STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Multiplikativní funkce v teorii čísel

Autor: Vít Jelínek
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Kraj: Jihomoravský

Brno 2017

STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor č. 1: Matematika a statistika

Multiplikativní funkce v teorii čísel
Multiplicative functions in number theory

Autor: Vít Jelínek
Škola: Gymnázium Brno, třída Kapitána Jaroše, p. o.
Konzultant: Mgr. Petr Pupík
Kraj: Jihomoravský

Brno 2017

Prohlášení

Prohlašuji, že svou práci na téma Multiplikativní funkce v teorii čísel jsem vypracoval samostatně pod vedením Mgr. Petra Pupíka a s využitím odborné literatury a dalších informačních zdrojů, které jsou všechny citovány v práci a uvedeny v seznamu literatury na konci práce.
Dále prohlašuji, že tištěná i elektronická verze práce SOČ jsou shodné a nemám závažný důvod proti zpřístupňování této práce v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a změně některých zákonů (autorský zákon) v platném znění.

V Brně dne ..... Podpis .....

Poděkování

Rád bych poděkoval Mgr. Petru Pupíkovi za jeho čas, za kritiku, za skvělé poznámky a připomínky a za obrovskou trpělivost, bez které by tato práce nikdy nevznikla. Také bych chtěl poděkovat tvůrcům systému LaTeX, ve kterém je tato práce vysázena.
Tato práce byla vypracována za finanční podpory JMK.

Anotace

Cílem je podat v češtině práci, která ukáže, co to jsou multiplikativní funkce. V práci je uveden Dirichletův součin a z něj odvozena Möbiova inverzní formule. Následně jsou ukázány některé aplikace Möbiovy inverzní formule jako je Eulerova funkce. Eulerova funkce bude následně užitečná pro zkoumání Fareyových zlomků. Nakonec je vysvětleno, v čem spočívá Riemannova hypotéza, a je ukázána její souvislost s multiplikativními funkcemi.

Klíčová slova

multiplikativní funkce, Möbiova inverzní formule, Eulerova funkce, Fareyovy zlomky, Riemannova hypotéza

Annotation

The aim of this thesis is to explain in Czech language what multiplicative functions are. The Dirichlet product is introduced to the reader and Möbius inversion theorem is derived. Then several applications of Möbius inversion theorem as Euler function are shown. Euler function is then important in exploration of Farey sequence. In the final part is explained what Riemann hypothesis is and its connection to multiplicative functions is shown.

Key words

multiplicative functions, Möbius inversion theorem, Euler function, Farey sequence, Riemann hypothesis

Obsah

Úvod

Ústředním tématem práce jsou aritmetické a hlavně multiplikativní funkce. Oba tyto pojmy jsou pojmy z teorie čísel, které ovšem nejsou moc známé a v českém jazyce neexistuje prakticky žádná literatura, která by se jimi v takovéto míře zabývala. V první kapitole se budu zabývat obecně multiplikativními a aritmetickými funkcemi, uvedu, o co se jedná, a jaké mají vlastnosti. V druhé kapitole se budu zabývat operací s aritmetickými funkcemi – Dirichletovým součinem. Nejdůležitějším pojmem druhé kapitoly bude Möbiova inverzní formule. Díky ní odvodím vztah pro výpočet hodnot Eulerovy funkce. A pak se budu zabývat Fareyovými zlomky. Ve třetí kapitole se budu zabývat jedním z „problémů tisíciletí“ – Riemannovou hypotézou. Nejprve vysvětlím, v čem problém spočívá, a následně ukáži jeho souvislost s teorií čísel. Zatímco v prvních dvou kapitolách se budu snažit, aby se jednalo o text poměrně formální, ve třetí kapitole to vzhledem k náročnosti problému nebude možné. Text by měl být srozumitelný pro středoškolského čtenáře, který zná základy teorie čísel a setkal se se sumační symbolikou.

V celém textu bude platit, že všemi děliteli daného čísla myslím všechny kladné dělitele. Navíc, pokud uvažuji rozklad nějakého čísla na prvočísla či prvočíselný rozklad, tak předpokládám, že všechna prvočísla z rozkladu jsou různá.

Kapitola 1

Multiplikativní funkce

V první kapitole si řekneme něco o multiplikativních funkcích a uvedeme nějaké příklady, z nichž nejdůležitější bude Möbiova funkce.

1.1 Definice multiplikativních funkcí

Definice 1.1.1. Nechť je dána funkce $f\colon \mathbb{N} \to \mathbb{C}$, pak funkci f nazveme aritmetickou funkcí.

Příklad 1.1.1. Některé aritmetické funkce:

- Libovolná konstantní funkce $f(n) = c$, kde c je libovolné komplexní číslo.
- Funkce, která k přirozenému číslu n přiřadí počet jeho cifer.
- Funkce $S(n)$, která k přirozenému číslu přiřadí jeho ciferný součet.

Definice 1.1.2. Aritmetickou funkci f nazveme multiplikativní, pokud pro každá nesoudělná $m, n \in \mathbb{N}$ platí:

1. $f(mn) = f(m)f(n)$;
2. $f(1) = 1$.

Příklad 1.1.2. Některé multiplikativní funkce:

- Konstantní funkce $f(n) = 1$ je multiplikativní.
- Funkce tvaru $f(n) = n^k$ pro libovolné reálné k jsou multiplikativní.

Dále se budeme zajímat o funkce, které závisí na dělitelích daného čísla – jejich počtu, součtu a součinu.

Definice 1.1.3. Nechť funkce $\tau(n)$ značí počet dělitelů čísla n, $\sigma(n)$ značí jejich součet a funkce $\nu(n)$ jejich součin.

Pro všechny tyto funkce existují vztahy, pomocí kterých můžeme určit jejich hodnoty. Pojďme si tyto vztahy odvodit.

Nechť n je přirozené číslo s prvočíselným rozkladem $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, kde p_i jsou navzájem různá prvočísla a α_i jsou přirozená čísla. Potom každého dělitele d čísla n můžeme vyjádřit jako $d = \prod_{i=1}^{k} p_i^{\beta_i}$, kde β_i jsou nezáporná celá čísla taková, že $\beta_i \leq \alpha_i$ pro všechna $i = 1, 2, \ldots, k$. Potom ale β_i může nabývat $\alpha_i + 1$ možných hodnot (od nuly po α_i). A podle kombinatorického pravidla součinu tak platí, že $\tau(n) = \prod_{i=1}^{k}(\alpha_i + 1)$.

Nyní budeme počítat součet všech těchto dělitelů. Pro pozdější potřeby označme $D_i = \frac{n}{p_i^{\alpha_i}}$ pro všechna $i = 1, 2, \ldots, k$. A nyní už k samotnému součtu. Vezměme si prvočíslo p_l – jedno z prvočísel dělících n, a ukažme, že součet můžeme přepsat takto: na první řádek napíšeme všechny dělitele čísla n, které nejsou dělitelné prvočíslem p_l. Zřejmě jde o všechny dělitele čísla D_l. Na druhý řádek napišme ten stejný součet, jenom vynásobený prvočíslem p_l, na třetí ten samý součet vynásobený p_l^2, …, na $\alpha_l + 1$-tý řádek napišme součet z prvního řádku vynásobený číslem $p_l^{\alpha_l}$. Pokud si všechny dělitele čísla D_l označíme jako d_1, d_2,…, d_m, tak získáváme toto:

$$\begin{gathered} d_1 + d_2 + \cdots + d_m + \\ + p_l d_1 + p_l d_2 + \cdots + p_l d_m + \\ + p_l^2 d_1 + p_l^2 d_2 + \cdots + p_l^2 d_m + \\ \vdots \\ + p_l^{\alpha_l} d_1 + p_l^{\alpha_l} d_2 + \cdots + p_l^{\alpha_l} d_m. \end{gathered}$$

A proč vlastně můžeme součet takto přepsat? Vzhledem k jednoznačnosti rozkladu na prvočísla je zřejmé, že žádný sčítanec se v tomto součtu nevyskytuje dvakrát. Navíc všechny sčítance dělí číslo n, takže pokud se tento součet liší od našeho hledaného, tak to musí znamenat, že je sčítanců méně než v hledaném součtu. Ovšem hledaný součet má $\tau(n)$ sčítanců. Na každém řádku tohoto součtu je $\tau(D_l) = \frac{\tau(n)}{\alpha_l + 1}$ sčítanců, a protože máme $\alpha_l + 1$ řádků, tak celkem má tento součet $(\alpha_l + 1)\tau(D_l) = \tau(n)$ sčítanců. To je ale stejný počet jako má hledaný součet, a tak mají stejnou hodnotu. Vzhledem k tomu, jak je součet výše napsaný, je zřejmé, že z každého řádku můžeme vytknout $\sigma(D_l)$ a získáváme

$$\sigma(n) = (1 + p_l + p_l^2 + p_l^3 + \ldots + p_l^{\alpha_l})\sigma(D_l).$$

Podle vztahu pro součet prvních $\alpha_l + 1$ členů geometrické posloupnosti:

$$(1 + p_l + p_l^2 + p_l^3 + \ldots + p_l^{\alpha_l})\sigma(D_l) = \frac{p_l^{\alpha_l + 1} - 1}{p_l - 1}\sigma(D_l).$$

A takto můžeme pokračovat i pro další prvočísla (na prvočíslo p_l jsme nekladli žádné speciální podmínky), která dělí číslo n, jenom je budeme vytýkat ze součtu dělitelů čísla

D_l a ne ze součtu dělitelů čísla n. A tak získáváme vztah:

$$\sigma(n) = \prod_{i=1}^{k} \frac{p_i^{\alpha_i+1} - 1}{p_i - 1}.$$

Nakonec uvažme součin dělitelů čísla n: $\nu(n) = \prod_{d|n} d$. Budeme zkoumat v jaké mocnině budou v celkovém součinu všechna prvočísla z rozkladu čísla n. Zkoumejme tedy nějaké prvočíslo p_l (pro jednoduchost se může jednat o stejné prvočíslo jako výše). Uvažme obdobné schéma jako při odvozování hodnot funkce $\sigma(n)$ s tím rozdílem, že čísla nesčítáme, ale násobíme. Protože násobení je komutativní, činitele můžeme přepsat tak, že na každém řádku vedle sebe postavíme mocniny prvočísla p_l a za ně až všechny ostatní činitele. A když tedy chceme vědět, v jaké mocnině bude ve výsledném součinu pročíslo p_l, tak vezměme v úvahu, že na prvním řádku máme $(p_l^0)^{\tau(D_l)}$, na druhém máme $(p_l^1)^{\tau(D_l)}$,..., a na posledním řádku máme $(p_l^{\alpha_l})^{\tau(D_l)}$ a ve výsledku dostáváme:

$$\prod_{j=1}^{\alpha_l} \left(p_l^j\right)^{\tau(D_l)} = \prod_{j=1}^{\alpha_l} p_l^{j\tau(D_l)}.$$

Nyní sečteme exponenty:

$$\sum_{j=1}^{\alpha_l} j\tau(D_l) = \tau(D_l) \sum_{j=1}^{\alpha_l} j = \tau(D_l)\frac{1}{2}\alpha_l(\alpha_l + 1).$$

U poslední rovnosti jsme využili toho, že $\sum_{j=1}^{\alpha_l} j$ je vlastně součet čísel $1 + 2 + 3 \cdots + \alpha_l$. Z definice čísel D_i platí, že $\tau(D_i)(\alpha_i + 1) = \tau(n)$. A v našem konkrétním případě:

$$\tau(D_l)\frac{1}{2}\alpha_l(\alpha_l + 1) = \frac{1}{2}\alpha_l\tau(n).$$

Vzhledem k tomu, že jsme na prvočíslo p_l nekladli žádné zvláštní podmínky, to stejné musí platit i pro všechna ostatní prvočísla z rozkladu čísla n. Tím získáváme:

$$\nu(n) = \prod_{i=1}^{k} p_i^{\frac{1}{2}\alpha_i\tau(n)} = \left(\prod_{i=1}^{k} p_i^{\alpha_i}\right)^{\frac{1}{2}\tau(n)} = n^{\frac{1}{2}\tau(n)}.$$

Pomocí těchto vztahů už snadno určíme hodnoty funkcí, tedy například pro $n = 12$:
$\tau(12) = \tau(3^1 \cdot 2^2) = (1 + 1)(2 + 1) = 6$ a číslo 12 má dělitele 1, 2, 3, 4, 6 a 12.
$\sigma(12) = \sigma(3^1 \cdot 2^2) = \frac{3^2-1}{3-1}\frac{2^3-1}{2-1} = \frac{8\cdot 7}{2} = 28$ a 1+2+3+4+6+12=28.
$\nu(12) = 12^{\frac{1}{2}6} = 12^3 = (12 \cdot 1)(2 \cdot 6)(3 \cdot 4) = 1 \cdot 2 \cdot 3 \cdot 4 \cdot 6 \cdot 12$.

Odvozené vztahy nám pomohou v následujícím příkladu.

Příklad 1.1.3. Funkce $\tau(n)$ a $\sigma(n)$ jsou multiplikativní, zatímco $\nu(n)$ nikoliv. *Důkaz:* Zvolme 2 nesoudělná čísla a, b, přičemž jejich prvočíselné rozklady jsou: $a = \prod_{i=1}^{m} p_i^{\alpha_i}$ a $b = \prod_{j=1}^{n} q_j^{\beta_j}$, přičemž platí: $p_i \neq q_j$ pro libovolná i, j. Z toho plyne:

$$\tau(ab) = \tau(p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_m^{\alpha_m} \cdot q_1^{\beta_1} q_2^{\beta_2} \cdots q_n^{\beta_n}) =$$

$$= (\alpha_1+1)(\alpha_2+1)\cdots(\alpha_m+1)(\beta_1+1)(\beta_2+1)\cdots(\beta_n+1) =$$
$$= [(\alpha_1+1)(\alpha_2+1)\cdots(\alpha_m+1)][(\beta_1+1)(\beta_2+1)\cdots(\beta_n+1)] =$$
$$= \tau(p_1^{\alpha_1}p_2^{\alpha_2}\cdots p_m^{\alpha_m})\tau(q_1^{\beta_1}q_2^{\beta_2}\cdots q_n^{\beta_n}) =$$
$$= \tau(a)\tau(b)$$

a $\tau(n)$ je tedy multiplikativní. Pro $\sigma(n)$ se multiplikativita ukáže analogicky. Pro důkaz toho, že $\nu(n)$ není multiplikativní stačí nalézt 2 nesoudělná čísla $a, b : \nu(ab) \neq \nu(a)\nu(b)$, tedy například $a = 2, b = 3, ab = 6$ a dělitelé čísla 6 jsou: 1, 2, 3, 6, $\nu(6) = 6 \cdot 3 \cdot 2 \cdot 1 = 36 \neq 6 = \nu(2)\nu(3)$, tedy funkce $\nu(n)$ není multiplikativní.

Poznámka 1.1.1. Někdy se místo funkcí τ a σ definuje obecnější funkce $\sigma_k(n) = \sum_{d|n} d^k$, kde $k, n \in \mathbb{N}$. Je vidět, že $\sigma_0(n) = \tau(n)$ a $\sigma_1(n) = \sigma(n)$. Tato funkce je také multiplikativní.

Věta 1.1.1. *Nechť $g(n)$ je multiplikativní funkce. Pak aritmetická funkce $f(n)$ definovaná vztahem*

$$f(n) = \sum_{d|n} g(n)$$

je také multiplikativní.

Důkaz. Nechť a, b jsou nesoudělná přirozená čísla. Potom:

$$f(a)f(b) = \left(\sum_{d_1|a} g(d_1)\right)\left(\sum_{d_2|b} g(d_2)\right) = \sum_{d_1|a}\left[g(d_1)\sum_{d_2|b} g(d_2)\right] = \sum_{d_1|a}\sum_{d_2|b} g(d_1)g(d_2).$$

Zatím jsme jenom roznásobili závorky. Navíc, protože jsou a a b nesoudělná, musí platit, že libovolný dělitel čísla a je s libovolným dělitelem čísla b nesoudělný, takže platí:

$$\sum_{d_1|a}\sum_{d_2|b} g(d_1)g(d_2) = \sum_{d_1|a}\sum_{d_2|b} g(d_1d_2) = \sum_{d_1|a\wedge d_2|b} g(d_1d_2).$$

Ale každého dělitele čísla $a \cdot b$ určitě můžeme zapsat jako součin dvou čísel tak, že první dělí a a druhé dělí b, takže dostáváme:

$$\sum_{d_1|a\wedge d_2|b} g(d_1d_2) = f(ab).$$

Tedy $f(n)$ je multiplikativní funkcí. □

A k čemu nám vlastně je definovat nějakou funkci takto na první pohled zvláštně? Podívejme se na funkce $\tau(n)$ a $\sigma(n)$. Platí, že $\tau(n) = \sum_{d|n} 1$ a $\sigma(n) = \sum_{d|n} d$.

1.2 Möbiova funkce

V této části se budeme zabývat jednou multiplikativní funkcí, která, ač se na první pohled zdá být komplikovaně definovaná, bude velice důležitá v další kapitole pro zkonstruování Möbiovy inverzní formule.

Definice 1.2.1. Möbiova funkce $\mu\colon \mathbb{N} \to \mathbb{Z}$, kde prvočíselný rozklad čísla n je $n = \prod_{i=1}^{k} p_i^{\alpha_i}$, je definována takto:

$$\mu(n) = \begin{cases} 1 & \text{pokud } n = 1, \\ 0 & \text{pokud } \exists d \in \mathbb{N} \setminus \{1\} : d^2 | n, \\ (-1)^k & \text{jinak.} \end{cases}$$

Příklad 1.2.1. Hodnoty funkce μ snadno spočítáme z rozkladu na prvočísla:

- $\mu(18) = \mu(2 \cdot 3^2) \Rightarrow 3^2 | 18 \Rightarrow \mu(18) = 0.$
- $\mu(42) = \mu(2 \cdot 3 \cdot 7) = (-1)^3 = -1.$

Věta 1.2.1. *Möbiova funkce $\mu(n)$ je multiplikativní.*

Důkaz. Nechť a, b jsou nesoudělná čísla s prvočíselným rozkladem: $a = \prod_{i=1}^{k} p_i^{\alpha_i}$ a $b = \prod_{j=1}^{l} q_j^{\beta_j}$, kde p_i a q_j jsou různá prvočísla pro všechna i, j a $\alpha_i, \beta_j \in \mathbb{N}$.

1. Předpokládejme, že a nebo b jsou dělitelné druhou mocninou nějakého přirozeného čísla jiného než 1. Bez újmy na obecnosti předpokládejme, že tímto číslem bude a. Potom pro nějaké i určitě platí, že $\alpha_i > 1$. Potom $p_i^2 | a$, a tím pádem taky $p_i^2 | ab$, tedy $\mu(ab) = 0 = \mu(a) = \mu(a)\mu(b)$.

2. Nyní předpokládejme, že a, b nejsou dělitelná druhou mocninou přirozeného čísla. Potom ale musí platit, že jejich rozklad na prvočísla vypadá následovně: $a = \prod_{i=1}^{k} p_i$, $b = \prod_{j=1}^{l} q_j$, potom $\mu(ab) = \mu(\prod_{i=1}^{k} p_i \prod_{j=1}^{l} q_j) = (-1)^{k+l}$
$\mu(a)\mu(b) = (-1)^k(-1)^l = (-1)^{k+l} = \mu(ab)$. Takže funkce $\mu(n)$ je multiplikativní.

□

Věta 1.2.2. *Nechť $n \in \mathbb{N} \setminus \{1\}$, pak platí:*

$$\sum_{d|n} \mu(d) = 0.$$

Důkaz. Napišme si rozklad čísla n na součin prvočísel: $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Vzhledem k tomu, kdy Möbiova funkce nabývá hodnoty 0, je zřejmé, že do součtu nám přispějí pouze ti dělitelé čísla n, kteří jsou ve tvaru: $d = \prod_{i=1}^{k} p_i^{\beta_i}$, kde $\beta_i \in \{0, 1\}$. Spočítejme, kolik dělitelů čísla n je v tom tvaru, který požadujeme, a $\beta_i = 1$ právě pro l různých hodnot i. Těch je právě $\binom{k}{l}$ a každý z nich přispěje do celkového součtu číslem $(-1)^l$, potom:

$$\sum_{d|n} \mu(d) = \sum_{l=0}^{k} \binom{k}{l} (-1)^l = (1-1)^k = 0.$$

Předposlední rovnost plyne z binomické věty. □

Lemma 1.2.1. *Každé přirozené číslo $n \in \mathbb{N}$ můžeme zapsat ve tvaru: $n = a \cdot b^2$, kde a a b jsou přirozená čísla a a není dělitelné druhou mocninou žádného prvočísla.*

Důkaz. Uvažme prvočíselný rozklad čísla $n = \prod_{i=1}^{k} p_i^{\alpha_i}$. Pak položme $a = \prod_{j \in L} p_j$, kde L je množina obsahující všechna taková přirozená čísla x, pro která platí, že α_x je liché číslo. Určitě platí, že $a|n$, protože a je součinem stejných prvočísel jako n, jen exponenty u prvočísel v rozkladu a jsou 0 nebo 1 a exponenty v rozkladu n jsou větší nebo rovny 1. Pak $\frac{n}{a}$ je druhou mocninou přirozeného čísla, neboť je to součin prvočísel se sudými exponenty. Tedy pokud položíme $b = \sqrt{\frac{n}{a}}$, tak platí, že $n = a \cdot b^2$ a zároveň neexistuje $d \in \mathbb{N} \setminus \{1\}$ takové, že $d^2|a$. □

Věta 1.2.3. *Nechť $n \in \mathbb{N}$, pak platí:*

$$\sum_{d^2|n} \mu(d) = \mu^2(n).$$

Důkaz. Podle předchozího lemmatu můžeme n psát jako $n = a \cdot b^2$. Samotný důkaz rozdělme do dvou částí:

1. $b = 1$ Tím pádem $n = a$ a jediné přirozené číslo, jehož druhá mocnina dělí číslo n je číslo 1. Tedy hodnota $\mu(n)$ je $+1$ nebo -1 a tedy $\mu^2(n) = 1$. Zároveň platí:

$$\sum_{d^2|n} \mu(d) = \mu(1) = 1 = \mu^2(n).$$

2. $b \neq 1$ Tedy $b^2|n$ a protože jsme našli číslo různé od 1, jehož druhá mocnina dělí n, tak platí, že $\mu(n) = \mu^2(n) = 0$. A jelikož žádná druhá mocnina nedělí číslo a, tak platí: $\sum_{d^2|n} \mu(d) = \sum_{d^2|b^2} \mu(d) = \sum_{d|b} \mu(d)$, ale podle věty 1.2.2 platí:

$$\sum_{d|b} \mu(d) = 0 = \mu^2(n).$$

□

Kapitola 2

Dirichletův součin a Möbiova inverzní formule

V následující kapitole se budeme zabývat operací s aritmetickými funkcemi – Dirichletovým součinem a následující otázkou: jsou dány 2 aritmetické funkce f, g, přičemž platí, že $f(n) = \sum_{d|n} g(d)$. Zvládneme z tohoto vztahu vyjádřit hodnoty funkce g v závislosti na funkci f? Odpověď nám dá právě Möbiova inverzní formule.

2.1 Dirichletův součin

Definice 2.1.1. Nechť jsou dány 2 aritmetické funkce f, g, pak jejich Dirichletův součin $\circ$ definujeme následujícím vztahem:

$$(f \circ g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

Poznámka 2.1.1. Definici Dirichletova součinu můžeme také přepsat: pro aritmetické funkce f, g a $d_1, d_2, n \in \mathbb{N}$ definujeme Dirichletův součin následovně:

$$(f \circ g)(n) = \sum_{\substack{(d_1,d_2) \\ d_1 d_2 = n}} f(d_1) g(d_2).$$

Jedná se o to stejné, jako v předchozí definici, jelikož ze vztahu $d_1 d_2 = n$ můžeme d_2 vyjádřit jako $d_2 = \frac{n}{d_1}$.

Příklad 2.1.1. $(\tau \circ \mu)(4) = \tau(1)\mu(4) + \tau(2)\mu(2) + \tau(4)\mu(1) = 1 \cdot 0 + 2 \cdot (-1) + 3 \cdot 1 = 1$

V následující větě shrneme důležité vlastnosti Dirichletova součinu.

Věta 2.1.1. *Pro Dirichletův součin platí:*

1. *Dirichletův součin je na množině multiplikativních funkcí uzavřený.*
2. *Dirichletův součin je komutativní.*
3. *Dirichletův součin je asociativní.*
4. *Existuje aritmetická funkce e, pro kterou platí, že pro libovolnou aritmetickou funkci f je $(f \circ e)(n) = f(n)$.*

Důkaz. Označme M množinu všech multiplikativních funkcí a A množinu všech aritmetických funkcí.

1. Vzhledem k tomu, že důkaz je velice podobný jako důkaz věty 1.1.1, tak ho pouze naznačím. Uvažme 2 funkce $f, g \in M$ a funkci $h = f \circ g$. Chceme dokázat, že $h \in M$. Pro nesoudělná $a, b \in \mathbb{N}$ vezměme součin $h(a)h(b) = ((f \circ g)(a))((f \circ g)(b))$ a téměř stejným postupem jako při důkazu věty 1.1.1 ukážeme, že $h(a)h(b) = h(ab)$.

2. Nechť $f, g \in A, n \in \mathbb{N}$

$$(f \circ g)(n) = \sum_{d|n} f(d) g\left(\frac{n}{d}\right).$$

   Položme $c = \frac{n}{d}$, pak $c|n$ právě tehdy, když $d|n$, a tedy:

$$\sum_{d|n} f(d) g\left(\frac{n}{d}\right) = \sum_{c|n} f\left(\frac{n}{c}\right) g(c) = (g \circ f)(n).$$

   A Dirichletův součin je komutativní.

3. Dirichletův součin je asociativní. Nechť $f, g, h \in M, n \in \mathbb{N}$, pak chceme ukázat:

$$(f \circ (g \circ h))(n) = ((f \circ g) \circ h)(n)$$

$$(f \circ (g \circ h))(n) = \sum_{\substack{(d_1,d)\\ d_1 d = n}} f(d_1)(g \circ h)(d) = \sum_{\substack{(d_1,d)\\ d_1 d = n}} \left(f(d_1) \sum_{\substack{(d_2,d_3)\\ d_2 d_3 = d}} g(d_2)h(d_3) \right) =$$

$$= \sum_{\substack{(d_1,d)\\ d_1 d = n}} \sum_{\substack{(d_2,d_3)\\ d_2 d_3 = d}} f(d_1)g(d_2)h(d_3) = \sum_{\substack{(d_1,d_2,d_3)\\ d_1 d_2 d_3 = n}} f(d_1)g(d_2)h(d_3)$$

$$((f \circ g) \circ h)(n) = \sum_{\substack{(d_3,d)\\ d_3 d = n}} (f \circ g)(d)h(d_3) = \sum_{\substack{(d_3,d)\\ d_3 d = n}} \left(h(d_3) \sum_{\substack{(d_1,d_2)\\ d_1 d_2 = d}} f(d_1)g(d_2) \right) =$$

$$= \sum_{\substack{(d_3,d)\\ d_3 d=n}} \sum_{\substack{(d_2,d_1)\\ d_2 d_1=d}} h(d_3) f(d_1) g(d_2) = \sum_{\substack{(d_1,d_2,d_3)\\ d_1 d_2 d_3=n}} f(d_1) g(d_2) h(d_3) = (f \circ (g \circ h))(n).$$

4. Nechť $n \in \mathbb{N}$, pak funkce $e\colon \mathbb{N} \to \mathbb{C}$, definovaná předpisem:

$$e(n) = \begin{cases} 1 & \text{pokud } n = 1, \\ 0 & \text{jinak,} \end{cases}$$

má požadovanou vlastnost. Platí totiž $(f \circ e)(n) = \sum_{d|n} e(d) f\left(\frac{n}{d}\right)$, přičemž ale $e(d) \neq 0$ právě tehdy, když $d = 1$, a tak $(f \circ e)(n) = f(n)$.

□

2.2 Möbiova inverzní formule a její aplikace

Když už jsme seznámeni s Dirichletovým součinem, tak si můžeme ukázat Möbiovu inverzní formuli. Nejprve je ale třeba nadefinovat si ještě jednu jednoduchou funkci.

Definice 2.2.1. Definujme funkci $I\colon \mathbb{N} \to \mathbb{C}$ jako konstantní funkci $I(n) = 1$.

Poznámka 2.2.1. Funkce I je zjevně multiplikativní. Kromě toho má ještě další zajímavé vlastnosti, které shrnuje následující věta.

Věta 2.2.1. *Pro funkci I platí:*

1. *Nechť f je libovolnou aritmetickou funkcí, pak $(f \circ I)(n) = \sum_{d|n} f(d)$.*
2. *$(I \circ \mu)(n) = e(n)$.*

Důkaz. Ad 1: Podle definice Dirichletova součinu platí: $(f \circ I)(n) = \sum_{d|n} f(d) I\left(\frac{n}{d}\right)$, ale protože I nabývá pouze hodnoty 1, dostáváme požadované, tedy $\sum_{d|n} f(d) I\left(\frac{n}{d}\right) = \sum_{d|n} f(d)$.

Ad 2: Pro $n = 1$ je tvrzení zřejmé. Pro $n \neq 1$ platí (podle 1. části):

$$(I \circ \mu)(n) = \sum_{d|n} \mu(d) = 0.$$

Což platí podle věty 1.2.2. □

Věta 2.2.2. *(Möbiova inverzní formule) Nechť f, g jsou aritmetické funkce, pro které platí vztah:*

$$g(n) = \sum_{d|n} f(d).$$

Pak funkci f můžeme vyjádřit jako:

$$f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right).$$

Důkaz. Funkci f určitě můžeme vyjádřit následujícím způsobem:

$$f = f \circ e = f \circ (\mu \circ I) = f \circ \mu \circ I = (f \circ I) \circ \mu.$$

Poslední krok jsme mohli učinit, protože Dirichletův součin je komutativní a asociativní, navíc podle předchozí věty platí, že $g(n) = \sum_{d|n} f(d) = (f \circ I)(n)$. Tím pádem dostáváme: $(f \circ I) \circ \mu = g \circ \mu = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right)$, což je dokazované tvrzení. □

Poznámka 2.2.2. Platí i opačné tvrzení, tedy pokud máme 2 aritmetické funkce f, g, pro které platí, že $f(n) = \sum_{d|n} g(d)\mu\left(\frac{n}{d}\right)$, pak $g(n) = \sum_{d|n} f(d)$. Dokazuje se analogicky.

Příklad 2.2.1. V příkladu 2.1.1 nám vyšlo, že $(\tau \circ \mu)(4) = 1$, ale $\tau(n) = \sum_{d|n} 1$, zobecnění $((\tau \circ \mu)(n) = 1)$ nám přináší právě Möbiova inverzní formule. Vzhledem k tomu, že $\tau(n) = \sum_{d|n} I(d)$, tak podle Möbiovy inverzní formule: $I(n) = (\tau \circ \mu)(n) = 1$. Analogicky dostaneme také $\sum_{d|n} \sigma(d)\mu\left(\frac{n}{d}\right) = n$.

Dále se budeme zabývat velice důležitou funkcí v teorii čísel – Eulerovou funkcí $\varphi(n)$. Ta je důležitá zejména kvůli Eulerově větě, která je jedním ze základních nástrojů používaných při šifrování pomocí algoritmu RSA.

Definice 2.2.2. Nechť $n \in \mathbb{N}$, pak Eulerovou funkci $\varphi(n)$ definujme jako počet čísel menších nebo rovných n, která jsou s n nesoudělná, tedy $\varphi(n) = |\{k \in \mathbb{N} | k \leq n, (n, k) = 1\}|$.

Snadno zvládneme určit hodnotu Eulerovy funkce pro prvočísla – všechna čísla menší než dané prvočíslo p jsou s p nesoudělná. Tedy $\varphi(p) = p - 1$. Pro mocniny prvočísel je to také jednoduché. S číslem p^k jsou menší a soudělná právě ta čísla, která jsou dělitelná p. To jsou ale násobky prvočísla p, tedy čísla $1 \cdot p, 2 \cdot p, \ldots, p^{k-1} \cdot p$, což je p^{k-1} čísel, tedy $\varphi(p^k) = p^k - p^{k-1}$. A jak je to se složenými čísly, která nejsou mocninou prvočísla? Ukážeme, že pro $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ platí

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Tvrzení se dá dokázat různými způsoby (například pomocí principu inkluze a exkluze nebo ukázáním, že Eulerova funkce je multiplikativní), my si ho dokážeme pomocí Möbiovy inverzní formule.

Lemma 2.2.1. *Pro Eulerovu funkci $\varphi(n)$ platí:* $\sum_{d|n} \varphi(d) = n$.

Důkaz. Uvažme n zlomků:

$$\frac{1}{n}, \frac{2}{n}, \ldots, \frac{n}{n}$$

a všechny je pokraťme do základního tvaru. Určitě se mezi čitateli nezkrácených zlomků vyskytnou všichni dělitelé čísla n (jedná se o všechna čísla, která jsou menší nebo rovna n a všichni dělitelé n jsou taky čísla menší nebo rovna n). A taky se určitě vyskytnou mezi jmenovateli po tom, co se všechny zlomky zkrátí do základního tvaru, neboť pokud $d|n$, tak po zkrácení se ve jmenovateli objeví číslo $\frac{n}{d}$ – označme ho c – a toto číslo určitě také dělí n, tedy se objeví v nějakém jiném čitateli. Ale zlomek, který bude mít v čitateli c, bude mít po zkrácení ve jmenovateli d. Uvažme zlomek, který bude mít po pokrácení ve jmenovateli číslo b. A kolika hodnot může nabývat čitatel? No, aby se jednalo o zlomek v základním tvaru, tak se musí jednat o číslo nesoudělné s b. A protože čitatel původního zlomku byl menší než jmenovatel původního zlomku, tak i čitatel pokráceného zlomku musí být menší než jmenovatel pokráceného zlomku. A tím pádem máme $\varphi(b)$ zlomků se jmenovatelem b. Kde b je ale libovolné číslo, které dělí n. Takže celkový počet zlomků je $\sum_{b|n} \varphi(b)$, ale zlomků jsme měli n. Tedy $\sum_{d|n} \varphi(d) = n$. □

Věta 2.2.3. *Nechť $n \in \mathbb{N}$, $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ pak platí:*

$$\varphi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right).$$

Důkaz. Z předchozího lemmatu víme, že $n = \sum_{d|n} \varphi(d)$, tedy podle Möbiovy inverzní formule získáváme: $\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d}$. A protože se do výsledného součtu započítají pouze ty, kde d vznikne součinem několika různých prvočísel, tak získáváme:

$$\varphi(n) = \sum_{d|n} \mu(d)\frac{n}{d} = n + \sum_{i=1}^{k}(-1)^i \sum_{\substack{(p_{j_1},p_{j_2},\ldots,p_{j_i}) \\ 1\le j_1<j_2<\ldots<j_i\le k}} \frac{n}{p_{j_1}p_{j_2}\cdots p_{j_i}} =$$

$$= n - \sum_{i=1}^{k}\frac{n}{p_i} + \sum_{\substack{(p_i,p_j) \\ 1\le i<j\le k}} \frac{n}{p_ip_j} - \sum_{\substack{(p_i,p_j,p_l) \\ 1\le i<j<l\le k}} \frac{n}{p_ip_jp_l} + \ldots + (-1)^k\frac{n}{p_1p_2\cdots p_k} \Rightarrow$$

$$\frac{\varphi(n)}{n} = 1 - \sum_{i=1}^{k}\frac{1}{p_i} + \sum_{\substack{(p_i,p_j) \\ 1\le i<j\le k}} \frac{1}{p_ip_j} - \sum_{\substack{(p_i,p_j,p_l) \\ 1\le i<j<l\le k}} \frac{1}{p_ip_jp_l} + \ldots + (-1)^k\frac{1}{p_1p_2\cdots p_k}.$$

Nyní si povšimněme, co se stane, když osamostatníme všechny sčítance, které mají prvočíslo p_1 ve svém jmenovateli. Pokud si z posledního řádku vybereme součet, ve kterém sčítáme

přes uspořádané s-tice (kde s je libovolné přirozené číslo menší než k), platí následující vztah:

$$\sum_{\substack{(p_{r_1},p_{r_2},\ldots,p_{r_s})\\1\le r_1<r_2<\ldots<r_s\le k}} \frac{1}{p_{r_1}p_{r_2}\cdots p_{r_s}} = \sum_{\substack{(p_{r_1},p_{r_2},\ldots,p_{r_s})\\2\le r_1<r_2<\ldots<r_s\le k}} \frac{1}{p_{r_1}p_{r_2}\cdots p_{r_s}} + \sum_{\substack{(p_{r_1},p_{r_2},\ldots,p_{r_{s-1}})\\2\le r_1<r_2<\ldots<r_{s-1}\le k}} \frac{1}{p_1p_{r_1}p_{r_2}\cdots p_{r_{s-1}}}.$$

Vztah platí, protože na levé straně máme součet všech s-tic prvočísel a na pravé straně máme součet všech s-tic, které obsahují prvočíslo p_1 a těch, které ho neobsahují, což jsou zřejmě všechny s-tice. Potom ale můžeme $\frac{\varphi(n)}{n}$ přepsat takto:

$$\begin{aligned}
\frac{\varphi(n)}{n} =& 1 - \sum_{i=2}^{k}\frac{1}{p_i} + \sum_{\substack{(p_i,p_j)\\2\le i<j\le k}}\frac{1}{p_ip_j} - \sum_{\substack{(p_i,p_j,p_l)\\2\le i<j<l\le k}}\frac{1}{p_ip_jp_l} + \ldots + (-1)^k\frac{1}{p_2p_3\cdots p_k} - \\
&- \left(\frac{1}{p_1} - \sum_{i=2}^{k}\frac{1}{p_1p_i} + \sum_{\substack{(p_i,p_j)\\2\le i<j\le k}}\frac{1}{p_1p_ip_j} - \sum_{\substack{(p_i,p_j,p_l)\\2\le i<j<l\le k}}\frac{1}{p_1p_ip_jp_l} + \ldots + (-1)^k\frac{1}{p_1p_2p_3\cdots p_k}\right) = \\
=& 1 - \sum_{i=2}^{k}\frac{1}{p_i} + \sum_{\substack{(p_i,p_j)\\2\le i<j\le k}}\frac{1}{p_ip_j} - \sum_{\substack{(p_i,p_j,p_l)\\2\le i<j<l\le k}}\frac{1}{p_ip_jp_l} + \ldots + (-1)^k\frac{1}{p_2p_3\cdots p_k} - \\
&- \frac{1}{p_1}\left(1 - \sum_{i=2}^{k}\frac{1}{p_i} + \sum_{\substack{(p_i,p_j)\\2\le i<j\le k}}\frac{1}{p_ip_j} - \sum_{\substack{(p_i,p_j,p_l)\\2\le i<j<l\le k}}\frac{1}{p_ip_jp_l} + \ldots + (-1)^k\frac{1}{p_2p_3\cdots p_k}\right) = \\
=& \left(1-\frac{1}{p_1}\right)\left(1 - \sum_{i=2}^{k}\frac{1}{p_i} + \sum_{\substack{(p_i,p_j)\\2\le i<j\le k}}\frac{1}{p_ip_j} - \sum_{\substack{(p_i,p_j,p_l)\\2\le i<j<l\le k}}\frac{1}{p_ip_jp_l} + \ldots + (-1)^k\frac{1}{p_2p_3\cdots p_k}\right).
\end{aligned}$$

Ovšem takto můžeme pokračovat i pro ostatní prvočísla z rozkladu čísla n. A dostaneme požadovaný vztah:

$$\varphi(n) = n\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

□

Poznámka 2.2.3. Eulerova funkce je multiplikativní. Tvrzení by se dokazovalo stejně jako multiplikativita funkce τ v příkladu 1.1.3.

Příklad 2.2.2. S Eulerovou funkcí se, díky dokázanému vzorci a multiplikativitě, dá pěkně pracovat. Dokažme například následující tvrzení: $\varphi(n) = \frac{n}{2}$ právě tehdy, když $n = 2^\alpha$, $\alpha \in \mathbb{N}$. To, že s mocninami čísla 2 jsou nesoudělná a menší právě všechna lichá čísla, kterých je polovina, je zřejmé. Předpokládejme tedy, že $\varphi(n) = \frac{n}{2}$. Vzhledem k tomu, že Eulerova funkce je zobrazení do přirozených čísel, tak n musí být sudé a tím pádem ho můžeme zapsat jako $n = 2^\alpha m$, kde α je přirozené číslo a m je liché přirozené číslo, a tedy nesoudělné s číslem 2^α. Potom ale $\varphi(n)$ můžeme vypočítat následujícím způsobem:

$$\begin{aligned} \varphi(n) = \varphi(2^\alpha m) = \varphi(2^\alpha)\varphi(m) &= 2^{\alpha-1}\varphi(m), \\ \frac{n}{2} &= 2^{\alpha-1}\varphi(m), \\ 2^{\alpha-1}m &= 2^{\alpha-1}\varphi(m), \\ m &= \varphi(m). \end{aligned}$$

Pro která m ale platí, že $m = \varphi(m)$? No pro každé přirozené číslo k větší než 1 platí, že $\varphi(k) < k$, protože číslo k je samo se sebou soudělné. Tedy $m = 1$, ale potom $n = 2^\alpha \cdot 1$, což je to, co jsme chtěli dokázat.

Jednou z mnoha aplikací Eulerovy funkce jsou například Fareyovy zlomky.

Fareyovy zlomky

Fareyovy zlomky jsou zajímavým pojmem z teorie čísel. Jejich využití je převážně praktické – používají se k aproximaci reálných čísel.

Definice 2.2.3. Fareyovými zlomky řádu n myslíme množinu zlomků

$$F_n = \left\{ \frac{a}{b} \middle| a \in \mathbb{N}_0, b \in \mathbb{N}, a \leq b \leq n \right\}$$

zkrácených do základního tvaru a seřazenou od nejmenšího po největší.

Fareyovy zlomky byly objeveny na počátku 19. století. Zajímavé je, že s jejich jmenovcem geologem Johnem Fareyem starším toho nemají zas tak moc společného. Ten je zkoumal a bez důkazu uvedl svá pozorování, která byla následně otištěna ve francouzském časopise. Tam si jich všiml Cauchy, který tvrzení dokázal. Všechno už ale bylo dokázáno o několik let dříve matematikem Charlesem Harlosem.

Ukažme si, jak vypadají Fareyovy zlomky pro prvních pár hodnot n. Vzhledem k tomu, že platí $0 \leq a \leq b$, jde vidět, že se jedná o čísla z intervalu $\langle 0; 1 \rangle$.

Příklad 2.2.3.

$$F_1 = \left\{ \frac{0}{1}; \frac{1}{1} \right\}$$

$$F_2 = \left\{\frac{0}{1}; \frac{1}{2}; \frac{1}{1}\right\}$$

$$F_3 = \left\{\frac{0}{1}; \frac{1}{3}; \frac{1}{2}; \frac{2}{3}; \frac{1}{1}\right\}$$

$$F_4 = \left\{\frac{0}{1}; \frac{1}{4}; \frac{1}{3}; \frac{1}{2}; \frac{2}{3}; \frac{3}{4}; \frac{1}{1}\right\}$$

$$F_5 = \left\{\frac{0}{1}; \frac{1}{5}; \frac{1}{4}; \frac{1}{3}; \frac{2}{5}; \frac{1}{2}; \frac{3}{5}; \frac{2}{3}; \frac{3}{4}; \frac{4}{5}; \frac{1}{1}\right\}$$

$$F_9 = \left\{\frac{0}{1}; \frac{1}{9}; \frac{1}{8}; \frac{1}{7}; \frac{1}{6}; \frac{1}{5}; \frac{2}{9}; \frac{1}{4}; \frac{2}{7}; \frac{1}{3}; \frac{3}{8}; \frac{2}{5}; \frac{3}{7}; \frac{4}{9}; \frac{1}{2}; \frac{5}{9}; \frac{4}{7}; \frac{3}{5}; \frac{5}{8}; \frac{2}{3}; \frac{5}{7}; \frac{3}{4}; \frac{7}{9}; \frac{4}{5}; \frac{5}{6}; \frac{7}{8}; \frac{8}{9}; \frac{1}{1}\right\}$$

Při zkoumání Fareyových zlomků je důležitým pojmem mediant.

Definice 2.2.4. Nechť $\frac{a}{b}, \frac{c}{d}$ jsou 2 libovolné zlomky. Pak jejich mediantem $\frac{a}{b} \oplus \frac{c}{d}$ rozumíme zlomek $\frac{a+c}{b+d}$.

Mediant má totiž jednu velice pěknou vlastnost:

Věta 2.2.4. *Uvažme libovolné zlomky $\frac{a}{b}, \frac{c}{d}$ takové, že $\frac{a}{b} < \frac{c}{d}$ a jejich mediant $\frac{a+c}{b+d}$, pak platí: $\frac{a}{b} < \frac{a+c}{b+d} < \frac{c}{d}$.*

Důkaz. Nejprve si uvědomme, že z předpokladu věty plyne, že $ad < bc$, tedy $bc - ad > 0$. Dokazujme postupně obě nerovnosti:

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

A analogicky:

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

□

O mediantu platí navíc také to, že pokud uvážíme libovolné 3 po sobě jdoucí členy Fareyových zlomků řádu n, tak prostřední z nich je mediantem zbylých dvou. K tomuto tvrzení existuje ekvivalentní tvrzení: pokud $\frac{a}{b}, \frac{c}{d}$ jsou po sobě jdoucí členy Fareyových zlomků řádu n, tak platí: $|ad - bc| = 1$. Obě tvrzení se dají ukázat elementárními prostředky, ovšem poměrně zdlouhavě a složitě, a tak je zde dokazovat nebudeme. Jejich důkaz je možné nalézt v [2].

Uvedené vlastnosti nám nabízí už druhý způsob, jak vygenerovat Fareyovy zlomky řádu n. Buď podle definice uvážíme všechny zlomky se jmenovatelem menším nebo rovným n a zkrátíme je do základního tvaru nebo vytvoříme zlomky řádu 1 a následně ze zlomků

řádu k vygenerujeme zlomky řádu $k+1$ tak, že mezi každé 2 sousedící vložíme jejich mediant a pokud jeho jmenovatel bude větší, než $k+1$, tak ho smažeme. Takovýto zlomek se objeví až ve zlomcích vyššího řádu. Tedy například pojďme vygenerovat z F_4 všechny nové zlomky, které se objeví v F_5, sestrojme medianty všech sousedních zlomků a ty, které budou mít jmenovatel 5, jsou ty, které přibudou.

$$F_4 = \left\{ \frac{0}{1}; \frac{1}{4}; \frac{1}{3}; \frac{1}{2}; \frac{2}{3}; \frac{3}{4}; \frac{1}{1} \right\}$$

Podíváme-li se na součty sousedních jmenovatelů, dostáváme: 5, 7, 5, 5, 7, 5, což znamená, že přibudou zlomky $\frac{0+1}{1+4} = \frac{1}{5}$, $\frac{1+1}{3+2} = \frac{2}{5}$, $\frac{1+2}{2+3} = \frac{3}{5}$, $\frac{3+1}{4+1} = \frac{4}{5}$.

Zajímavé je, kolik vzniklo nových zlomků, které jsou v F_5 a nejsou v F_4, a kolik vznikne nových zlomků, které jsou v F_5 a nejsou v F_6. Vzhledem k tomu, že $|F_2| - |F_1| = = 1 \leq |F_3| - |F_2| = 2 \leq |F_4| - |F_3| = 2 \leq |F_5| - |F_4|$, by se mohlo zdát, že se bude jednat o neklesající posloupnost, ovšem právě rozdíl $|F_6| - |F_5|$ toto zdání ukáže jako chybné. Podíváme-li se totiž na součty jmenovatelů sousedních zlomků v F_5, získáme číslo 6 pouze na začátku a na konci, tím pádem $|F_6| - |F_5| = 2$. Kolik je tedy Fareyových zlomků řádu n?

Věta 2.2.5. *Nechť $n \in \mathbb{N}, n > 1$, pak pro počet Fareyových zlomků řádu n platí následující vztahy:*

1. $|F_n| = |F_{n-1}| + \varphi(n)$,
2. $|F_n| = 1 + \sum_{d=1}^{n} \varphi(d)$.

Důkaz. Ad 1: plyne z toho, že pokud chceme vytvořit F_n z F_{n-1}, tak musíme přidat všechny zlomky tvaru $\frac{k}{n}, 1 \leq k \leq n$, ale zlomky, které nebudou v základním tvaru, se pokrátí a zmenší se jmenovatel. Bude se tedy jednat o některý ze zlomků, které patří do F_{n-1}, a pokrátí se ty, kde bude čitatel soudělný s n, a tím pádem přibudou ty, kde je čitatel nesoudělný s n, ale těch je právě $\varphi(n)$. Ad 2: plyne z toho, že $|F_1| = 2$ a z první části. □

Bez důkazu ještě uveďme asymptotické chování $|F_n|$.

Věta 2.2.6. *Počet Fareyových zlomků řádu n lze odhadnout takto:*

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

A co se týče využití Fareyových zlomků, tak to napovídá následující věta, kterou opět uvedu bez důkazu:

Věta 2.2.7. *Nechť x je libovolné reálné číslo a n je libovolné přirozené, pak existují nesoudělná čísla $p, q \in \mathbb{Z}$ taková, že $0 < q \leq n$ a platí:*

$$\left| x - \frac{p}{q} \right| \leq \frac{1}{q(n+1)}.$$

Důkaz. Důkaz lze najít v literatuře [2]. □

Předchozí tvrzení nám v podstatě říká, že pro každé reálné číslo existuje aproximace ve formě zlomku v základním tvaru (to, že se nejedná o zlomek menší nebo roven 1, jenom znamená, že ho můžeme napsat jako součet nějakého celého čísla a některého Fareyova zlomku), o kterém dokážeme říci, o kolik se bude lišit od daného reálného čísla. Toto se v praxi dá použít tak, že například iracionální číslo nahradíme zlomkem, se kterým se mnohem lépe pracuje. Zajímavé také je, že toto se někdy používá k aproximaci „nevhodných“ racionálních čísel. Uveďme si čistě hypotetický příklad. Představme si, že potřebujeme vyrobit hodiny, které budou mít velkou vteřinovou ručičku a malou „roční“ ručičku, tedy malá ručička se pohne o 1 dílek poté, co velká ručička obkrouží celé kolečko. V každých hodinách jsou nějaká ozubená kolečka, která určitě mají celočíselný počet zubů. Navíc platí, že pokud nějaké kolečko má $m \cdot n$ zubů, tak ho můžu nahradit soustavou dvou koleček, které budou mít m a n zubů. Představme si, že v našem hypotetickém příkladě by vyšlo, že rok se skládá z prvočíselného počtu sekund. Potom bychom ale museli museli použít jedno obrovské kolo čítající o něco málo více zubů, než $365 \cdot 24 \cdot 3600$, které by ale bylo velice nepraktické. Hodilo by se tedy ho nahradit menšími kolečky, ale jelikož se jedná o prvočíslo, tak to není přesně možné. Souvislost se zlomky získáváme, podíváme-li se na úhlovou rychlost, která je rovna u kolečka s x zuby číslu $\frac{1}{x}$. Takže aproximujeme výraz $\frac{1}{p}$, kde p je nějaké velké prvočíslo, na nějaké složené číslo, jehož jmenovatel můžeme rozložit na více menších čísel, a tím pádem bychom mohli nahradit velké kolečko několika malými a získali bychom hodinky „rozumné“ velikosti. Hodinky sice nebudou tak přesné jako ty s jedním jediným kolečkem, ale budou praktičtější a díky předchozí větě i zvládneme odhadnout, jakou budou mít chybu. K nalezení „dobré“ aproximace se využívá vlastností mediantu – konkrétně toho, že mediant dvou zlomků je zlomek s nejmenším jmenovatelem, který leží mezi nimi.

Kapitola 3

Riemannova hypotéza

Roku 1900 matematik David Hilbert vydal seznam 23 problémů, které považoval za největší nevyřešené problémy své doby. Roku 2000 Clayův matematický institut sestavil podobný seznam 7 tzv. „problémů tisíciletí“, přičemž za vyřešení každého z nich nabízí odměnu jednoho milionu dolarů. Z Hilbertova seznamu zbývají 3 problémy, které nebyly vyřešeny, z „problémů tisíciletí“ byl vyřešen jediný. Zajímavé je, že tyto 2 seznamy největších problémů své doby mají právě jeden společný – Riemannovu hypotézu. Už to, že se více jak 100 let jedná o jeden z největších problémů, vypovídá o jeho významu a také o náročnosti jeho vyřešení. V této kapitole bych chtěl vysvětlit, v čem problém spočívá, a následně ukázat některé překvapivé souvislosti s předchozím textem.

3.1 Formulace Riemannovy hypotézy

Ač to není správně, jelikož Riemannova hypotéza je stále pouze hypotézou, uveďme si ji jako větu.

Věta 3.1.1. *Všechny netriviální nulové body Riemannovy zeta funkce mají reálnou část rovnu jedné polovině.*

Pojďme si nyní vysvětlit, co to vlastně znamená. Nejprve si něco řekněme, o Riemannově zeta funkci.

Definice 3.1.1. Nechť $s \in \mathbb{R}$, pak Riemannovu zeta funkci $\zeta\colon \mathbb{R} \to \mathbb{R}$ definujeme následujícím předpisem:

$$\zeta(s) = \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \ldots = \sum_{n=1}^{\infty} \frac{1}{n^s}.$$

Je vidět, že čím větší je s, tím menší hodnoty funkce nabývá. Zkusme dosadit za s

některé hodnoty a podívejme se, co vychází.

$$\zeta(0) = \frac{1}{1^0} + \frac{1}{2^0} + \frac{1}{3^0} + \frac{1}{4^0} + \ldots = 1 + 1 + 1 + 1 + 1 + 1 + 1 + \ldots$$
$$\zeta(-1) = \frac{1}{1^{-1}} + \frac{1}{2^{-1}} + \frac{1}{3^{-1}} + \frac{1}{4^{-1}} + \ldots = 1 + 2 + 3 + 4 + \ldots$$
$$\zeta(2) = \frac{1}{1^2} + \frac{1}{2^2} + \frac{1}{3^2} + \frac{1}{4^2} + \ldots = \frac{\pi^2}{6}.$$

U prvních 2 hodnot není problém o výsledku rozhodnout, je vidět, že řada diverguje (jde do nekonečna). Co se týče třetí hodnoty, tak určení hodnoty $\zeta(2)$ se nazývá Basilejský problém a jeho vyřešení je poměrně obtížné. Problém byl poprvé vyřešen Leonardem Eulerem. Dá se dokonce ukázat, že pro všechny kladné sudé s můžeme $\zeta(s)$ vyjádřit nějakým explicitním výrazem s číslem π. Zajímavé je, že o lichých s nic podobného nevíme. Vidíme, že pro některá s zeta funkce diverguje, pro jiná konverguje. Vzhledem k tomu, že funkce je klesající, tak by měla existovat nějaká hraniční hodnota, pro kterou bude platit, že je největší hodnotou, pro kterou Riemannova zeta funkce diverguje.

Věta 3.1.2. $\zeta(1)$ *diverguje.*

Důkaz. Rozepišme si, jak vypadá $\zeta(1)$:

$$\begin{aligned}
\zeta(1) &= \frac{1}{1} + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8} + \ldots =, \\
&= \left(\frac{1}{1}\right) + \left(\frac{1}{2}\right) + \left(\frac{1}{3} + \frac{1}{4}\right) + \left(\frac{1}{5} + \frac{1}{6} + \frac{1}{7} + \frac{1}{8}\right) + \ldots, \\
&> \left(\frac{1}{2}\right) + \left(\frac{1}{2}\right) + \left(\frac{1}{4} + \frac{1}{4}\right) + \left(\frac{1}{8} + \frac{1}{8} + \frac{1}{8} + \frac{1}{8}\right) + \ldots =, \\
&= \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \frac{1}{2} + \ldots
\end{aligned}$$

Na posledním řádku je divergentní řada a tak $\zeta(1)$ také diverguje. □

Součet převrácených hodnot všech přirozených čísel se nazývá harmonická řada a to, že diverguje bylo dokázáno už před mnoha staletími. Důkaz, že pro všechna $s > 1$ platí, že $\zeta(s)$ konverguje, je mnohem náročnější a přesahuje rámec tohoto textu.

Z formulace Riemannovy hypotézy se dá očekávat, že souvisí s tím, kdy Riemannova zeta funkce nabývá hodnoty 0. Ovšem všechny sčítance můžeme zapsat jako a^x, kde x je reálné a a kladné. No ale pro všechna takováto a a x platí, že $a^x > 0$. A celkový součet tak nemůže být nulový. Aby mohla být Riemannova hypotéza formulována, tak je třeba rozšířit definiční obor na množinu všech komplexních čísel. Tedy Riemannova zeta funkce by se měla definovat jako funkce z komplexních čísel do komplexních čísel. Naznačme tedy, jak se zavádí exponenciální funkce pro komplexní exponent. Hlavní myšlenkou bude to,

že chceme, aby exponenciální funkce v komplexních číslech měla stejné vlastnosti jako exponenciální funkce v číslech reálných, tedy chceme, aby pro $x, y \in \mathbb{C}$ platilo:

$$e^{x+y} = e^x e^y.$$

Začneme tak, že určíme, jak se bude chovat pro $z = a + bi$, kde $a, b \in \mathbb{R}$:

$$e^z = e^{a+bi} = e^a e^{bi}.$$

Výraz e^a je normální umocňování na reálné číslo, takže stačí vyřešit umocňování na ryze imaginární číslo. Výsledkem umocnění na ryze imaginární číslo $ix, x \in \mathbb{R}$ bude nějaké komplexní číslo, které mohu napsat v algebraickém tvaru jako $a+bi$, kde $a, b \in \mathbb{R}$. Ale čísla a a b musí být závislá na čísle x. Tedy je mohu napsat jako $a = c(x)$ a $b = s(x)$, kde $c(x)$ a $s(x)$ jsou nějaké funkce reálné proměnné. Nyní se opět vraťme k tomu, že chceme, aby pro exponenciální funkci platilo, že pro $x, y \in \mathbb{C}$ je $e^{x+y} = e^x e^y$. Dosaďme $x = ix_1, y = ix_2$, kde $x_1, x_2 \in \mathbb{R}$:

$$\begin{aligned}
e^{ix_1+ix_2} &= e^{ix_1}e^{ix_2} \\
e^{i(x_1+x_2)} &= e^{ix_1}e^{ix_2} \\
c(x_1+x_2) + is(x_1+x_2) &= (c(x_1) + is(x_1))(c(x_2) + is(x_2)) \\
c(x_1+x_2) + is(x_1+x_2) &= c(x_1)c(x_2) - s(x_1)s(x_2) + i(c(x_1)s(x_2) + s(x_1)c(x_2)).
\end{aligned}$$

Porovnáním reálných a imaginárních částí dostáváme soustavu:

$$c(x_1 + x_2) = c(x_1)c(x_2) - s(x_1)s(x_2)$$

$$s(x_1 + x_2) = c(x_1)s(x_2) + s(x_1)c(x_2).$$

Vidíme, že soustava připomíná součtové vzorce pro funkce sinus a kosinus. Ty sice nejsou jediným řešením této soustavy, ale vzhledem k některým dalším podmínkám je nejvhodnější definovat exponenciální funkci tak, že funkce $c(x)$ a $s(x)$ nahradíme právě funkcemi sinus a kosinus. Tedy pro $a, b \in \mathbb{R}$ platí:

$$e^{a+bi} = e^a(\cos(b) + i\sin(b)).$$

Zajímavé je, že i když takto rozšíříme definiční obor funkce na množinu komplexních čísel, tak stále platí, že $\zeta(s)$ konverguje právě tehdy, když pro reálnou část čísla s (značme $\Re(s)$) platí, že je větší než 1.

Nyní už víme, co to je Riemannova zeta funkce a můžeme se vrátit k dalším pojmům, které se vyskytují ve formulaci Riemannovy hypotézy. Nulový bod je takové s, pro které platí $|\zeta(s)| = 0$. Co znamená, že je některý nulový bod netriviální nebo triviální, si vysvětlíme až nakonec. Nejprve se zamyslíme nad tím, že reálná část nějakého s má být rovna jedné polovině. Problém spočívá v tom, že $\zeta(s)$ není definována pro $\Re(s) \leq 1$ a my chceme, aby $\Re(s) = \frac{1}{2}$. Důvodem, proč to můžeme udělat, je to, že nevezmeme funkci ζ v takové

podobě, v jaké ji známe, ale trochu ji upravíme. Občas se může stát, že pro nějakou komplexní funkci platí, že v některých místech komplexní roviny diverguje, ale my bychom s ní rádi pracovali i v těchto místech. Problém se řeší tak, že se najde jiná šikovná funkce, která v těch místech, ve kterých byla původní funkce definovaná, nabývá stejných hodnot, ale je definovaná i pro některé hodnoty, ve kterých původní funkce divergovala. Takovéto funkci se říká analytické pokračování původní funkce.

Definice 3.1.2. Nechť f, g jsou komplexní funkce po řadě definované na oblastech F, G z komplexní roviny takové, že $F \subseteq G \subseteq \mathbb{C}$, a platí, že $g(z) = f(z)$ pro všechna $z \in F$, tak funkci g nazveme analytickým pokračováním funkce f.

Předchozí definice není úplně korektní, funkce f, g musí totiž být analytické, tento pojem ale není pro tuto práci důležitý. Dá se ukázat, že analytické pokračování dané funkce je jediné na množině G. Pro funkci ζ existuje analytické pokračování pro všechna s taková, že $\Re(s) \neq 1$. Toto pokračování vyhovuje (pro $\Re(s) < 1$) následující funkcionální rovnici:

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s)\zeta(1-s). \tag{3.1}$$

Kde Γ je známá gama funkce, která je zobecněním faktoriálu do komplexních čísel. Uveďme si její definici.

Definice 3.1.3. Nechť $z \in \mathbb{C} \setminus \{n | -n \in \mathbb{N}_0\}$, pak $\Gamma(z)$ je definována následujícím vztahem:

$$\Gamma(z) = \int_0^\infty e^{-t} t^{z-1} dt.$$

Matematickou indukcí a integrací per partes se dá ukázat, že pro $n \in \mathbb{N}$ platí, že $\Gamma(n) = (n-1)!$.
Díky uvedené rovnici tak dokážeme spočítat hodnoty zeta funkce pro ta s, která mají zápornou reálnou část, pomocí těch, která ji mají větší než 1. Už z této rovnice jde vidět, že ζ nějak souvisí s jednou polovinou. Dosadíme-li $s = \frac{1}{2}$, tak dostáváme na levé i pravé straně $\zeta(\frac{1}{2})$.

Nyní se konečně můžeme podívat na poslední pojem z Riemannovy hypotézy – (ne)triviální nulový bod. Dosaďme $s = -2k$, kde $k \in \mathbb{N}$ do 3.1. Dostáváme:

$$\zeta(-2k) = 2^{-2k} \pi^{-2k-1} \sin\left(\frac{\pi(-2k)}{2}\right) \Gamma(1+2k)\zeta(1+2k).$$

Podíváme-li se na argument sinu, tak vidíme, že zůstane $\sin(-k\pi)$, což je 0. A tak $\zeta(-2k) = 0$. Všechna sudá záporná čísla tedy jsou nulovými body a jsou to ty, které se nazývají triviální. Všechny ostatní jsou netriviální. O netriviálních nulových bodech toho už poměrně hodně víme. Všechny leží v tzv. *kritickém pásu*, což je množina všech komplexních čísel s, pro něž platí, že $0 < \Re(s) < 1$. Kromě kritického pásu se ještě

definuje kritická přímka – množina všech komplexních čísel, jejichž reálná část je rovna jedné polovině. Je dokázáno, že na této přímce dokonce leží nekonečně mnoho netriviálních nulových bodů a nalezených na ní jich bylo více než 1 500 000 000. Navíc žádný nebyl nalezený mimo přímku, ale to, že žádný takový neexistuje, stále nikdo nedokázal. Bod s nejmenší imaginární částí (přesněji s nejmenší absolutní hodnotou imaginární části) je $s \doteq \frac{1}{2} + 14,134725\ldots i$. Ale z rovnice 3.1 vidíme, že pokud je $s = \frac{1}{2} + it$ nulovým bodem (pro nějaké $t \in \mathbb{R}$), pak jím také musí být bod $s = \frac{1}{2} - it$, takže hned máme další: $s \doteq \frac{1}{2} - 14,134725\ldots i$.

3.2 Riemannova hypotéza a teorie čísel

V předchozí části jsme si řekli, co to je Riemannova zeta funkce, a vysvětlili jsme si, v čem spočívá Riemannova hypotéza. Ovšem zatím není vůbec jasné, proč je zařazena do práce o teorii čísel a ne do práce o komplexní analýze. Pojďme si to ukázat na jednom vztahu, který znal už švýcarský matematik Leonhard Euler.

Vynásobme $\zeta(s)$ číslem $\frac{1}{2^s}$:

$$\begin{aligned} \zeta(s) &= \frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \frac{1}{6^s} + \ldots, \\ \frac{1}{2^s}\zeta(s) &= \qquad \frac{1}{2^s} \quad + \quad \frac{1}{4^s} \quad + \quad \frac{1}{6^s} + \ldots \end{aligned}$$

Po odečtení dostáváme:

$$\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{1^s} + \frac{1}{3^s} + \frac{1}{5^s} + \ldots$$

Vidíme, že ze součtu nám zmizely všechny členy, u kterých byl základ jmenovatele dělitelný dvojkou. Vynásobme tento součet číslem $\frac{1}{3^s}$ a opět odečtěme:

$$\begin{aligned} \left(1 - \frac{1}{2^s}\right)\zeta(s) &= \frac{1}{1^s} + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{9^s} + \ldots \\ \frac{1}{3^s}\left(1 - \frac{1}{2^s}\right)\zeta(s) &= \qquad \frac{1}{3^s} \qquad + \qquad \frac{1}{9^s} + \ldots \\ \left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) &= \frac{1}{1^s} + \frac{1}{5^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \ldots \end{aligned}$$

Nyní nám zbyl součet čísel, u kterých je základ jmenovatele nesoudělný s číslem 6. Pokud celý postup zopakujeme i pro pětku dostáváme:

$$\left(1 - \frac{1}{5^s}\right)\left(1 - \frac{1}{3^s}\right)\left(1 - \frac{1}{2^s}\right)\zeta(s) = \frac{1}{1^s} + \frac{1}{7^s} + \frac{1}{11^s} + \frac{1}{13^s} + \frac{1}{17^s} + \ldots$$

Tedy součet, kde základ jmenovatelů je nesoudělný s číslem 30. Pokud bychom takto pokračovali pro všechna prvočísla, tak z pravé strany odstraníme všechny jejich násobky a tak zbude pouze číslo 1 (označme $\mathbb{P}$ množinu všech prvočísel):

$$\zeta(s)\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)=1.$$

Tedy:

$$\zeta(s)=\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)^{-1}. \tag{3.2}$$

Tím pádem se nám podařilo vyjádřit $\zeta(s)$ v závislosti na prvočíslech.

Na závěr si ještě ukažme další vztahy podobné Eulerovu vzorci. Začněme tím, že určeme $\zeta(s)^{-1}$. Upravujme vzorec 3.2.

$$\begin{aligned}
\zeta(s)&=\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)^{-1}\\
\zeta(s)^{-1}&=\prod_{p\in\mathbb{P}}\left(1-\frac{1}{p^s}\right)\\
\zeta(s)^{-1}&=\left(1-\frac{1}{2^s}\right)\left(1-\frac{1}{3^s}\right)\left(1-\frac{1}{5^s}\right)\left(1-\frac{1}{7^s}\right)\cdots
\end{aligned}$$

Je vidět, že výsledkem součinu bude nějaký součet zlomků, které budou mít ve jmenovateli přirozená čísla umocněná na s-tou a v čitateli budou mít jedničku – po roznásobení totiž, vzhledem k základní větě aritmetiky, nemohou ve jmenovateli být u 2 různých zlomků 2 stejná čísla. Zkoumejme, která přirozená čísla mohou ve jmenovateli být. Určitě v součtu vznikne číslo 1 – bude to člen, který vznikne tak, že se při roznásobování vynásobí všechny jedničky. Určitě taky vznikne libovolné prvočíslo p – vynásobíme $\frac{-1}{p^s}$ se samými jedničkami. Důležité je všimnout si, že ve výsledném součtu bude se znaménkem mínus. A určitě také mohou vzniknout i čísla, která jsou součinem libovolného počtu různých prvočísel. A naopak nemohou vzniknout čísla, která nejsou dělitelná druhou mocninou libovolného prvočísla. Tedy ve výsledku dostáváme:

$$\begin{aligned}
\zeta(s)^{-1}&=\frac{1}{1^s}-\frac{1}{2^s}-\frac{1}{3^s}-\frac{1}{5^s}+\frac{1}{6^s}-\frac{1}{7^s}+\frac{1}{10^s}+\ldots,\\
&=\sum_{n=1}^{\infty}\frac{\mu(n)}{n^s}.
\end{aligned}$$

Vypočtěme nyní $\zeta(s)^2$. Postupujme podle definice zeta funkce:

$$\zeta(s)^2 = \left(\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots\right)\left(\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots\right).$$

Opět po roznásobení určitě dostaneme součet zlomků, ale tentokrát budou všechny kladné. Navíc se tentokrát ve jmenovatelích těchto zlomků objeví všechna přirozená čísla (umocněná na s-tou), protože po roznásobení jeden ze sčítanců bude tvaru $\frac{1}{1^s}\frac{1}{n^s}$. Kolika způsoby ale můžeme vytvořit zlomek se jmenovatelem n^s? No pro každého dělitele čísla n právě jedním. Ale počet dělitelů daného čísla jsme určovali na začátku celého textu, a tak dostáváme:

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

Analogicky můžeme dostat různá další tvrzení. Určeme $\zeta(s)\zeta(s-1)$:

$$\begin{aligned}\zeta(s)\zeta(s-1) &= \left(\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots\right)\left(\frac{1}{1^{s-1}} + \frac{1}{2^{s-1}} + \frac{1}{3^{s-1}} + \frac{1}{4^{s-1}} + \frac{1}{5^{s-1}} + \dots\right), \\ &= \left(\frac{1}{1^s} + \frac{1}{2^s} + \frac{1}{3^s} + \frac{1}{4^s} + \frac{1}{5^s} + \dots\right)\left(\frac{1}{1^s} + \frac{2}{2^s} + \frac{3}{3^s} + \frac{4}{4^s} + \frac{5}{5^s} + \dots\right).\end{aligned}$$

Stejně jako v předchozím příkladě platí, že výsledek roznásobení bude součet zlomků, které budou kladné, a jejich jmenovatelé budou všechna přirozená čísla umocněná na s-tou. A do čitatele zlomku se jmenovatelem n^s přispějí všichni dělitelé čísla n. Zatímco v předchozím příkladě každý přispěl číslem 1, tak nyní bude v čitateli součet všech dělitelů. Tedy:

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

Pokud si vzpomeneme na funkci σ_k z poznámky 1.1.1, tak můžeme poslední úvahy zobecnit:

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

Našli jsme tedy souvislost Riemannovy hypotézy s multiplikativními funkcemi.

Závěr

V průběhu první kapitoly jsme se seznámili se spoustou multiplikativních funkcí. Ukázali jsme si různé jejich vlastnosti, které většinou plynuly ze základní věty aritmetiky.

V druhé kapitole jsme se seznámili s Dirichletovým součinem. Ten byl důležitý zejména pro zavedení Möbiovy inverzní formule. Möbiova inverzní formule je zajímavé tvrzení, jejíž využití se prolíná různými oblastmi matematiky. Möbiových inverzních formulí totiž existuje více druhů než jen ten, který byl ukázán v této práci. Následně jsme mluvili o Eulerově funkci, která je jednou z možných aplikací Möbiovy inverzní formule, a nakonec jsme si ukázali, co to jsou Fareyovy zlomky, které souvisí právě s Eulerovou funkcí.

V poslední kapitole jsme se věnovali jednomu z největších nevyřešených problémů současné matematiky – Riemannově hypotéze. Jedná se o problém, jehož krása spočívá v tom, že propojuje dvě na první pohled velice vzdálené matematické disciplíny – analýzu a teorii čísel. Nejprve jsme vysvětlili, v čem problém spočívá a následně jsme si nastínili souvislost s teorií čísel a multiplikativními funkcemi. Hlavním důvodem, proč je Riemannova hypotéza tak důležitá, je její souvislost s rozložením prvočísel. Bernhard Riemann, po kterém je hypotéza pojmenovaná, byl německý matematik, který za celý život napsal jedinou známou práci týkající se teorie čísel. V této práci objevil úžasný vztah, který vyjadřuje funkci, která počítá počet prvočísel menších než daná hodnota v závislosti na zeta funkci a výrazu souvisejícím s jejími netriviálními nulovými body. Kdyby byla Riemannova hypotéza dokázána, tak bychom dokázali poměrně přesně určit počet prvočísel menších než daná hodnota. Bohužel pochopení Riemannových metod vyžaduje velice rozsáhlé znalosti komplexní analýzy.

Literatura

[1] PUPÍK, Petr. *Ireducibilní polynomy nad konečnými tělesy* [online]. Brno, 2007 [cit. 2017-02-02]. Dostupné z: http://is.muni.cz/th/150640/prif_b/. Bakalářská práce. Masarykova univerzita, Přírodovědecká fakulta. Vedoucí práce Radan Kučera.

[2] HARDY, G. H. a E. M. WRIGHT. *An introduction to the theory of numbers* [online]. 4th ed. Oxford: Clarendon Press, 1975 [cit. 2017-02-02]. ISBN 0-19-853310-7. Dostupné z: http://matematica.cubaeduca.cu/medias/pdf/842.pdf

[3] AINSWORTH Jonathan, Michael DAWSON, John PIANTA a James WARWICK. *The Farey Sequence* [online]. Edinburgh, 2012 [cit. 2017-01-28]. Dostupné z: http://www.maths.ed.ac.uk/~aar/fareyproject.pdf

[4] RÁB, Miloš. *Komplexní čísla a jejich užití v elementární matematice: určeno pro posl. fak. přírodovědecké*. Brno: Masarykova univerzita, 1990. ISBN 80-210-0207-7.

[5] FOLTÝNOVÁ, Patricie. *Problémy milénia: Riemannova hypotéza* [online]. Olomouc, 2011 [cit. 2017-02-05]. Dostupné z: http://theses.cz/id/2vytq5/. Bakalářská práce. Univerzita Palackého v Olomouci, Přírodovědecká fakulta. Vedoucí práce RNDr. Tomáš Fürst, Ph.D.

[6] Weisstein, Eric W. *Logarithmic integral*. In: MathWorld a Wolfram web resource [online]. Wolfram Research, Inc., ©1999-2017 [cit. 2017-02-09]. Dostupné z: http://mathworld.wolfram.com/LogarithmicIntegral.html

[7] Stankova, Zvezdelina. *Multiplicative functions and Möbius inversion formula* [online]. In: Stanford Math Circle. Stanford, Stanford Pre-Collegiate Studies [cit. 2017-02-09]. Dostupné z: http://precollegiate.stanford.edu/circle/math/notes09w/Multiplicative.pdf

[8] Weisstein, Eric W. *Analytic continuation*. In: MathWorld a Wolfram web resource [online]. Wolfram Research, Inc., ©1999-2017 [cit. 2017-02-09]. Dostupné z: http://mathworld.wolfram.com/AnalyticContinuation.html

[9] *Riemann hypothesis*. In: Wikipedia, the free encyclopedia [online]. St. Petersburg (Florida), Wikipedia Foundation, last modified on 8 February 2017 [cit. 2017-02-09]. Dostupné z: https://en.wikipedia.org/wiki/Riemann_hypothesis

[10] Riemann, Bernhard 1859. *On the number of prime numbers less than a given quantity* [online]. Translated by D. R. Wilkins, preliminary version December 1998 [cit. 2017-02-09]. Dostupné z: `http://www.maths.tcd.ie/pub/HistMath/People/Riemann/Zeta/EZeta.pdf`

[11] *Riemann zeta function*. In: Wikipedia, the free encyclopedia [online]. St. Petersburg (Florida), Wikipedia Foundation, last modified on 8 February 2017 [cit. 2017-02-09]. Dostupné z: `https://en.wikipedia.org/wiki/Riemann_zeta_function`

[12] *Farey sequence*. In: Wikipedia, the free encyclopedia [online]. St. Petersburg (Florida), Wikipedia Foundation, last modified on 28 January 2017 [cit. 2017-02-09]. Dostupné z: `https://en.wikipedia.org/wiki/Farey_sequence`

[13] Komplexní čísla. In: *Matematický korespondenční seminář* [online]. Praha, 2011 [cit. 2017-02-15]. Dostupné z: urlhttps://mks.mff.cuni.cz/archive/30/9.pdf