Jaromír Šimša

Eukleidův důkaz nekonečnosti množiny všech prvočísel

In: Jindřich Bečvář (editor); Eduard Fuchs (editor): Historie matematiky. I. Seminář pro vyučující na středních školách, Jevíčko, 19.8.-22.8.1993, Sborník. (Czech). Brno: Jednota českých matematiků a fyziků, 1993. pp. 162–169.

Persistent URL: http://dml.cz/dmlcz/400582

EUKLEIDŮV DŮKAZ NEKONEČNOSTI MNOŽINY VŠECH PRVOČÍSEL

JAROMÍR ŠIMŠA

Úvod. Ze školních let si dobře pamatuji (a jistě nejsem sám) na nevšední zážitek, když jsem pochopil způsob, jakým Eukleides zdůvodnil, proč mezi prvočísly neexistuje největší. I když jsem tehdy ještě nevěděl, co to matematický důkaz je, přesvědčivost a vtip Eukleidovy úvahy na mne silně zapůsobily. Podívejme se proto spolu ještě jednou na tento starý důkaz a posuďme, zda je zajímavý i pro současnou matematiku, pěstovanou nejen profesionály akademických institucí, ale i milovníky – amatéry, mezi které patří učitelé základních a středních škol a jejich zvídaví žáci.

Poučení z historie. Není to žádná náhoda, že Eukleidův výsledek zůstával až do začátku 19. století jediným beze zbytku dokázaným výsledkem o rozložení prvočísel v posloupnosti všech přirozených čísel, přestože zásadní a jednoduše formulované otázky o prvočíslech zaměstnávaly mysl mnoha antických a středověkých učenců. Koho by netěšila věčná sláva, jež by přinesl objev vzorce udávající n-té prvočíslo nebo vzorce pro hodnotu $\pi(n)$, značící počet prvočísel mezi čísly $1, 2, \ldots, n$?

Nerozvíjejme ale dále tyto vzrušující otázky, které se ukázaly být nesmírně obtížné. *Téměř všechny významné výsledky o prvočíslech dokázané v posledních třech stoletích byly získány neelementárními postupy matematické analýzy.* Jejich důkazy jsou pojmově náročné, a tak lidem bez dobré průpravy v reálné a komplexní analýze zůstávají nepřístupné. Přesto můžeme na jednoduchém a historicky nejstarším příkladu ukázat, jak se prvočísla (objekt diskrétní matematiky) dostala do sféry působnosti zdánlivě tak odlehlé oblasti matematiky, jakou je infinitezimální počet. Sestavme pro každé prvočíslo p formální nekonečný součet

$$\Sigma_p = 1 + p + p^2 + p^3 + p^4 + \cdots$$

Zapišme součin všech těchto součtů

$$\Sigma_2 \cdot \Sigma_3 \cdot \Sigma_5 \cdot \Sigma_7 \cdot \Sigma_{11} \cdot \Sigma_{13} \cdot \Sigma_{17} \cdot \Sigma_{19} \cdot \Sigma_{23} \cdots$$

a podle distributivního zákona formálně roznásobme. Co dostaneme? Není těžké zdůvodnit, že vyjde součet všech přirozených čísel (stačí vzít na pomoc větu o rozkladu přirozených čísel na prvočinitele). Stejný postup vede pro každé číslo s k formální rovnosti

$$\prod_p (1 + p^s + p^{2s} + p^{3s} + \cdots) = \sum_{n=1}^{\infty} n^s ,$$

kde nalevo se násobí přes všechna prvočísla p. Uvědomme si, že každý činitel nalevo je geometrická řada s kvocientem p^s, která konverguje pro každé $s < 0$

a jejíž součet je znám ze střední školy. Proto můžeme pro záporné hodnoty s přepsat naši formální rovnost do tvaru

$$\text{(R)} \qquad \prod_p \frac{1}{1-p^s} = \sum_{n=1}^{\infty} n^s .$$

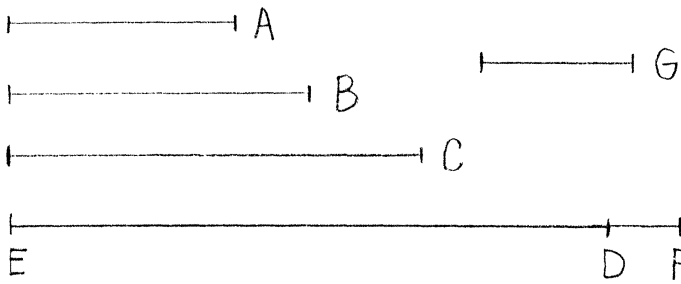
Tento vzorec objevil L. Euler, který navíc ukázal, že rovnost (R) skutečně platí pro každé $s < -1$. (Jak dobře víme, pro $s \geq -1$ řada v pravé části (R) diverguje.) Protože součet řady na pravé straně (R) roste nade všechny meze při s jdoucím zleva k -1, plyne z Eulerova tvrzení, že součin

$$\left(1-\frac{1}{2}\right)\left(1-\frac{1}{3}\right)\left(1-\frac{1}{5}\right)\left(1-\frac{1}{7}\right)\left(1-\frac{1}{11}\right)\left(1-\frac{1}{13}\right)\left(1-\frac{1}{17}\right)\cdots$$

má hodnotu nula, takže obsahuje nekonečně mnoho činitelů. Tímto analytickým postupem Euler znovu potvrdil skutečnost, že prvočísel je nekonečně mnoho.

Eukleidův text. Vraťme se však do antických dob a uveďme nyní bez jakýchkoliv poznámek text z Eukleidových *Základů*, a to podle překladu [1]:

> *Kmenných čísel jest více než jakékoliv dané množství kmenných čísel.*
>
> *Danými čísly buďtež A, B, C; pravím, že jest více kmenných čísel než A, B, C. Nuže vezměme v úvahu nejmenší číslo, jehož měrami jsou A, B, C, a budiž to DE a přičtěme k DE jednotku DF. EF tedy buď je kmenné buď není. Budiž dříve kmenné; jsou tedy nalezena čísla kmenná A, B, C, EF počtem více než A, B, C. Avšak již nebuď EF kmenné; tedy jest mu nějaké číslo kmenné měrou. Budiž mu měrou kmenné G; pravím, že G není rovno žádnému z čísel A, B, C. Nuže, možno-li, budiž rovno. Avšak A, B, C jsou měrami čísla DE; tedy též G bude měrou čísla DE. Jest pak měrou i čísla EF; také zbývající jednotky DF měrou bude G, ač jest číslo; což právě nesmyslno. Tedy G není rovno žádnému z čísel A, B, C. A bylo vzato za kmenné. Tedy jest nalezeno více kmenných než dané množství A, B, C, totiž A, B, C, G; což bylo právě dokázati.*



Dnešní interpretace. Eukleidův důmyslný postup se v současných školských učebnicích podává nejčastěji v následující jednoduché formě:

Chceme-li najít nějaké prvočíslo větší než předem zvolené přirozené číslo N (jakkoliv velké), stačí vzít na pomoc číslo

$$1 \cdot 2 \cdot 3 \cdots (N-1) \cdot N + 1 = N! + 1 .$$

Toto číslo, které je jistě větší než N, není dělitelné žádným z čísel 2, 3, ..., N, neboť dává při dělení každým z nich zbytek 1. Je to tedy buď prvočíslo větší než N, nebo součin několika prvočísel větších než N. Tak či onak, prvočíslo větší než N existuje.

Je jasné, že v takové úvaze bychom místo čísla $N!$ mohli vzít menší číslo, a to součin všech prvočísel nepřevyšujících N. To by více odpovídalo původnímu Eukleidovu textu, pro žáky by to ale bylo asi méně přehledné, a tím i méně přesvědčivé. Závěr úvahy je stejný: *Mezi prvočísly není největší, neboť jsme ukázali, že neexistuje přirozené číslo N, které by bylo větší než jakékoliv prvočíslo.*

Odhad následujícího prvočísla. Původní Eukleidův postup nejen dokazuje, že prvočísel je nekonečně mnoho, ale poskytuje i určitou informaci o tom, jak rychle roste posloupnost všech prvočísel

(*) $p_1 = 2, p_2 = 3, p_3 = 5, p_4 = 7, p_5 = 11, p_6 = 13, p_7 = 17, p_8 = 19, \ldots$

Stačí uvážit číslo

$$M = p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 ,$$

které není násobkem žádného z prvočísel $p_1, p_2, \ldots, p_n$. Je to tedy buď nějaké větší prvočíslo (ne nutně p_{n+1}), nebo součin několika takových (ne nutně různých) prvočísel. V každém případě platí odhad $p_{n+1} \leq M$, tj.

$$p_{n+1} \leq p_1 \cdot p_2 \cdot p_3 \cdots p_n + 1 ,$$

který lze nepatrně vylepšit tak, že místo čísla M uvážíme číslo

$$M' = p_1 \cdot p_2 \cdot p_3 \cdots p_n - 1 .$$

(Vysvětlete proč to má smysl, jen když $n \neq 1$.) Dostaneme tak odhad

(E) $$p_{n+1} < p_1 \cdot p_2 \cdot p_3 \cdots p_n \quad \text{pro každé } n \geq 2 ,$$

který pracovně nazveme *Eukleidův*. Získaný výsledek je přesný pro $n = 2$:

$$5 = 2 \cdot 3 - 1 \quad \text{neboli} \quad p_3 = p_1 \cdot p_2 - 1 .$$

Trochu hůře to dopadne pro další hodnoty n:

$$2 \cdot 3 \cdot 5 - 1 = 29 > p_4 = 7, \quad 2 \cdot 3 \cdot 5 \cdot 7 - 1 = 209 = 11 \cdot 19 > p_5 = 11 , \text{ atd.}$$

Naše zkušenost s prvočísly podpořená letmým pohledem do tabulek potvrzuje, že Eukleidův odhad (E) má pro velká n pouze teoretický význam. Doložme to příkladem prvočísla $p_{301} = 1\,991$: protože $p_{168} = 1\,009$, je pravá strana odhadu (E) pro $n = 300$ větší než $1\,000^{300-167} = 10^{399}$. Je téměř jisté, že nerovnost $1\,991 < 10^{399}$ asi k ničemu není.

V další části ukážeme dva způsoby, kterými lze původní Eukleidův postup rozvinout a získat tak odhady přesnější než (E). I když tyto výsledky budou pochopitelně slabší než slavný Čebyševův odhad

(Č) $$p_{n+1} < 2 \cdot p_n \qquad \text{pro každé } n \geq 1$$

(který lze mimochodem rovněž dokázat elementárními prostředky, viz [U]), podíváme se přitom na Eukleidův postup novým pohledem. Znovu se tak potěšíme jeho krásou a možná i inspirujeme k dalšímu bádání.

Odhad A. Mąkowského. Tento polský matematik inspirován Eukleidem dokázal před čtyřiceti lety (viz [S]), že pro posloupnost (*) všech prvočísel platí

(M) $$p_{n+1} + p_{n+2} < p_1 \cdot p_2 \cdot p_3 \cdots p_n \quad \text{pro každé } n \geq 3\,.$$

Dokažme toto vylepšení odhadu (E). Zkoumejme dvě čísla

$$M_1 = p_2 \cdot p_3 \cdots p_n + 2 \quad \text{a} \quad M_2 = p_2 \cdot p_3 \cdots p_n - 2\,.$$

(Všimněte si, že v součinech chybí činitel $p_1 = 2$.) Pro každé $n \geq 3$ jsou M_1 a M_2 dvě lichá čísla, přičemž

$$M_1 - 4 = M_2 \geq p_2 \cdot p_3 - 2 \geq 13\,.$$

Navíc žádné z obou čísel M_i není dělitelné žádným z prvočísel $p_1, p_2, \ldots, p_n$, takže je to buď prvočíslo, nebo součin několika prvočísel větších než p_n. Proto existují prvočísla p_j a p_k s indexy $j > n$ a $k > n$ taková, že p_j dělí M_1 a p_k dělí M_2. Protože $M_1 - M_2 = 4$, jsou lichá čísla M_1 a M_2 nesoudělná, takže prvočísla p_j a p_k musí být různá, tj. musí platit $j \neq k$. Odtud vyplývá odhad

$$p_{n+1} + p_{n+2} \leq p_j + p_k\,,$$

takže z nerovností $p_j \leq M_1$ a $p_k \leq M_2$ plyne

$$p_{n+1} + p_{n+2} \leq M_1 + M_2 = 2 \cdot p_2 \cdot p_3 \cdots p_n = p_1 \cdot p_2 \cdot p_3 \cdots p_n$$

a důkaz odhadu (M) je hotov.

Zamyslíme-li se nad předchozím postupem, napadne nás otázka, zda nelze získat další odhady podobné (M) úvahami o číslech tvaru

$$p_{k+1} \cdot p_{k+2} \cdots p_n \pm p_1 \cdot p_2 \cdots p_k$$

(Mąkowski použil hodnotu $k = 1$), nebo obecnějšího tvaru

$$A \cdot p_{i_1} \cdot p_{i_2} \cdots p_{i_k} \pm B \cdot p_{j_1} \cdot p_{j_2} \cdots p_{j_\ell},$$

kde $\{i_1, \ldots, i_k\} \cup \{j_1, \ldots, j_\ell\}$ je libovolný rozklad n-tice $\{1, 2, \ldots, n\}$ na dvě třídy a A, B vhodná přirozená čísla. Je to otázka, na kterou autor příspěvku nezná odpověď.

Odhad M. Dehna. Eukleidovu ideu krásným způsobem uplatnil M. Dehn[1], když v roce 1907 dokázal, že pro posloupnost (*) všech prvočísel platí odhad

$$\text{(D)} \qquad p_{n+1} < \sqrt{p_1 \cdot p_2 \cdot p_3 \cdots p_n} \quad \text{pro každé } n \geq 4.$$

Podívejme se, jak důmyslně přitom postupoval.

Důkaz odhadu (D) provedl M. Dehn takto: zdůvodnil, že nerovnost

$$p_{n+1} < p_1 \cdot p_2 \cdot p_3 \cdots p_x$$

platí pro „dostatečně malý" index x (závislý na čísle n). Prozatím předpokládejme, že index x $(1 < x < n)$ je libovolný a rozdělme prvních n prvočísel do dvou skupin

$$\mathcal{A} = \{p_1, p_2, \ldots, p_{x-1}\} \quad \text{a} \quad \mathcal{B} = \{p_x, p_{x+1}, \ldots, p_n\}.$$

Dále uvažujme p_x čísel

$$\begin{aligned} M_1 &= 1 \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_{x-1} - 1 \\ M_2 &= 2 \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_{x-1} - 1 \\ M_3 &= 3 \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_{x-1} - 1 \\ &\cdots\cdots\cdots \\ M_{p_x} &= p_x \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_{x-1} - 1 \end{aligned}$$

Je jasné, že žádné z těchto čísel není dělitelné žádným prvočíslem ze skupiny $\mathcal{A}$. Vypočtěme nyní rozdíl libovolných dvou různých čísel M_i a M_j $(1 \leq i < j \leq p_x)$:

$$M_j - M_i = (j - i) \cdot p_1 \cdot p_2 \cdot p_3 \cdots p_{x-1}.$$

Protože $0 < j - i < p_x$, není rozdíl $M_j - M_i$ dělitelný žádným prvočíslem ze skupiny $\mathcal{B}$. Proto každé prvočíslo z $\mathcal{B}$ dělí *nejvýše jedno* z uvažovaných čísel M_i. Odtud plyne: bude-li počet prvků v $\mathcal{B}$ (tedy číslo $n - x + 1$) menší než počet p_x všech čísel M_i, pak některé číslo M_i nebude dělitelné žádným prvočíslem z $\mathcal{B}$

[1]M. Dehn (1878 – 1952), významný německý matematik. V r. 1939 uprchnul před nacismem do USA, kde působil jako profesor na mnoha předních univerzitách. Publikoval řadu prací z geometrie, teorie grup, topologie, historie a filosofie matematiky. Vyřešil jeden z 23 Hilbertových problémů (o kongruentních čtyřstěnech).

(a ovšem ani z $\mathcal{A}$). Toto číslo M_i pak bude buď prvočíslo větší než p_n, nebo součin několika takových prvočísel, takže bude platit nerovnost

$$p_{n+1} \leq M_i \, (\leq M_{p_x} < p_1 \cdot p_2 \cdots p_x).$$

Dokázali jsme toto pomocné tvrzení:

Je-li index x $(1 < x < n)$ takový, že $n - x + 1 < p_x$, pak $p_{n+1} < p_1 \cdot p_2 \cdots p_x$.

Čím je index x menší, tím je poslední odhad přesnější. Pro náš cíl (kterým je důkaz (D)) stačí ukázat, že podmínka na index x, tj. nerovnost $n + 1 < x + p_x$, je splněna pro některé $x \leq \frac{n}{2}$. Skutečně, při takovém x totiž platí $2x \leq n$, takže z dokázaného tvrzení plyne

$$p_{n+1}^2 < p_1^2 \cdot p_2^2 \cdots p_x^2 < (p_1 \cdot p_{x+1})(p_2 \cdot p_{x+2}) \cdots (p_x \cdot p_{2x}) \leq p_1 \cdot p_2 \cdots p_n \, .$$

Zabývejme se proto nerovností $n + 1 < x + p_x$. Ze srovnání posloupnosti všech prvočísel (*) s posloupností lichých čísel

$$\begin{aligned} &2, 3, 5, 7, 11, 13, 17, 19, \ldots \\ &\quad 3, 5, 7, \ 9, 11, 13, 15, \ldots \end{aligned}$$

plyne, že pro každý index $x \geq 2$ platí $p_x \geq 2x - 1$. Proto nerovnost $n+1 < x+p_x$ platí, pokud $n + 1 < x + (2x - 1)$, tj. pokud $x > \frac{n+2}{3}$. Celé číslo $x \geq 2$ splňující nerovnosti

$$\frac{n+2}{3} < x \leq \frac{n}{2}$$

zřejmě existuje, pokud $n \geq 6$. Pro hodnoty $n = 4, 5$ ověříme Dehnův odhad (D) přímým dosazením:

$$\begin{aligned} n = 4: &\quad p_4 = 11 < \sqrt{2 \cdot 3 \cdot 5 \cdot 7} = \sqrt{210} \\ n = 5: &\quad p_5 = 13 < \sqrt{2 \cdot 3 \cdot 5 \cdot 7 \cdot 11} = \sqrt{2310} \end{aligned}$$

Tím je důkaz odhadu (D) ukončen. Všimněme si, že výsledný odhad (D), který je „řádově" dvakrát lepší než Eukleidův odhad (E), by mohl být ještě kvalitnější, kdybychom lépe odhadli nejmenší index x splňující nerovnost $n + 1 < x + p_x$. Pokuste se o to sami tak, že srovnáte posloupnost (*) všech prvočísel (od členu p_3) s posloupností

$$5, 7, 11, 13, 17, 19, 23, 25, 31, 33, \ldots$$

přirozených čísel tvaru $6k \pm 1$.

Jedna vlastnost čísla 30. Nyní ukážeme, že Dehnův odhad (D) má jednu pěknou praktickou aplikaci (podle článku [Ra]). Všimněme si, že číslo $A = 30$ má zajímavou vlastnost: vypíšeme-li všechna menší čísla, která jsou s ním nesoudělná

$$1, 7, 11, 13, 17, 19, 23, 29,$$

vidíme, že jsou to (až na číslo 1) prvočísla. Tuto vlastnost mají i některá menší čísla A (např. 3, 4, 18). Marně však budeme hledat takové číslo A, které by bylo větší než 30. Dokažme s pomocí odhadu (D), že žádné takové číslo neexistuje. Skutečně, má-li číslo A popsanou vlastnost a je-li přitom větší než 25, pak je dělitelné čísly 2, 3 a 5 (jinak by 2^2, 3^2 nebo 5^2 bylo číslo menší než A jsoucí s číslem A nesoudělné). Proto je A násobkem čísla 30, takže buď $A = 30$, nebo $A \geq 60$. Ve druhém případě číslo A musí být násobkem sedmi, neboť $A > 7^2$. Proto $A \geq 60 \cdot 7 > 11^2$. Obecně: je-li A dělitelné všemi prvočísly p_1, p_2, ..., p_n, potom platí $A \geq p_1 \cdot p_2 \cdots p_n$, což podle odhadu (D) znamená, že $A > p_{n+1}^2$; pak ale číslo A musí být dělitelné i prvočíslem p_{n+1} a indukční „smyčka" se uzavírá. Vychází, že číslo A by v případě $A \geq 60$ muselo být násobkem *všech* prvočísel, což není možné. Tak jsme dokázali, že číslo $A = 30$ je největší přirozené číslo s vlastností: *každé přirozené číslo* x $(1 < x < A)$, *které je s číslem* A *nesoudělné, je prvočíslo.*

Počet prvočísel tvaru 3k+2. Každé prvočíslo, které se nerovná třem, dává při dělení třemi buď zbytek 1, nebo zbytek 2. Říkáme, že v prvním případě jde o prvočíslo tvaru $3k + 1$, ve druhém o prvočíslo tvaru $3k + 2$. Malá obměna Eukleidova postupu vede k závěru, že prvočísel tvaru $3k+2$ je nekonečně mnoho. Skutečně, pro libovolně velké přirozené $N \geq 3$ uvážíme číslo

$$M = 2 \cdot 3 \cdots N - 1 = N! - 1 .$$

Jak jsme zdůraznili už dříve, číslo M není dělitelné žádným prvočíslem nepřevyšujícím číslo N. Protože číslo $N!$ je násobkem tří, je zbytek čísla M při dělení třemi roven dvěma. Proto je buď samo číslo M prvočíslem, které je větší než N a je tvaru $3k + 2$, nebo je součinem několika prvočísel, která jsou větší než N. Mezi těmito činiteli *musí být aspoň jedno prvočíslo tvaru* $3k + 2$, neboť je jasné, že součin

$$(3k_1 + 1) \cdot (3k_2 + 1) \cdots (3k_s + 1)$$

je číslo, které při dělení třemi dává zbytek 1. Tím jsme dokázali, že *neexistuje největší prvočíslo tvaru* $3k + 2$.

Je překvapivé, že se doposud nikomu nepodařilo obměnit Eukleidův postup tak, aby vedl k závěru, že i prvočísel tvaru $3k + 1$ je nekonečně mnoho. (Autor má věrohodné informace, že se o to pokoušeli a pokoušejí docela seriózní matematikové.) Elementární důkaz o nekonečnosti množiny prvočísel tvaru $3k + 1$ existuje, využívá však některé výsledky teorie kvadratických forem (viz [Ry]), takže je hodně vzdálen Eukleidově myšlence. Sami se můžete přesvědčit, že obměnou Eukleidova postupu lze rovněž dokázat existenci nekonečně mnoha prvočísel tvarů $4k + 3$ a $6k + 5$. V této souvislosti připomeňme na závěr Dirichletovu větu, významný výsledek analytické teorie čísel:

Jsou-li a *a* b *dvě nesoudělná přirozená čísla, pak v aritmetické posloupnosti*

$$a + b,\ 2a + b,\ 3a + b,\ 4a + b,\ \ldots$$

se vyskytuje nekonečně mnoho prvočísel. (Jinak řečeno, existuje nekonečně mnoho prvočísel tvaru $a \cdot k + b$.)

LITERATURA

[E] Eukleides, *Základy*, přeložil František Servít, Jednota českých matematiků, Praha, 1907, Kniha devátá, oddíl 20, str. 149-150.

[Ra] Rademacher G., *Ob odnom svojstve čisla 30*, Kvant č. 3 (1992), str. 6-11.

[Ry] Rychlík K., *Úvod do elementární číselné theorie*, Přírodovědecké nakladatelství (JČ-MF), Praha, 1950.

[S] Sierpiń W., *250 zadač po elementarnoj těorii čisel*, Prosvěščenije, Moskva, 1968.

[U] Ufnarovskij V., *Progulka do těoremy Čebyševa*, Kvant č. 6 (1992), str. 8-13.