned}$$

V enakosti (5) smo uporabili dejstvo, da vrednosti  $\frac{bk}{a}$  za  $k \in \{0, 1, \dots, a-1\}$  pretečejo vse vrednosti iz množice  $\{0, \frac{1}{a}, \dots, \frac{a-1}{a}\}$ .

Naj bo sedaj  $c$  največji skupni delitelj  $a$  in  $b$ . Zapišimo  $a = c\alpha$  in  $b = c\beta$  (seveda sta  $\alpha$  in  $\beta$  tuji si števili).

$$\begin{aligned}
 I_{ab} &= \int_0^1 \bar{B}_1(c\alpha u) \bar{B}_1(c\beta u) du \stackrel{(6)}{=} \frac{1}{c} \int_0^c \bar{B}_1(\alpha t) \bar{B}_1(\beta t) dt \\
 (26) \quad &\stackrel{(7)}{=} I_{\alpha\beta} = \frac{1}{12\alpha\beta} = \frac{c^2}{12ab}
 \end{aligned}$$

V enakosti (6) smo uvedli novo spremenljivko  $t = cu$ . Enakost (7) sledi iz računa

$$\begin{aligned}
 \int_k^{k+1} \bar{B}_1(\alpha t) \bar{B}_1(\beta t) dt &= \int_0^1 \bar{B}_1(\alpha s + \alpha k) \bar{B}_1(\beta s + \beta k) ds \\
 &= \int_0^1 \bar{B}_1(\alpha s) \bar{B}_1(\beta s) ds = I_{\alpha\beta}.
 \end{aligned}$$

Izračunano vrednost integrala  $I_{ab}$  vstavimo v enakost 23 in dobimo

$$(27) \quad I = \sum_{a=1}^{\infty} \sum_{b=1}^{\infty} M\left(\frac{n}{a}\right) M\left(\frac{n}{b}\right) \frac{c^2}{12ab}.$$

## 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] H. M. Edwards, *Riemann's zeta function*, Academic Press, Inc., New York, 1974.
- [3] L. R. Ford, *Fractions*, v: The American Mathematical Monthly (ur. E. J. Moulton) **45**, Mathematical Association of America, 1938, str. 586–601.
- [4] S. B. Guthery, *A motif of mathematics*, Docent Press, Boston, 2011; dostopno tudi na <https://www.maths.ed.ac.uk/~v1ranick/papers/farey.pdf>.
- [5] G. H. Hardy in E. M. Wright, *An introduction to the theory of numbers*, 4th ed., Oxford University Press, Oxford, 1960.
- [6] A. Hatcher, *Topology of numbers*, verzija junij 2018, [ogled 31. 10. 2018], dostopno na <https://pi.math.cornell.edu/~hatcher/TN/TNpage.html>.



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