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

V delu je predstavljeno Fareyevo zaporedje, njegova motivacija in lastnosti. Navedena je rekurzivna formula za izračun dolžine zaporedja n-tega reda in njeno asimptotično obnašanje. Izkaže se, da je Fareyevo zaporedje v bijekciji z množico Fordovih krogov. Razložen je geometrijski pomen lastnosti mediante in Fareyevih sosedov ter opisana konstrukcija vseh Fordovih sosedov danega Fordovega kroga. Definirane so Fordove krogle. S pomočjo delovanja grupe Möbiusovih transformacij na množico Fordovih krogov je dokazana lastnost mediante. Predstavljena je Riemannova hipoteza in dve njeni ekvivalentni formulaciji. Dokazan je izrek, ki Fareyevo zaporedje preko Mertensove funkcije poveže z Riemannovo hipotezo.

The Farey Sequence and The Riemann Hypothesis

Abstract

The work presents the Farey sequence, its motivation and properties. A recursive formula for caculating the length of the sequence of order n and its asymptotic behaviour are stated. The Farey sequence is in bijection with the set of Ford circles, therefore a geometric meaning of the mediant and the neighbours property is explained as well as the construction of all Ford neighbours to a given Ford circle. Moreover, Ford spheres are defined. Using the fact that the group of Möbius transformations acts on the set of Ford circles, the mediant property for Ford circles is proved. Additionally, the Riemann hypothesis and two of its equivalent statements are presented. A theorem, connecting the Farey sequence, the Mertens function and the Riemann hypothesis, is proved.

Math. Subj. Class. (2010): 11B57, 11M26, 51N20

Ključne besede: Fareyevo zaporedje, Fordov krog, zeta funkcija, Riemannova hipoteza

Keywords: Farey sequence, Ford circle, zeta function, Riemann hypothesis

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, večjih od 0 in manjših od 1, katerih imenovalec je manjši od 100. Odziv je bil precejšen, saj so se z iskanjem rešitve ukvarjali tako javnost kot pomembni matematiki tiste dobe. To je vodilo v razvoj Fareyevega zaporedja, ki ima nekaj presenetljivih lastnosti in uporabo na različnih področjih matematike.

Delo diplomskega seminarja je sestavljeno iz treh večjih enot. V prvi bomo predstavili zgodovinski pregled, definicijo, lastnosti in ocenili dolžino Fareyevega zaporedja. V drugem razdelku se bomo posvetili njeni geometrijski interpretaciji – Fordovim krogom – in opazili, da imata dve najpomembnejši lastnosti Fareyevega zaporedja tudi geometrijski pomen. Konstruirali bomo vse Fordove sosede danega Fordovega kroga. Navedli bomo možno posplošitev Fordovih krogov in definirali Fordove krogle. Ogledali si bomo predstavitev Fordovih krogov z uporabo algebre in kompleksne analize – dokazali bomo, da grupa Möbiusovih transformacij deluje na množico Fordovih krogov, od koder bo sledila že znana lastnost mediante. V zadnjem delu bomo obravnavali znamenit matematični problem, Riemannovo hipotezo. Predstavili bomo njeno motivacijo in navedli dve ekvivalentni formulaciji te domneve. Dokazali bomo povezavo Riemannove hipoteze s Fareyevim zaporedjem, pred tem pa se bomo seznanili s pojmi kot so Eulerjev produkt, Riemannova zeta funkcija, Bernoullijeva števila in polinomi, ter Möbiusova in Mertensova funkcija.

Vse slike, pri katerih ni naveden vir, so avtorske; izdelane so s pomočjo programov GeoGebra in Octave.

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 manjšimi od 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 bodo pripeljale do rešitve.

Definicija 2.1. Preslikava $\varphi\colon \mathbb{N} \to \mathbb{N}$, ki za vsako naravno število $n \geq 2$ prešteje števila, manjša od n, ki so n tuja, za $n = 1$ pa predpišemo $\varphi(1) = 1$, se imenuje *Eulerjeva funkcija* φ.

Primer 2.2. Izračunajmo nekaj vrednosti Eulerjeve funkcije:
$\varphi(1) = 1$,
$\varphi(2) = 1$,
$\varphi(3) = 2$,
$\varphi(4) = 2$,
$\varphi(8) = 4$,
$\varphi(9) = 6$.
Opazimo, da za praštevilo p velja $\varphi(p) = p - 1$. ♢

Trditev 2.3. *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 2.4. *Vrednost Eulerjeve funkcije je enaka*

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

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 različna praštevila. Vrednost $\varphi(p^r)$ dobimo tako, da preštejemo 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 za ena manj 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 2.5. *Obstajajo* 3003 *racionalna števila $\frac{p}{q}$, za katera velja $0 < \frac{p}{q} < 1$ ter je $q < 100$.*

Namesto formalnega dokaza trditve bomo predstavili Flitconovo rešitev. Sledili bomo [1, poglavje 1.2]. Naredimo tabelo s tremi stolpci in 98 vrsticami. V prvi stolpec vsake vrstice napišemo po eno izmed naravnih števil od 2 do 99. 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 2.3 in 2.4. 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 99 pa število vseh okrajšanih ulomkov med 0 in 1 z imenovalci med 2 in 99.[1]

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

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. Zgodovina je povzeta po [5, poglavje 2].

2.2. **O Fareyevem zaporedju.** Motivacijo za razvoj Fareyevega zaporedja smo si ogledali v prejšnjem razdelku. Sedaj bomo zaporedje korektno definirali in izpeljali njegove lastnosti.

Definicija 2.6. *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 2.7. Poglejmo si Fareyeva zaporedja najnižjih redov:

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

Opomba 2.8. Če pogoj $0 \leq p \leq q \leq n$ v definiciji 2.6 omilimo v pogoj $0 \leq p, q \leq n$, okrajšane ulomke z intervala $[0, 1]$ razširimo na interval $[0, \infty)$. V primeru, ko za števili p in q predpišemo $|p|, |q| \leq n$, 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 2.9. Sosednja člena v Fareyevem zaporedju imenujemo *Fareyeva soseda.*

Definicija 2.10. Naj bosta $\frac{a}{b}$ in $\frac{c}{d}$ sosednja člena nekega Fareyevega zaporedja. Ulomek

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

imenujemo *medianta.*

Trditev 2.11. *Za medianto okrajšanih ulomkov, kjer je* $\frac{a}{b} < \frac{c}{d}$*, 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, ki jo dokazujemo, res velja. □

Kako dobimo člen Fareyevega zaporedja reda $(n+1)$? Označimo iskani okrajšan ulomek s $\frac{k}{n+1}$. Seveda velja $k, n \in \mathbb{N}$ in $k < n+1$ sta 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 celi 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. Opomnimo, da je ulomek $\frac{k-a}{n+1-b}$ pozitiven; iz zadnje enakosti namreč sledi, da sta števec in imenovalec naravni števili. 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 naslednjo lemo.

Lema 2.12. *Dano naj bo Fareyevo zaporedje. Elemente zaporedja višjega reda dobimo z računanjem mediant elementov danega zaporedja.*

Trditev 2.13 (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 zaporedju natanko tedaj, ko velja* $bc - ad = 1$*.*

Dokaz. ($\Rightarrow$) Denimo, da sta ulomka $\frac{a}{b}$ in $\frac{c}{d}$, kjer je $\frac{a}{b} < \frac{c}{d}$, Fareyeva soseda v zaporedju F_n. Trdimo, da velja $bc-ad = 1$. Dokaz bo potekal z indukcijo na red Fareyevega zaporedja, torej na n. Za $n = 1$ je $F_1 = \{\frac{0}{1}, \frac{1}{1}\}$, $bc - ad = 1 \cdot 1 - 0 \cdot 1 = 1$, 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 višjega reda dobimo z računanjem mediant. Če je $b + d > n + 1$, potem ulomek $\frac{a+c}{b+d} \notin F_{n+1}$ in je $F_{n+1} = \{\ldots, \frac{a}{b}, \frac{c}{d}, \ldots\}$ ter po indukcijski predpostavki velja $bc - ad = 1$. Če je $b + d < n + 1$, je $\frac{a+c}{b+d}$ že nek člen v zaporedju F_n; skupaj s trditvijo 2.11 pa prispemo v protislovje s predpostavko, da sta ulomka $\frac{a}{b}$ in $\frac{c}{d}$ Fareyeva soseda. Ta primer se zato ne more zgoditi. Preostane še možnost $b + d = n + 1$. Po lemi 2.12 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 $F_{n+1} = \{\ldots, \frac{a}{b}, \frac{a+c}{b+d}, \frac{c}{d}, \ldots\}$ 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.

($\Leftarrow$) Naj za okrajšana ulomka $\frac{a}{b}$ in $\frac{c}{d}$ velja $bc-ad=1$. Trdimo, da sta ulomka Fareyeva soseda v nekem Fareyevem zaporedju. Denimo, da to ne drži. Naj v vsakem Fareyevem zaporedju obstaja tak ulomek $\frac{p}{q}$, da velja relacija $\frac{a}{b} < \frac{p}{q} < \frac{c}{d}$, kjer število q ustreza $q \leq \max\{b,d\}$. (Če v Fareyevem zaporedju $F_{\max\{b,d\}}$ obstaja ulomek, ki leži med ulomkoma $\frac{a}{b}$ in $\frac{c}{d}$, potem ju bo ta ulomek ločil v vsakem Fareyevem zaporedju višjega reda.) Izračunajmo razliko med ulomkoma $\frac{c}{d}$ in $\frac{a}{b}$. Velja

$$\frac{c}{d} - \frac{a}{b} = \frac{bc-ad}{bd} = \frac{1}{bd}. \tag{2}$$

Sedaj si oglejmo dva primera glede na vrednost števila q in ocenimo razliko med ulomkoma $\frac{p}{q}$ in $\frac{a}{b}$ ter $\frac{c}{d}$ in $\frac{p}{q}$.

Če je $q \leq d$, velja $\frac{p}{q} - \frac{a}{b} = \frac{pb-aq}{qb} \geq \frac{pb-aq}{bd} \geq \frac{1}{bd}$, kar je v protislovju z enakostjo 2.

Če je $q \leq b$, ocenimo $\frac{c}{d} - \frac{p}{q} = \frac{cq-pd}{dq} \geq \frac{cq-pd}{bd} \geq \frac{1}{bd}$, kar je zopet v protislovju z enakostjo 2.

Zato obstaja Fareyevo zaporedje, v katerem noben ulomek ne leži med ulomkoma $\frac{a}{b}$ in $\frac{c}{d}$. Torej sta $\frac{a}{b}$ in $\frac{c}{d}$ res Fareyeva soseda v nekem Fareyevem zaporedju. □

Lema 2.14. *Medianta je okrajšan ulomek.*

Dokaz. Naj za ulomka $\frac{a}{b} < \frac{c}{d}$ velja $bc-ad=1$. Trdimo, da je njuna medianta $\frac{a+c}{b+d}$ 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 števili $a+c$ in $b+d$ nimata skupnega faktorja. Ulomek $\frac{a+c}{b+d}$ je torej okrajšan. □

Opomba 2.15. Medianta $\frac{a+c}{b+d}$ je enolično določena z ulomkoma $\frac{a}{b}$ in $\frac{c}{d}$. To imenujemo *lastnost mediante*.

2.3. **Dolžina Fareyevega zaporedja.** Flitconova metoda za izračun števila okrajšanih ulomkov z imenovalci, manjšimi od danega števila, nas pripelje do naslednje rekurzivne formule, ki podaja dolžino Fareyevega zaporedja.

Trditev 2.16. *Naj bo φ Eulerjeva funkcija. Dolžina Fareyevega zaporedja reda n je enaka*

$$|F_n| = |F_{n-1}| + \varphi(n). \tag{3}$$

Opomba 2.17. Z upoštevanjem vrednosti $|F_1| = 2$ iz trditve 2.16 sledi

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

Trditev 2.18. *Asimptotično se dolžina Fareyevega zaporedja obnaša kot*

$$|F_n| \sim \frac{3n^2}{\pi^2}. \tag{4}$$

Opomba 2.19. Simbol $\sim$ v trditvi 2.18 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 se lotimo dokazovanja zgornje trditve, definirajmo naslednjo oznako in dve funkciji, ki jih bomo v dokazu potrebovali.

Definicija 2.20 (Notacija veliki O)**.** Funkcija f pripada razredu $O(g(x))$, če absolutna vrednost funkcije f ne raste hitreje od funkcije g, pomnožene s konstanto. Natančneje, $f(x) = O(g(x))$, če obstajata konstanta K in vrednost x_0, da za vsak $x \geq x_0$ velja $|f(x)| < K \cdot g(x)$.

Definicija 2.21. Preslikava $\mu\colon \mathbb{N} \to \mathbb{N}$, definirana s predpisom

$$\mu(n) = \begin{cases} 0 & , \text{ če je } n \text{ deljiv s kvadratom praštevila} \\ (-1)^p & , \text{ če je } n \text{ produkt } p \text{ različnih praštevil} \end{cases}, \tag{5}$$

se imenuje *Möbiusova*[2] *funkcija.*

Primer 2.22. 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 2.23. *Riemannova zeta funkcija* je za $s \in \mathbb{C}\backslash\{1\}$ definirana s predpisom

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

Sedaj lahko dokažemo trditev 2.18. Dokaz sledi [6, poglavje 18.5, str. 268].

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

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

kjer so p, p' praštevilski delitelji števila n. Z upoštevanjem Möbiusove funkcije je zgornji izraz enak

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

[2] August Ferdinand Möbius, 17. 11. 1790–26. 9. 1868, nemški matematik in astronom. Po njem se med drugim imenujejo Möbiusov trak, Möbiusova transformacija in Möbisuova funkcija.

Sedaj računajmo vsoto

$$\begin{aligned}
\sum_{i=1}^{n}\varphi(i) &= \sum_{i=1}^{n} i\sum_{d|i}\frac{\mu(d)}{d} = \sum_{dd'\le n} d'\mu(d) = \sum_{d=1}^{n}\mu(d)\sum_{d'=1}^{\left\lfloor\frac{n}{d}\right\rfloor} d' \\
&= \frac{1}{2}\sum_{d=1}^{n}\mu(d)\left(\left\lfloor\frac{n}{d}\right\rfloor^2 + \left\lfloor\frac{n}{d}\right\rfloor\right) = \frac{1}{2}\sum_{d=1}^{n}\mu(d)\left(\frac{n^2}{d^2} + O\left(\frac{n}{d}\right)\right) \\
&= \frac{1}{2}n^2\sum_{d=1}^{n}\frac{\mu(d)}{d^2} + O\left(n\sum_{d=1}^{n}\frac{1}{d}\right) \\
&\overset{(1)}{=} \frac{1}{2}n^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} - \frac{1}{2}n^2\sum_{d=n+1}^{\infty}\frac{\mu(d)}{d^2} + O(n\ln n) \\
&= \frac{1}{2}n^2\sum_{d=1}^{\infty}\frac{\mu(d)}{d^2} + O\left(n^2\sum_{d=n+1}^{\infty}\frac{1}{d^2}\right) + O(n\ln n) \\
&\overset{(2)}{=} \frac{n^2}{2\zeta(2)} + O(n) + O(n\ln n) \overset{(3)}{=} \frac{3n^2}{\pi^2} + O(n\ln n). \qquad (7)
\end{aligned}$$

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

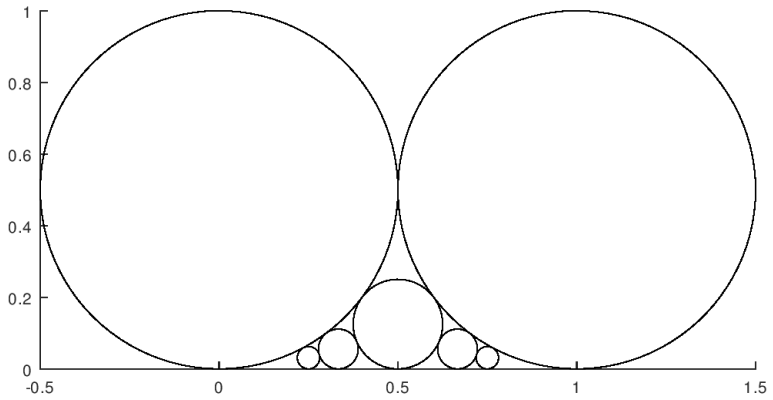
$$\zeta(2) = \sum_{n=1}^{\infty}\frac{1}{n^2} = \frac{\pi^2}{6}.$$

Po opombi 2.17 iz izraza (7) sledi, da je $|F_n| = \frac{3n^2}{\pi^2} + O(n\ln n) \sim \frac{3n^2}{\pi^2}$. □

3. Fordovi krogi

V tem poglavju bomo obravnavali Fordove kroge, ki so tesno povezani s Fareyevim zaporedjem. Večino lastnosti bomo dokazali z uporabo elementarnih geometrijskih sredstev in v analognih trditvah tistim iz prejšnjega poglavja prepoznali geometrijski pomen. Na kratko si bomo ogledali posplošitve Fordovih krogov ter Fordove krogle – Fordove kroge v treh dimenzijah. V zadnjem razdelku bomo Fordove kroge predstavili v kompleksni ravnini in z algebraičnim znanjem na drugačen način dokazali eno od lastnosti. Ideje poglavja so povzete po [1, poglavje 4] in[3].

Definicija 3.1. Naj bosta p in q tuji si števili v množici celih števil. *Fordov*[3] *krog* $\mathrm{C}(\frac{p}{q})$ je krog v zgornji polravnini, ki se abscisne osi dotika v točki $\frac{p}{q}$, njegov polmer pa meri $\frac{1}{2q^2}$.



SLIKA 1. Fordovi krogi na intervalu $[0,1]$ s polmeri $\frac{1}{2}$, $\frac{1}{8}$, $\frac{1}{18}$ in $\frac{1}{32}$.

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 periodično razširimo na celotno realno os. V nadaljevanju bomo s pojmom množica Fordovih krogov označevali množico Fordovih krogov z dotikališči na intervalu $[0,1]$.

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

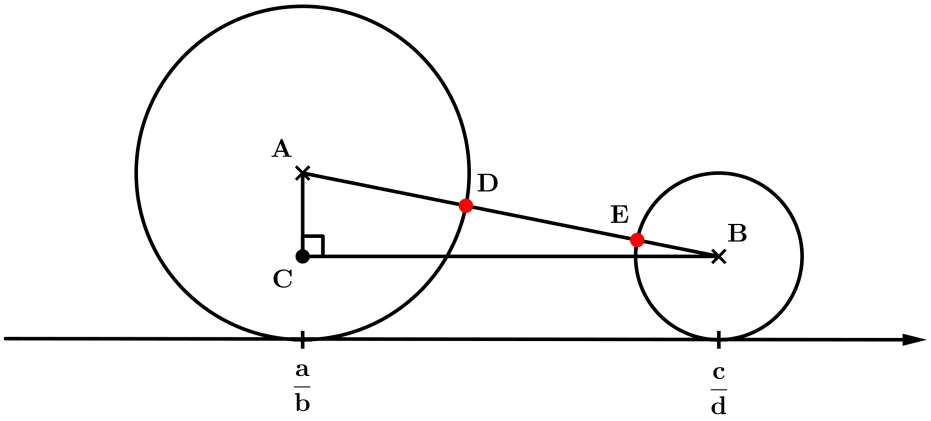
Oglejmo si konstrukcijo pravokotnega trikotnika, določenega s parom Fordovih krogov, ki bo ključna pri dokazovanju trditev v tem poglavju. Izberimo okrajšana ulomka $\frac{a}{b}$ in $\frac{c}{d}$, ter jima priredimo ustrezna Fordova kroga. Naj bosta A središče Fordovega kroga $\mathrm{C}(\frac{a}{b})$ in B središče Fordovega kroga $\mathrm{C}(\frac{c}{d})$. Če je $b < d$, kar pomeni, da je polmer kroga $\mathrm{C}(\frac{a}{b})$ večji od polmera kroga $\mathrm{C}(\frac{c}{d})$, 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. Primer, ko velja $b = d$, nam da izrojen trikotnik, zato ga izpustimo. Povežimo središči obeh krogov. Točki D in E naj bosta presečišči daljice AB s Fordovima krogoma $\mathrm{C}(\frac{a}{b})$ in $\mathrm{C}(\frac{c}{d})$.

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

$$|AB|^2 = |AC|^2 + |BC|^2. \tag{8}$$

Opomba 3.3. Enačba 8 je neodvisna od relacije med polmeroma Fordovih krogov; velja tako v primeru, ko je $b > d$, kot za $b < d$.

[3]Lester Randolph Ford Sr., 25. 10. 1886–11. 11. 1967, ameriški matematik.



SLIKA 2. Konstrukcija pravokotnega trikotnika, ki pripada paru Fordovih krogov. Slika prikazuje primer, ko je $b < d$.

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 iz enačbe (8). Dolžine stranic trikotnika izrazimo z a, b, c in d, kar nam da enakost

$$\begin{aligned} |AB|^2 &= \left(\left|\frac{1}{2b^2} - \frac{1}{2d^2}\right|\right)^2 + \left(\left|\frac{c}{d} - \frac{a}{b}\right|\right)^2 \\ &= \frac{1}{4b^4} - \frac{1}{2b^2d^2} + \frac{1}{4d^4} + \left(\frac{bc-ad}{bd}\right)^2 \\ &= \left(\frac{1}{2b^2} + \frac{1}{2d^2}\right)^2 - \frac{1}{b^2d^2} + \frac{(bc-ad)^2}{b^2d^2} \\ &= (|AD| + |EB|)^2 + \frac{(bc-ad)^2 - 1}{b^2d^2}. \end{aligned} \tag{9}$$

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

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

3.1. **Fordovi sosedi.** V poglavju o Fareyevem zaporedju smo dokazali lastnosti mediante in Fareyevih sosedov. Izkaže se, da imata ti dve lastnosti geometrijski pomen. Pokazali bomo namreč, da veljata tudi za tangentne Fordove kroge. V nadaljevanju bomo konstruirali vse tangentne Fordove kroge danega kroga in si ogledali še eno lastnost paroma tangentnih Fordovih krogov.

Trditev 3.5 (Lastnost Fordovih sosedov)**.** *Fordova kroga $C(\frac{a}{b})$ in $C(\frac{c}{d})$ sta tangentna 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 novo enakost poenostavimo. Dobimo

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

kar smo želeli pokazati. □

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

Trditev 3.7 (Lastnost mediante 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 tangenten 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 pripadajočih Fordovih krogov Fareyeva soseda v nekem Fareyevem zaporedju (razširjenem na celotno realno os). Po lemi 2.14 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 Fordov krog $C(\frac{a+c}{b+d})$ 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. □

Naslednji izrek pove, kako konstruiramo množico vseh Fordovih sosedov danega Fordovega kroga. Izrek in dokaz sledita [3, poglavje 2, Theorem 3, str. 588–589].

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 $C(\frac{P_n}{Q_n})$ 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, saj sta $C(\frac{p}{q})$ in $C(\frac{P}{Q})$ Fordova soseda.

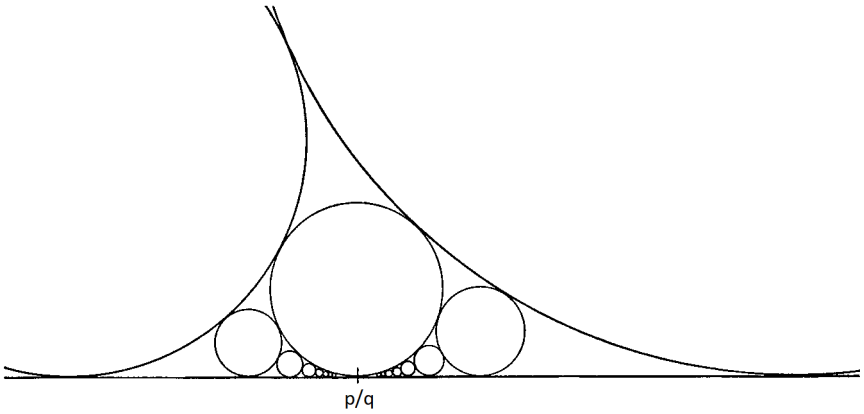
Sedaj preverimo, če obstajajo še Fordovi sosedi, ki niso zgornje oblike. Opazovali bomo množico Fordovih krogov $\mathcal{M} = \{\mathrm{C}(\frac{P_n}{Q_n}); n \in \mathbb{Z}\}$. Iz računa

$$\begin{aligned} |Q_nP_{n+1} - P_nQ_{n+1}| &= |(Q+nq)(P+(n+1)p) - (P+np)(Q+(n+1)q)| \\ &= |QP + (n+1)Qp + nPq + n(n+1)pq \\ &\quad - PQ - (n+1)Pq - npQ - n(n+1)pq| \\ &= |Qp - Pq| \\ &= 1 \end{aligned} \tag{10}$$

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

$$\begin{aligned} \frac{P_n}{Q_n} &= \frac{P+np}{Q+nq} = \frac{Pq+npq}{q(Q+nq)} = \frac{Pq+npq+pQ-pQ}{q(Q+nq)} \\ &= \frac{p(Q+nq)+(Pq-pQ)}{q(Q+nq)} = \frac{p}{q} + \frac{Pq-pQ}{q(Q+nq)} \\ &= \frac{p}{q} \pm \frac{1}{q(Q+nq)} = \frac{p}{q} \pm \frac{1}{q^2\left(n+\frac{Q}{q}\right)}. \end{aligned} \tag{11}$$

V limiti, ko gre n preko vseh meja, gre $\frac{P_n}{Q_n}$ proti $\frac{p}{q}$. Opazimo, da Fordovi krogi oblike



SLIKA 3. Fordov krog $\mathrm{C}(\frac{p}{q})$ in nanj tangentni Fordovi krogi iz množice $\mathcal{M}$. Vir slike je [3, poglavje 2, Figure 2, str. 589].

$\mathrm{C}(\frac{P_n}{Q_n})$ geometrijsko tvorijo "obroč" okoli Fordovega kroga $\mathrm{C}(\frac{p}{q})$. 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 $\mathrm{C}(\frac{p}{q})$, zaradi medsebojne tangentnosti pa so njihovi polmeri vse manjši. Zato ne obstaja Fordov krog, tangenten na $\mathrm{C}(\frac{p}{q})$, ki ni zgornje oblike in ne seka katerega izmed krogov iz zaporedja $\mathcal{M}$. □

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*[4]. 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 $\mathrm{C}(\frac{a}{b})$ 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 $b < d$ in $b' < d'$. Naj prvemu paru Fordovih sosedov pripada pravokotni trikotnik ABC, drugemu paru pa pravokotni trikotnik $A'B'C'$. Trdimo, 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 naslednje zveze:

$$\frac{1}{2b^2} - \frac{1}{2d^2} = \lambda \left(\frac{1}{2b'^2} - \frac{1}{2d'^2} \right), \tag{12}$$

$$\frac{1}{2b^2} + \frac{1}{2d^2} = \lambda \left(\frac{1}{2b'^2} + \frac{1}{2d'^2} \right), \tag{13}$$

$$\frac{c}{d} - \frac{a}{b} = \lambda \left(\frac{c'}{d'} - \frac{a'}{b'} \right). \tag{14}$$

Če seštejemo enačbi (12) in (13), dobimo

$$\begin{aligned} \frac{1}{b^2} &= \lambda \frac{1}{b'^2}, \\ b'^2 &= \lambda b^2, \\ b' &= \sqrt{\lambda} b. \end{aligned} \tag{15}$$

Enačbo (14) lahko poenostavimo, saj gre za para Fordovih sosedov. Velja

$$\pm \frac{1}{bd} = \frac{bc - ad}{bd} = \frac{c}{d} - \frac{a}{b} = \lambda \left(\frac{c'}{d'} - \frac{a'}{b'} \right) = \lambda \frac{b'c' - a'd'}{b'd'} = \pm \lambda \frac{1}{b'd'}. \tag{16}$$

Oba predznaka sta enaka. Iz enakosti (15) in (16) sledi

$$\begin{aligned} \frac{1}{bd} &= \lambda \frac{1}{\sqrt{\lambda} b d'}, \\ \frac{1}{d} &= \frac{\sqrt{\lambda}}{d'}, \\ d' &= \sqrt{\lambda} d. \end{aligned} \tag{17}$$

Nazadnje še v pogoj za tangentnost krogov $\mathrm{C}(\frac{a'}{b'})$ in $\mathrm{C}(\frac{c'}{d'})$ vstavimo zvezi (15) in (17), kar nam da

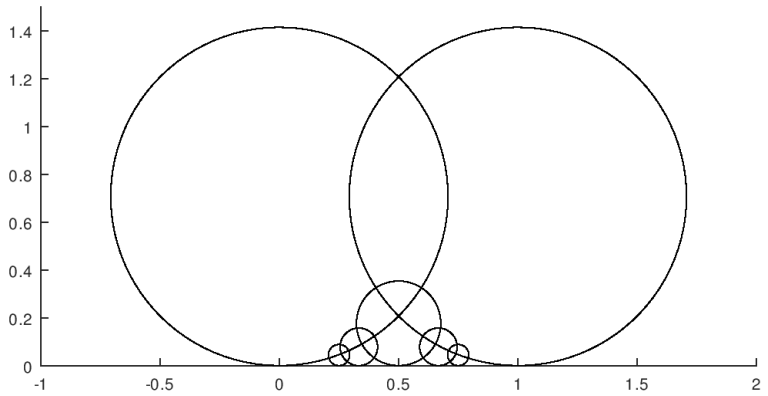
$$\begin{aligned} |b'c' - a'd'| &= 1, \\ |\sqrt{\lambda} b c' - a' \sqrt{\lambda} d| &= 1, \\ \sqrt{\lambda} |bc' - a'd| &= 1. \end{aligned} \tag{18}$$

[4]Pojem pitagorejska trojica nosi ime starogrškega matematika Pitagore (okoli 570 pr. n. št.–495 pr. n. št.), ki ga poznamo predvsem po Pitagorovem izreku.

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 naravna števila, že določajo primitivno pitagorejsko trojico. Če imajo ta naravna 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. □

Opomba 3.11. Enoličnost pitagorejskih trojic je določena do simetrij Fordovih krogov natančno. Fordovi krogi so namreč tako kot Fareyevo zaporedje simetrični okoli vrednosti $\frac{1}{2}$.

3.2. **Posplošeni Fordovi krogi.** Do sedaj smo se ukvarjali s Fordovimi krogi, ki so enolično določeni z racionalnim številom. Natančneje, danemu okrajšanemu ulomku $\frac{p}{q}$ smo priredili 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[5] krogi. Če izberemo $h = 1$, dobimo običajne Fordove kroge. Posplošeni Fordovi krogi so povezani z geometrijo modularnih grup in teorijo kvadratnih form.



SLIKA 4. Posplošeni Fordovi krogi, kjer je $h = \sqrt{2}/2$. Sosednji posplošeni Fordovi krogi niso tangentni, pač pa se sekajo.

3.3. **Fordove krogle.** V tem razdelku bomo sledili [3, poglavje 8]. 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

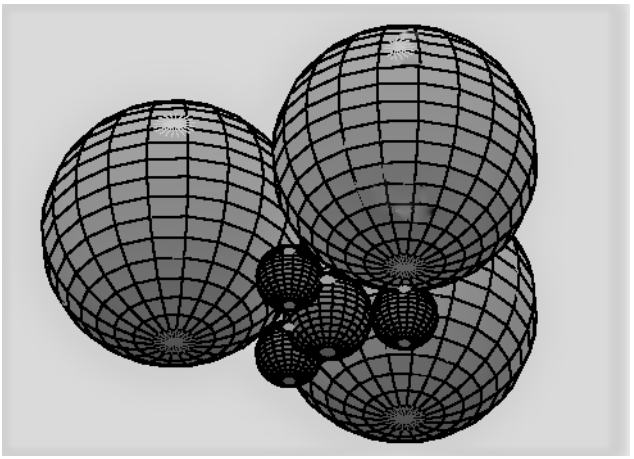
$$\frac{p}{q} = \frac{p' + ip''}{q' + iq''} = \frac{(p' + ip'')(q' - iq'')}{(q' + iq'')(q' - iq'')} = \frac{p'q' + p''q''}{q'^2 + q''^2} + i\frac{p''q' - p'q''}{q'^2 + q''^2}, \tag{19}$$

ki pripada kompleksnim številom, ter okrajšajmo posebej njegov realni in imaginarni del. Geometrijsko predstavlja točko v Gaussovi xy-ravnini z realno in imaginarno komponento. Gaussovo ravnino postavimo v prostor, določen z osjo z, pravokotno

[5]Andreas Speiser, 10. 6. 1885–12. 10. 1970, švicarski matematik, ki se je ukvarjal s teorijo števil in teorijo grup.

na Gaussovo ravnino, in opazujmo podprostor, ki pripada pozitivnim vrednostim na z-osi. Analogno Fordovim krogom v ravnini pridemo do naslednjega pojma.

Definicija 3.12. *Fordova krogla* $\mathrm{S}(\frac{p}{q})$, 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 $\frac{1}{2|q|^2}$.



Slika 5. Fordove krogle.

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 krogli 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 krogli sta disjunktni; sicer je $|Pq - pQ| = 1$, zato je $|AB| = |AD| + |EB|$ in krogli sta tangentni.

Naj bosta $\mathrm{S}(\frac{p}{q})$ in $\mathrm{S}(\frac{P}{Q})$ tangentni Fordovi krogli. Kot prej vse tangentne Fordove krogle na dano kroglo $\mathrm{S}(\frac{p}{q})$ pripadajo vrednostim

$$\frac{P_n}{Q_n} = \frac{P + np}{Q + nq}, \tag{20}$$

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

$$\begin{aligned} |P_nQ_m - P_mQ_n| &= |(P + np)(Q + mq) - (P + mp)(Q + nq)| \\ &= |PQ + mPq + npQ + mnpq - PQ - nPq - mpQ - mnpq| \\ &= |Pq - pQ||m - n| = 1. \end{aligned} \tag{21}$$

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, ki so tangentne na obe.

3.4. **Möbiusove transformacije na Fordovih krogih.** Zaenkrat smo Fordove kroge obravnavali s pomočjo geometrijskih sredstev. V tem razdelku 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 $z = x + iy$, pri čemer sta $x, y, \in \mathbb{R}$.

Najprej se spomnimo naslednjega pojma iz kompleksne analize.

Definicija 3.13. Preslikava $f\colon \mathbb{CP}^1 \to \mathbb{CP}^1$, 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 3.14. 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 3.15. Števila a, b, c, d lahko pomnožimo s poljubnim neničelnim kompleksnim številom, zato brez škode za splošnost 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 torej 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 kot elemente splošne linearne grupe $SL_2(\mathbb{Z})$.

Pri izpeljavi rezultatov o Fordovih krogih je ključen pojem, ki ga v algebri pogosto uporabljamo.

Definicija 3.16. *Delovanje grupe* G na množico M je taka preslikava $\circ\colon G \times M \to M$, 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 3.17. Naj bo G grupa permutacij n elementov, torej $G = S_n$, za množico M pa izberimo $M = \{1, 2, \ldots, n\}$. Delovanje grupe G na množico M je preslikava $\circ\colon G \times M \to M$ s predpisom $(\pi, \alpha) \mapsto \pi(\alpha) = \pi \circ \alpha$. ♢

Definicija 3.18. Fordov krog $\mathrm{C}(\frac{1}{0})$, katerega polmer je neskončen, je premica $\mathbb{R} + i$.

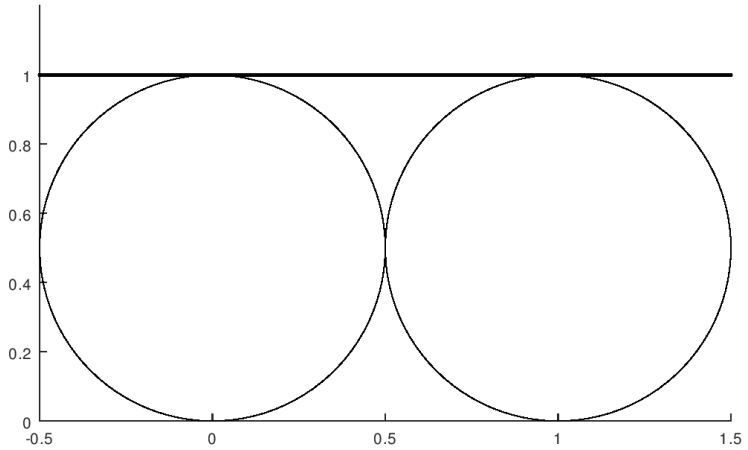
V nadaljevanju tega razdelka bomo s pojmom množica Fordovih krogov označevali Fordove kroge na celotni realni osi vključno s krogom $\mathrm{C}(\frac{1}{0})$.

Izrek 3.19. *Möbiusova transformacija $A \in SL_2(\mathbb{Z})$ 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.



SLIKA 6. Fordovi krogi $\mathrm{C}(\frac{1}{0})$, $\mathrm{C}(\frac{0}{1})$ in $\mathrm{C}(\frac{1}{1})$ v kompleksni ravnini se dotikajo v točkah i, $1+i$ in $\frac{1}{2}+\frac{1}{2}i$.

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 zgornjima generatorjema. Trdimo, da Möbiusova transformacija preslika Fordov krog v Fordov krog.

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 α, predstavljen z enačbo $|z-\alpha| = r$. Prepišimo enačbo v

$$\begin{aligned} (z-\alpha)(\bar{z}-\bar{\alpha}) &= r^2, \\ z\bar{z} - \alpha\bar{z} - \bar{\alpha}z + \alpha\bar{\alpha} - r^2 &= 0 \end{aligned} \tag{22}$$

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

$$\begin{aligned} \left(-\frac{1}{z}\right)\left(-\frac{1}{\bar{z}}\right) + \alpha\frac{1}{\bar{z}} + \bar{\alpha}\frac{1}{z} + R &= 0, \\ 1 + \alpha z + \bar{\alpha}\bar{z} + Rz\bar{z} &= 0, \\ z\bar{z} + \frac{\bar{\alpha}}{R}\bar{z} + \frac{\alpha}{R}z + \frac{1}{R} &= 0. \end{aligned} \tag{23}$$

Sedaj vzemimo Fordov krog $\mathrm{C}(\frac{p}{q})$, za katerega velja $p, q \neq 0$. 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 prav tako Fordov krog. Res, središče slike je po enačbi (23) v točki

$$-\frac{\bar{\alpha}}{R} = -\frac{\frac{p}{q} - i\frac{1}{2q^2}}{\frac{p^2}{q^2}} = -\frac{q}{p} + i\frac{1}{2p^2}, \tag{24}$$

polmer pa meri

$$\sqrt{\left|-\frac{\bar{\alpha}}{R}\right|^2 - \frac{1}{R}} = \sqrt{\frac{\bar{\alpha}}{R}\frac{\alpha}{R} - \frac{1}{R}} = \frac{1}{R}\sqrt{|\alpha|^2 - R} = \frac{1}{R}\frac{1}{2q^2} = \frac{q^2}{2p^2q^2} = \frac{1}{2p^2}. \tag{25}$$

Sliki Fordovih krogov $\mathrm{C}(\frac{0}{1})$ in $\mathrm{C}(\frac{1}{0})$ bomo obravnavali posebej. Preslikava $z \mapsto -\frac{1}{z}$ je Möbiusova transformacija, ki slika premice in krožnice v premice in krožnice, krožnica pa je natanko določena s tremi točkami. Zato v našem primeru zadostuje poznati slike treh točk na Fordovem krogu. Izberimo točke 0, i in $\frac{1}{2} + \frac{1}{2}i$, ki ležijo na Fordovem krogu $\mathrm{C}(\frac{0}{1})$. Preslikajo se v točke $-\infty$, i in $-1+i$; te ležijo na premici $\{x + i; x \in \mathbb{R}\}$, to je Fordovem krogu $\mathrm{C}(\frac{1}{0})$. Zato je slika kroga $\mathrm{C}(\frac{0}{1})$ Fordov krog $\mathrm{C}(\frac{1}{0})$. Ker je preslikava bijekcija, se Fordov krog $\mathrm{C}(\frac{1}{0})$ preslika v $\mathrm{C}(\frac{0}{1})$.

Dokazali smo, da preslikavi, ki generirata grupo Möbiusovih transformacij, Fordov krog preslikata v Fordov krog. Ker identiteta slika Fordov krog vase in je kompozitum Möbiusovih transformacij dobro definiran, grupa $SL_2(\mathbb{Z})$ res deluje na množico Fordovih krogov. □

Lema 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 $|eh - fg|$.*

Dokaz. Kot v definiciji 3.13 zapišimo Möbiusovo transformacijo v obliki $m(z) = \frac{az+c}{bz+d}$, kjer so $a, b, c, d \in \mathbb{Z}$ in velja $ad - bc = 1$. Vzemimo Fordova kroga $\mathrm{C}(\frac{e}{f})$ in $\mathrm{C}(\frac{g}{h})$, ter poglejmo, kam se preslikata. Ker velja izrek 3.19 in je Fordov krog enolično določen s točko, v kateri se dotika realne osi v kompleksni ravnini, je dovolj poznati sliko te točke. Izračunajmo

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

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

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

zato se $\mathrm{C}(\frac{g}{h})$ preslika v $\mathrm{C}(\frac{ag+ch}{bg+dh})$. 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. □

Iz zgornjega neposredno sledi naslednja ugotovitev.

Posledica 3.21. *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 mediante za Fordove kroge*.

Dokaz lastnosti mediante za Fordove kroge z Möbiusovimi transformacijami. Kroga $\mathrm{C}(\frac{r}{s})$ in $\mathrm{C}(\frac{p}{q})$ naj bosta Fordova soseda. Naj bo Fordov krog $\mathrm{C}(\frac{k}{l})$ tangenten na oba. Trdimo, da je $\mathrm{C}(\frac{k}{l})$ medianta Fordovih krogov $\mathrm{C}(\frac{r}{s})$ in $\mathrm{C}(\frac{p}{q})$, torej je enak $\mathrm{C}(\frac{r+p}{s+q})$.

Vzemimo točke v dotikališčih Fordovih krogov $\mathrm{C}(\frac{r}{s})$, $\mathrm{C}(\frac{p}{q})$ in $\mathrm{C}(\frac{k}{l})$. Vemo, da za točke α, β, γ obstaja Möbiusova transformacija, ki jih preslika v poljubne točke λ, μ, ν. Torej obstaja Möbiusova transformacija M, ki izbrane točke v dotikališčih 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 sliki dveh točk na vsakem izmed krogov $\mathrm{C}(\frac{r}{s})$, $\mathrm{C}(\frac{p}{q})$ in $\mathrm{C}(\frac{k}{l})$, poznamo slike vseh treh Fordovih krogov. Te pa so točno $\mathrm{C}(\frac{1}{0})$, $\mathrm{C}(\frac{0}{1})$ in $\mathrm{C}(\frac{1}{1})$.

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

Vse zgornje preslikave so Möbiusove transformacije, ki ohranjajo medianto Fordovih krogov (saj velja posledica 3.21 ter je $\mathrm{C}(\frac{1}{1})$ medianta $\mathrm{C}(\frac{1}{0})$ in $\mathrm{C}(\frac{0}{1})$), zato tudi kompozitum $M_4 \circ M_3 \circ M_2 \circ M_1$ ohranja medianto. Sledi, da je naš kandidat $\mathrm{C}(\frac{k}{l})$ res medianta Fordovih krogov $\mathrm{C}(\frac{r}{s})$ in $\mathrm{C}(\frac{p}{q})$. Z drugimi besedami, za poljubna Fordova soseda obstaja enolično določen Fordov krog, ki je tangenten na oba. □

4. Riemannova hipoteza

Riemannova hipoteza, znana tudi kot 8. Hilbertov problem[6], je eno najbolj slavnih, še vedno nerešenih matematičnih vprašanj. Ime je dobila po nemškem matematiku Bernhardu Riemannu (17. 9. 1826–20. 7. 1866), ki jo je formuliral med preučevanjem lastnosti velikih praštevil. Domnevo je leta 1859 zapisal v članku *Über die Anzahl der Primzahlen unter einer gegebenen Grösse*. Na le osmih straneh je postavil temelje teorije, s katero se matematiki ukvarjajo vse od takrat in ima pomembne aplikacije na raznovrstnih področjih.

Riemann je izhajal iz Eulerjeve trditve, da vsota obratnih vrednosti praštevil divergira. Od tod je sklepal, da so praštevila gostejša podmnožica množice celih števil kot kvadrati celih števil (vedel je, da vrsta $\sum_{n=1}^{\infty} \frac{1}{n^2}$ konvergira). Vendar Euler in Riemann nista bila edina, ki so ju zanimala praštevila. Gauss je v 90-ih letih 18. stoletja na podlagi tabelaričnih izračunov domneval, da gostost praštevil lahko približno ocenimo s funkcijo $1/\log x$. Nekaj let za njim je Legendre na isto vprašanje odgovoril z oceno $1/(a\log x + b)$, konstanti a in b pa empirično določil. Funkcijo, ki šteje praštevila, manjša od danega števila, označimo s π. *Izrek o praštevilih* trdi, da

[6]Nemški matematik David Hilbert je l. 1900 objavil seznam 23 nerešenih matematičnih problemov, za katere je menil, da bodo pomembno vplivali na razvoj matematike 20. stoletja.

velja

$$\pi(x) \sim \frac{x}{\log x}. \tag{26}$$

Relativno napako med $\int_2^x \frac{dt}{\log t}$ in $\pi(x)$ je v sredini 19. stoletja izračunal Čebišev, šele nekaj desetletij kasneje pa so Hadamard, von Mangoldt in de la Vallée Poussin dokazali izrek o praštevilih in nekaj sorodnih trditev. Zdi se, da nas vse vodijo k Riemannovi domnevi, ob kateri je avtor zapisal, da se mu zdi precej verjetno, da je pravilna, vendar dokaza zanjo ne pozna. Sledila je vrsta neuspešnih dokazov v prid hipotezi, ki vključujejo različna področja matematike, v želji po rešitvi problema pa je nastalo tudi več ekvivalentnih formulacij hipoteze. Čeprav večina matematikov Riemannu pritrjuje, obstajajo študije, ki razlagajo argumente proti njeni pravilnosti. Zgodovina je povzeta po [2, poglavje 1.1].

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

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

Dokazov tega fundamentalnega izreka je veliko, velja pa omeniti Evklidovo idejo dokazovanja s protislovjem, ki jo pogosto uporabljamo še danes. Denimo, da izrek ne velja. Potem so $p_1, p_2, \ldots, p_s$ edina praštevila in p_s je največje. Označimo $N = p_1 p_2 \cdots p_s + 1$. Naravno število N je deljivo z nekim praštevilom (saj je večje od 1), recimo s praštevilom p_j, $1 \leq j \leq s$. Potem za $m \in \mathbb{N}$ velja $p_j m = p_1 p_2 \cdots p_s + 1$, od koder sledi $p_j(m - p_1 \cdots p_{j-1} p_{j+1} \cdots p_s) = 1$. Ker je $p_j > 1$, smo prispeli do protislovja. Zato je praštevil res neskončno mnogo.

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

$$\begin{aligned} \zeta &\colon \mathbb{R} \to \mathbb{R}, \\ \zeta(n) &= \sum_{r=1}^{\infty} \frac{1}{r^n}. \end{aligned} \tag{27}$$

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

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

$$\sum_n \frac{1}{n^s} = \prod_p \frac{1}{1 - p^{-s}}. \tag{28}$$

Dokaz. Zapišimo predpis za zeta funkcijo. V naslednjem koraku jo 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. Dobimo

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

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

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

od koder lahko izrazimo

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

kar smo želeli pokazati. □

V dokazu smo sledili Eulerju in [9].

V 19. stoletju so začeli računati s kompleksnimi števili, tako je Riemann leta 1859 razširil Eulerjevo definicijo zeta funkcije. Riemannova zeta funkcija množico $\mathbb{C}\backslash\{1\}$ preslika na množico $\mathbb{C}$, njen predpis pa podaja definicija 2.23.

Opomba 4.3. V izreku 4.2 nismo povedali, kateri množici pripada spremenljivka s. Euler je zvezo namreč formuliral za celoštevilske s, Riemann pa je z razširitvijo funkcije zeta dokazal, da enakost velja za vse s, ki ustrezajo neenakosti $\mathrm{Re}(s)>1$.

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

Kako je z ničlami na polravnini $\{s;\mathrm{Re}(s)<0\}$? Pomagali si bomo z Bernoullijevimi števili [8, poglavje 3]. Naj bo $|z|<2\pi$. *Bernoullijeva*[7] *števila* B_k definiramo preko funkcije

$$G(z)=\frac{z}{e^z-1}=\sum_{k=0}^{\infty}B_k\frac{z^k}{k!}. \tag{29}$$

Najprej za občutek izračunajmo prvih nekaj Bernoullijevih števil. Funkcijo G lahko razvijemo v Taylorjevo vrsto okoli ničle in dobimo

$$G(z)=\left(1+\frac{z}{2!}+\frac{z^2}{3!}+\frac{z^3}{4!}+\cdots\right)^{-1}.$$

[7]Jacob Bernoulli, 27. 12. 1654–16. 8. 1705, rojen v družini znamenitih švicarskih matematikov. Med drugim mu pripisujemo odkritje konstante e.

Iščemo potenčno vrsto $p(z) = a_0 + a_1 z + a_2 z^2 + a_3 z^3 + \cdots$, za katero bo veljalo

$$\left(1 + \frac{z}{2!} + \frac{z^2}{3!} + \frac{z^3}{4!} + \cdots\right) p(z) = 1.$$

Z rekurzivnim računanjem koeficientov pri potencah z dobimo koeficiente potenčne vrste p: $a_0 = 1$, $a_1 = -\frac{1}{2}$, $a_2 = \frac{1}{12}$, $a_3 = 0$, $a_4 = -\frac{1}{720}$, ... Od tod preberemo prvih nekaj Bernoullijevih števil: $B_0 = 1$, $B_1 = -\frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, $B_4 = -\frac{1}{30}$. Več o njih nam pove naslednja lema.

Lema 4.4. *Naj bo $k \in \mathbb{N}$. Za Bernoullijeva števila velja $B_{2k+1} = 0$.*

Dokaz. Spomnimo se funkcije G, definirane v enakosti (29). Oglejmo si novo funkcijo, podano s predpisom $z \mapsto G(z) + \frac{z}{2}$, in jo nekoliko preoblikujmo:

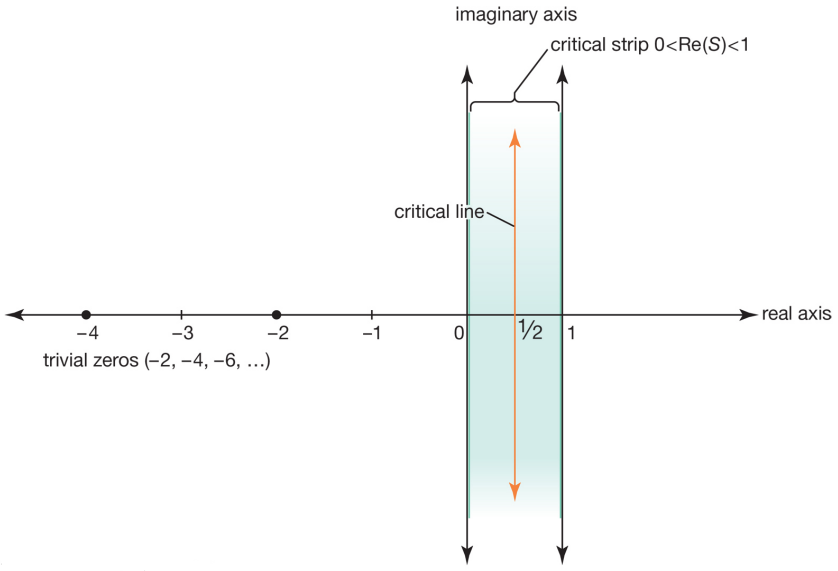
$$G(z) + \frac{z}{2} = \frac{z}{2}\left(\frac{2}{e^z - 1} + 1\right) = \frac{z}{2}\frac{e^z + 1}{e^z - 1} = \frac{z}{2}\frac{e^{z/2} + e^{-z/2}}{e^{z/2} - e^{-z/2}} = \frac{z}{2}\coth\frac{z}{2}. \tag{30}$$

Zapisali smo jo kot produkt dveh lihih funkcij, kar je soda funkcija. Upoštevamo, da je $B_1 = -\frac{1}{2}$. Oboje skupaj nam pove, da so koeficienti funkcije G pri lihih potencah stopnje vsaj 3 enaki 0, s tem pa vsa števila B_{2k+1} za $k \geq 1$. □

Tudi za Bernoullijeva števila oblike B_{2k} obstaja formula, ki pa ni preprosta. Za nas so pomembna tista z lihimi indeksi, saj so povezana z Riemannovo zeta funkcijo, ki je podrobno obravnavana v [2, poglavje 1.5]. Mi bomo navedli le rezultat. Naj bo $n \in \{0, 1, 2, \dots\}$. Potem velja

$$\zeta(-n) = (-1)^n \frac{B_{n+1}}{n+1}. \tag{31}$$

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 zeta funkcije. Ostal je še pas $\{s; 0 < \mathrm{Re}(s) < 1\}$, o ničlah na njem pa govori naslednji izrek.



Slika 7. Netrivialne ničle Riemannove zeta funkcije ležijo na pasu $\{s; 0 < \mathrm{Re}(s) < 1\}$. Vir slike je [7].

Izrek 4.5 (Riemannova hipoteza)**.** *Vse netrivialne ničle Riemannove zeta funkcije ležijo na premici* $s = \{\frac{1}{2} + it; t \in \mathbb{R}\}$.

4.2. **Ekvivalentne trditve.** Obstaja več ekvivalentnih formulacij Riemannove hipoteze. Dokazali bomo eno izmed njih, ki vključuje Fareyevo zaporedje. Pred tem se spomnimo Möbiusove funkcije μ – srečali smo jo v definiciji 2.21. Z njo je povezana naslednja funkcija.

Definicija 4.6. Preslikava $M\colon \mathbb{N} \to \mathbb{N}$, definirana s predpisom

$$M(n) = \sum_{k \le n} \mu(k), \tag{32}$$

se imenuje *Mertensova*[8] *funkcija.*

Primer 4.7. Izračunajmo vrednosti Mertensove funkcije za nekaj naravnih števil:
$M(2) = \mu(1) + \mu(2) = 1 - 1 = 0$,
$M(3) = \mu(1) + \mu(2) + \mu(3) = 1 - 1 - 1 = -1$,
$M(6) = \mu(1) + \mu(2) + \mu(3) + \mu(4) + \mu(5) + \mu(6) = 1 - 1 - 1 + 0 - 1 + 1 = -1$. $\diamondsuit$

Mertensova funkcija ni monotona, njena vrednost pa se v vsakem naslednjem naravnem številu spremeni kvečjemu za ± 1. Za vsako naravno število n velja $|M(n)| \le n$.

Naslednjo trditev, ki jo bomo navedli brez izpeljave, je leta 1912 dokazal Litllewood[9]. Njeno bistvo je, da Riemannovo hipotezo lahko prevedemo na ekvivalentno trditev, ki opisuje rast Mertensove funkcije. Več podrobnosti o njej si bralec lahko prebere v [2, poglavje 12.1]. Oglejmo si le idejo za formulacijo trditve.

Če faktorje v Eulerjevi produktni formuli pomnožimo, dobimo na polravnini $\{s; \mathrm{Re}(s) > 1\}$ izražavo $\frac{1}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\mu(n)}{n^s}$. Po nekaj korakih pridemo do zveze $\frac{1}{\zeta(s)} = s \int_0^\infty M(x) x^{-s-1} dx$. Mertensovo funkcijo tu razumemo kot definirano za vse nenegativne vrednosti: predpišemo $M(0) = 0$, funkcija pa je konstantna, razen v naravnih številih n, kjer ima skok $\mu(n)$. Ker za vse x velja $|M(x)| \le x$, je na polravnini $\{s; \mathrm{Re}(s) > 1\}$ $\lim_{x\to\infty} x^{-s} M(x) = 0$ in integral $\int_0^\infty M(x) x^{-s-1} dx$ na tej polravnini konvergira. Če obstaja tako pozitivno število a, da funkcija M raste počasneje od funkcije $x \mapsto x^a$, potem zgornji integral konvergira na polravnini $\{s; \mathrm{Re}(a - s) < 0\} = \{s; \mathrm{Re}(s) > a\}$. To pomeni, da je funkcija $s \mapsto \zeta^{-1}(s)$ na tej polravnini analitična. Vendar obstajajo ničle funkcije ζ na premici $s = \{\frac{1}{2} + it; t \in \mathbb{R}\}$, torej ima na tej premici funkcija ζ^{-1} singularnosti. Od tod sledi, da za poljuben $0 < a < \frac{1}{2}$ ne velja $M(x) = o(x^a)$. Naslednja trditev pove, da velja celo več. Še prej pa vpeljimo nov pojem.

Definicija 4.8 (Notacija mali o)**.** Funkcija f pripada razredu $o(g(x))$, če absolutna vrednost funkcije f raste počasneje od funkcije g. Natančneje, $f(x) = o(g(x))$, če za vsak $\varepsilon > 0$ obstaja vrednost x_0, da za poljuben $x \ge x_0$ velja $|f(x)| < \varepsilon \cdot g(x)$.

Trditev 4.9. *Za vsak* $\varepsilon > 0$ *velja* $M(n) = o(n^{1/2+\varepsilon})$ *natanko tedaj, ko velja Riemannova hipoteza.*

Pred drugo ekvivalenco Riemannove hipoteze potrebujemo definicijo, ki sledi.

[8] Franz Mertens, 20. 3. 1840–5. 3. 1927, poljski matematik.
[9] John Edensor Littlewood, 9. 6. 1885–6. 9. 1977, angleški matematik.

Definicija 4.10. Naj bosta $L(n)$ dolžina Fareyevega zaporedja reda n in r_v njegov v-ti element. Definiramo razliko

$$\delta_v = r_v - v/L(n). \tag{33}$$

Primer 4.11. Vzemimo Fareyevo zaporedje reda 4 in poglejmo nekaj razlik:
$F_4 = \left\{\frac{0}{1}, \frac{1}{4}, \frac{1}{3}, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{1}{1}\right\}$,
$L(4) = 7$,
$\delta_1 = \frac{0}{1} - \frac{1}{7} = -\frac{1}{7}$,
$\delta_2 = \frac{1}{4} - \frac{2}{7} = -\frac{1}{28}$,
$\delta_7 = \frac{1}{1} - \frac{7}{7} = 0$.
Opazimo, da za poljuben n velja $\delta_{L(n)} = 0$. ♢

Trditev 4.12 (Franel-Landau, 1924)**.** *Za vsak $\varepsilon > 0$ velja $\sum_{v=1}^{L(n)} |\delta_v| = o(n^{1/2+\varepsilon})$ natanko tedaj, ko velja Riemannova hipoteza.*

Dokaz zgornje trditve izpustimo. V obliki, kot sta ga dokazala Franel in Landau leta 1924, se nahaja v viru [4]. Pač pa bomo v nadaljevanju dokazali povezavo med navedenima ekvivalentnima formulacijama Riemannove hipoteze, ki jo lahko združimo v izrek.

Izrek 4.13. *Naj bo $\varepsilon > 0$. $\sum_{v=1}^{L(n)} |\delta_v| = o(n^{1/2+\varepsilon})$ velja tedaj in le tedaj, ko velja $M(n) = o(n^{1/2+\varepsilon})$.*

4.3. **Fareyevo zaporedje in Riemannova hipoteza.** V tem razdelku bomo dokazali glavni izrek 4.13, ki Riemannovo hipotezo poveže s Fareyevim zaporedjem. Najprej bomo dokazali lemo, ki bo ključ do dokaza izreka. Še prej pa se spomnimo Eulerjeve produktne formule ter Fourierovih transformacij.

Trditev 4.14 (Möbiusova inverzija)**.** *Naj bosta vrsti $\sum_{n=1}^{\infty} f(nx)$ in $\sum_{n=1}^{\infty} g(nx)$ absolutno konvergentni. Tedaj velja*

$$g(x) = \sum_{n=1}^{\infty} f(nx) \Longleftrightarrow f(x) = \sum_{n=1}^{\infty} \mu(n) g(nx). \tag{34}$$

Formulo lahko zapišemo v ekvivalentni obliki

$$g(x) = \sum_{n=1}^{\infty} f\left(\frac{x}{n}\right) \Longleftrightarrow f(x) = \sum_{n=1}^{\infty} \mu(n) g\left(\frac{x}{n}\right). \tag{35}$$

Trditev navajamo brez izpeljave – ta se nahaja v [2, poglavje 10.9]. Möbiusovo inverzijo bomo namreč potrebovali le v enem koraku dokaza napovedane leme, kjer bomo uporabili ekvivalenco (35).

Lema 4.15. *Realna funkcija f naj bo definirana na intervalu $[0, 1]$. Naj bodo r_v elementi Fareyevega zaporedja reda n, $r_0 = 0$ in $r_{L(n)} = 1$*[10]*. Tedaj velja enakost*[11]

$$\sum_{v=1}^{L(n)} f(r_v) = \sum_{k=1}^{\infty} \sum_{j=1}^{k} f\left(\frac{j}{k}\right) M\left(\frac{n}{k}\right). \tag{36}$$

[10] Zgolj zaradi preglednejšega zapisa bomo za potrebe dokaza v tem razdelku Fareyevo zaporedje F_n 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.

[11] Vsota na desni strani je končna, saj je za $k > n$ vrednost $M(\frac{n}{k}) = 0$.

Dokaz. Funkcijo $D : \mathbb{R} \to \{0, 1\}$ definirajmo s predpisom

$$D(n) = \begin{cases} 1 & , \text{ če } n \geq 1 \\ 0 & , \text{ če } n < 1 \end{cases} . \tag{37}$$

Spomnimo se definicije Mertensove funkcije in upoštevajmo predpis (37). Dobimo

$$M(n) = \sum_{x \leq n} \mu(x) = \sum_{x=1}^{\infty} \mu(x) D\left(\frac{n}{x}\right),$$

Möbiusova inverzija pa nam da ekvivalenco

$$M(n) = \sum_{x=1}^{\infty} \mu(x) D\left(\frac{n}{x}\right) \iff D(n) = \sum_{x=1}^{\infty} M\left(\frac{n}{x}\right).$$

Naj bosta celi števili p in q tuji ter $0 < p \leq q \leq n$, z drugimi besedami, ulomek $\frac{p}{q}$ ustreza nekemu elementu r_v Fareyevega zaporedja F_n. Primerjali bomo koeficiente pri $f(\frac{p}{q})$ na levi in desni strani enakosti (36). Ker je $f(\frac{p}{q}) = f(\frac{2p}{2q}) = f(\frac{3p}{3q}) = \cdots$, je koeficient pri $f(\frac{p}{q})$ na desni strani enak

$$\begin{aligned} M\left(\frac{n}{q}\right) + M\left(\frac{n}{2q}\right) + M\left(\frac{n}{3q}\right) + \cdots &= \sum_{l=1}^{\infty} M\left(\frac{n}{ql}\right) \\ &= D\left(\frac{n}{q}\right) = \begin{cases} 1 & , \text{ če } n \geq q \\ 0 & , \text{ če } n < q \end{cases} . \end{aligned}$$

To pa je ravno koeficient pri $f(r_v)$ na levi strani. Lema zato res drži. □

4.3.1. *Dokaz implikacije v desno izreka 4.13.* Naj bo $\varepsilon > 0$. Naj bo $u \in [0, 1]$ in definirajmo funkcijo $f(u) = e^{2\pi i u}$. Uporabimo lemo 4.15 in funkcijo vstavimo v enakost (36); dobimo

$$\sum_{v=1}^{L(n)} e^{2\pi i r_v} = \sum_{k=1}^{\infty} \sum_{j=1}^{k} e^{2\pi i \frac{j}{k}} M\left(\frac{n}{k}\right). \tag{38}$$

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 (38) zato prepišemo v

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

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

$$\begin{aligned} |M(n)| &\leq \sum_{v=1}^{L(n)} \left|e^{\frac{2\pi i v}{L(n)}}\right| \left|e^{2\pi i \delta_v} - 1\right| = \sum_{v=1}^{L(n)} \left|e^{2\pi i \delta_v} - 1\right| = \sum_{v=1}^{L(n)} \left|e^{\pi i \delta_v}\right| \left|e^{\pi i \delta_v} - e^{-\pi i \delta_v}\right| \\ &= 2 \sum_{v=1}^{L(n)} |\sin(\pi \delta_v)| \leq 2 \sum_{v=1}^{L(n)} |\delta_v| \pi = 2\pi \sum_{v=1}^{L(n)} |\delta_v| \\ &< 2\pi K_1(\varepsilon) n^{1/2+\varepsilon} = K(\varepsilon) n^{1/2+\varepsilon}. \end{aligned}$$

V zadnji neenakosti smo uporabili predpostavko $\sum_{v=1}^{L(n)} |\delta_v| = o(n^{1/2+\varepsilon})$, kar je ekvivalentno $\sum_{v=1}^{L(n)} |\delta_v| < K_1(\varepsilon) n^{1/2+\varepsilon}$ za neko konstanto K_1, ki je odvisna od ε. Od tod sledi, da je $M(n) = o(n^{1/2+\varepsilon})$, kar smo želeli pokazati.

4.3.2. *Bernoullijevi polinomi.* 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. Rezultati so povzeti po [2, poglavje 6.2].

Definicija 4.16. Naj bo $n \in \mathbb{N} \cup \{0\}$. *$n$-ti Bernoullijev polinom* B_n je polinom stopnje n, ki ustreza zvezi

$$\int_x^{x+1} B_n(t)dt = x^n. \tag{39}$$

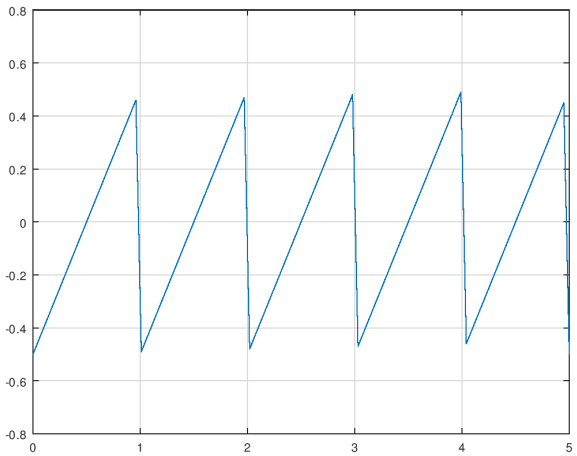
Primer 4.17. Zapišimo nekaj Bernoullijevih polinomov najnižjih stopenj. Izračunamo jih tako, da zapišemo polinom $B_n(t) = a_0 + a_1 t + \cdots + a_n t^n$ in rekurzivno računamo koeficiente pri potencah x v enakosti (39):

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

Definicija 4.18. 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 4.19. Iz definicije sledi, da je $\bar{B}_n$ periodična funkcija s periodo 1.

Primer 4.20. Funkcijo $\bar{B}_1(x) = x - \lfloor x \rfloor - \frac{1}{2}$ bomo potrebovali v dokazu. ♢



SLIKA 8. Graf funkcije $\bar{B}_1(x) = x - \lfloor x \rfloor - \frac{1}{2}$.

Trditev 4.21. *Naj bo $k \in \mathbb{N}$. Tedaj je*

$$B_n(ku) = k^{n-1}\left(B_n(u) + B_n\left(u + \frac{1}{k}\right) + \cdots + B_n\left(u + \frac{k-1}{k}\right)\right). \tag{40}$$

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

4.3.3. *Dokaz implikacije v levo izreka 4.13.* Spomnimo se funkcije $\bar{B}_1(x) = x - \lfloor x \rfloor - \frac{1}{2}$ in enačbe (40). 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 (40) zato dobi obliko

$$\begin{aligned} \bar{B}_1(ku) &= \bar{B}_1(u) + \bar{B}_1\left(u + \frac{1}{k}\right) + \cdots + \bar{B}_1\left(u + \frac{k-1}{k}\right) \\ &= \bar{B}_1\left(u + \frac{1}{k}\right) + \bar{B}_1\left(u + \frac{2}{k}\right) + \cdots + \bar{B}_1\left(u + 1\right). \end{aligned} \tag{41}$$

Ključni korak dokaza je, da v enakost iz leme 4.15 vstavimo funkcijo $\bar{B}_1$, pri čemer uporabimo zvezo (41). Označimo

$$G(u) = \sum_{v=1}^{L(n)} \bar{B}_1(u + r_v) = \sum_{k=1}^{\infty} \sum_{j=1}^{k} \bar{B}_1\left(u + \frac{j}{k}\right) M\left(\frac{n}{k}\right) = \sum_{k=1}^{\infty} \bar{B}_1(ku) M\left(\frac{n}{k}\right), \tag{42}$$

kar nam da dva izraza za funkcijo G. Izračunali bomo integral

$$I = \int_0^1 G(u)^2 du. \tag{43}$$

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

$$\begin{aligned} G(u) &= \sum_{v=1}^{L(n)} \bar{B}_1(u + r_v) = \sum_{v=1}^{L(n)} \left(u + r_v - \lfloor u + r_v \rfloor - \frac{1}{2}\right) \\ &= L(n)u + \sum_{v=1}^{L(n)} r_v - \sum_{v=1}^{L(n)} \lfloor u + r_v \rfloor - \frac{L(n)}{2} \end{aligned} \tag{44}$$

in opazujmo člen s spodnjim celim delom. Ker so členi Fareyevega 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 Fareyevega 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 Fareyevega 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,

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

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

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

Izrazimo še

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

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

Sedaj lahko izračunamo integral

$$\begin{aligned}
I &\overset{(1)}{=} \sum_{v=1}^{L(n)} \int_{r_{v-1}}^{r_v} \left(L(n)u - v - \frac{1}{2} + 1 \right)^2 du \\
&= \sum_{v=1}^{L(n)} \frac{(L(n)u - v + \frac{1}{2})^3}{3L(n)} \Bigg|_{r_{v-1}}^{r_v} \\
&= \frac{1}{3L(n)} \sum_{v=1}^{L(n)} \left(\left(L(n)\delta_v + \frac{1}{2} \right)^3 - \left(L(n)\delta_{v-1} - \frac{1}{2} \right)^3 \right) \\
&\overset{(2)}{=} \frac{1}{3L(n)} \sum_{v=1}^{L(n)} \left(\left(L(n)\delta_v + \frac{1}{2} \right)^3 - \left(L(n)\delta_v - \frac{1}{2} \right)^3 \right) \\
&= \frac{1}{3L(n)} \sum_{v=1}^{L(n)} \left(3\left(L(n)\delta_v \right)^2 + \frac{1}{4} \right) \\
&= L(n) \sum_{v=1}^{L(n)} \delta_v^2 + \frac{1}{12L(n)} L(n) \\
&= L(n) \sum_{v=1}^{L(n)} \delta_v^2 + \frac{1}{12}. \qquad (45)
\end{aligned}$$

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

$$\begin{aligned}
I &= \int_0^1 \left(\sum_{k=1}^{\infty} \bar{B}_1(ku) M\left(\frac{n}{k}\right) \right)^2 du \\
&= \int_0^1 \sum_{a=1}^{\infty} \sum_{b=1}^{\infty} \bar{B}_1(au)\bar{B}_1(bu) M\left(\frac{n}{a}\right) M\left(\frac{n}{b}\right) du \\
&= \sum_{a=1}^{\infty} \sum_{b=1}^{\infty} M\left(\frac{n}{a}\right) M\left(\frac{n}{b}\right) \int_0^1 \bar{B}_1(au)\bar{B}_1(bu) du, \qquad (46)
\end{aligned}$$

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

Naj bo $b = 1$. Tedaj je

$$\begin{aligned} I_{a1} &= \int_0^1 \bar{B}_1(au)\bar{B}_1(u)du \overset{(1)}{=} \frac{1}{a}\int_0^a \bar{B}_1(v)\bar{B}_1\left(\frac{v}{a}\right)dv \\ &\overset{(2)}{=} \frac{1}{a}\sum_{k=0}^{a-1}\int_0^1 \bar{B}_1(k+t)\bar{B}_1\left(\frac{k}{a}+\frac{t}{a}\right)dt \\ &\overset{(3)}{=} \frac{1}{a}\int_0^1 \bar{B}_1(t)\bar{B}_1\left(a\frac{t}{a}\right)dt \overset{(4)}{=} \frac{1}{a}\int_0^1 \left(t-\frac{1}{2}\right)^2 dt \\ &= \frac{1}{3a}\left(t-\frac{1}{2}\right)^3\Big|_0^1 = \frac{1}{12a}. \end{aligned} \tag{47}$$

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 (41). V enakosti (4) smo uporabili dejstvo, 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. Računamo

$$\begin{aligned} I_{ab} &= \int_0^1 \bar{B}_1(au)\bar{B}_1(bu)du = \frac{1}{a}\int_0^a \bar{B}_1(v)\bar{B}_1\left(\frac{bv}{a}\right)dv \\ &= \frac{1}{a}\sum_{k=0}^{a-1}\int_0^1 \bar{B}_1(k+t)\bar{B}_1\left(\frac{bk}{a}+\frac{bt}{a}\right)dt \\ &\overset{(5)}{=} \frac{1}{a}\int_0^1 \bar{B}_1(t)\bar{B}_1\left(a\frac{bt}{a}\right)dt = \frac{1}{a}I_{1b} = \frac{1}{12ab}. \end{aligned} \tag{48}$$

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

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

$$\begin{aligned} I_{ab} &= \int_0^1 \bar{B}_1(c\alpha u)\bar{B}_1(c\beta u)du \overset{(6)}{=} \frac{1}{c}\int_0^c \bar{B}_1(\alpha t)\bar{B}_1(\beta t)dt \\ &\overset{(7)}{=} I_{\alpha\beta} = \frac{1}{12\alpha\beta} = \frac{c^2}{12ab}. \end{aligned} \tag{49}$$

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 (46) in dobimo

$$I = \sum_{a=1}^{\infty}\sum_{b=1}^{\infty} M\left(\frac{n}{a}\right) M\left(\frac{n}{b}\right)\frac{c^2}{12ab}, \tag{50}$$

kjer je c največji skupni delitelj a in b.

Naj bo $\varepsilon > 0$. Predpostavljamo, da je $M(n) = o(n^{1/2+\varepsilon})$, kar pomeni, da obstaja taka konstanta C, odvisna od ε, da za poljubno velik n velja $|M(n)| < C(\varepsilon)n^{1/2+\varepsilon}$.

Če to uporabimo v enačbi (50), dobimo

$$\begin{aligned}
|I| &< \sum_{a=1}^{\infty}\sum_{b=1}^{\infty} C(\varepsilon)^2 \left(\frac{n}{a}\right)^{1/2+\varepsilon}\left(\frac{n}{b}\right)^{1/2+\varepsilon}\frac{c^2}{12ab} \\
&= n^{1+2\varepsilon}\frac{C(\varepsilon)^2}{12}\sum_{a=1}^{\infty}\sum_{b=1}^{\infty}\frac{c^2}{a^{3/2+\varepsilon}b^{3/2+\varepsilon}} \\
&= n^{1+2\varepsilon}\frac{C(\varepsilon)^2}{12}\sum_{a=1}^{\infty}\sum_{b=1}^{\infty}\frac{c^2}{\alpha^{3/2+\varepsilon}\beta^{3/2+\varepsilon}c^{3+2\varepsilon}} \\
&\overset{(8)}{<} n^{1+2\varepsilon}K_1(\varepsilon)\sum_{\alpha=1}^{\infty}\sum_{\beta=1}^{\infty}\sum_{c=1}^{\infty}\frac{1}{\alpha^{3/2}\beta^{3/2}c^{1+2\varepsilon}} \\
&= K_2(\varepsilon)n^{1+2\varepsilon}. \qquad (51)
\end{aligned}$$

V neenakosti (8) smo vsoto po tujih si številih α in β zamenjali z vsoto po vseh naravnih številih α in β.

Sedaj se vrnimo k enakosti (45), upoštevajmo, da je $|I| = I$, kar implicira

$$I = L(n)\sum_{v=1}^{L(n)}\delta_v^2 + \frac{1}{12} < K_2(\varepsilon)n^{1+2\varepsilon},$$

od koder sledi

$$\sum_{v=1}^{L(n)}\delta_v^2 < K_3(\varepsilon)n^{1+2\varepsilon}.$$

Cauchy-Schwarzova neenakost nam da končno oceno

$$\sum_{v=1}^{L(n)}|\delta_v| = \left|\sum_{v=1}^{L(n)}(\pm 1)\delta_v\right| \le \sqrt{\sum_{v=1}^{L(n)}(\pm 1)^2}\sqrt{\sum_{v=1}^{L(n)}\delta_v^2} = L(n)^{1/2}\sqrt{\sum_{v=1}^{L(n)}\delta_v^2} < K(\varepsilon)n^{1/2+\varepsilon},$$

kar dokazuje obratno implikacijo.

Slovar strokovnih izrazov

Bernoulli $\sim$ **number** Bernoullijevo število; $\sim$ **polynomial** Bernoullijev polinom

Euler product formula Eulerjeva produktna formula – povezuje Riemannovo zeta funkcijo s praštevili

Farey neighbour Fareyev sosed – Fareyeva soseda sta sosednja elementa Fareyevega zaporedja

Ford neighbour Fordov sosed – Fordova soseda sta tangentna Fordova kroga

group action delovanje grupe – delovanje grupe G na množico M je homomorfizem iz grupe G v grupo permutacij množice M

little-o notation notacija mali o – funkcija f pripada razredu $o\,(g(x))$, če absolutna vrednost funkcije f raste počasneje od funkcije g

mediant medianta; $\sim$ **property** lastnost mediante – lastnost mediante velja za Fareyevo zaporedje in Fordove kroge

Mertens function Mertensova funkcija

Möbius function Möbiusova funkcija

Riemann zeta function Riemannova zeta funkcija – Riemannova hipoteza govori o ničlah te funkcije

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*, The American Mathematical Monthly, **45**, 1938, str. 586–601; dostopno tudi na `https://www.maths.ed.ac.uk/~v1ranick/papers/ford.pdf`.

[4] J. Franel in E. Landau, *Les suites de Farey et le problème des nombres premiers*, Göttinger Nachr., 1924, str. 198–206.

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

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

[7] W. L. Hosch, *Riemann hypothesis*, [ogled 8. 8. 2019], dostopno na `https://www.britannica.com/science/Riemann-hypothesis`.

[8] P. Sebah in X. Gourdon, *Introduction on Bernoulli's numbers*, verzija 12. 6. 2002, [ogled 20. 7. 2019], dostopno na `http://math.ucr.edu/~res/math153/s12/bernoulli-numbers.pdf`.

[9] J. Veisdal, *The Riemann hypothesis, explained*, verzija 21. 8. 2016, [ogled 30. 4. 2019], dostopno na `https://medium.com/cantors-paradise/the-riemann-hypothesis-explained-fa01c1f75d3f`.