PŘÍRODOVĚDECKÁ FAKULTA UNIVERZITY PALACKÉHO
KATEDRA ALGEBRY A GEOMETRIE

# BAKALÁŘSKÁ PRÁCE

Některé nestandardní důkazy klasických tvrzení

2014

Petr Sapák

Prohlašuji, že jsem tuto bakalářskou práci vypracoval samostatně pod vedením prof. Mgr. Radomíra Halaše, Dr. a že jsem uvedl veškerou použitou literaturu.

V Olomouci 30. května 2014 .....

Rád bych poděkoval svému vedoucímu bakalářské práce panu prof. Mgr. Radomíru Halašovi, Dr. za cenné rady, připomínky a za ochotu ujmout se vedení mého tématu.

# Obsah

# Úvod

Hlavním cílem bakalářské práce je nastudovat a zpracovat nestandardní a neobvyklé metody použité při dokazování některých klasických matematických tvrzení. Motivací k výběru tohoto tématu bylo seznámení se s knihou *Proofs from the Book* a absence jejího ekvivalentu v českém jazyce. Zdaleka se však nejedná o jedinou publikaci, ze které jsem čerpal.

Ve většině případů jsou důkazům jednotlivých tvrzení věnovány celé kapitoly. Pouze ve dvou případech jsou v jedné kapitole uvedeny dva různé důkazy stejného tvrzení. Kapitoly, pokud je to nutné, začínají definicí použitých pojmů z příslušných matematických disciplín.

Důkazy jsem vybral podle svého uvážení, případně na doporučení vedoucího mé práce. Jedná se především o důkazy vět z teorie čísel, dále pak algebry, kombinatoriky a teorie grafů.

# 1 Nekonečnost množiny prvočísel

Čím jiným začít práci o zajímavých důkazech, než kapitolou o nekonečnosti množiny prvočísel. Ta fascinují matematiky již dva a půl tisíce let. První notoricky známý důkaz, který podal Eukleides ve svých *Základech*, zde uvádět nebudeme. Nejedná se totiž o nikterak nestandardní důkaz, ale o vyjádření naprosto přesné myšlenky, která jde přímo k jádru problému. Zájemcům o problematiku tohoto důkazu lze doporučit knihu [3].

Počet důkazů jistě převyšuje několik desítek, ale v této práci uvedeme pouze dva z nich. Poznamenejme, že v celém textu budeme množinu všech prvočísel značit $\mathbb{P}$.

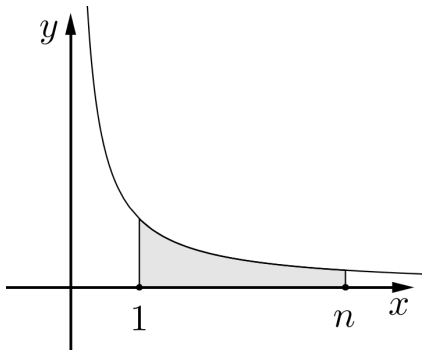
## 1.1 Eulerův důkaz

První důkaz pochází od Leonharda Eulera[1]. Jedná se o použití metody odhadu pomocí integrálů, která není nikterak složitá, a přesto nám dává pozoruhodné výsledky.

Jádrem důkazu jsou vhodné odhady funkce $\ln x$. Vycházejme z rovnosti

$$\ln n = \int_1^n \frac{1}{t}\mathrm{d}t.$$

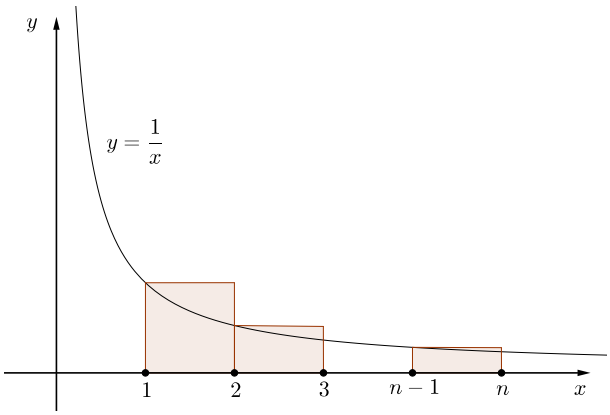
Vidíme, že hodnota $\ln n$ vyjadřuje obsah plochy ohraničené grafem funkce $y = \frac{1}{t}$, osou $x$ a přímkami $x = 1$ a $x = n$ (viz obrázek 1).




Obrázek 1: Geometrické znázornění $\ln n$

[1]Leonhard Euler (1707-1783). Švýcarský matematik a fyzik, bývá považován za nejvýznamějšího matematika 18. století.

Dalším krokem je uvědomění si geometrického významu součtu $\sum_{k=1}^{n} \frac{1}{k}$, který můžeme vidět na následujícím obrázku.




Obrázek 2: Geometrické znázornění $\sum_{k=1}^{n} \frac{1}{k}$

Porovnáme-li oba obrázky, vidíme, že platí následující nerovnost:

$$\sum_{k=2}^{n} \frac{1}{k} \quad > \quad \int_1^n \frac{1}{t} \mathrm{d}t.$$

Ta je naším hledaným, pro důkaz dostačujícím odhadem.

**D ů k a z.** Nechť $\mathbb{P} = \{p_1, p_2, p_3, \ldots\}$ je množina prvočísel uspořádaných podle velikosti. Dále nechť $\pi(x) := |\{p \leq x : \ p \in \mathbb{P}\}|$ pro $x \in \mathbb{R}$ je počet všech prvočísel, která jsou menší nebo rovna $x$.

Budeme porovnávat plochu ohraničenou grafem funkce $f(t) = \frac{1}{t}$ s horní schodovitou funkcí (viz obrázek 2). Pro $n \leq x < n+1$ dostáváme

$$\ln x \quad \leq \quad 1 + \frac{1}{2} + \frac{1}{3} + \cdots + + \frac{1}{n-1} + \frac{1}{n} \quad \leq \quad \sum_{p \leq x} \frac{1}{m}, \tag{1}$$

kde v poslední sumě sčítáme přes všechna $m \in \mathbb{N}$, která mají pouze prvočíselné dělitele $p \leq x$. Je zřejmé, že každé takové $m$ můžeme jednoznačně napsat jako součin $\prod_{p \leq x} p^{k_p}$. Pak ale vidíme, že poslední sumu lze přepsat do tvaru

$$\prod_{\substack{p \in \mathbb{P} \\ p \leq x}} \left( \sum_{k \geq 0} \frac{1}{p^k} \right).$$

Všimněme si, že vnitřní suma je geometrickou řadou s kvocientem $\frac{1}{p}$, její součet je roven $\frac{1}{1-\frac{1}{p}}$. Přepišme nerovnost (1) takto:

$$\ln x \quad \leq \quad \prod_{\substack{p\in\mathbb{P}\\ p\leq x}} \frac{1}{1-\frac{1}{p}} \quad = \quad \prod_{\substack{p\in\mathbb{P}\\ p\leq x}} \frac{p}{p-1} \quad = \quad \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k-1}.$$

Je zřejmé, že $p_k \geq k+1$, a tedy

$$\frac{p_k}{p_k-1} \quad = \quad 1+\frac{1}{p_k-1} \quad \leq \quad 1+\frac{1}{k} \quad = \quad \frac{k+1}{k}.$$

Můžeme odhadnout

$$\ln x \quad \leq \quad \prod_{k=1}^{\pi(x)} \frac{k+1}{k} \quad = \quad \pi(x)+1.$$

Víme, že funkce $\ln x$ je neomezená, a tedy ani její horní odhad není omezený. Z toho vyplývá, že i funkce $\pi(x)$ je neomezená, a tedy $\mathbb{P}$ je nekonečná.

□

Všimněme si, že nám výše uvedený důkaz dává metodu jak odhadnout, kolik existuje prvočísel menších než dané přirozené číslo $n$.

## 1.2 Erdösův kombinatorický důkaz

Následující důkaz využívá kombinatoriky a pochází od Paula Erdöse[2]. Dokazuje dokonce mnohem více. Například to, že řada $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverguje. Připomeňme, že $\lfloor x \rfloor$ značí dolní celou část čísla $x$.

**D ů k a z.** Nechť $p_1, p_2, p_3, \ldots$ jsou prvočísla, která jsme seřadili vzestupně a dále předpokládejme sporem, že řada $\sum_{p\in\mathbb{P}} \frac{1}{p}$ konverguje. Musí tedy existovat číslo $k \in \mathbb{N}$ takové, že

$$\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}. \tag{2}$$

Nyní si rozdělme prvočísla do dvou množin, na „malá“ a „velká“. Malá prvočísla $p_1, p_2, \ldots, p_k$ a $p_{k+1}, p_{k+2}, \ldots$ velká prvočísla.

[2]Paul Erdős (1913-1996). Maďarský matematik, zabýval se kombinatorikou, teorií grafů, čísel a dalšími oblastmi matematiky. Jeden z nejvýznamnějších matematiků 20. století.

Z (2) plyne, že pro libovolné $l \in \mathbb{N}$ platí:

$$\sum_{i \geq k+1} \frac{l}{p_i} < \frac{l}{2}.$$

Označme $l_v$ počet kladných čísel $n \leq l$, která jsou dělitelná alespoň jedním velkým prvočíslem a $l_m$ počet kladných $n \leq l$, která jsou dělitelná pouze malými prvočísly. Ukážeme, že pro určité $l$ platí

$$l_m + l_v < l,$$

což bude spor, protože podle definice musí pro všechna $l$ platit

$$l_m + l_v = l.$$

Chceme tedy odhadnout $l_m$ a $l_v$. Všimněme si, že $\lfloor \frac{l}{p_i} \rfloor$ je počet kladných $n \in \mathbb{N}$, $n \leq l$, která jsou násobkem $p_i$. Tudíž z (2) dostáváme

$$l_v \leq \sum_{i \geq k+1} \left\lfloor \frac{l}{p_i} \right\rfloor < \frac{l}{2}. \tag{3}$$

Nyní potřebujeme odhadnout $l_m$. Každé $n \leq l$, které má pouze malá prvočísla jako dělitele, napíšeme ve tvaru $n = a_n b_n^2$, kde $a_n$ není čtvercem žádného čísla. Tudíž $a_n$ je součinem různých malých prvočísel. Takových $a_n$ je $2^k$. Počet čísel $b_n$ lze odhadnout:

$$b_n \leq \sqrt{n} \leq \sqrt{l},$$

a tedy

$$l_m \leq 2^k \sqrt{l}.$$

Jelikož (3) platí pro libovolné $l$, zbývá najít takové číslo $l$, pro které

$$2^k \sqrt{l} < \frac{l}{2},$$

neboli

$$2^{k+1} < \sqrt{l}.$$

Stačí položit $l = 2^{2k+2}$, a dostaneme spor.

□

# 2 Eulerova řada

Je dobře známo, že nekonečná řada $\sum_{n\geq 1}\frac{1}{n}$ (tzv. harmonická řada) diverguje. Lze to lehce dokázat např. použitím integrálního kritéria. Nicméně je velmi zajímavé, že nekonečná řada převrácených mocnin kvadrátů přirozených čísel dává pozoruhodnou hodnotu. Platí totiž následující vztah:

$$\sum_{n\geq 1}\frac{1}{n^2}=\frac{\pi^2}{6}.$$

Na tento důležitý výsledek přišel roku 1734 Leonhard Euler.

## 2.1 Důkaz pomocí dvojného integrálu

**D ů k a z.** Provedeme důkaz pocházející od Williama J. LeVequa[3], který se objevil jako cvičení v jeho knize o teorii čísel z roku 1956. Hlavní myšlenkou je zde dvojí různý výpočet dvojného integrálu

$$I:=\int_0^1\int_0^1\frac{1}{1-xy}\mathrm{d}x\,\mathrm{d}y.$$

V prvním případě vyjádříme $\frac{1}{1-xy}$ jako geometrickou řadu a integrujeme:

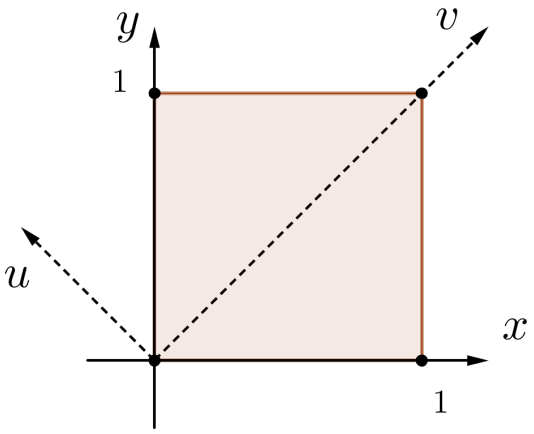
$$I=\int_0^1\int_0^1\frac{1}{1-xy}\mathrm{d}x\mathrm{d}y=\int_0^1\int_0^1\sum_{n\geq 0}(xy)^n\mathrm{d}x\mathrm{d}y=\sum_{n\geq 0}\int_0^1\int_0^1 x^n y^n\mathrm{d}x\mathrm{d}y=$$

$$=\sum_{n\geq 0}\left(\int_0^1 x^n\mathrm{d}x\right)\left(\int_0^1 y^n\mathrm{d}y\right)=\sum_{n\geq 0}\left[\frac{x^{n+1}}{n+1}\right]_0^1\left[\frac{y^{n+1}}{n+1}\right]_0^1=$$

$$=\sum_{n\geq 0}\frac{1}{n+1}\frac{1}{n+1}=\sum_{n\geq 0}\frac{1}{n+1^2}=\sum_{n\geq 1}\frac{1}{n^2}.$$

Toto vyčíslení nám ukazuje, že uvedený dvojný integrál je konečný.

[3]William Judson LeVeque (1923–2007). Americký matematik, který se zabýval především teorií čísel. V 70. a 80. letech byl výkonným ředitelem American Mathematical Society.

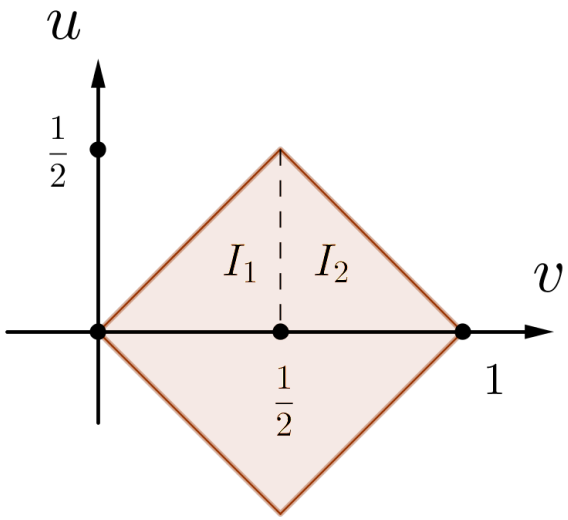



Obrázek 3: První vyčíslení dvojného integrálu

Nyní provedeme výpočet $I$ jiným způsobem. Změníme souřadnice takto:

$$u = \frac{x+y}{2}; \quad v = \frac{x-y}{2}.$$

Původní čtverec se transformuje na menší a pootočený o 45° (viz obrázek 4).




Obrázek 4: Transformace souřadnic

Provedeme-li substituci $x = u - v$ a $y = u + v$, dostaneme

$$\frac{1}{1-xy} = \frac{1}{1-u^2+v^2}.$$

Spočítejme Jakobián této transformace. Označíme-li $g : x = u - v$ a $h : y = u + v$, dostaneme Jakobián ve tvaru

$$J = \begin{vmatrix} \frac{\mathrm{d}g}{\mathrm{d}u} & \frac{\mathrm{d}g}{\mathrm{d}v} \\ \frac{\mathrm{d}h}{\mathrm{d}u} & \frac{\mathrm{d}h}{\mathrm{d}v} \end{vmatrix} = \begin{vmatrix} 1 & -1 \\ 1 & 1 \end{vmatrix} = 2.$$

Součin diferenciálů $\mathrm{d}x\mathrm{d}y$ se tedy transformuje na $2\,\mathrm{d}u\mathrm{d}v$. Uvědomme si, že díky symetrii oblasti integrace (viz obrázek 4) lze integrovaný výraz přepsat na tvar

$$I = 4\int_0^{\frac{1}{2}} \left( \int_0^u \frac{\mathrm{d}v}{1-u^2+v^2} \right) \mathrm{d}u + 4\int_{\frac{1}{2}}^1 \left( \int_0^u \frac{\mathrm{d}v}{1-u^2+v^2} \right) \mathrm{d}u.$$

Lze si všimnout, že můžeme použít vzorec

$$\int \frac{\mathrm{d}x}{a^2+x^2} = \frac{1}{a} \operatorname{arctg} \frac{x}{a} + C.$$

Dostaneme tedy vyjádření ve tvaru

$$I = \underbrace{4\int_0^{\frac{1}{2}} \frac{1}{\sqrt{1-u^2}} \operatorname{arctg}\left( \frac{u}{\sqrt{1-u^2}} \right) \mathrm{d}u}_{I_1} + \underbrace{4\int_{\frac{1}{2}}^1 \frac{1}{\sqrt{1-u^2}} \operatorname{arctg}\left( \frac{1-u}{\sqrt{1-u^2}} \right) \mathrm{d}u}_{I_2}.$$

Vypočítáme každý z integrálů zvlášť.

$$I_1 = 4\int_0^{\frac{1}{2}} \frac{1}{\sqrt{1-u^2}} \operatorname{arctg}\left( \frac{u}{\sqrt{1-u^2}} \right) \mathrm{d}u = \begin{vmatrix} u = \sin z \\ \mathrm{d}u = \cos z\,\mathrm{d}z \\ u = \frac{1}{2} \quad z = \frac{\pi}{6} \\ u = 0 \quad z = 0 \end{vmatrix} =$$

$$= 4\int_0^{\frac{\pi}{6}} \frac{\cos z\,\mathrm{d}z}{\sqrt{1-\sin z^2}} \operatorname{arctg}\left( \frac{\sin z}{\sqrt{1-\sin z^2}} \right) = 4\int_0^{\frac{\pi}{6}} \operatorname{arctg}\left( \frac{\sin z}{\cos z} \right) \mathrm{d}z =$$

$$= 4 \int_0^{\frac{\pi}{6}} z \,\mathrm{d}z = 2 \left[z^2\right]_0^{\frac{\pi}{6}} = \frac{\pi^2}{18}.$$

Nyní vypočtěme $I_2$:

$$I_2 = 4 \int_{\frac{1}{2}}^{1} \frac{1}{\sqrt{1-u^2}} \operatorname{arctg}\left(\frac{1-u}{\sqrt{1-u^2}}\right) \mathrm{d}u = \left| \begin{array}{c} u = \sin z \\ \mathrm{d}u = \cos z \,\mathrm{d}z \\ u = 1 \quad z = \frac{\pi}{2} \\ u = \frac{1}{2} \quad z = \frac{\pi}{6} \end{array} \right| =$$

$$= 4 \int_{\frac{\pi}{6}}^{\frac{\pi}{2}} \operatorname{arctg}\left(\frac{1-\sin z}{\cos z}\right) \mathrm{d}z = \textit{per partes} \left| \begin{array}{ccc} f = \arctan\left(\frac{1-\sin z}{\cos z}\right) & & f' = -\frac{1}{2}\,\mathrm{d}z \\ g = z & & g' = \mathrm{d}z \end{array} \right| =$$

$$= \left[4v \operatorname{arctg}\left(\frac{1-\sin z}{\cos z}\right)\right]_{\frac{\pi}{6}}^{\frac{\pi}{2}} + 2 \int_{\frac{\pi}{6}}^{\frac{\pi}{2}} z \,\mathrm{d}z = -\frac{\pi^2}{9} + 2 \left[\frac{z^2}{2}\right]_{\frac{\pi}{6}}^{\frac{\pi}{2}} = -\frac{\pi^2}{9} + 2\frac{\pi^2}{9} = \frac{\pi^2}{9}.$$

Sečteme-li $I_1$ a $I_2$, dostaneme hledanou hodnotu $I$:

$$I = \frac{\pi^2}{18} + \frac{\pi^2}{9} = \frac{\pi^2}{6}.$$

Porovnáním obou způsobů výpočtu $I$ dostaneme dokazované tvrzení.

□

## 2.2 Důkaz algebraický

Po důkazu, ve kterém jsme pracovali s transformacemi souřadnic, ukážeme důkaz více algebraický. První zmínka o něm pochází z knihy Challenging Mathematical Problems with Elementary Solutions, jejímiž autory jsou bratři Akiva[4] a Isaak[5] Yaglom. Kniha byla poprvé vydána v roce 1954. Důkaz byl později zapomenut, aby mohl být v 80. letech znovu objeven.

[4]Akiva Moiseevich Yaglom (1921- 2007). Ruský fyzik, matematik, statistik a meteorolog, proslavil se svou prací ve statistické teorii turbulencí a teorii náhodných procesů.

[5]Isaak Moiseevich Yaglom (1921 - 1988). Ruský matematik a autor populárních matematických knih.

**D ů k a z.** Myšlenka důkazu spočívá v ohraničení uvažované sumy zdola i shora výrazy konvergujícími k uvedeném součtu.

Nechť $x$ je reálné číslo z intervalu $0 < x < \frac{\pi}{2}$ a $n$ nechť je liché přirozené číslo. Z Moivreovy věty a definice funkce kotangens dostáváme

$$\frac{\cos(nx) + \mathrm{i}\sin(nx)}{\sin^n x} = \frac{(\cos x + \mathrm{i}\sin x)^n}{\sin^n x} = \left(\frac{\cos x + \mathrm{i}\sin x}{\sin x}\right)^n = (\operatorname{cotg} x + \mathrm{i})^n.$$

Nyní uvažujme binomický rozvoj posledního výrazu:

$$(\operatorname{cotg} x + \mathrm{i})^n = \binom{n}{0} \operatorname{cotg}^n x + \ldots + \binom{n}{n-1} (\operatorname{cotg} x)\mathrm{i}^{n-1} + \binom{n}{n} \mathrm{i}^n.$$

Ten má po rozdělení na reálnou a imaginární část tvar

$$\begin{aligned} &\left[\binom{n}{0} \operatorname{cotg}^n x - \binom{n}{2} \operatorname{cotg}^{n-2} x \pm \ldots\right] + \\ +\mathrm{i}&\left[\binom{n}{1} \operatorname{cotg}^{n-1} x - \binom{n}{3} \operatorname{cotg}^{n-3} x \pm \ldots\right]. \end{aligned}$$

Porovnáním imaginárních částí obou rovností dostaneme

$$\frac{\sin(nx)}{\sin^n x} = \left[\binom{n}{1} \operatorname{cotg}^{n-1} x - \binom{n}{3} \operatorname{cotg}^{n-3} x \pm \ldots\right].$$

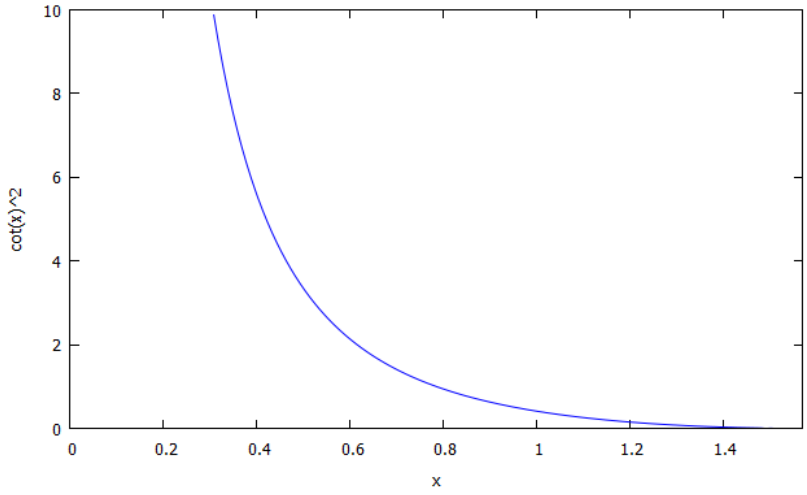
Vezměme tuto identitu a zvolme kladné číslo $m$ tak, že $n = 2m + 1$. Uvažujme $x_r = \frac{r\pi}{2m+1}$ pro $r = 1, 2, \ldots, m$. Pak je vidět, že $nx_r$ je násobkem $\pi$, a tudíž je pro něj hodnota funkce sinus rovna nule. Po dosazení dostáváme

$$0 = \binom{2m+1}{1} \operatorname{cotg}^{2m} x_r - \binom{2m+1}{3} \operatorname{cotg}^{2m-2} x_r \pm \ldots + (-1)^m \binom{2m+1}{2m+1}.$$

Hodnoty $x_1, x_2, \ldots, x_m$ jsou čísla z intervalu $(0, \pi/2)$. Jelikož funkce $\operatorname{cotg}^2 x$ je na tomto intervalu prostá (viz obrázek 5), čísla $t_r = \operatorname{cotg}^2 x_r$ jsou různá pro $r = 1, 2, \ldots, m$.

Podíváme-li se na poslední rovnost, vidíme, že tato čísla jsou kořeny polynomu $m$-tého stupně

$$p(t) := \binom{2m+1}{1} t^m - \binom{2m+1}{3} t^{m-1} \pm \ldots + (-1)^m \binom{2m+1}{2m+1}.$$




Obrázek 5: $\operatorname{cotg}^2 x$ na intervalu $(0, \pi/2)$

Použitím Viètových vztahů získáme součet kořenů ve tvaru

$$\operatorname{cotg}^2 x_1 + \operatorname{cotg}^2 x_2 + \ldots + \operatorname{cotg}^2 x_m = \frac{\binom{2m+1}{3}}{\binom{2m+1}{1}} = \frac{\frac{(2m+1)!}{6(2m-2)!}}{\frac{(2m+1)!}{2m!}} = \frac{2m(2m-1)}{6}.$$

Nalezli jsme jeden ohraničující výraz. Funkce kosekans se dá v závislosti na funkci kotangens vyjádřit takto:

$$\operatorname{cosec}^2 x = \frac{1}{\sin^2 x} = \frac{\sin^2 x + \cos^2 x}{\sin^2 x} = 1 + \frac{\cos^2 x}{\sin^2 x} = 1 + \operatorname{cotg}^2 x.$$

Použitím výše uvedeného vztahu dostáváme

$$\operatorname{cosec}^2 x_1 + \operatorname{cosec}^2 x_2 + \ldots + \operatorname{cosec}^2 x_m = \frac{2m(2m-1)}{6} + m = \frac{2m(2m+2)}{6}.$$

Nyní použijeme následující nerovnost pro $0 < x < \frac{\pi}{2}$:

$$0 < \sin^2 x < x^2 < \tan^2 x.$$

Tudíž pro převrácené hodnoty dostáváme na uvedeném intervalu nerovnost

$$\operatorname{cotg}^2 x < \frac{1}{x^2} < \operatorname{cosec}^2 x.$$

Sečtením posledních nerovností pro všechna čísla $x_r = \frac{r\pi}{2m+1}$ s využitím uvedených ohraničení dostaneme nerovnosti

$$\frac{2m(2m-1)}{6} < \left(\frac{2m+1}{\pi}\right)^2 + \ldots + \left(\frac{2m+1}{m\pi}\right)^2 < \frac{2m(2m+2)}{6}.$$

Dále upravíme nerovnosti do požadovaného tvaru. Vynásobíme je výrazem $\frac{\pi^2}{(2m+1)^2}$ a dostaneme

$$\frac{\pi^2}{6}\left(\frac{2m}{2m+1}\right)\left(\frac{2m-1}{2m+1}\right) < 1 + \frac{1}{2^2} + \ldots + \frac{1}{m^2} < \frac{\pi^2}{6}\left(\frac{2m}{2m+1}\right)\left(\frac{2m+2}{2m+1}\right).$$

V limitě $m$ jdoucí k nekonečnu posloupnosti na pravé i levé straně nerovností konvergují k $\frac{\pi^2}{6}$. Podle věty o třech limitách platí, že

$$\sum_{k=1}^{\infty} \frac{1}{k^2} = \lim_{m\to\infty}\left(1 + \frac{1}{2^2} + \frac{1}{3^2} + \ldots + \frac{1}{m^2}\right) = \frac{\pi^2}{6}.$$

□

# 3 Fermatova věta

Není téměř možné psát o důkazech z teorie čísel a nenarazit na alespoň jednu hypotézu, pod níž by nebyl podepsán Pierre de Fermat[6]. Podrobný důkaz jednoho z Fermatových tvrzení, který si ukážeme, pochází od Leonharda Eulera. V následujícím textu budeme největší společný dělitel čísel $a$ a $b$ značit takto $(a, b)$.

**Věta 1 (Fermatova)** [7] *Číslo ve tvaru $p = 4k + 1$ je prvočíslem, právě když jej lze jednoznačně vyjádřit jako součet dvou nesoudělných kvadrátů.*

Uveďme nejprve následující pomocná tvrzení, která později v důkaze použijeme:

**Věta 2 (Eukleidova)** *Je-li $p$ prvočíslo a $p \mid ab$, pak $p \mid a$ nebo $p \mid b$.*

**D ů k a z.** Předpokládejme, že $p \nmid a$, což znamená, že $(a, p) = 1$. Pak ale existují celá čísla $u, v$ taková, že $au + pv = 1$. Vynásobíme-li poslední rovnost číslem $b$, dostaneme $abu + pbv = b$. Nyní je vidět, že pokud $p \mid ab$, pak i $p \mid b$.

□

**Věta 3 (malá Fermatova věta)** *Jestliže $a \in \mathbb{Z}$ a $p$ je prvočíslo, pak $p \mid (a^p - a)$.*

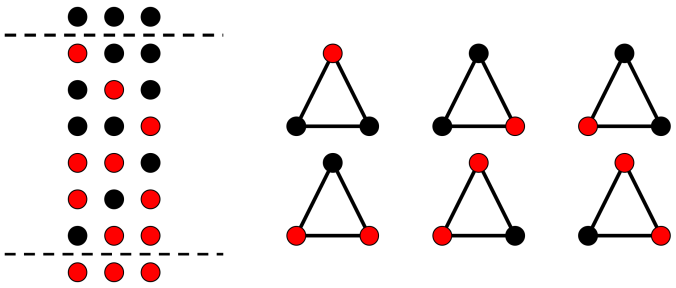
Poznamenejme, že důkazů malé Fermatovy věty existuje celá řada. My si ukážeme důkaz kombinatorický, ve kterém budeme počítat, kolik lze z $p$ korálků o $a$ barvách vytvořit náramků.

**D ů k a z.** Vezměme si $p$ korálků a skládejme je za sebe do řady. V každém kroku máme možnost volit z $a$ barevných variant. Takových řad nám tedy vznikne $a^p$. Uvědomme si, že v tomto počtu jsou zahrnuty i řady obsahující pouze jednobarevné korálky, kterých je $a$. Z toho vyplývá, že počet řad, které nejsou jednobarevné, je $a^p - a$.

Nyní tyto řady spojme do $a^p - a$ různobarevných náramků. Všimněme si, že po spojení dostáváme ke každému náramku $p - 1$ náramků, které se liší pouze tím, že jsou pootočené. Každý různobarevný náramek odpovídá $p$ různým řadám.

[6] Pierre de Fermat (1601 - 1665). Francouzský právník a matematik, spoluzakladatel teorie čísel a teorie pravděpodobnosti, zabýval se matematickou analýzou a analytickou geometrií, je autorem jednoho z nejznámějších tvrzení z teorie čísel - tzv. Velké Fermatovy věty, kterou roku 1995 dokázal Andrew Wiles.

[7] Někdy bývá označována jako „vánoční“ věta viz [8],[13].



Obrázek 6: Ukázka pro případ $a = 2$ a $p = 3$

V tom případě dostáváme pouze

$$\frac{(a^p - a)}{p}$$

od sebe odlišitelných náramků. Toto číslo je přirozené, a proto $p$ dělí $(a^p - a)$.

□

Poslední důležitou součástí důkazu Věty 1 jsou tzv. Viètovy identity

$$(a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2 = (ac - bd)^2 + (ad - bc)^2,$$

které použijeme hned několikrát. Tyto identity použil ve svém prvním důkaze i Fermat, který byl Viètovou prací ovlivněn. Nyní provedeme důkaz Věty 1:

**D ů k a z.** Rozdělíme jej na dvě části. Nejdříve dokážeme jednoznačnost a poté existenci uvedeného rozkladu.

Předpokládejme, že prvočíslo $p = 4k + 1$ se dá zapsat jako součet nesoudělných čtverců dvěma způsoby:

$$p = a^2 + b^2 = c^2 + d^2. \tag{4}$$

Pak

$$a^2d^2 - b^2c^2 = a^2(a^2 + b^2 - c^2) - b^2(c^2 + d^2 - a^2) = a^2(a^2 + b^2) - c^2(c^2 + d^2) = \\ = a^2p - c^2p = p(a^2 - c^2).$$

Odkud plyne, že $p \mid (ad - bc)(ad + bc)$. Pokud by byly obě závorky dělitelné $p$, pak by musel být $p$ dělitelný i jejich součet, a tedy $p \mid 2ad$, z čehož plyne, že $p \mid a$ nebo $p \mid d$. Pak ale z (4) plyne, že také $p \mid b$ nebo $p \mid c$, což by byl spor s předpokladem $(a, b) = (c, d) = 1$.

Vezměme dále součin dvou vyjádření čísla $p$ dle (4):

$$p^2 = (a^2 + b^2)(c^2 + d^2).$$

Tuto rovnost můžeme pomocí Viètových identit přepsat na

$$p^2 = (ac \pm bd)^2 + (ad \pm bc)^2. \tag{5}$$

Víme, že nastane jediná z možností: buď $p \mid (ad - bc)$ nebo $p \mid (ad + bc)$. Podívejme se na první z nich. Je-li $p \mid (ad - bc)$, pak $p^2 \mid (ad - bc)^2$. Z vyjádření (5) plyne, že $p^2 \mid (ac + bd)^2$. Rovnost (5) můžeme vydělit $p^2$:

$$1 = \frac{(ac + bd)^2}{p^2} + \frac{(ad - bc)^2}{p^2}.$$

Pak $ad - bc = 0$, a tedy $ad = bc$. Jelikož $(a, b) = (c, d) = 1$, pak i $a \mid c$, $c \mid a$ a odtud již $a = c$, $b = d$.

Uvažujme druhou možnost: $p \mid (ad + bc)$. Pak $p^2 \mid (ad + bc)^2$. Stejně jako v předchozím případě vydělíme rovnost (5) $p^2$:

$$1 = \frac{(ac - bd)^2}{p^2} + \frac{(ad + bc)^2}{p^2}.$$

Pak $ac - bd = 0$, a tedy $ac = bd$. Vidíme, že $a \mid d$, $d \mid a$ a odtud $a = d$, $b = c$. Máme tedy dokázanou jednoznačnost a nyní zbývá dokázat, že takový rozklad existuje.

Z Fermatovy věty plyne, že každé číslo ve tvaru $4k + 1$, které je součtem čtverců, má pouze prvočíselné dělitele dávající zbytek 1 po dělení 4. Vezměme si dvě taková prvočísla $p_1 = a^2 + b^2$ a $p_2 = c^2 + d^2$, kde $a > b > 0$, $c > d > 0$. Vynásobením a přepsáním opět dle Viètových identit máme

$$p_1p_2 = (ac \pm bd)^2 + (ad \pm bc)^2.$$

Nyní stačí dokázat, že

$$(ac+bd)^2 > (ac-bd)^2, (ac+bd)^2 > (ad \pm bc)^2.$$

První nerovnost vyplývá přímo z požadavku na nenulovost čísel $a, b, c, d$. Dokážeme, že

$$ac+bd > ad+bc > ad-bc.$$

Nerovnost $ad+bc > ad-bc$ plyne přímo z podmínek $a > b > 0$, $c > d > 0$. Zbývá dokázat platnost $ac+bd > ad+bc$. Postupnými úpravami dostaneme nerovnost

$$ac+bd-ad-bc > 0,$$

$$-a(d-c)+b(d-c) > 0,$$

$$(d-c)(b-a) > 0.$$

Poslední rovnost opět plyne z požadavků na vlastnosti čísel $a, b, c, d$. Pro další prvočísla, která dávají zbytek 1 po dělení 4, bychom opět dostali rozklady alespoň dvěma způsoby.

□

# 4 Cayleyho věta o počtu stromů

Věta, jejíž důkaz si v této kapitole uvedeme, patří ke klasickým tvrzením teorie grafů. Jejím autorem je Arthur Cayley[8]. Existuje mnoho různých a různě složitých důkazů, z nichž většina je založena na indukci nebo na nalezení jisté bijekce. Následující důkaz je zajímavý tím, že je zde použita metoda dvojího počítání. Přišel na něj Jim Pitman, profesor z Kalifornské univerzity v Berkeley. Je také ukázkou toho, že i k dávno dokázaným tvrzením se dá zkonstruovat jednoduchý důkaz použitím nových myšlenek. Než začneme s důkazem, definujme některé nezbytné pojmy.

**Definice 1** ***Prostý orientovaný graf*** *$G$ je dvojice $(V, E)$, kde $V$ je* ***množina vrcholů*** *grafu $G$ a $E$, která obsahuje uspořádané dvojce prvků z $V$ ($E \subseteq \binom{V}{2}$), se nazývá* ***množina orientovaných hran*** *grafu $G$.*

Značení hrany orientovaného grafu je znázorněno na obrázku 7.

Obrázek 7: Orientovaná hrana

**Definice 2** ***Cestou*** *$v$ grafu $G = (V, E)$ označujeme posloupnost*

$$P = (v_0, e_1, v_1, \ldots, e_n, v_n),$$

*pro kterou platí $e_i = (v_{i-1}, v_i)$ a navíc $v_i \neq v_j$ pro $i \neq j$.*

**Definice 3** ***Souvislým grafem*** *nazveme graf $v$ němž platí, že pro každé dva vrcholy $x, y \in V$ existuje alespoň jedna cesta z $x$ do $y$.*

**Definice 4** *Graf $H = (V_H, E_H)$ je* ***podgrafem*** *grafu $G = (V_G, E_G)$, jestliže $V_H \subseteq V_G$ a $E_H \subseteq E_G$. Maximální souvislý podgraf grafu nazýváme jeho* ***komponentou****.*

[8] Arthur Cayley (1821-1895). Britský matematik, věnoval se teorii matic a jako první podal moderní definici grupy.

**Definice 5** *Prostý orientovaný graf $T = (V, E)$ nazveme* ***stromem****, jestliže je souvislý a platí $|V| = |E| + 1$.*

**Definice 6** *Dvojici $(T, r)$, kde $T = (V, E)$ je strom a $r \in V$, nazýváme* ***kořenový strom****. Vrchol $r$ nazýváme* ***kořen****.*

**Definice 7** *Les, ve kterém je každý strom kořenový, nazveme* ***kořenovým lesem****.*

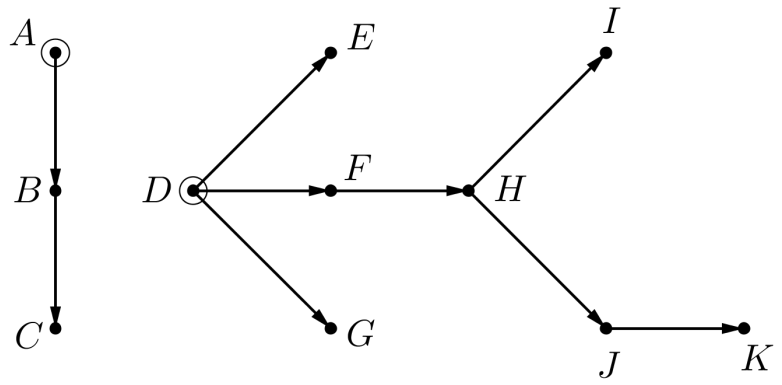
**Věta 4 (Cayleyho věta)** *Pro každé $n \leq 2$ je počet stromů na $n$ vrcholech roven $n^{n-2}$.*

**D ů k a z.** Mějme kořenový les na množině vrcholů $\{1, \ldots, n\}$. Každý strom z tohoto lesa má kořen. Označme $\mathcal{F}_{n,k}$ množinu všech kořenových lesů, které se skládají z $k$ kořenových stromů. Tedy $\mathcal{F}_{n,1}$ je množina všech kořenových stromů.

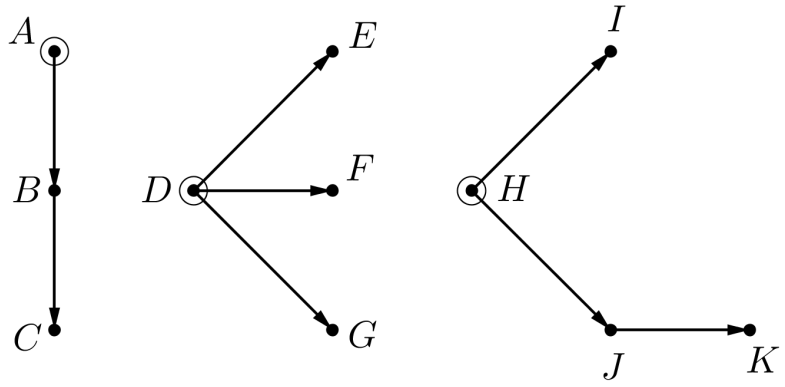
Všimněme si, že $|\mathcal{F}_{n,1}| = nT_n$, kde $T_n$ je strom s $n$ vrcholy, tj. máme $n$ možností pro výběr kořene. Vezměme nyní $F_{n,k} \in \mathcal{F}_{n,k}$ orientovaný strom se všemi hranami směřujícími od kořene. Řekneme, že les $F$ obsahuje jiný les $F'$, jestliže ho obsahuje jako orientovaný podgraf. Je zřejmé, že obsahuje-li $F$ graf $F'$, pak $F$ má méně komponent než $F'$.

Posloupnost $F_1, \ldots, F_k$ lesů nazveme zjemňující posloupností, jestliže $F_i \in \mathcal{F}_{n,i}$ a $F_i$ obsahuje $F_{i+1}$ pro všechna $i$. Nyní nechť $F_k$ je pevně zvolený les v $\mathcal{F}_{n,k}$ a označme

$N(F_k)$ - počet kořenových stromů obsahujících $F_k$,
$N^*(F_k)$ - počet zjemňujících posloupností, které v $F_k$ končí.




Obrázek 8: Kořenový les $F$




Obrázek 9: Kořenový les $F'$

Dále využijeme zmíněné metody dvojího počítání. Vypočítáme $N^*(F_k)$ dvěma způsoby. Nejprve začneme se stromem. Předpokládejme, že $F_1 \in \mathcal{F}_{n,1}$ obsahuje $F_k$. Jelikož můžeme odstranit $k-1$ hran z $F_1 \setminus F_k$ v libovolném pořadí tak, abychom dostali zjemňující posloupnost z $F_1$ na $F_k$, zjišťujeme, že platí

$$N^*(F_k) = N(F_k)(k-1)!. \tag{6}$$

Počítejme hodnotu $N^*(F_k)$ jinak. Abychom dostali $F_{k-1}$ z $F_k$, musíme přidat orientovanou hranu z nějakého vrcholu $a$ do nějakého z $k-1$ kořenů stromů, které neobsahují $a$. Máme tedy $n(k-1)$ možností. Podobně bychom pokračovali v případě $F_{k-1}$ a $F_{k-2}$, kde máme $n(k-2)$ možností. Dostáváme tedy

$$N^*(F_k) = n^{k-1}(k-1)!. \tag{7}$$

Porovnáním rovností (6) a (7) dostáváme $N(F_k) = n^{k-1}$ pro všechna $F_k$ z $\mathcal{F}_{n,k}$.

□

# 5 Eulerova charakteristika planárních grafů

Eulerova (někdy také Euler-Poincarého) charakteristika je číslo, které popisuje topologický tvar nebo strukturu prostoru bez ohledu na to, jak je ohnutý. Euler původně odvodil tuto charakteristiku pro mnohostěny, kde díky ní dokázal mnohá tvrzení a charakterizoval Platónská tělesa.

Dokážeme tvrzení pro rovinné (planární) grafy - tedy pro případ, kdy je charakteristika rovna 2. Věta sama i její důkaz používají pouze elementární pojmy z teorie grafů.

**Definice 8** ***Rovinné nakreslení*** *grafu $G = (V, E)$ je zobrazení $h$, které každému vrcholu $v_i \in V$ přiřadí bod roviny $h(v_i)$ a každé hraně $(v_j, v_k)$ přiřadí oblouk s koncovými vrcholy $h(v_j), h(v_k)$.*

**Definice 9** ***Rovinný graf*** *je graf, pro který existuje takové rovinné nakreslení, že se žádné dvě hrany nekříží.*

**Definice 10** ***Stěnou*** *rovinného grafu nazveme část roviny, ve které lze dva libovolné body spojit souvislou čarou neprotínající žádnou hranu grafu.*

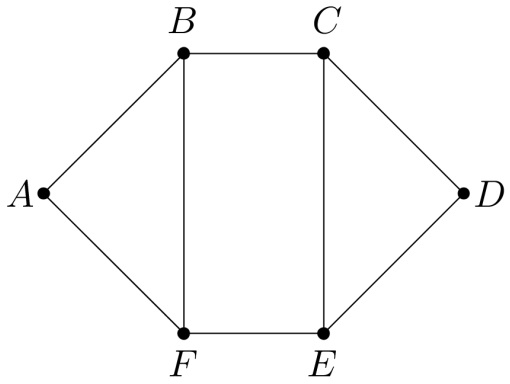
**Definice 11** ***Kostrou*** *souvislého grafu $G$ nazveme takový podgraf na množině všech jeho vrcholů, který je stromem.*

**Definice 12** ***Duálním grafem*** *ke grafu $G$ nazveme graf $G^*$, jehož stěny odpovídají vrcholům grafu $G$ a hrany vedou mezi každou dvojicí stěn, které mají společnou hranu v $G$.*

**Věta 5 (Eulerova věta)** *Nechť $G = (V, E)$ je souvislý rovinný graf a $n = |V|$ označuje počet vrcholů, $e = |E|$ počet hran a $f$ počet stěn tohoto grafu. Pak platí:*

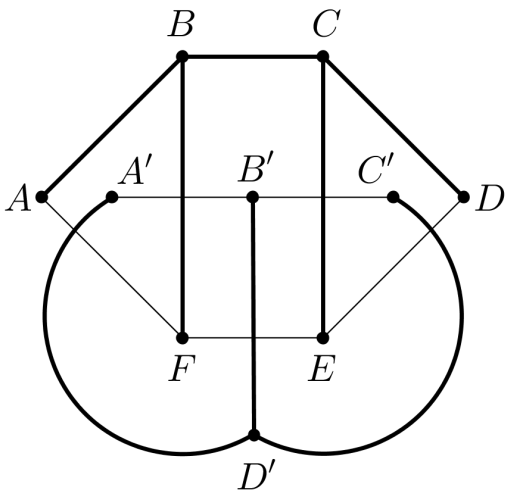
$$n - e + f = 2.$$

**D ů k a z.** Uvažujme planární graf $G$. Nechť $T \subseteq E$ je kostra grafu $G$. Označme $G^* = (V^*, E^*)$ duální graf ke $G$. Pro něj uvažujme množinu $T^* \subseteq E^*$ tak, že hrany v $T^*$ protínají hrany v $E \setminus T$ (viz obrázek 11). Je zřejmé, že $T^*$ tvoří kostru grafu $G^*$.




Obrázek 10: Graf $G$

Víme, že pro každý strom je počet vrcholů o jedna větší než počet hran. To se dá dokázat například tak, že vybereme jeden z vrcholů jako kořen, a povedeme všechny hrany (určíme orientaci) směrem od tohoto kořenu. Taková orientace nám dá bijekci mezi ostatními (nekořenovými) vrcholy a hranami. Přiřazujeme každé hraně vrchol, na který tato hrana míří.




Obrázek 11: Graf $G$ s grafem duálním $G^*$ se zvýrazněnými kostrami

Použijeme-li toto tvrzení na strom $T$, dostáváme $n = e_T + 1$ a pro strom $T^*$ dostáváme rovnost $f = e_{T^*} + 1$. Součet těchto rovností nám dává

$$n + f = (e_T + 1) + (e_{T^*} + 1) = e + 2,$$

neboli

$$n - e + f = 2.$$

□

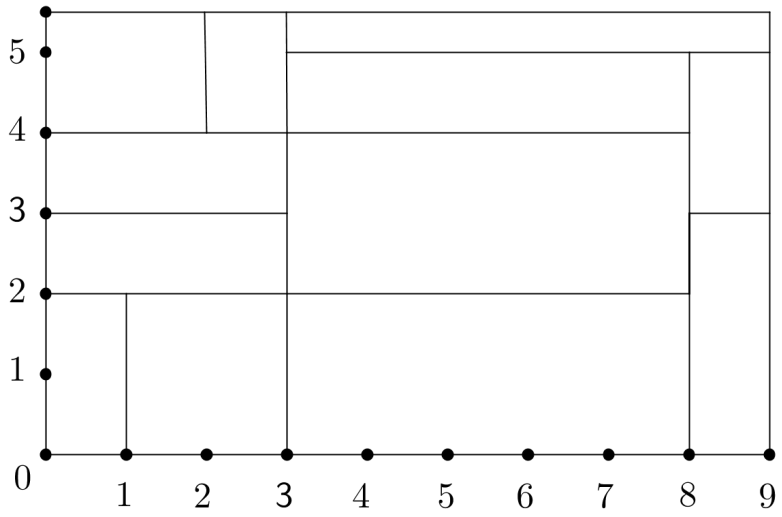
Uveďme pro zajímavost, že dalších 20 zajímavých důkazů tohoto tvrzení lze nalézt na webové stránce [4].

# 6 Rozdělení obdélníka

Následující věta je ukázkovým příkladem toho, kdy relativně elementární tvrzení může být poměrně těžké dokázat. Uvedený důkaz je od Nicolaase de Bruijn[9] a využijeme v něm trik z matematické analýzy.

**Věta 6** *Nechť $T$ je obdélník. Rozdělíme-li $T$ na menší navzájem disjunktní obdélníky $T_i$, které pokrývají $T$, a mají alespoň jednu stranu délky $t_j \in \mathbb{N}$, pak $T$ má alespoň jednu stranu délky $a \in \mathbb{N}$.*

**D ů k a z.** Příklad výše zmíněného dělení můžeme vidět na obrázku 12.




Obrázek 12: Příklad dělení obdélníka

Nechť $T$ je obdélník umístěný do kartézské soustavy souřadnic dle obrázku 12. Uvažujme dvojný integrál nad $T = [a, b] \times [c, d]$

$$I \quad = \quad \int_c^d \int_a^b e^{2\pi i(x+y)} \mathrm{d}x \, \mathrm{d}y. \tag{8}$$

[9]Nicolaas Govert de Bruijn (1918-2012). Nizozemský matematik, zabýval se matematickou analýzou, teorií čísel, kombinatorikou a logikou.

Zřejmě $I$ můžeme napsat ve tvaru

$$I \quad = \quad \int_c^d \int_a^b e^{2\pi i(x+y)} \mathrm{d}x \, \mathrm{d}y \quad = \quad \int_a^b e^{2\pi ix} \mathrm{d}x \quad \cdot \quad \int_c^d e^{2\pi iy} \mathrm{d}y.$$

Nás zajímá případ, kdy $I = 0$. To nastane právě tehdy, je-li alespoň jedna z hodnot $\int_a^b e^{2\pi ix} \mathrm{d}x$ nebo $\int_c^d e^{2\pi iy} \mathrm{d}y$ rovna nule. Dokážeme, že

$$\int_a^b e^{2\pi ix} \mathrm{d}x \quad = \quad 0 \quad \Leftrightarrow \quad (b-a) \in \mathbb{N}. \tag{9}$$

Pokud se nám to podaří, budeme s důkazem tvrzení hotovi. Dle předpokladů je $T$ rozděleno na obdélníky $T_i$. Můžeme integrovat přes jednotlivé obdélníky a díky aditivitě integrálu platí

$$I \quad = \quad \sum_i \int_{T_i} f(x,y) \mathrm{d}x \mathrm{d}y \quad = \quad \iint_R f(x,y) \mathrm{d}x \mathrm{d}y. \tag{10}$$

Pokud každá z hodnot $\iint_{T_i} f(x,y) = 0$, pak z (10) plyne $\iint_R f(x,y) = 0$. Vraťme se k ověření (9). Máme

$$\int_a^b e^{2\pi ix} \mathrm{d}x \quad = \quad \left[ \frac{e^{2\pi ix}}{2\pi i} \right]_a^b \quad = \quad \frac{1}{2\pi i} \left( e^{2\pi ib - 2\pi ia} \right) \quad = \quad \frac{e^{2\pi ia}}{2\pi i} \left( e^{2\pi i(b-a)} - 1 \right).$$

Vidíme, že

$$\int_a^b e^{2\pi ix} \mathrm{d}x \quad = \quad 0 \quad \Leftrightarrow \quad e^{2\pi i(b-a)} \quad = \quad 1.$$

Z Eulerovy identity $e^{ix} = \cos x + \mathrm{i} \sin x$ dostáváme $e^{2\pi ix} = \cos 2\pi x + \mathrm{i} \sin 2\pi x$. Tudíž rovnost $e^{2\pi i(b-a)} = 1$ je ekvivalentní s

$$\cos 2\pi(b-a) = 1 \quad , \quad \sin 2\pi(b-a) = 0.$$

Je tedy vidět, že $b - a \in \mathbb{Z}$.

□

# 7 Cantorova diagonální metoda

Uvedeme důkaz nespočetnosti množiny reálných čísel, který prezentoval v roce 1890 Georg Cantor[10]. Je vhodné zmínit, že Cantor se dokazováním tohoto tvrzení zabýval již dříve, a tento důkaz byl až třetím v pořadí. Nicméně níže uvedený důkaz je známější než jeho dva předchůdci a to z toho důvodu, že použitá metoda, tzv. Cantorova diagonální metoda, byla použita v důkazech mnoha dalších vět. Jedná se například o Cantorovu větu z teorie množin, kde se použije její lehká modifikace. Dále pak byla použita v problému zastavení stroje v teorii vyčíslitelnosti.

Připomeňme, že množinu M nazveme spočetnou, jestliže existuje bijektivní zobrazení, které M zobrazí na některou podmnožinu $\mathbb{N}$. Pokud taková bijekce neexistuje, množina M se nazývá nespočetná.

**Věta 7** *Množina reálných čísel je nespočetná.*

**D ů k a z.** Budeme sporem dokazovat, že interval $[0, 1]$ na $\mathbb{R}$ není spočetný. Předpokládejme sporem, že $[0, 1]$ je spočetný interval. Z definice spočetnosti plyne, že můžeme všechna čísla tohoto intervalu libovolně uspořádat do posloupnosti $p_1, p_2, p_3, \ldots$. Jak víme, každé reálné číslo se dá zapsat jeho desetinným rozvojem. Nechť tedy

$$\begin{aligned} p_1 &= 0, a_{11}a_{12}a_{13}a_{14}\ldots \\ p_2 &= 0, a_{21}a_{22}a_{23}a_{24}\ldots \\ p_3 &= 0, a_{31}a_{32}a_{33}a_{34}\ldots \\ &\vdots \end{aligned}$$

Z posloupnosti $p_1, \ldots, p_n, \ldots$ vybereme prvky $r_1, \ldots, r_n, \ldots$, pro něž $a_{ij} \in \{1, 2\}$ pro $i, j \in \mathbb{N}$, a vzniklou množinu označme $A_{12}$. Pro ilustraci si uveďme část takového uspořádání:

$$\begin{aligned} r_1 &= 0, 12122212\ldots \\ r_2 &= 0, 11221212\ldots \\ r_3 &= 0, 21221112\ldots \\ r_4 &= 0, 12211121\ldots \\ r_5 &= 0, 21212121\ldots \\ &\vdots \end{aligned}$$

[10]Georg Cantor (1845-1918). Německý matematik, zakladatel teorie množin.

Nyní sestrojme číslo $q \in [0,1]$, které v posloupnosti $r_1, r_2, r_3, \ldots$ není. Díky předpokladu $a_{ij} \in \{1,2\}$ jsme předešli situaci tzv. synonymních rozvojů, tedy případu, kdy jednomu reálnému číslu odpovídají dva desetinné rozvoje: např.

$$0,4299999\ldots = 0,4300000\ldots.$$

Pro $k$-tou číslici v desetinném rozvoji čísla $q$ uvažujeme $k$-tou číslici v rozvoji čísla $r_k$. Uvažované číslice jsou v další ukázce zvýrazněny tučně.

$$\begin{aligned}
r_1 &= 0,\mathbf{1}\,2122212\ldots \\
r_2 &= 0,1\,\mathbf{1}\,221212\ldots \\
r_3 &= 0,21\,\mathbf{2}\,21112\ldots \\
r_4 &= 0,122\,\mathbf{1}\,1121\ldots \\
r_5 &= 0,2121\,\mathbf{2}\,121\ldots \\
&\vdots
\end{aligned}$$

Z těchto číslic vygenerujeme číslo $q = 0, q_1 q_2 q_3 q_4 \ldots$ takto:

$$q_i = \begin{cases} 1, & \text{jestliže } a_{ii} = 2 \\ 2, & \text{jestliže } a_{ii} = 1. \end{cases}$$

V našem příkladě by tedy $q = 0,22121\ldots$. Zřejmě $q \in A_{12}$. Na začátku jsme předpokládali, že v posloupnosti $r_1, r_2, r_3, \ldots$ jsou všechna čísla z množiny $A_{12}$. Pak tedy musí existovat $n \in \mathbb{N}$ takové, že $r_n = q$. Díky našemu způsobu sestrojení čísla $q$ to ale není možné, protože $q$ se liší od každého $r_n$ na $n$-té desetinné pozici, a neleží tedy v posloupnosti $r_1, r_2, r_3, \ldots$. Množina $A_{12}$ je tedy nespočetná a tudíž i interval $[0,1]$ a celá množina $\mathbb{R}$ jsou nespočetné.

□

# Závěr

Cílem práce bylo prostudovat a zpracovat zajímavé nestandardní důkazy vybraných klasických tvrzení. Může být také zdrojem inspirace při hledání nových a elegantnějších důkazů k již dávno dokázaným tvrzením. Pro snazší porozumění je text doplněn o komentář a grafická znázornění. Ve většině případů jsou výpočty doplněny o některé „mezikroky“.

V prvních třech kapitolách jsme se věnovali důkazům tvrzení z teorie čísel. První kapitola obsahovala dva důkazy nekonečnosti množiny prvočísel. První důkaz nám navíc umožnil odhadnout, kolik prvočísel je menších než dané $n \in \mathbb{N}$ a důkaz kombinatorický rovněž dokazuje, že řada $\sum_{p\in\mathbb{P}} \frac{1}{p}$ diverguje. V druhé kapitole jsme se zabývali Eulerovou řadou. Finální výpočet prvního důkazu jsme provedli jiným způsobem než autoři knihy *Proofs from the Book*. Ovšem i tento výpočet nás dovedl k cíli. Dále je zde uveden důkaz čistě algebraický. Čtenář může opět porovnat, který z důkazů je elegantnější. Třetí kapitola je věnována Pierru de Fermat a důkazu jeho „vánoční“ věty. Naleznete zde také zajímavý důkaz malé Fermatovy věty. V kapitole číslo čtyři jsme již opustili teorii čísel a věnovali jsme se Caleyho větě z teorie grafů. Byl zde rozebrán relativně nový důkaz kombinatorickou metodou dvojího počítání. Kapitola pět pokračovala v teorii grafů, a sice Eulerovou charakteristikou planárních grafů. Kombinatorické tvrzení kapitoly šest nám předvedlo, že i intuitivně snadno pochopitelné tvrzení může mít obtížný důkaz vyžadující pokročilé myšlenky. V poslední kapitole jsme si na nespočetnosti množiny reálných čísel předvedli jednu z možností použití Cantorovy diagonální metody.

Za největší přínos této práce považuji inspiraci a prohloubení znalostí, týkajících se metod dokazování. Obzvláště použití metod matematické analýzy při důkazech tvrzení z oblasti algebry a kombinatoriky. Text byl vysázen v typografickém prostředí LaTeX. Všechny obrázky uvedené v textu byly vytvořeny pomocí programu GeoGebra.

# Reference


[1] Aigner, M.; Ziegler, G.M.: *Proofs from the book.* Springer, Berlin 1998.

[2] Demel, J.: *Grafy a jejich aplikace.* Academia, Praha 2002.

[3] Eukleidés: *Základy. Knihy VII-IX*, Překlad F. Servít, OPS, Kanina 2010.

[4] Eppstein, D.: *Twenty Proofs of Euler's Formula: V-E+F=2.* [online]. Dostupné na: `http://www.ics.uci.edu/~eppstein/junkyard/euler/`

[5] Halaš, R.: *Teorie čísel.* VUP, Olomouc 1997.

[6] Klemsa, J.: *RSA pro začátečníky.* [online]. Dostupné na: `http://jakub.klemsa.cz/sections/research/prase_lectures/rsa.pdf`

[7] Kolektiv autorů: *Handbook of graph theory.* CRC Press.

[8] Křížek, M.; Lawrence, S.; Šolcová, A.: *Kouzlo čísel.* Academia, Praha 2009.

[9] Mareš, M.: *Příběhy matematiky.* Pistorius & Olšanská, Příbram 2008.

[10] Matematický korespondenční seminář: *Nekonečné množiny.* [online]. Dostupné na: `http://mks.mff.cuni.cz/archive/21/10.pdf`

[11] Matoušek, J.; Nešetřil, J.: *Kapitoly z diskrétní matematiky.* Karolinum, Praha 2007.

[12] Švrček, J.: *Úvod do kombinatoriky.* VUP, Olomouc 2008.

[13] *Fermat's Christmas Theorem.* [online]. Dostupné na: `https://proofwiki.org/wiki/Fermat's_Christmas_Theorem`