Učitel matematiky

Eduard Fuchs

Co ještě nevíme o přirozených číslech (1) aneb Některé vlastnosti prvočísel

Učitel matematiky, Vol. 7 (1999), No. 1, 1–8

Persistent URL: http://dml.cz/dmlcz/150960

CO JEŠTĚ NEVÍME O PŘIROZENÝCH ČÍSLECH (1)

aneb

Některé vlastnosti prvočísel

EDUARD FUCHS

Moderní matematika prodělává převratný vývoj. Vznikají nové disciplíny a matematické metody se prosazují i v těch oborech, kde to ještě nedávno bylo zcela nepředstavitelné. Specializace uvnitř matematiky samotné dostoupila takového stupně, že odborníci z různých oblasti se jen obtížně dorozumívají a zcela jistě neexistuje člověk, který by rozuměl všem matematickým oborům. Za této situace se zdá téměř neuvěřitelné, že dodnes neumíme zodpovědět řadu na první pohled banálních otázek o vlastnostech přirozených čísel. Vždyť přirozená čísla patří mezi nejzákladnější matematické pojmy; jejich intuitivní představu si samostatně vytvářejí již děti v předškolním věku a provázejí nás celým životem. I lidé, kteří hrdě prohlašují, že *matematiku k ničemu nepotřebují*, s přirozenými čísly denně operují.

Nebude snad proto nezajímavé, všimnout si v seriálu několika článků některých překvapujících vlastností přirozených čísel a uvést některé hypotézy, na něž dodnes neznáme odpověď.

1. Kolik je všech prvočísel?

Otázka v nadpisu je samozřejmě pouze řečnická. Každý středoškolák by měl umět dokázat, že *prvočísel je nekonečně mnoho.* Připustíme-li totiž, že všech pročísel je pouze konečně mnoho, můžeme je označit například $p_1, p_2, \ldots, p_n$. Číslo $p_1 \cdot p_2 \cdot \ldots \cdot p_n + 1$ pak ale není dělitelné žádným z čísel $p_i, i = 1, \ldots, n$ (neboť při dělení je zbytek 1), takže je prvočíslem různým od všech p_i nebo je dělitelné některým dalším prvočíslem. Předpoklad tedy vede ke sporu, takže prvočísel je nekonečně mnoho.

Naznačený důkaz je možno nalézt již v EUKLEIDOVÝCH[1] *Základech.* V této souvislosti je však nutno se zmínit o jedné věci. Kdybychom četli pozorně Eukleida, povšimli bychom si, že výše uvedené tvrzení o prvočíslech formuluje takto: *Prvočísel je více než jakékoli dané množství.*

Nebudeme zde podrobně rozvádět důvody, proč se u Eukleida (a ani u dalších matematiků té doby) nenajde formulace, že nějaký systém je tvořen **nekonečně mnoha** prvky. To souvisí s chápáním nekonečna, které bylo nejen v matematice až do konce minulého století zcela odlišné od našeho dnešního přístupu. Teprve s vybudováním teorie množin v závěru 19. století se v matematice začalo pracovat s tzv. **aktuálním nekonečnem**, začaly se zkoumat nekonečné množiny chápané jako jeden — definitivně vytvořený — celek. A tak dnes považujeme tvrzení typu, že *přirozených čísel je nekonečně mnoho* za banální a samozřejmé. Přestože nikdy nevypíšeme **všechna** přirozená čísla, přestože nikdy množinu všech přirozených čísel nevytvoříme, pracujeme běžně s množinou *všech* přirozených čísel a s podobnými matematickým objekty. Své zkušenosti s chováním „malých" přirozených čísel bez zábran přenášíme na celou nekonečnou množinu a tuto představu vštěpujeme od školních let dětem. Tak se nám během několika málo minulých desetiletí podařilo překonat „strach z nekonečna", typický pro myšlení od antických dob.

Naznačme si však alespoň ve stručnosti, jakého stupně abstrakce se odvažujeme, když z faktu, že za každým přirozeným n následuje číslo $n + 1$ a tedy přirozených čísel je *více než jakýkoliv předem daný počet* (řečeno s Eukleidem), přejdeme k tomu, že zkoumáme celou množinu

$$1, 2, 3, \ldots, 10, \ldots, 100, \ldots, 1\,000\,000, \ldots, 10^{7\,000\,000}, \ldots$$

v níž platí, že když napíšeme jakkoliv velké číslo, je úsek od 1 k tomuto číslu pouze **konečný** a to podstatné, tj. **nekonečně mnoho** přirozených čísel za napsaným číslem teprve následuje.

---

[1] EUKLEIDÉS z Alexandrie (asi 340 - asi 278 př. Kr.), jeden z největších starořeckých matematiků. V knize *Základy* shrnul většinu tehdejších matematických poznatků. Význam tohoto díla přesáhl tisíciletí a dodnes je aktuální.

Protože se v dalším textu budou různá „velká“ čísla často vyskytovat, uvědomme si, o čem to vlastně bez „obav a strachu“ hovoříme.

Uvažujme knihu standardní velikosti, která má na stránce cca 50 řádků a na řádku je cca 70 znaků, takže průměrná stránka obsahuje přibližně 3 500 symbolů. Protože — snad až na naprosté výjimky — mají všechny knihy maximálně 10 000 stránek, obsahují maximálně 35 miliónů znaků. Uvědomíme-li si, že jakýkoliv text (alespoň ve „standardních“ evropských jazycích) dnes napíšeme pomocí počítače, jehož klávesnice má přibližně 100 kláves, zjistíme snadno, že všech „textů“ udané délky (a samozřejmě i všech kratších — stačí je přece doplnit mezerníkem) je maximálně $10^{70\,000\,000}$.

Proč jsme slovo *texty* dávali do uvozovek? Většina těchto „textů“ totiž budou jen chaotické posloupnosti symbolů. Přesto však mezi nimi budou prakticky všechna smysluplná díla, která kdy kdo napsal a v budoucnosti napíše (a navíc každé z nich v překladu do všech evropských jazyků). Budou zde všechny vaše dopisy, i ty nikdy nenapsané, a všechny písemky, které si kdy vymysleli a v budoucnosti učitelé na své žáky vymyslí, všechny vědecké práce, které kdy lidé napsali a napíší, ... A to všechno lze „vyrobit“ v **konečném** čase. Kdybychom — obrazně řečeno — posadili k počítači šimpanze, který bude namátkově tisknout klávesy na počítači rychlostí 10 úhozů za sekundu, pak by (kdyby pracoval bez přestávky) všechny popisované záznamy vyrobil za $10^{7\,000\,000}$ sekund, což je číslo, které jsme před chvílí ve výčtu přirozených čísel napsali, aniž pravděpodobně vzbudilo čtenářovu zvláštní pozornost.

Abychom si uvědomili, jakou informaci vlastně poslední věta sděluje, zamysleme se nad tím, jak dlouho by ona hypotetická opice musela ve skutečnosti pracovat; pak si ihned uvědomíme, že se velikost udaného čísla vymyká naší veškeré představivosti. Stačí snad, abychom si připomenuli, že od tzv. „velkého třesku“, při němž vznikl náš vesmír, uplynulo cca 15 miliard let, což je méně než 10^{17} sekund. Náš fiktivní šimpanz by ovšem neměl málo jen času, ale i materiálu k uskutečnění posaného procesu. Počet všech

atomů v našem vesmíru je totiž odhadován číslem 10^{100}. Je nám nyní jasná velikost čísla $10^{7\,000\,000}$? A snad budeme také trochu méně sebevědomě přistupovat k faktu, že teprve **za** tímto číslem následuje podstatná část množiny $\mathbb{N}$ všech přirozených čísel, o níž tak suverénně v hodinách matematiky hovoříme.

2. Jak jsou prvočísla rozmístěna v $\mathbb{N}$?

Vraťme se nyní k úvahám o množině všech prvočísel, která — jak jsme si již připomenuli — je rovněž nekonečná. Za **každým** přirozeným číslem tedy následuje nekonečně mnoho prvočísel. Jak však jsou prvočísla v množině $\mathbb{N}$ rozmístěna?

256	255	254	253	252	251	250	249	248	247	246	245	244	243	242	241
197	196	195	194	193	192	191	190	189	188	187	186	185	184	183	240
198	145	144	143	142	141	140	139	138	137	136	135	134	133	182	239
199	146	101	100	99	98	97	96	95	94	93	92	91	132	181	238
200	147	102	65	64	63	62	61	60	59	58	57	90	131	180	237
201	148	103	66	37	36	35	34	33	32	31	56	89	130	179	236
202	149	104	67	38	17	16	15	14	13	30	55	88	129	178	235
203	150	105	68	39	18	5	4	3	12	29	54	87	128	177	234
204	151	106	69	40	19	6	1	2	11	28	53	86	127	176	233
205	152	107	70	41	20	7	8	9	10	27	52	85	126	175	232
206	153	108	71	42	21	22	23	24	25	26	51	84	125	174	231
207	154	109	72	43	44	45	46	47	48	49	50	83	124	173	230
208	155	110	73	74	75	76	77	78	79	80	81	82	123	172	229
209	156	111	112	113	114	115	116	117	118	119	120	121	122	171	228
210	157	158	159	160	161	162	163	164	165	166	167	168	169	170	227
211	212	213	214	215	216	217	218	219	220	221	222	223	224	225	226

Některé hypotézy je obtížné byť jen zformulovat. Na ukázku uvádíme zajímavost, kterou odhalil americký matematik polského

původu Stanislaw Marcin ULAM (1909 – 1984) při řešení úloh na šachovnici. Když začneme do polí (nekonečné) šachovnice zapisovat postupně „do spirály" přirozená čísla, začnou se prvočísla zajímavým způsobem skládat do různě dlouhých „úhlopříček" vytvářeného schématu. Prohlédneme-li si na předchozí stránce uvedený začátek této „Ulamovy spirály" (prvočísla jsou zvýrazněna), je zřejmé, že prvočísla zde nejsou rozložena nahodile. Nějaká zákonitost však zatím popsána není.

Vraťme se však k některým klasickým výsledkům. Zajímavou hypotézu vyslovili nezávisle na sobě v roce 1783 EULER[2] a v r. 1785 LEGENDRE[3].

Hypotéza. *Jsou-li a, b libovolná přirozená nesoudělná čísla, obsahuje aritmetická posloupnost*

$$a, a+b, a+2b, \ldots, a+nb, \ldots$$

nekonečně mnoho prvočísel.

Legendre tuto hypotézu dokázal v r. 1808, později se však ukázalo, že jeho důkaz byl chybný. Přesný důkaz podal až v roce 1837 DIRICHLET.[4]

Položme si v této souvislosti opačný úkol: chceme najít úsek aritmetické posloupnosti tvořený výhradně prvočísly. První tři následující příklady lze nalézt vcelku snadno:

3, 5, 7
5, 11, 17, 23, 29
7, 37, 67, 97, 127, 157

Podstatně komplikovanější je však nalezení delších úseků aritmetických posloupností. Nejdelší dodnes známý příklad je tvořen 18 prvočísly:

$$107\,928\,278\,317 + k \cdot 9\,922\,782\,870, \quad k = 0, 1, 2, \ldots, 17.$$

---

[2]Leonhard EULER (1707 – 1783), švýcarský matematik, jeden z nejvýznamnějších matematiků všech dob

[3]Adrian-Marie LEGENDRE (1752 – 1833), francouzský matematik

[4]Peter Gustav Lejeune DIRICHLET (1805 – 1859), německý matematik

Jen pro ilustraci výsledků, které bylo možno zjistit jen s nasazením výkonné výpočetní techniky, uveďme ještě jeden výsledek o aritmetických posloupnostech přirozených čísel.

Když si prohlédneme uvedené aritmetické posloupnosti, vidíme, že — až na první velmi jednoduchý příklad — jsou sice uvedené úseky aritmetických posloupností tvořeny prvočísly, avšak tato prvočísla nenásledují bezprostředně po sobě; některá jsou jednoduše vynechána (například ve druhé jsou vynechána prvočísla 7, 13 a 19). Nabízí se tedy otázka, *jaká je nejdelší známá aritmetická posloupost po sobě jdoucích prvočísel*?

Harvey DUBNER a Harry NELSON nalezli 29. 8. 1995 takovou posloupnost tvořenou 7 prvočísly:

1 089 533 431 247 059 310 875 780 378 922 957 732 908 036 492 993 138 195 385 213 105 561 742 150 447 308 967 213 141 717 486 151 $+k \cdot 210$, $k = 0, 1, \ldots, 6$.

Snad ještě zajímavější je však problém, *jak dlouhý může být v* $\mathbb{N}$ *úsek bez prvočísel*? Při pozorné prohlídce tabulky prvočísel bychom takovou „pauzu“ například mohli nalézt mezi čísly 1 671 800 a 1 671 900. Existují však v množině prvočísel mezery podstatně delší?

Do značné míry je překvapující zjištění, že *v množině přirozených čísel existují bez prvočísel* **libovolně dlouhé** *úseky*. Důkaz tohoto překvapujícího zjištění je navíc zcela banální. Zvolíme-li totiž libovolné přirozené n, neleží v úseku

$$(n+1)! + 2,\ (n+1)! + 3, \ldots, (n+1)! + n + 1$$

zcela jistě žádné prvočíslo, protože číslo $(n+1)! + 2$ je dělitelné 2, číslo $(n+1)! + 3$ je dělitelné 3 atd. (Připomeňme si v této souvislosti, jak obrovská mohou být přirozená čísla a znovu si uvědomme, že **jakkoliv velké** přirozené číslo zvolíme, existuje v $\mathbb{N}$ úsek této délky bez prvočísel, ačkoliv je jich **nekonečně mnoho**!)

3. Formule pro vyhledávání prvočísel

Přestože je posloupnost všech prvočísel nekonečná, neřekli jsme si zatím nic o tom, jak lze prvočísla vyhledávat, respektive jak je lze postupně „vypočítávat“.

První relativně účinnou metodu pro vzhledávání prvočísel popsal již kolem roku 225 př. Kr. ERATOSTHENÉS.[5] Tzv. *Eratostenovo síto* spočívá v postupném vyškrtávání násobků přirozených čísel, takže nakonec v takto vzniklém „sítu" uvíznou jen prvočísla. Tomuto postupu se učí školáci již déle než dva tisíce let. Za zmínku však stojí skutečnost, že je vhodné si toto síto představit napsáno do šesti sloupců. Protože každé prvočíslo větší než 5 je evidentně tvaru $6k+1$ nebo $6k+5$, zůstanou kromě prvního řádku všechna další prvočísla v 1. a 5. sloupci:

–	2	3	–	5
7	–	–	–	11
13	–	–	–	17
19	–	–	–	23
–	–	–	–	29
31	–	–	–	–
37	–	–	–	41
43	–	–	–	47
–	–	–	–	53
–	–	–	–	59
61	–	–	–	–
67	–	–	–	71
73	–	–	–	–
79	–	–	–	83
–	–	–	–	89
–	–	–	–	–
97	–	–	–	101

Jakkoliv je Eratostenovo síto jednoduché a užitečné, je zřejmé, že k vyhledávání větších prvočísel nám příliš nepomůže. Označíme-li rostoucí posloupnost všech prvočísel

$$p_1, p_2, \ldots, p_n, \ldots$$

(a toto označení budeme dodržovat v celém dalším textu), bylo by jistě nejpohodlnější, kdyby existovala taková funkce $f(x)$, že

[5] ERATOSTHENÉS z Kyrény (asi 276 př. Kr. – asi 194 př. Kr.), starořecký matematik a astronom, přítel Archimédův

by pro každé přirozené n platilo

$$f(n) = p_n.$$

Potíž je v tom, že takovou formuli dodnes neznáme a dokonce ani nevíme, zda taková formule v „rozumném“ tvaru vůbec existuje.

Když tedy není k dispozici formule, která by umožňovala počítat postupně **všechna** prvočísla, je přirozené snažit se odvodit takovou formuli

$$g(n) = p_{n_k},$$

že (p_{n_k})je rostoucí posloupnost prvočísel, tj. — jinak řečeno — $g(n)$ postupně nabývá stále větších **prvočíselných** hodnot.

O tom, že ani tato úloha není dodnes vyřešena a o zajímavých výsledcích s ní spojených, budeme hovořit v příštím pokračování našeho seriálu. Nyní se závěrem zmiňme o ještě mírnější úpravě popsaného problému. Neznáme-li funkci $g(x)$, která by v přirozených číslech postupně nabývala prvočíselných hodnot, je přirozené hledat takovou funkci $h(x)$, že funkce $h(n)$ je rostoucí a nabývá „co nejčastěji“ prvočíselných hodnot .

Pozoruhodných výsledků v tomto směru dosáhl především již zmiňovaný Leonhard EULER. Z řady funkcí s uvedenou vlastností, které nalezl, uveďme jen následující tři polynomy:

$$x^2 + x + 17, \qquad x^2 + x + 41, \qquad x^2 - 79x + 1,$$

které nabývaji prvočíselných hodnot *bez přerušení* pro $x = 0, 1, \ldots$ $\ldots, 15$, resp. $x = 0, 1, \ldots, 39$, resp. $x = 0, 1, \ldots, 78$.

V jistém smyslu „nejlepší“ z uvedených tří polynomů je druhý z nich, který pro hodnoty $x = 0, 1, \ldots, 2\,377$ nabývá prvočíselných hodnot v polovině případů.

Pokračování příště