Různé pohledy na matematiku a vnímání její krásy

Pavel Drábek

Katedra matematiky FAV ZČU
Univerzitní 22
306 14 Plzeň

1 Motivace

Když jsem si připravoval přednášku na stejné téma, jako je tento článek, vyslovil jsem před svými kolegy z Centra aplikované matematiky přání, mít k dispozici seznam všech prvočísel, například od dvou do milionu, abych měl v ruce vhodnou „demoverzi“ pro motivaci toho, co budu říkat. Ke svému překvapení jsem nedlouho poté dostal od jednoho mladšího kolegy 422 stránek hustě potištěných prvočísly od 2 do 2 841 823. Když jsem v ruce držel tuto „knihu prvočísel“, uvědomil jsem si, že jejím prostřednictvím je možné ilustrovat různé pohledy na matematiku, resp. na její poslání a postavení v kontextu jiných odvětví života či vědy. Při čtení následujících řádek, prosím, na chvíli zapomeňte na to, že důkaz faktu, že prvočísel je nekonečně mnoho, je již dlouhou dobu dobře známý.

Tak například, kdyby se takový seznam prvočísel ocitl v rukou novináře, ten by s největší pravděpodobností po letmém pohledu na hustě potištěnou první stranu prvočísly od 2 do 6 047 napsal reportáž, jejíž úvodní věta by mohla znít přibližně takto: „Vědci z Centra aplikované matematiky FAV ZČU v Plzni dokázali, že prvočísel je nekonečně mnoho“. Reportáž by pak nejspíše pokračovala tím, kde se zmíněné Centrum aplikované matematiky nachází, kolik pracovníků v něm působí, jaký je jeho rozpočet a jak výkonné počítače v centru máme. Novinářův článek by jistě obsahoval celou řadu pravdivých údajů, jeho základní tvrzení by však bylo zcela zavádějící.

Strojní inženýr, který již má svoje smutné zkušenosti s novinovými články, by si jistě chtěl pravdivost tvrzení o důkazu nekonečnosti množiny všech prvočísel ověřit. Nespokojil by se pouze pohledem na první stránku, prohlédl by si jich alespoň 10. Poté by provedl odhad lineární extrapolací, podíval by se na poslední stranu knihy prvočísel a zjistil by, že jeho odhad je správný. A nakonec by se tedy rozhodl, že zcela výjimečně novinovému článku uvěří.

Experimentální fyzik by pravdivost novinového článku vůbec neřešil. Podíval by se na poslední stránku knihy prvočísel a zjistil by, že prvočísla, která se na této stránce vyskytují, zdaleka přesahují možnosti jeho měřicích přístrojů a jdou daleko nad rámec rozlišitelnosti jeho modelů. Pro jeho potřeby je tedy také prvočísel nekonečně mnoho a basta.

Matematik by nejspíš nevěděl, že nějaký novinový článek na uvedené téma vůbec kdy vyšel. S knihou prvočísel v ruce by se však začal trápit celou řadou otázek. V době „neomezených možností“ moderní výpočetní techniky by se nejspíš pokusil pokračovat v rozkladu na prvočinitele dalších a dalších přirozených čísel. Po zjištění, že vždycky po čase narazí na některé přirozené číslo, které nelze na jiné než samozřejmé prvočinitele (1 a samo sebe) rozložit, by si uvědomil, že to co drží v ruce není ani důkaz, ani protipříklad, ale jen „pouhá hypotéza“. Uvědomil by si také, že trpělivé opakování stejného algoritmu rozkládání přirozených čísel na prvočinitele nikam nevede a že jedinou cestou k nalezení „absolutní pravdy“ je hlubší pohled na celý problém. Matematik by mimo jiné jistě záhy zjistil, že v tom dlouhém seznamu prvočísel, který se mu ocitl v ruce, se některá dvě sousední čísla liší pouze o dvojku[1] a naopak mezi jinými dvěma sousedy je podivuhodně velká „mezera“. Čím déle by si kladl otázku, proč tomu tak je, tím více by byl posedlý hledáním absolutní pravdy, tím hůř by spal a tím častěji by se v nejrůznějších životních situacích přistihl při tom, že nemyslí na nic jiného, než jak by této pravdě přišel na kloub. Ten, kdo zažil takové období „posedlosti“ se právě v těchto okamžicích stal „matematikem“. Zásadní rozdíl mezi generováním dalších a dalších prvočísel podle některého z dostupných algoritmů a důkazem nekonečnosti množiny všech prvočísel spočívá v tom, že musíme opustit „experimentální přístup“ a začít zkoumat „kvalitativní podstatu věci“.

Cílem následujících odstavců je ukázat šest různých důkazů nekonečnosti množiny všech prvočísel. Tyto důkazy jsou převzaty z knihy [1] a představují různé pohledy a přístupy. Smyslem tohoto článku tak není informovat čtenáře o dobře známém faktu, nýbrž výše uvedené přístupy podrobně rozebrat a ilustrovat.

2 Malý výlet do teorie čísel

V tomto článku budeme značit $\mathbb{N} = \{1, 2, \ldots\}$ množinu všech přirozených čísel, $\mathbb{Z} = \{\ldots, -2, -1, 0, 1, 2, \ldots\}$ množinu všech celých čísel a $\mathbb{P} = \{2, 3, 5, 7, \ldots\}$ množinu všech prvočísel. Symbol $p|n$ znamená, že celé číslo n je dělitelné přirozeným číslem p, tj. existuje jiné celé číslo m takové, že $n = pm$. Je dobře známo, že každé přirozené číslo má alespoň jednoho prvočíselného dělitele (v krajním případě sama sebe). Tento fakt dále používáme bez dalšího upozornění. Následující tvrzení bude pro nás podstatné.

[1] Taková dvě prvočísla se nazývají prvočíselná dvojčata.

Lemma 2.1 *Nechť $p \in \mathbb{N}, n_1, n_2 \in \mathbb{Z}$ a $p|n_1$ a $p|n_2$. Potom $p|(n_1 - n_2)$.*

Důkaz Z $p|n_1$ a $p|n_2$ plyne existence $m_1, m_2 \in \mathbb{Z}$ takových, že $pm_1 = n_1$ a $pm_2 = n_2$. Potom

$$n_1 - n_2 = p(m_1 - m_2),$$

a tedy $p|(n_1 - n_2)$.

■

Symbolem $\sum$ budeme značit (konečný nebo nekonečný) součet, symbolem $\prod$ budeme značit součin. Symbolem $|M|$ budeme značit mohutnost množiny M; speciálně pro konečnou množinu M značí $|M|$ počet prvků této množiny.

3 Důkaz „aritmetický I“ (Eukleides[2])

Jde o klasický důkaz sporem. Předpokládejme, že prvočísel je pouze konečný počet: $\{p_1, p_2, \ldots, p_r\}$. Přirozené číslo

$$n = p_1 p_2 \ldots p_r + 1$$

pak musí mít prvočíselného dělitele p: $p|n$. Kdyby existovalo $i = 1, \ldots, r$, pro které $p = p_i$, potom $p|(p_1 \ldots p_r)$, což spolu s $p|(p_1 \ldots p_r + 1)$ na základě Lemmatu 2.1 implikuje $p|1$. Odtud plyne, že $p = 1$, což je však ve sporu s tím, že číslo p je prvočíslem. Předpoklad důkazu je tedy nepravdivý výrok, takže množina všech prvočísel je nekonečná.

4 Fermatova[3] čísla

Takzvaná Fermatova čísla jsou definována takto:

$$F_n = 2^{2^n} + 1,\ n = 0, 1, 2, \ldots.$$

Všechna Fermatova čísla jsou lichá přirozená čísla. Mnohá Fermatova čísla, např. $F_0 = 3, F_1 = 5, F_2 = 17, F_3 = 257, F_4 = 65\,537$ jsou prvočísla, některá další, např. již $F_5 = 4\,294\,967\,297$, jsou čísla složená. Jde o velmi rychle rostoucí posloupnost přirozených čísel, která má následující kvalitativní vlastnost.

[2]Eukleides, žil asi ve druhé polovině 4. stol. až první polovině 3. stol. př. n. l., řecký filosof a matematik, je znám sepsáním nejslavnější učebnice v dějinách, tzv. „Základů“.

[3]Pierre de Fermat, 1601–1665, francouzský právník a matematik. Je znám svojí slavnou hypotézou pod názvem Velká Fermatova věta, kterou až v devadesátých letech 20. století dokázal anglický matematik Andrew Wiles. Fermat se domníval, že všechna čísla F_n jsou prvočísla. Rozklad F_5 na prvočinitele neznal.

Lemma 4.1 *Pro každé $n \in \mathbb{N}$ platí*

$$\prod_{k=0}^{n-1} F_k = F_n - 2. \tag{1}$$

Důkaz Vztah (1) dokážeme matematickou indukcí podle indexu n. Pro $n = 1$ vztah (1) platí: $F_1 - 2 = 3 (= F_0)$. Předpokládejme nyní, že vztah (1) platí pro libovolně zvolené přirozené číslo $n > 1$. Naším cílem je ukázat, že pak platí také pro $n + 1$, tj.

$$\prod_{k=0}^{n} F_k = F_{n+1} - 2.$$

Skutečně,

$$\prod_{k=0}^{n} F_k = \left(\prod_{k=0}^{n-1} F_k \right) F_n = (F_n - 2)F_n =$$

$$= (2^{2^n} - 1)(2^{2^n} + 1) = (2^{2^n})^2 - 1 = 2^{2^{n+1}} - 1 = F_{n+1} - 2.$$

(Indukční předpoklad byl využit ve druhé rovnosti.)

■

5 Důkaz „aritmetický II“ (Christian Goldbach[4] 1730)

Nejprve ukážeme, že žádná dvě různá Fermatova čísla nemají společného dělitele většího než 1. Provedeme důkaz sporem. Nechť existuje $m \in \mathbb{N}$ a indexy $l, n \in \mathbb{N}$ tak, že $l < n$ a $m|F_l$ a $m|F_n$. Potom $m| \prod_{k=0}^{n-1} F_k$ (neboť platí, že $l \leq n-1$). Tento fakt společně s $m|F_n$, (1) a Lemmatem 2.1 implikují $m|2$. Nutně tedy je buď $m = 1$, nebo $m = 2$. Druhá možnost je však vyloučena, neboť všechna Fermatova čísla jsou lichá.

Protože Fermatových čísel je nekonečně mnoho a neexistuje žádné prvočíslo, které by zároveň dělilo dvě různá z nich, musí být i prvočísel nekonečně mnoho.

6 Malý výlet do algebry

Neprázdná (konečná nebo nekonečná) množina G, na které je definována nějakým způsobem operace násobení, jež každým dvěma prvkům $a, b \in G$ přiřazuje právě

[4]Christian Goldbach, 1690–1764, německý právník a matematik. Byl pruským velvyslancem v Rusku a učitelem mladého cara Petra II. Je autorem známé Goldbachovy hypotézy (z roku 1742), že každé sudé číslo lze rozložit na součet dvou prvočísel. Tuto hypotézu dodnes nikdo nedokázal, ani nevyvrátil.

jeden prvek $c = ab$, patřící opět do G, a která splňuje následující požadavky (axiomy):

1. $(ab)c = a(bc)$,
2. $\forall a, b \in G\ \exists x, y \in G\colon ax = b\ \ \wedge\ \ ya = b$,

se nazývá multiplikativní grupa (stručně grupa). Je možné ukázat, že z axiomů 1. a 2. plyne existence právě jednoho prvku $e \in G$ (zvaného jednotkový prvek) takového, že

$$\forall a \in G\colon ea = ae = a$$

a dále pak, že

$$\forall a \in G\, \exists a^{-1} \in G \text{ (prvek inverzní)} : aa^{-1} = a^{-1}a = e.$$

Je-li U podmnožina grupy G a jsou pro ni také splněny výše uvedené axiomy, pak se U nazývá podgrupa grupy G.
Speciálně konečná podgrupa $U = \{a, a^2, \ldots, a^m\}$ kde $a \in G$, $a^2 = aa$, atd. a m je nejmenší přirozené číslo s vlastností $a^m = e$, se nazývá cyklická grupa řádu m a platí $|U| = m$. Pro každé $q \in \mathbb{P}$ můžeme provést rozklad množiny $\mathbb{Z}$ na třídy ekvivalence podle toho, jaký zbytek nám dané číslo dává po dělení číslem q. Systém těchto tříd ekvivalence označíme $\mathbb{Z}_q$. Tak například pro $q = 3$ se množina $\mathbb{Z}$ rozpadne na tři třídy ekvivalence:

$$\begin{aligned}\underline{0} &= \{\ldots, -6, -3, 0, 3, 6, \ldots\}\\ \underline{1} &= \{\ldots, -5, -2, 1, 4, 7, \ldots\}\\ \underline{2} &= \{\ldots, -4, -1, 2, 5, 8, \ldots\}\end{aligned}$$

a tedy $\mathbb{Z}_3 = \{\underline{0}, \underline{1}, \underline{2}\}$.
Množina $\mathbb{Z}_q \setminus \underline{0}$ je pak cyklickou grupou řádu $q - 1$, v níž je násobení indukováno obvyklým násobením celých čísel. Tak například řád cyklické grupy $\mathbb{Z}_3 \setminus \underline{0}$ je 2, neboť $\mathbb{Z}_3 \setminus \underline{0} = \{\underline{1}, \underline{2}\}$, kde $\underline{1}$ je jednotkovým prvkem a $\underline{2}^2 = \underline{1}$.

Následující tvrzení je klíčové pro náš další důkaz.

Lemma 6.1 **[Lagrangeova[5] věta]** *Nechť G je konečná multiplikativní grupa a U je její podgrupa. Potom platí: $|U|$ dělí $|G|$.*

Důkaz Z axiomů grupy plyne, že relace na množině G definovaná vztahem

$$a \sim b \Longleftrightarrow ba^{-1} \in U$$

je ekvivalence (je reflexivní: $a \sim a$, symetrická: $a \sim b \Leftrightarrow b \sim a$, tranzitivní: $a \sim b \wedge b \sim c \Rightarrow a \sim c$). Množina G se nám tak rozpadne na třídy ekvivalence a pro každé $a \in G$ množina

[5] Joseph-Louis Lagrange, 1736-1813, slavný francouzský fyzik a matematik.

$$Ua = \{xa \colon x \in U\}$$

je třída ekvivalence obsahující prvek $a \in G$. Lze snadno nahlédnout, že $|Ua| = |U|$ (skutečně, nerovnost $|Ua| \leq |U|$ je triviální; nechť pro $x_1, x_2 \in U, x_1 \neq x_2$ platí $x_1 a = x_2 a$, potom $x_1 a a^{-1} = x_2 a a^{-1} \Rightarrow x_1 = x_2$, což je spor a tedy $|U| \leq |Ua|$). Velikost každé třídy ekvivalence je tedy $|U|$, tj. $|U|$ dělí $|G|$.

■

7 Důkaz „algebraický“ (autor neznámý)

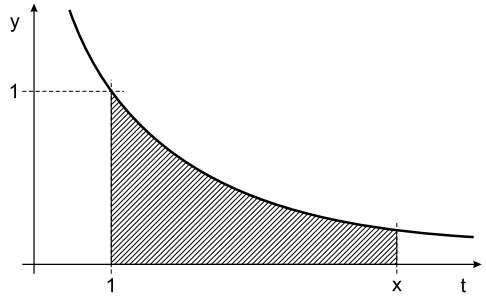
Předpokládejme, že $|\mathbb{P}| < \infty$ a označme $p = \max \mathbb{P}$ (p je největší z prvočísel). Uvažujme příslušné tzv. Mersennovo číslo $2^p - 1$. Dokážeme, že pro každé $q \in \mathbb{P}$, pro které $q|(2^p - 1)$, musí nutně platit $q > p$, což bude spor s předpokladem, že p je největší prvočíslo.
Nechť tedy $q|(2^p - 1)$, jinými slovy číslo 2^p dělené číslem q dává zbytek 1, tj. $\underline{2}^p = \underline{1}$. Potom cyklická grupa $\{\underline{2}, \underline{2}^2, \ldots, \underline{2}^p\}$ řádu p je podgrupou cyklické grupy $\mathbb{Z}_q \setminus \underline{0}$ a $|\mathbb{Z}_q \setminus \underline{0}| = q - 1$. Z Lemmatu 6.1 tedy plyne, že $p|(q-1)$, tj. $p < q$, což je spor.

8 Malý výlet do analýzy

Funkční hodnoty funkce přirozený logaritmus (o základu e) $\ln x$, se pro $x > 1$ dají vyjádřit integrálem

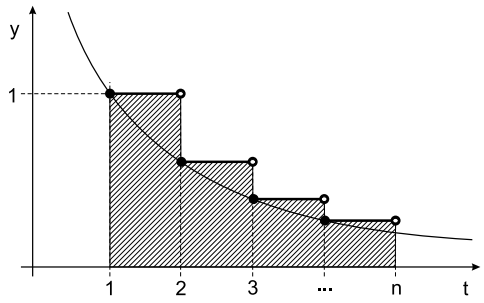
$$\ln x = \int_1^x \frac{1}{t}\, dt.$$

Geometrický význam hodnoty $\ln x$ je obsah plochy omezené grafem funkce $y = \frac{1}{t}$, osou t a rovnoběžkami s osou y, protínajícími osu t v bodech 1 a x (obr. 1), a platí $\ln x \to +\infty$ pro $x \to +\infty$.



obr. 1

Geometrický význam součtu $\sum_{k=1}^{n} \frac{1}{k}$ je obsah plochy omezené grafem po částech konstantní „schodovité“ funkce, osou t a přímkami o rovnicích $t = 1$ a $t = n$ (obr. 2).



obr. 2

Pro $n \leq x < n + 1$ pak zřejmě platí nerovnost

$$\ln x \leq 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} = \sum_{k=1}^{n} \frac{1}{k}.$$

9 Důkaz „analytický“ (Leonhard Euler[6])

Seřadíme prvočísla do posloupnosti podle jejich velikosti: $\mathbb{P} = \{p_1, p_2, p_3, \dots\}$, tj. pro $n > m$ platí $p_n > p_m$. Označíme symbolem $\pi(x)$ počet všech prvočísel, která jsou menší nebo rovná libovolně zvolenému reálnému číslu x, tj. $\pi(x) = |\{p \leq x \colon p \in \mathbb{P}\}|$. Pro $n \in \mathbb{N}$ a $n \leq x < n + 1$ máme (viz odst. 8)

$$\ln x \leq \sum_{k=1}^{n} \frac{1}{k} \leq \sum \frac{1}{m}, \tag{2}$$

kde poslední součet bereme přes všechna $m \in \mathbb{N}$, která jsou dělitelná pouze prvočísly $p \leq x$. Pro každé takové m pak platí

$$m = \prod_{p \leq x} p^{k_p}.$$

Poslední součet v (2) tedy můžeme psát ve tvaru

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

[6]Leonhard Euler, 1707–1783, švýcarský matematik, fyzik a astronom. Byl považován za „ztělesnění matematické analýzy“ a za nejplodnějšího matematika všech dob.

kde $\sum_{k\geq 0} \frac{1}{p^k}$ je konvergentní geometrická řada s kvocientem $\frac{1}{p}$ a prvním členem 1, tj.

$$\sum_{k\geq 0} \frac{1}{p^k} = \frac{1}{1-\frac{1}{p}} = \frac{p}{p-1}.$$

Z (2) tedy plyne

$$\ln x \leq \prod_{\substack{p\in\mathbb{P}\\ p\leq x}} \frac{p}{p-1} = \prod_{k=1}^{\pi(x)} \frac{p_k}{p_k-1}. \tag{3}$$

Protože $p_k \geq k+1$, platí také $\frac{p_k}{p_k-1} \leq \frac{k+1}{k}$, tj. z (3) plyne

$$\ln x \leq \prod_{k=1}^{\pi(x)} \frac{k+1}{k} = \frac{2}{1}\cdot\frac{3}{2}\cdot\frac{4}{3}\cdots\frac{\pi(x)+1}{\pi(x)} = \pi(x)+1.$$

Protože pro $x \to +\infty$: $\ln x \to +\infty$, platí také $\pi(x) \to +\infty$ pro $x \to +\infty$.

10 Malý výlet do topologie

Neprázdná množina G, na níž je definován systém otevřených množin, splňující následující tři axiomy:

1. sjednocení libovolného počtu otevřených množin je opět množina otevřená,
2. průnik konečného počtu otevřených množin je množina otevřená,
3. $\emptyset$ a G jsou otevřené množiny,

se nazývá topologický prostor. Systém otevřených množin se pak nazývá topologií na G. Množina $F \subset G$ se nazývá uzavřená, pokud $G \setminus F$ je množina otevřená. Množiny $\emptyset$ a G jsou tedy zároveň otevřené a uzavřené, a systém všech uzavřených množin pak splňuje požadavky (axiomy):

1'. průnik libovolného počtu uzavřených množin je množina uzavřená,

2'. sjednocení konečného počtu uzavřených množin je množina uzavřená.

11 Důkaz „topologický“ (Harry Fürstenberg[7])

Pro každé $a \in \mathbb{Z}$, $b \in \mathbb{N}$ položíme

[7]Harry Fürstenberg, izraelský matematik, v roce 1958 získal doktorát na Princetonské univerzitě, jeho školitelem byl Salomon Bochner.

$$N_{a,b} = \{a + nb\colon\ n \in \mathbb{Z}\}.$$

Potom $N_{a,b}$ je nekonečná aritmetická posloupnost:

$$\{\dots, a-3b, a-2b, a-b, a, a+b, a+2b, a+3b, \dots\}.$$

Řekneme, že $O \subset \mathbb{Z}$ je otevřená množina, když je buď $O = \emptyset$, nebo pro každé $a \in O$ existuje $b \in \mathbb{N}$ takové, že $N_{a,b} \subset O$. ($N_{a,b}$ je tzv. okolí bodu $a \in \mathbb{Z}$ s hustotou $b \in \mathbb{N}$.) Je zřejmé, že libovolné sjednocení otevřených množin je podle výše uvedené definice opět otevřená množina. Nechť nyní O_1 a O_2 jsou dvě otevřené množiny. Je-li $O_1 \cap O_2 = \emptyset$, potom $O_1 \cap O_2$ je otevřená množina. Nechť $O_1 \cap O_2 \neq \emptyset$ a $a \in O_1 \cap O_2$ je libovolný prvek. Potom existují $b_1, b_2 \in \mathbb{N}$ tak, že $N_{a,b_1} \subset O_1$ a $N_{a,b_2} \subset O_2$. Odtud plyne, že $a \in N_{a,b_1b_2} \subset O_1 \cap O_2$, tj. $O_1 \cap O_2$ je otevřená množina. Proto také každý konečný průnik $\cap_{i=1}^{n} O_i$ otevřených množin O_i je opět otevřená množina. Množina všech celých čísel $\mathbb{Z}$ je tedy topologickým prostorem. Protože každá neprázdná otevřená množina obsahuje nekonečnou aritmetickou posloupnost, platí:

(1) Každá neprázdná otevřená množina je nekonečná.

Protože je

$$N_{a,b} = \mathbb{Z} \setminus \bigcup_{i=1}^{b-1} N_{a+i,b}$$

a každá z množin $N_{a+i,b}$ je otevřená, platí

(2) Každá množina $N_{a,b}$ je také uzavřená.

Pro každé $n \notin \{-1, 1\}$ existuje $p \in \mathbb{P}$ tak, že $p|n$. Odtud plyne $n \in N_{0,p}$, a tedy

$$\mathbb{Z} \setminus \{-1, 1\} = \bigcup_{p \in \mathbb{P}} N_{0,p}.$$

Důkaz faktu $|\mathbb{P}| = \infty$ provedeme sporem. Předpokládejme, že $|\mathbb{P}| < \infty$. Potom $\bigcup_{p\in\mathbb{P}} N_{0,p}$ je konečné sjednocení uzavřených množin (viz (2)), a tedy množina uzavřená. Pak ovšem $\{-1, 1\}$ je množina otevřená, což je ve sporu s (1).

12 Malý výlet do kombinatoriky

Nechť $\{p_1, p_2, \dots, p_k\} \subset \mathbb{P}$ je množina prvních k prvočísel. Otázka zní: „Kolik celých čísel dostaneme jako součin navzájem různých prvních k prvočísel?“
Pro $\{2, 3\}$ dostáváme čísla $2, 3, 6$, pro $\{2, 3, 5\}$ dostáváme čísla $2, 3, 5, 6, 10, 15, 30$, atd. Obecně pro $\{p_1, p_2, \dots, p_k\}$ dostáváme $2^k - 1$ různých čísel, neboť 2^k je počet všech podmnožin k -prvkové množiny.

13 Důkaz „kombinatorický“ (Paul Erdös[8])

Nechť $\mathbb{P} = \{p_1, p_2, \ldots\}$ je vzestupně uspořádaná množina všech prvočísel. Naším cílem bude dokázat, že $\sum_{p\in\mathbb{P}} \frac{1}{p} = +\infty$, odkud již plyne, že $|\mathbb{P}| = \infty$. (Plyne odtud dokonce daleko více! Například to, že prvočísla jsou v $\mathbb{N}$ rozložena „hustěji“ než mocniny libovolného přirozeného čísla většího než 1 nebo čtverce přirozených čísel.) Provedeme důkaz sporem. Předpokládejme, že $\sum_{p\in\mathbb{P}} \frac{1}{p} < +\infty$. Potom existuje $k \in \mathbb{N}$ takové, že

$$\sum_{i\geq k+1} \frac{1}{p_i} < \frac{1}{2}. \tag{4}$$

Dále budeme $p_1, \ldots, p_k$ nazývat malá prvočísla a $p_{k+1}, p_{k+2}, \ldots$ velká prvočísla. Z (4) plyne, že pro každé $N \in \mathbb{N}$ platí

$$\sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{5}$$

Označíme N_v počet všech přirozených čísel $n \leq N$, která jsou dělitelná alespoň jedním velkým prvočíslem, a N_m počet všech ostatních přirozených čísel $n \leq N$. Jsou to taková $1 < n \leq N$, jež mají za dělitele jenom malá prvočísla a také $n = 1$. Pro každé $N \in \mathbb{N}$ zřejmě platí

$$N_v + N_m = N.$$

Ke sporu dojdeme tak, že dokážeme existenci takového $\hat{N} \in \mathbb{N}$, pro které

$$\hat{N}_v + \hat{N}_m < \hat{N}. \tag{6}$$

Symbolem $[x]$ budeme značit celou část reálného čísla x, tj. největší celé číslo, které je menší nebo rovné x. Potom $\left[\frac{N}{p_i}\right]$ značí počet všech přirozených čísel $n \leq N$, která jsou násobky prvočísla p_i. Ze vztahu (5) plyne, že pro libovolné $N \in \mathbb{N}$ platí

$$N_v \leq \sum_{i\geq k+1} \left[\frac{N}{p_i}\right] \leq \sum_{i\geq k+1} \frac{N}{p_i} < \frac{N}{2}. \tag{7}$$

[8]Paul Erdös, 1913-1996, maďarský matematik. Kromě mnoha zásadních objevů v matematice je znám tzv. „Erdösovým číslem“: Erdös sám měl číslo 0, kdo byl spoluautorem nějaké publikace s Erdösem, má číslo 1, kdo byl spoluautorem Erdösova spoluautora, ale sám Erdösovým spoluautorem nebyl, má číslo 2, atd.

Každé $n \in \mathbb{N}, n \leq N$, které má jen malá prvočísla jako své dělitele, píšeme ve tvaru

$$n = a_n b_n^2,$$

kde a_n je buď 1, nebo není čtvercem žádného přirozeného čísla, tj. a_n je součinem navzájem různých malých prvočísel, nebo $a_n = 1$. Podle odst. 12 je takových a_n celkem 2^k. Dále pak zřejmě $b_n \leq \sqrt{n} \leq \sqrt{N}$, tj. čísel b_n je nejvýše $\sqrt{N}$. Proto

$$N_m \leq 2^k \sqrt{N}.$$

Pokud vezmeme $\hat{N} \geq 2^{2k+2}$, potom $2^k \sqrt{\hat{N}} \leq \frac{\hat{N}}{2}$, a tedy

$$\hat{N}_m \leq \frac{\hat{N}}{2}.$$

Protože zároveň ze (7) plyne, že

$$\hat{N}_v < \frac{\hat{N}}{2},$$

dostáváme (6), což je spor.

14 Závěr

Základní dvě myšlenky jsou všem výše uvedeným důkazům společné:

- Přirozená čísla rostou nade všechny meze.
- Každé přirozené číslo větší nebo rovné dvěma má alespoň jednoho prvočíselného dělitele.

Na druhou stranu, každý z výše uvedených důkazů je jiný než ty ostatní. Každý v sobě skrývá svoji osobitou krásu. Stejně jako u žen však lze jen těžko říci, který je nejkrásnější, stejně jako u žen je jejich krása věcí osobního vkusu posuzovatele. Důkaz Eukleidův je krásný svojí přímočarostí, „jde tvrdě k podstatě věci“ a neohlíží se nalevo či napravo. Krása druhého, Goldbachova důkazu spočívá v tom, že nám dává možnost nahlédnout hlouběji do struktury množiny všech Fermatových čísel. Třetí, algebraický důkaz je krásný proto, že odhaluje složitou strukturu množiny všech celých čísel. Čtvrtý, Eulerův analytický důkaz je krásný tím, že nám umožní odhadnout, kolik prvočísel je menších než libovolné přirozené číslo n. Pátý, topologický důkaz je krásný proto, že nám ukazuje, jak zjednodušené byly naše představy o topologických prostorech, a v tomto směru nám otevírá oči. A krása šestého, Erdösova důkazu spočívá, stejně jako u důkazu čtvrtého, v tom, že nám dává mnohem více než jsme původně žádali.

Myslím, že šťastný je každý člověk, kdo nabízenou krásu dokáže vychutnat. A to platí v plné míře nejen o matematice a o výše uvedených šesti důkazech!

Poděkování

Autor děkuje svým kolegům z katedry matematiky, doc. Josefu Polákovi a RNDr. Jiřímu Čížkovi za řadu podnětných připomínek.

Reference

[1] M. Aigner, G. M. Ziegler: Proofs from the Book, Springer-Verlag, Berlin, Heidelberg, New York, 2nd printing, 2002.