Eduard Fuchs

Co ještě nevíme o prvočíslech

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. 140–161.

Persistent URL: http://dml.cz/dmlcz/400592

CO JEŠTĚ NEVÍME O PRVOČÍSLECH

EDUARD FUCHS

Zdá se téměř neuvěřitelné, že současná matematika, přes veškerý závratný rozvoj, neumí zodpovědět řadu na první pohled banálních otázek o vlastnostech přirozených čísel a prvočísel zejména. Přirozená čísla patří mezi nejzákladnější matematické pojmy; jejich intuitivní představu si samostatně vytvářejí již děti předškolního věku. A přesto dodnes neznáme odpovědi na řadu hypotéz zformulovaných již před staletími.

Z širšího okruhu problémů a výsledků o vlastnostech prvočísel si povšimněme blíže následujících: kolik je všech prvočísel, jak jsou prvočísla rozložena v množině **N** a jak se hledají „velká" prvočísla. Nakonec uvedeme několik nejznámějších a dodnes nezodpovězených hypotéz.

1. Kolik je všech prvočísel?

Každý středoškolák by měl dnes vědět a měl by také umět dokázat, že *prvočísel je nekonečně mnoho*. Připustíme-li totiž, že všech prvočísel je pouze konečně mnoho, můžeme je označit například $p_1, p_2, \ldots, p_n$. Číslo $p_1.p_2.\ldots.p_n + 1$ 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. Předpoklad tedy vede ke sporu, takže prvočísel je nutně nekonečně mnoho.

Uvedená úvaha je natolik jednoduchá, že by bylo překvapující, kdyby nebyla známa již dávno. Skutečně, nekonečný počet prvočísel dokazuje již EUKLEIDÉS v „Základech" kolem r. 300 př. n. l. Pro ilustraci Eukleidova stylu a pro demonstraci mnoha typických postupů antické matematiky ocitujme příslušnou část 9. knihy Eukleidových Základů.

...

XX.

Prvočísel jest více než jakékoli dané množství prvočísel.

Buďte dána prvočísla A, B, C; tvrdím, že jest více prvočísel než A, B, C.

Uvažme nejmenší číslo dělitelné čísly A, B, C, nechť to je DE a přičtěme k DE jednotku DF. Číslo EF tedy buďto prvočíslo je nebo není. Nechť nejprve prvočíslem jest; jsou tedy nalezena prvočísla A, B, C, EF, jejichž počet jest více než A, B, C.

Nechť tedy EF není prvočíslo; je tedy některým prvočíslem dělitelné. Nechť ho dělí prvočíslo G; tvrdím, že G není rovno žádnému z čísel A, B, C. Nuže, připusťme, že je některému z těchto čísel rovno. Avšak A, B, C dělí číslo DE;tedy číslo G rovněž dělí DE. Pak ale dělí i číslo EF; G pak ale dělí i zbývající jednotku DF, ačkoliv je číslem a to jest nesmysl. G tedy není rovno žádnému z čísel A, B, C. A přitom jest prvočíslem. Jest tedy nalezeno více prvočísel než je dané množství A, B, C, totiž A, B, C, G, což právě bylo dokázati.

...

Uvedený text je v Základech ilustrován úsečkami označenými písmeny A, B,C,G a úsečkou s koncovými body EF, na níž leží bod D. Z celého textu

je zřejmé, jak v praxi vypadal „geometrický" jazyk, v němž byla formulována tehdejší matematika včetně aritmetiky, což, jak víme, byl důsledek **krize** vyvolané objevem čísel iracionálních.

Ještě zajímavější je však Eukleidova formulace tvrzení samotného. Čtenář si jistě uvědomuje, proč Euklides nemohl - zdánlivě jednodušeji - říci, že prvočísel je nekonečně mnoho. To by totiž znamenalo připuštění **aktuálního nekonečna**; jak však víme, bylo v Eukleidově době (a ještě mnohem déle - až do 19. století) přípustné pouze **nekonečno potenciální**.

Z mnoha různých zobecnění uvedeného Eukleidova výsledku uveďme alespoň hypotézu, kterou nezávisle na sobě vyslovili v r. 1783 EULER a v r. 1785 LEGENDRE.

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 pak podal až v r. 1837 DIRICHLET.

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

$$\begin{array}{llllll} 3, & 5, & 7 & & & \\ 5, & 11, & 17, & 23, & 29 & \\ 7, & 37, & 67, & 97, & 127, & 157. \end{array}$$

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

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

Uvedené příklady nás však již uvádějí do následující problematiky.

2. Jak jsou prvočísla rozložena v množině N všech přirozených čísel?

První relativně účinnou metodu pro vyhledávání prvočísel popsal již kolem roku 225 př.n.l. ERATOSTHENÉS. 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	–
.	.	.	.	.	.

Takto lze poměrně snadno sestavit tabulku „malých" prvočísel. V následující tabulce jsou uvedena všechna prvočísla menší než 1 000.

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	103	107	109	113	127	131	137	139	149	151
157	163	167	173	179	181	191	193	197	199	211	223
227	229	233	239	241	251	257	263	269	271	277	281
283	293	307	311	313	317	331	337	347	349	353	359
367	373	379	383	389	397	401	409	419	421	431	433
439	443	449	457	461	463	467	479	487	491	499	503
509	521	523	541	547	557	563	596	571	577	587	593
599	601	607	613	617	619	631	641	643	647	653	659
661	673	677	683	691	701	709	719	727	733	739	743
751	757	761	769	773	787	797	809	811	821	823	827
829	839	853	857	859	863	877	881	883	887	907	911
919	929	937	941	947	953	967	971	977	983	991	997

Při podrobnějším zkoumání tabulky prvočísel si záhy povšimneme jistých zákonitostí . Tak například se v tabulce občas a nepravidelně objevují tzv. *prvočíselná dvojčata*, tj. dvojice prvočísel lišících se o 2, například 29, 31 nebo 881, 883 apod. „Hustota" prvočísel se však postupně snižuje. Pokusme se odpovědět na otázku, jak může být v **N** dlouhý úsek, v němž se nevyskytne **ani jedno prvočíslo?**

Kdybychom měli k dispozici dostatečně velké tabulky, snadno bychom například ověřili, že ani jedno prvočíslo neleží mezi čísly 1 671 800 a 1 671 900. Existují však v **N** delší úseky bez prvočísel?

Odpověď je velmi jednoduchá: *v* **N** *existují úseky libovolné délky neobsahující ani jedno prvočíslo.* Skutečně, zvolme libovolné přirozené číslo n. Pak v n-tici

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

není ani jedno prvočíslo, neboť $(n+1)!+2$ je dělitelné 2, $(n+1)+3$ dělitelné 3 atd.

Vraťme se však zpět k problému vyhledávání prvočísel v množině **N**. Protože je prvočísel nekonečně mnoho, označme pro další text jejich rostoucí posloupnost

$$p_1, p_2, p_3, \ldots, p_n, \ldots .$$

Pro určování prvočísel by jistě bylo nejpohodlnější, kdyby existovala taková funkce $f(x)$, že pro každé přirozené číslo n by platilo

$$f(n) = p_n.$$

Jak dnes víme, musely všechny pokusy o nalezení takového „vzorce" pro výpočet prvočísel skončit zákonitě nezdarem, neboť neexistuje **elementární** funkce f, která by výše uvedený požadavek splňovala.

* * *

V této souvislosti je nutno se zmínit o jednom nedorozumění. Leckdy se lze dočíst - viz například [7], že ruský matematik MATIJASEVIČ dokázal tvrzení, z něhož vyplývá existence polynomu 5. stupně, který ve výše uvedeném smyslu generuje všechna prvočísla. Pokud by toto tvrzení bylo správné, bylo by samozřejmě výše uvedené tvrzení o funkci f nesprávné. Oč tedy jde?

Německý matematik HILBERT v roce 1900 zformuloval 23 slavných problémů, které měly, dle jeho mínění, podstatně ovlivnit vývoj matematiky ve 20. století. V drtivé většině případů Hilbert skutečně odhadl velmi správně další vývoj matematiky a jím zformulované problémy se pro matematiku 20. století ukázaly jako klíčové. Na Hilbertově jasnozřivosti přitom nic nemění ani skutečnost, že v řadě případů bylo řešení problémů zcela jiné, než Hilbert samotný očekával.

Ačkoliv 8. z Hilbertových problémů je věnován přímo problematice prvočísel, nás nyní zajímá 10. Hilbertův problém, byť se na první pohled týká úplně jiné oblasti matematiky. Abychom však mohli zformulovat jeho podstatu, připomeňme si, co rozumíme *diofantickou rovnicí.*

Buď P polynom s celočíselnými koeficienty v proměnných $x_1, \ldots, x_n$. *Diofantickou rovnicí* nazýváme rovnici tvaru

$$P(x_1, \ldots, x_n) = 0,$$

přičemž *řešením* rozumíme každou n-tici **celých čísel**, která daný polynom anuluje.

Diofantická rovnice přitom řešení mít může a nemusí. Tak například rovnice

$$x^3y + 2xyz - 3xz + 2y^2 - 1 = 0$$

řešení má (například $x = 1$, $y = 1$, $z = 2$), diofantická rovnice

$$x^4 + 2y^2 + x^2y^2 - 1 = 0$$

evidentně žádné řešení nemá.

Pomocí diofantických rovnic lze zformulovat řadu klasických matematických problémů. Tak například tzv. *pytagorejské trojice* čísel jsou řešením diofantické rovnice

$$x^2 + y^2 = z^2,$$

tzv. **velká Fermatova věta** tvrdí, že diofantická rovnice

$$x^n + y^n = z^n$$

nemá řešení pro $n > 2$.

Ačkoliv byly diofantické rovnice od starověku intenzívně studovány, nebyl ještě ani na sklonku 19. století znám obecný algoritmus, který by umožnil zjistit, zda daná diofantická rovnice má či nemá řešení. Proto Hilbert zformuloval následující problém:

„Buď dána diofantická rovnice s libovolnými neznámými a s celočíselnými koeficienty. **Je třeba najít metodu, která by umožnila po konečném počtu operací rozhodnout, má-li tato rovnice řešení v celých číslech.**"

Z Hilbertovy formulace je zřejmé, že i když to výslovně neuvádí, byl přesvědčen, že požadovaný algoritmus jistě existuje a proto bude dříve nebo později objeven. Otázka, zda takový algoritmus **vůbec existuje**, nemohla být v roce 1900 dost dobře ani vyslovena.

K tomu, aby mohl být vůbec 10. Hilbertův problém řešen a vyřešen, musela matematika čekat na převratné výsledky GÖDELA, CHURCHE, TURINGA a dalších.

Definitivní vyřešení problému však podal až v r.1970 mladý petrohradský matematik J.V. MATIJASEVIČ. A jeho odpověď byla překvapivě **záporná**: hledaný algoritmus neexistuje.

Nyní již můžeme také odpovědět na otázku, jak 10. Hilbertův problém a Matijasevičovo řešení souvisí s námi studovanou problematikou prvočísel.

V r. 1960 dokázal H. PUTNAM mimořádně důvtipnou konstrukcí následující výsledek: „Existuje takový polynom $Q(y_1, \ldots, y_k, z)$ pátého stupně s celočíselnými koeficienty, že každou tzv. *rekurzivně spočetnou* množinu M přirozených čísel lze získat jako množinu nezáporných hodnot polynomu $Q(y_1, \ldots, y_k, a_M)$, kde a_M je konstanta, kterou lze pomocí množiny M vypočítat."

Matijasevič pak při řešení 10. Hilbertova problému dokázal, že množina P všech prvočísel je takovou rekurzivně spočetnou množinou, takže lze pomocí polynomu Q 5. stupně a ze znalosti konstanty a_P vypočítat.

Uvedená možnost je však přitom pouze **hypotetická** a vůbec nám neumožňuje množinu P takto získat, neboť k určení konstanty a_P je nutno sestavit vhodnou diofantickou rovnici, což vůbec neumíme a i kdyby se nám to podařilo, neuměli bychom ani zjistit, zda má nějaké řešení. Matijsevičův výsledek proto není v žádném rozporu s naším tvrzením, že neexistuje **elementární** funkce f taková, že $f(n) = p_n$.

* * *

Když tedy neexistuje elementární funkce f, jejíž hodnoty $f(n)$ jsou postupně **všechna** prvočísla, spokojme se alespoň se slabším požadavkem: hledejme takovou funkci f, že všechny hodnoty $f(n)$, $n \in \mathbf{N}$, jsou prvočíselné. V této souvislosti si všimněme tzv. Fermatových a Mersennových prvočísel.

Fermatova prvočísla

P. FERMAT v r. 1640 vyslovil domněnku, že pro každé celé číslo $n \geq 0$ je

$$F_n = 2^{2^n} + 1$$

prvočíslo, neuměl však tuto hypotézu dokázat.

Ověřit správnost Fermatovy hypotézy pro $n = 0, 1, 2, 3$ je triviální, neboť

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257.$$

Obtížné není ani ověřit, že prvočíslem je i číslo

$$F_4 = 2^{16} + 1 = 65\,537.$$

Vzhledem k tomu, jak nesmírně rychle roste posloupnost $(F_n)_{n=0}^{\infty}$, je však další ověřování Fermatovy hypotézy velmi obtížné.

Jakkoliv byl Fermat v mnoha případech až neuvěřitelně jasnozřivý, v tomto případě se spletl. (Dokonce, jak za chvíli ukážeme, zmýlil se téměř totálně.) V roce 1732 EULER dokázal, že

$$F_5 = 2^{32} + 1 = 4\ 294\ 967\ 297 = 641 \times 6\ 700\ 417,$$

čímž tedy Fermatovu hypotézu vyvrátil.

Prověření dalšího čísla F_6 se podařilo až téměř o 150 let později. V roce 1880 dokázal F. LANDRY, že F_6 je součinem dvou prvočísel:

$$F_6 = 2^{64} + 1 = 274\ 147 \times 67\ 280\ 421\ 310\ 721$$

V roce 1909 dokázali MOORHEAD a WESTERN, že i čísla F_7 a F_8 jsou složená, nenalezli však žádného dělitele těchto čísel. U čísla F_7, které má 39 číslic, se to podařilo až v r. 1970 MORRISONOVI a BRILHARTOVI, kteří dokázali, že F_7 je součinem dvou prvočísel

$$F_7 = (2^9.116503103764643 + 1)(2^9.11141971095088142685 + 1).$$

Dělitele čísla F_8 nalezli až v r. 1981 BRENT a POLLARD; je jím číslo

$$1\ 238\ 926\ 361\ 552\ 897.$$

SIERPINSKI v roce 1962 shrnul dosavadní výsledky a odvodil, že F_n není prvočíslem pro $n = 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 23, 36, 38, 39, 55, 58, 63, 73, 77, 81, 117, 125, 144, 150, 207, 226, 228, 260, 267, 284, 316, 452, 1945$.

Abychom docenili sílu těchto výsledků, stačí si uvědomit, že například číslo F_{1945} pravděpodobně nikdy nikdo nenapíše v dekadickém zápisu. Počet číslic tohoto čísla je totiž větší než 10^{582}, zatím co počet všech atomů v našem vesmíru je odhadován zhruba číslem 10^{100} a stáří našeho vesmíru od velkého třesku je menší než 10^{25} sekund.

Dovede si nyní někdo z nás alespoň představit, jak velké je číslo F_{9448}? Přesto byl v r. 1980 nalezen jeho dělitel

$$19.2^{9450} + 1.$$

Dnes se tedy zdá, že Fermat se v tomto případě spletl zcela zásadně: je více než pravděpodobné, že žádné číslo F_n pro $n > 4$ není prvočíslem. Zkoumání čísel F_n však přesto přineslo řadu pozoruhodných metod a výsledků, takže Fermatova hypotéza, byť nesprávná, přispěla k rozvoji teorie čísel podstatným způsobem.

Zmiňme se v této souvislosti o jedné zajímavé souvislosti čísel F_n a elementární geometrie. 30. března 1796 nalezl GAUSS konstrukci pravidelného

17-úhelníku pomocí kružítka a pravítka. Posléze pak odvodil následující tvrzení:

Nechť n je prvočíslo. Pravidelný n-úhelník lze sestrojit pomocí kružítka a pravítka právě tehdy, když je n Fermatovo prvočíslo.

Jak tedy vidíme, Fermatovi (ani nikomu dalšímu později), se nepodařilo najít takovou funkci f, aby všechny hodnoty $f(n)$ byla různá prvočísla. Zeslabme tedy tento požadavek ještě více. Chceme najít takovou funkci f, že **co nejvíce** hodnot $f(n)$ bude prvočíselných. Pozoruhodných výsledků v této souvislosti dosáhl již zmiňovaný EULER. Našel například následující kvadratické funkce:

$$x^2 + x + 17, \quad x^2 + x + 41, \quad x^2 - 79x + 1601,$$

které nabývají prvočíselných hodnot pro $x = 0, 1, \ldots, 15$, resp. $0, 1, \ldots, 39$, resp. $0, 1, \ldots, 78$.

V jistém smyslu „nejlepší" z uvedených tří polynomů je x^2+x+41, který pro hodnoty $x = 0, 1, 2, \ldots, 2377$ nabývá prvočíselných hodnot v polovině případů.

Poznamenejme v této souvislosti, že počtářská zručnost Eulera, Fermata a dalších byla obdivuhodná. Například o čísle 1 000 009 se dlouho myslelo, že je prvočíslem. Slepý Euler však odvodil, že je součinem čísel 293 a 3413. Podobně Fermat na dotaz, zda číslo 100 895 598 169 je prvočíslem, odpověděl takřka obratem, že nikoliv, neboť

$$100\,895\,598\,169 = 898\,423 \times 112\,303.$$

Jak jsme již uvedli, podobnou roli jako Fermatova prvočísla sehrála při studiu prvočísel tzv. *Mersennova prvočísla*. O těch se však zmíníme podrobněji v odstavci o hledání velkých prvočísel.

Studium vlastností funkce $\pi(x)$

Označme pro každé kladné číslo x symbolem $\pi(x)$ počet všech prvočísel $p \leq x$. Protože je prvočísel nekonečně mnoho, je $\pi(x)$ neomezená neklesající funkce.

Protože dodnes není známo, jak jsou prvočísla v $\mathbf{N}$ rozložena, je přirozená otázka, „jak rychle" funkce $\pi(x)$ vlastně roste. Jakou odpověď můžeme na tuto otázku očekávat? Hledáme nějakou „jednoduchou" funkci $f(x)$, která poroste „stejně rychle" jako funkce $\pi(x)$. Význam slov „stejně rychle" může být ovšem různý. Můžeme chtít, aby existovala kladná čísla $a < b$ taková, že pro všechna $x \geq 2$ platí $a \leq \frac{\pi(x)}{f(x)} \leq b$. Silnější požadavek na funkci $f(x)$ zní, aby si $f(x)$ a $\pi(x)$ byly tzv. „asymptoticky rovny", tj. aby $\lim_{x\to\infty} \frac{f(x)}{\pi(x)} = 1$. Můžeme dokonce chtít, aby samotný rozdíl $\pi(x) - f(x)$ byl „podstatně menší" než $f(x)$.

První hypotézu v tomto směru v r. 1798 naznačil a v r. 1808 přesně zformuloval A. M. LEGENDRE; uvedl, že za funkci $f(x)$ lze volit funkci $\frac{x}{\ln x}$, neboť

$$\lim_{x\to\infty} \frac{\pi(x).\ln x}{x} = 1. \qquad (*)$$

Naznačme stručně, jak mohl Legendre přijít na to, že funkcí, která roste „stejně rychle" jako $\pi(x)$ je právě funkce $\frac{x}{\ln x}$.

Již jsme uvedli, že i při zběžném pohledu do tabulky prvočísel uvidíme, že jejich hustota se postupně snižuje. Vyjádřeme nyní tuto tézi přesněji. V následující tabulce jsou v prvním sloupci mocniny 10, ve druhém sloupci jsou odpovídající hodnoty funkce $\pi(n)$, tj. počet prvočísel $p \leq n$ a v posledním sloupci jsou hodnoty podílu $\frac{n}{\pi(n)}$ zaokrouhlené na jedno desetinné číslo. Tento podíl tedy udává, na kolik přirozených čísel v intervalu $\langle 1, n\rangle$ připadá v průměru jedno prvočíslo.

n	$\pi(n)$	$n/\pi(n)$
10	4	2.5
100	25	4.0
1 000	168	6.0
10 000	1 229	8.1
100 000	9 592	10.4
1 000 000	78 498	12.7
10 000 000	664 579	15.0
100 000 000	5 761 455	17.4
1 000 000 000	50 847 534	19.7
10 000 000 000	455 052 512	22.0
⋮	⋮	⋮

Všimněme si nyní v tabulce pozorněji třetího sloupce. Vidíme, že při skoku o mocninu 10 na následující řádek, se hodnota příslušného podílu zvětší zhruba o 2,3 (například z 12.7 na 15.0, z 19.7 na 22.0 atd.). Uvědomíme-li si, že pro hodnotu přirozeného logaritmu 10 platí $\ln 10 = 2.30258\ldots$, je domněnka, že hodnota $\pi(n)$ je přibližně rovna zlomku $\frac{n}{\ln x}$, zcela přirozená.

Samotný Legendre však vztah $(*)$ nikdy nedokázal. První krok k důkazu uvedené rovnosti udělal v letech 1851-52 P.L. ČEBYŠEV. Ten především odvodil, že tzv. integrál-logaritmus, tj. funkce $\int_2^x \frac{du}{u}$ se hodí k aproximaci funkce $\pi(x)$ lépe než funkce $\frac{x}{\ln x}$. Z vlastností integrál-logaritmu pak odvodil, že pokud limita $\lim_{x\to\infty} \frac{\pi(x).\ln x}{x}$ existuje, je rovna jedné. Existenci této limity se však ani Čebyševovi nepodařilo dokázat. Velkým pokrokem však v té době byla jím odvozená skutečnost, že funkce $\frac{x}{\ln x}$ „dobře" aproximuje funkci $\pi(x)$ pro velká x. Odvodil totiž, že platí

$$a \leq \lim_{x\to\infty} \inf \frac{\pi(x).\ln x}{x} \leq \lim_{x\to\infty} \sup \frac{\pi(x).\ln x}{x} \leq \frac{6}{5}a,$$

kde $a = \ln(\sqrt{2}.\sqrt[3]{3}.\sqrt[5]{5}) - \ln \sqrt[30]{30} = 0,9129\ldots$, tj. $\frac{6}{5}a = 1,10555\ldots$.

Navíc z právě uvedených nerovností Čebyšev odvodil tzv. BERTRANDŮV postulát: *Pro každé přirozené číslo n leží mezi čísly n a $2n-2$ alespoň jedno prvočíslo.*

Z metodického hlediska spočívá Čebyševův přínos ve dvou hlavních skutečnostech .

Víme, že tzv. harmonická řada

$$\sum_{n=1}^{\infty} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n} + \ldots$$

diverguje, avšak pro každé reálné $s > 1$ řada

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \cdots + \frac{1}{n^s} + \ldots$$

konverguje. Vztah funkce $\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}$ k prvočíslům byl znám již EULEROVI: platí totiž (pro $s > 1$)

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \frac{1}{1 - \frac{1}{p^s}} \quad ,$$

kde v nekonečném součinu p probíhá všechna prvočísla. (Povšimněme si, jak odtud z divergence harmonické řady okamžitě vyplývá, že prvočísel je nekonečně mnoho. Protože harmonická řada diverguje, platí $\lim_{s \to 1+} \zeta(s) = \infty$. Kdyby prvočísel bylo jen konečně mnoho, byl by na pravé straně uvedené rovnosti součin konečně mnoha členů, takže jeho limita pro $s \to 1^+$ by byla konečná.)

Prvním Čebyševovým významným přínosem bylo, že při svých vyšetřováních podstatně využil vlastností funkce $\zeta(s)$. Dokázal například, že existuje konečná limita $\lim_{s \to 1+}[\zeta(s) - \frac{1}{s-1}]$

Druhým Čebyševovým přínosem bylo zavedení funkce $\vartheta(x) = \sum_{p \leq x} \ln p$ (p je prvočíslo). Dá se totiž ukázat, že asymptotické vlastnosti funkcí $\pi(x)$ a $\vartheta(x)$ jsou obdobné. Zejména platí, že formule $(*)$ je ekvivalentní se vztahem $\lim_{x \to \infty} \frac{\vartheta(x)}{x} = 1$, přičemž s funkcí $\vartheta(x)$ se pracuje podstatně lépe než s funkcí $\pi(x)$.

Vztah $(*)$ předpovídaný Legendrem dokázali nezávisle na sobě až v roce 1896 francouzští matematikové HADAMARD a VALLÉE POUSSIN. Jejich důkazy byly velmi obtížné a podstatně využívaly Riemannových metod, o nichž se zmíníme později.

Vztah $(*)$ samotný je pro svou důležitost často nazýván **základní větou o prvočíslech.**

3. Hledání velkých prvočísel

Víme, že prvočísel je sice nekonečně mnoho, nemáme však k dispozici žádnou formuli, která by nám je umožňovala postupně vypočítat. Hledání stále větších a větších prvočísel přitom bylo pro matematiky od dávnověku intelektuální výzvou, která v současné době má i významné aplikační aspekty. O některých postupech matematiků dřívějších období, kdy nebyla k dispozici výpočetní technika, se můžeme jen dohadovat. Již jsme se zmínili například o

některých podivuhodných výsledcích Fermata a Eulera. Fermat vyslovil, většinou bez důkazu, řadu hypotéz, které později Euler dokázal. Mezi takové případy patří například hypotéza, že *každé prvočíslo tvaru* $4n + 1$ $(n \in \mathbf{N})$, *lze jednoznačně vyjádřit jako součet čtverců dvou přirozených čísel*. Euler dokázal, že uvedená podmínka je dokonce nutná a postačující k tomu, aby číslo tvaru $4n + 1$ bylo prvočíslem. Je velmi pravděpodobné, že právě na základě tohoto poznatku Euler odvodil, že 1 000 009 není prvočíslo; snadno lze ověřit, že

$$1\,000\,009 = 1000^2 + 3^2 = 235^2 + 972^2.$$

Mezi „velká" prvočísla, která umožnila odhalit až moderní výpočetní technika, patří takové kuriozní případy, jako například *cyklické* číslo

$$1234567891234567891234567891234567891$$

nebo číslo

$$3141592653589793238462643383279502884 1,$$

které kopíruje začátek dekadického zápisu čísla π.

Zajímavá jsou v této souvislosti tzv. *„jedničková"* čísla R_n. (Označení je odvozeno od anglického názvu těchto čísel - *repunit*.) Jsou to čísla, jejichž dekadický zápis je tvořen samými jedničkami, tj.

$$R_1 = 1,\ R_2 = 11,\ R_3 = 111 \text{ atd.}$$

Číslo R_2 je prvočíslem a naskýtá se tedy otázka, zda jsou prvočísly i některá další jedničková čísla.

V roku 1918 dokázal čtenář jednoho zábavného časopisu, že prvočíslem je číslo R_{19}. Dodnes jsou známa jen tři další jedničková prvočísla: R_{23}, R_{317} a R_{1031}.

Číslo R_{317} nalezl H.C. WILLIAMS v r. 1978, důkaz toho, že R_{1031} je prvočíslem provedli Williams a DUNBAR po velkém úsilí až v r. 1985.

Jedničková čísla mají řadu zajímavých vlastností, až překvapivě mnoho údajů však o nich dodnes neznáme. Tak například číslo R_{71} je složené, neznáme však jeho řádného netriviálního dělitele. Některé rozklady čísel R_n jsou pozoruhodné; například

$$R_{38} = 11 \times 909090909090909091 \times 1111111111111111111,$$

přičemž

$$11 \times 909090909090909091 = 10000000000000000001.$$

Zajímavé jsou druhé mocniny jedničkových čísel; například

$$R_4^2 = 1234321$$

$$R_{13}^2 = 12345678900987654321.$$

Žádné jedničkové číslo není druhou mocninou přirozeného čísla, nevíme však, zda některé z nich je třetí mocninou. Nevíme ani, kolik je mezi čísly R_n prvočísel.

Mersennova prvočísla

V dnešní době se jako nejvýhodnější jeví hledat velká prvočísla mezi tzv. *Mersennovými čísly*.

Pro každé přirozené číslo n definujeme n-té Mersennovo číslo vztahem

$$M_n = 2^n - 1.$$

MERSENNE, přítel Descarta, Fermata, Pascala a řady dalších významných představitelů francouzské vědy 17. století, věděl, že když n **není** prvočíslo, nemůže být prvočíslem ani číslo M_n. S obráceným tvrzením je to však podstatně komplikovanější. Pro prvočíslo n **může** být číslo M_n prvočíslem, avšak - jak lze snadno ověřit - prvočíslem být nemusí.

Některá z těchto Mersennových prvočísel znali již staří Řekové:

$$M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127,\ M_{13} = 8191.$$

V r. 1603 dokázal P.A. CATALDI, že prvočísly jsou čísla M_{17} a M_{19}.

V r. 1644 vyslovil Mersenne hypotézu, že pro $n \leq 257$ jsou prvočísly právě M_n s indexy

$$1, 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257.$$

(Mersenne, na rozdíl od dnešní terminologie, považoval za prvočíslo i číslo 1.)

Prvočíselnost čísla M_{31} dokázal v roce 1750 EULER. V roce 1883 odvodil PERVUŠIN, že Mersenne zapomněl na index 61; číslo M_{61} je rovněž prvočíslem. První chybu v Mersennově seznamu objevil v roce 1903 americký matematik F.N. COLE, který na říjnovém zasedání Americké matematické společnosti v New Yorku předvedl, že

$$M_{67} = 2^{67} - 1 = 193\,707\,721 \times 761\,838\,257\,287.$$

Jak sám uvedl, hledal tuto faktorizaci celé víkendy po tři roky.

Již předtím, v r. 1876, potvrdil E. LUCAS, že číslo

$$M_{127} = 2^{127} - 1 = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727$$

je opravdu prvočíslem.

Později se ještě ukázalo, že v Mersennově seznamu chybí prvočísla M_{89} a M_{107}, na druhé straně tam nepatří číslo M_{257}, které je složené.

Jakkoliv se Mersenn ve svém seznamu v některých případech spletl, byla jeho výzva podnětná a jak se ukázalo, jsou čísla M_n mimořádně vhodná při snahách o nalezení velkých prvočísel. Dodnes je Mersennových prvočísel známo 32. Jejich přehled je uveden v tabulce, kterou uvedeme v následující části věnované tzv. *dokonalým číslům*.

Dokonalá čísla

S Mersennovými prvočísly úzce souvisí tzv. *dokonalá čísla*, jejichž vlastnosti fascinovaly již staré Řeky. Připomeňme si, že přirozené číslo n se nazývá *dokonalé*, jestliže je rovno součtu všech svých dělitelů, které jsou menší než n. První čtyři dokonalá čísla jsou 6, 28, 496 a 8 128. Skutečně,

$$6 = 1.2.3 = 1 + 2 + 3,\ 28 = 1 + 2 + 4 + 7 + 14 \text{ atd.}$$

Důležitou vlastnost dokonalých čísel popsal již EUKLEIDES v Základech; v IX. knize, části XXXVI dokazuje:

Když jest dáno po řadě od jednotky několik čísel v poměru jedné ku dvěma, až součet všech stane se prvočíslem, a když se ten součet znásobí číslem posledním a vznikne jiné, vzniklé číslo bude dokonalé.

Jinak řečeno, je-li $1+2+4+8+\cdots+2^n$ prvočíslo, pak je číslo $2^n(1+2+\cdots+2^n)$ dokonalé. Protože však

$$1 + 2 + \cdots + 2^n = 2^{n+1} - 1,$$

je souvislost dokonalých čísel a Mersennových prvočísel zřejmá: *je-li M_n Mersennovo prvočíslo, je číslo $2^{n-1}.M_n$ dokonalé.*

Eukleides samotný tedy dokázal **dostatečnost** uvedené podmínky. Až Euler o dva tisíce let později dokázal, že **sudá** dokonalá čísla jsou právě uvedeného tvaru $2^{n-1}.M_n$, kde M_n je Mersennovo prvočíslo. (Lichá dokonalá čísla jsou zcela jiným případem, o němž se zmíníme později.)

První čtyři výše uvedená dokonalá čísla znali již staří Řekové. Uvádí je například NÍKOMACHOS z Gerasy, řecký filosof z první poloviny 2. století n.l. ve své učebnici „Arithmétiké eisagógé" (Úvod do matematiky), která byla přeložena i do latiny a arabštiny. Asi o 150 let později komentoval Níkomachovu knihu IAMBLICHOS z Chalkidy (asi 275-330), který číslům připisoval různé mýtické vlastnosti. Protože čísla 6, 28, 496 a 8 128 mají postupně 1,2,3 a 4 cifry, vyslovil hypotézu, že pro každé přirozené n existuje právě jedno dokonalé číslo o n cifrách; dále pak Iamblichos předpokládá, že každé dokonalé číslo končí cifrou 6 nebo 8, přičemž se tyto cifry pravidelně střídají.

První část Iamblichovy hypotézy je nesprávná, což koneckonců není vůbec překvapující, neboť při této úvaze Iamblichos vychází z výhradné preference dekadického zápisu čísel, ačkoliv z čistě matematického hlediska není žádný důvod, proč desítkovou soustavu nadřazovat ostatním. Druhá část Iamblichovy hypotézy je alespoň zčásti správná; každé dokonalé číslo skutečně končí cifrou 6 nebo 8. Víme dokonce ještě více: každé dokonalé číslo končí buďto dvojčíslím 28 nebo cifrou 6, před kterou stojí liché číslo. Číslice 6 a 8 se však pravidelně nestřídají. Skutečná posloupnost koncových cifer je 6, 8, 6, 8, 6, 6, 8, 8, 6, 6, 8, 8, 6, 8, 8, ...

Dokonalá čísla mají řadu zajímavých vlastností. Tak například z jejich definice okamžitě plyne, že součet převrácených hodnot všech dělitelů dokonalého čísla je roven 2. Skutečně, jsou-li $d_1 < d_2 < \cdots < d_k$ všichni dělitelé dokonalého čísla n, je nutně $d_1 = 1$, $d_k = n$ a podle definice

$$d_1 + d_2 + \cdots + d_{k-1} = n.$$

Pak ale

$$n + n = d_1 + d_2 + \cdots + d_{k-1} + d_k,$$

takže

$$2 = \frac{1}{d_1} + \frac{1}{d_2} + \cdots + \frac{1}{d_k}.$$

Méně zřejmé je, že každé dokonalé číslo větší než 6 je některým částečným součtem nekonečné řady $\sum_{n=0}^{\infty}(2n+1)^3$; například

$$28 = 1^3 + 3^3, \quad 496 = 1^3 + 3^3 + 5^3 + 7^3.$$

Páté dokonalé číslo 33 550 336 se vyskytuje již ve středověkých rukopisech, není však známo, kdo je objevil. Šesté a sedmé dokonalé číslo našel v r. 1603 P. CATALDI; jejich hodnoty jsou 8 589 869 056 a 137 438 691 328.

Jak jsme již uvedli, je hledání dokonalých čísel bezprostředně spojeno s hledáním Mersennových prvočísel. Víme již tedy, že páté, šesté a sedmé dokonalé číslo je spojeno s objevem čísel M_{13}, M_{17} a M_{19}. Víme také, že další Mersennovo prvočíslo

$$M_{31} = 2\ 147\ 483\ 647$$

objevil Euler. Příslušné dokonalé číslo $2^{30}M_{31}$ bylo dlouho považované za největší dokonalé číslo, které bylo možno odhalit. Ještě například v roce 1814 napsal P. BARLOW ve své knize *A New Mathematical and Philosophical Dictionary*, že „*toto poslední dokonalé číslo je největším dokonalým číslem známým v současnosti a pravděpodobně největším, které kdy bude objeveno.*"

Zejména nástup výpočetní techniky ve 20. století umožnil odhalit podstatně větší dokonalá čísla. Přehled dosud známých dvaatřiceti dokonalých čísel (a tedy i dosud známých Mersennových prvočísel) je uveden v následující tabulce:

1	$2M_2$	6	znali již staří Řekové
2	2^2M_3	28	znali již staří Řekové
3	2^4M_5	496	znali již staří Řekové
4	2^6M_7	8128	znali již staří Řekové
5	$2^{12}M_{13}$	33550336	uvedeno ve středověkém rukopisu
6	$2^{16}M_{17}$	8589869056	Cataldi, 1588, $M_{17} = 131\ 071$
7	$2^{18}M_{19}$	137438691328	Cataldi, 1588, $M_{19} = 524\ 387$
8	$2^{30}M_{31}$		Euler, 1772, $M_{31} = 2\ 147\ 483\ 647$
9	$2^{60}M_{61}$		Pervušin, 1883
10	$2^{88}M_{89}$		Powers, 1911
11	$2^{106}M_{107}$		Powers, 1914
12	$2^{126}M_{127}$		Lucas, 1876; E.Fauquembergue, 1914
13	$2^{520}M_{521}$		počítač SWAC, 30. ledna 1952 National Standards Bureau
14	$2^{606}M_{607}$		nalezeno současně s $2^{520}M_{521}$
15	$2^{1278}M_{1279}$		rovněž SWAC, tatáž skupina
16	$2^{2202}M_{2203}$		rovněž SWAC, tatáž skupina
17	$2^{2280}M_{2281}$		rovněž SWAC, tatáž skupina
18	$2^{3216}M_{3217}$		

19	$2^{4252}M_{4253}$	
20	$2^{4422}M_{4423}$	
21	$2^{9688}M_{9689}$	
22	$2^{9940}M_{9941}$	
23	$2^{11212}M_{11213}$	University of Illinois at Urbana, 1963
24	$2^{19936}M_{19937}$	Bryant Tuckerman, 1971
25	$2^{21700}M_{21701}$	Laura Nickel a Curt Noll, 1978
26	$2^{23208}M_{23209}$	Curt Noll, 1979
27	$2^{44496}M_{44497}$	Harry Nelson, David Slowinski, 1979
28	$2^{86242}M_{86243}$	Harry Nelson, David Slowinski, 1982
29	$2^{132048}M_{132049}$	1983
30	$2^{216090}M_{216091}$	Chevron Geosciences, 1985
31	$2^{756838}M_{756839}$	David Slowinski, 1992
32	$2^{859432}M_{859433}$	

V této tabulce jsou všechna dokonalá čísla **sudá**. Vraťme se tedy nyní k otázce **lichých** dokonalých čísel. Jejich existence je jedním z dosud nevyřešených problémů a o důkazu jejich existence či neexistence panuje velká skepse. Ví se pouze, že pokud by existovala, musela by být nesmírně velká, patrně větší než 10^{200}, musí mít nejméně 8 prvočíselných dělitelů, z nichž největší musí být větší než 300 000; každé liché dokonalé číslo menší než 10^{9118} - pokud vůbec existuje - musí být dělitelné šestou mocninou některého prvočísla apod.

S dokonalými čísly souvisí tématika tzv. *spřátelených* čísel, proto se o nich stručně zmíníme.

Přirozená čísla a, b se nazývají *spřátelená*, jestliže součet vlastních dělitelů každého z nich je roven druhému číslu. První a nejmenší dvojici spřátelených čísel tvoří čísla 220 a 284. Skutečně,

$$220 = 2^2 \times 5 \times 11, \quad 284 = 2^2 \times 71.$$

Vlastní dělitelé čísla 220 jsou tedy 1, 2, 4, 5, 10, 11, 20, 22, 44, 55, 110, vlastní dělitelé čísla 284 jsou 1, 2, 4, 71 a 142 a platí

$$1+2+4+5+10+11+20+22+44+55+110 = 284, \; 1+2+4+71+142 = 220.$$

Podle již zmíněného Iamblicha znal tuto dvojici spřátelených čísel již Pythagoras. Ani Iamblichovi však nebylo jasné, zda existuje nějaká jiná spřátelená čísla a pokud ano, jak by je bylo možno najít. Zásadní krok v tomto směru učinil až arabský matematik, fyzik a astronom THABIT ibn Qurra, který podrobně studoval a popsal Eukleidovy výsledky o dokonalých číslech a v této souvislosti odhalil následující pozoruhodný výsledek:

jsou-li a, b, c prvočísla a pro vhodné $n > 1$ platí

$$a = 3 \times 2^n - 1, \quad b = 3 \times 2^{n-1} - 1, \quad c = 9 \times 2^{2n-1} - 1,$$

pak jsou čísla

$$2^n \times a \times b \quad \text{a} \quad 2^n \times c$$

spřátelená.

Nalezení dalších spřátelených čísel však podle uvedené Thabitovy formule není jednoduché, neboť vyžaduje současné nalezení tří prvočísel předepsaného tvaru. Thabit sám také žádnou další dvojici spřátelených čísel nenalezl.

Druhou dvojici spřátelených čísel nalezl až jiný arabský matematik ibn al-BANNA; jsou to čísla 17 296 a 18 416. Tato čísla odpovídají Thabitově formuli pro $n = 4$.

Thabitovy výsledky i uvedená druhá dvojice spřátelených čísel však upadly v zapomenutí. Jejich znovuobjevení čekalo téměř 800 let na FERMATA, který uvedenou dvojici sdělil v roce 1636 písemně Mersennovi. O pouhé dva roky později nalezl DESCARTES třetí dvojici: 9 363 584 a 9 437 056. Z Thabitovy formule ji obdržíme pro $n = 7$.

Thabitova formule **neplatí pro všechny** spřátelené dvojice. Dodnes není známo, kolik spřátelených dvojic ji splňuje, víme však, že pro $n < 20\,000$ jsou to právě jen uvedené dvojice pro $n = 2, 4$ a 7.

Problematice spřátelených čísel se intenzívně věnoval EULER. Nalezl více než 60 dvojic těchto čísel a jeho teoretické výsledky tvoří dodnes základ dalších zkoumání. V průběhu 17. a 18. století bylo postupně nalezeno mnoho dvojic spřátelených čísel. Vesměs však tato čísla byla velká - řádově v milionech nebo miliardách. Proto bylo pro matematickou veřejnost značným překvapením, když šestnáctiletý školák Niccolò PAGANINI v roce 1866 nalezl dvojici překvapivě „malých" spřátelených čísel: 1 184 a 1 210.

V současnosti je známo více než tisíc dvojic spřátelených čísel včetně všech těch, jejichž menší člen nepřesahuje jeden milion. Největší známou dvojicí spřátelených čísel jsou

$$3^4 \times 5 \times 11 \times 5\,281^{19} \times 29 \times 89(2 \times 1\,291 \times 5\,281^{19} - 1)$$

a

$$3^4 \times 5 \times 11 \times 5\,281^{19}(2^3 \times 3^3 \times 5^2 \times 1\,291 \times 5\,281^{19} - 1);$$

každé z těchto čísel má 152 číslic.

Víme, že dvojic spřátelených čísel je nekonečně mnoho. Všechny dosud známé dvojice jsou tvořeny soudělnými čísly, není však známo, zda existuje dvojice nesoudělných spřátelených čísel. Víme pouze, že v kladném případě by musel být jejich součin větší než 10^{67}.

Ve všech dosud známých dvojicích jsou obě čísla sudá nebo obě čísla lichá. Neví se však, zda existuje sudo-lichá dvojice spřátelených čísel. U dvojic sudých čísel nemůže být žádný člen dělitelný 3, známé dvojice lichých čísel jsou naopak zásadně násobky 3, není však dokázáno, zda tak tomu musí být vždy.

4. Hypotézy

V předcházejících odstavcích jsme se zmínili o řadě dodnes nedokázaných tvrzení a o mnoha nejasnostech, které problematiku prvočísel provázejí. Různých hypotéz v této oblasti je nepřeberně a jejich výčet by byl velmi pestrý. Jakkoliv je teorie v této oblasti velmi rozsáhlá, je stále možné a pravděpodobné,

že o mnoha zákonitostech zatím nemáme ani tušení. Jen na okraj uveďme v této souvislosti zajímavé odhalení, které učinil americký matematik ULAM 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 schematu. Prohlédneme-li si níže uvedený začátek této Ulamovy „spirály" (prvočísla jsou v rámečku), je zřejmé, že prvočísla zde nejsou rozložena nahodile. Nějaká zákonitost však zatím popsána není.

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	118	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
108	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

Nyní si však blíže povšimněme některých dnes již klasických hypotéz či problémů o prvočíslech.

Prvočíselná dvojčata

Již jsme se zmínili, že *prvočíselnými dvojčaty* rozumíme prvočísla a, b, jejichž rozdíl je 2. Tato dvojčata se vyskytují v celém dodnes probádaném úseku přirozených čísel; dobře zapamatovatelná prvočíselná dvojčata jsou například

$$1\,000\,000\,000\,061 \quad \text{a} \quad 1\,000\,000\,000\,063.$$

Největšími dodnes známými prvočíselnými dvojčaty jsou čísla

$$11\,591\,142\,985 \times 2^{2304} \pm 1.$$

Dodnes však není známo, zda je prvočíselných dvojčat **konečně nebo nekonečně** mnoho. Jistou nápovědou by snad mohla být následující skutečnost.

Již jsme se zmínili, že tzv. *harmonická řada* $\sum_{n=1}^{\infty} \frac{1}{n}$ diverguje, tj. ke každému kladnému číslu $A > 0$ existuje takové přirozené číslo n_0, že

$$\sum_{n=1}^{n_0} \frac{1}{n} = 1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n_0} > A.$$

* * *

Dovolme si nyní krátkou odbočku. Skutečnost, že *harmonická řada diverguje* je všeobecně známa a sdělení tohoto faktu například studenty při přednášce z matematické analýzy ponechá zcela chladnými. Uvědomme si však, že tato skutečnost například znamená, že když začneme pokrývat úsečku o délce rovné vzdálenosti naší Země od nejbližší hvězdy mimo naši sluneční soustavu - což, jak známo, je více než 4 světelné roky - úsečkami, z nichž první bude mít délku 1 mm, druhá $\frac{1}{2}$ mm, třetí $\frac{1}{3}$ mm atd., pak **konečným** počtem těchto úseček celou vzdálenost pokryjeme. I když samozřejmě nehrozí, že by někdy někdo náš vesmír takto konečným počtem prvků zahltil - stačí si totiž jen představit, jak obrovské musí potřebné číslo být, přece jen nám navozuje představu reálných problémů, které hrozí přijetím **aktuálního nekonečna**, kdy bez rozpaků pracujeme se součty **celých** nekonečných řad, kdy zkoumáme **nekonečné systémy** jako celky, které máme fakticky vytvořeny a studujeme jejich vlastnosti atd.

Harmonická řada je rovněž dobrým příkladem toho, jak mylná je domněnka, že by počítače mohly v dohledné době „vytlačit" matematiku z jejích pozic. Ani sebelepší počítače například dodnes „nepoznají", že tato řada diverguje. Její částečné součty totiž rostou tak pomalu, že ani nejvýkonnější současné počítače nedosáhnou hodnoty 20.

* * *

Jak jsme tedy uvedli, harmonická řada diverguje. Vybereme-li z této řady některé členy, může tato vybraná řada obecně rovněž divergovat nebo konvergovat. Například řada

$$\sum_{n=1}^{\infty} \frac{1}{2n} = \frac{1}{2} + \frac{1}{4} + \frac{1}{6} + \cdots$$

diverguje, zatímco řada

$$\sum_{n=1}^{\infty} \frac{1}{2^n} = \frac{1}{2} + \frac{1}{4} + \frac{1}{8} + \frac{1}{16} + \cdots$$

jak známo konverguje, neboť je to geometrická řada s kvocientem 1/2.

Nyní již můžeme zformulovat jeden významný rozdíl mezi posloupností $(p_n)_{n=1}^{\infty}$ všech prvočísel a posloupností těch prvočísel, která tvoří prvočíselná dvojčata. Řada

$$\sum_{n=1}^{\infty} \frac{1}{p_n} = \frac{1}{2} + \frac{1}{3} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{23} + \frac{1}{29} + \frac{1}{31} + \dots$$

diverguje, zatím co řada

$$\frac{1}{3} + \frac{1}{5} + \frac{1}{5} + \frac{1}{7} + \frac{1}{11} + \frac{1}{13} + \frac{1}{17} + \frac{1}{19} + \frac{1}{29} + \frac{1}{31} + \dots$$

odpovídající prvočíselným dvojčatům, konverguje. Součet této řady je nesmírně obtížné určit; nejlepší aproximace je 1.90195 ± 10^{-5}.

Tato skutečnost naznačuje, že pokud prvočíselných dvojčat není pouze konečně mnoho, je nicméně přechod od všech prvočísel k prvočíselným dvojčatům výraznějším kvalitativním zlomem než přechod od přirozených čísel k prvočíslům.

O prvočíselných dvojčatech však existuje řada hypotéz. Jak jsme již uvedli, ze *základní věty o prvočíslech* plyne, že když n je „velké" přirozené číslo, pak pravděpodobnost toho, že přirozené číslo $1 \leq x \leq n$ je prvočíslem, je přibližně $\frac{1}{\ln n}$. Čím větší je číslo n, tím lepší aproximaci přitom přitom tento vztah udává.

Na rozdíl od tohoto tvrzení, které - jak již víme - je **dokázáno**, jsou následující úvahy o prvočíselných dvojčatech pouhými **hypotézami**, i když podpořeny kvantitativními výsledky ověřenými na počítačích.

Zvolíme-li přirozené x tak, že $1 \leq x \leq n$, je pravděpodobnost toho, že x i $x+2$ jsou prvočísla, přibližně $\frac{1}{(\ln n)^2}$. Jinak řečeno, v intervalu $\langle 1, n\rangle$ leží přibližně $\frac{n}{(\ln n)^2}$ dvojic tvořících prvočíselná dvojčata. Jestliže číslo x z intervalu $\langle 1, n\rangle$ je prvočíslo, stoupne pravděpodobnost toho, že i $x + 2$ je prvočíslo, z hodnoty $\frac{n}{(\ln n)^2}$ na $\frac{(1.32032\dots)n}{(\ln n)^2}$.

Přitom platí, že $\lim_{n\to\infty} \frac{n}{(\ln n)^2} = \infty$, což by zase naznačovalo, že prvočíselných dvojčat je asi nekonečně mnoho. Jakkoliv jsou tyto úvahy nedokázané, panuje značná shoda z nich odvozených předpovědí se skutečností. V následující tabulce uvádíme pro zajímavost vztah mezi počtem předpovězených a nalezených dvojčat v několika intervalech o délce 150 000.

Interval	Prvočíselných dvojčat předpovězeno	nalezeno
< 100 000 000, 100 150 000 >	584	601
< 1 000 000 000, 1 000 150 000 >	461	466
< 10 000 000 000, 10 000 150 000 >	374	389
< 100 000 000 000, 100 000 150 000 >	309	276
< 1 000 000 000 000, 1 000 000 150 000 >	259	276
< 10 000 000 000 000, 10 000 000 150 000 >	221	208
< 100 000 000 000 000, 100 000 000 150 000 >	191	186
< 1 000 000 000 000 000, 1 000 000 000 150 000 >	166	161

Goldbachova hypotéza

Německý matematik GOLDBACH, který se zabýval především teorií čísel, zformuloval 7.7. 1742 v dopise Eulerovi hypotézu, že *každé sudé číslo větší než 2 je součtem dvou prvočísel.* (Jejím důsledkem je pak tzv. *ternární Goldbachův problém*: každé liché číslo $n > 7$ je součtem tří prvočísel.)

Uvedená Goldbachova hypotéza nebyla dodnes, přes nesmírné úsilí mnoha generací matematiků, ani dokázána ani vyvrácena. Mimořádně obtížnými metodami bylo dokázáno jen několik dílčích výsledků.

V r. 1937 dokázal I.M. VINOGRADOV jediný „definitivní" výsledek. Odvodil, že *existuje číslo n_0 takové, že každé liché číslo $n > n_0$ je součtem tří prvočísel.* Z jeho mimořádně obtížného důkazu však neplyne jak velké je ono číslo n_0, ví se pouze, že je nepředstavitelně velké. Tím je tedy, alespoň od jistého - i když nevíme kterého - čísla vyřešen ternární Goldbachův problém.

Již předtím, v r. 1930, dokázal L.G.ŠNIRELMAN, že *existuje takové přirozené k, že každé „dostatečně velké" číslo je součtem nejvýše k prvočísel.* Jeho metodami však nelze určit, jaká je hodnota onoho čísla k. Přestože od Šnirelmanova výsledku je k důkazu Goldbachovy hypotézy nesmírně daleko, jeden významný přínos tu přece jen je: víme alespoň, že všechna dostatečně velká sudá čísla jsou součtem takového počtu prvočísel, který nepřesáhne jistou hranici k.

Jiné zeslabení Goldbachovy hypotézy dokázal v roce 1957 již zmíněný VINOGRADOV: *každé dostatečně velké sudé číslo je součtem dvou „skoro prvočísel"* (tj. čísel, která lze rozložit na nejvýše tři prvočinitele).

Hypotéz o „součtových" vlastnostech přirozených čísel byla vyslovena celá řada. Z těch, které byly dokázány, uveďme například Fermatovu hypotézu z roku 1636: *každé přirozené číslo je součtem nejvýše tří trojúhelníkových čísel.* Správnost této domněnky potvrdil v roce 1801 GAUSS.

Z nevyřešených problémů tohoto typu uveďme alespoň tzv. **Waringův problém**, který patří spolu s Goldbachovou hypotézou k nejznámějším.

V roce 1770 zformuloval E. WARING ve své práci *Meditationes algebraicae* bez důkazu následující tvrzení: *každé přirozené číslo je součtem nejvýše devíti třetích mocnin, nejvýše devatenácti čtvrtých mocnin „a tak dále".* Přitom nespecifikoval smysl úsloví „a tak dále", ani nenaznačil, jak na svou úvahu přišel. Lze se jen dohadovat, že uvedený úsudek zformuloval na základě empiricky získaných výsledků pro relativně malá čísla.

Pro třetí mocniny je Waringovo tvrzení pravděpodobně správné, přičemž jsou známa pouze dvě přirozená čísla, k jejichž vyjádření je opravdu nutno využít 9 třetích mocnin:

$$23 = 2^3 + 2^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3 + 1^3,$$
$$239 = 4^3 + 4^3 + 3^3 + 3^3 + 3^3 + 3^3 + 1^3 + 1^3 + 1^3.$$

(Kdybychom ovšem připustili i třetí mocniny **záporných** čísel, platilo by například $23 = 3^3 + 4(-1)^3$, takže bychom vystačili s pěti třetími mocninami.)

Obecně se pak ukázalo, že je Waringův problém svou obtížností téměř srovnatelný s Goldbachovou hypotézou a dodnes nebyl obecně rozřešen. Až HIL-

BERT dokázal, že *pro každou mocninu k existuje takové číslo $g(k)$, že každé dostatečně velké přirozené číslo je součtem nejvýše $g(k)$ k-tých mocnin.* Ne všechna čísla jsou však „dostatečně velká" a otevřen zůstal i problém určení čísla $g(k)$.

Až v roce 1986 dokázali správnost Waringovy hypotézy pro $k = 4$ Ramachandran BALASUBRAMANIAN, Jean-Marc DESHOULLIERS a Francois DRESS. Nejmenším číslem, k jehož vyjádření opravdu potřebujeme 19 čtvrtých mocnin je 79, neboť

$$79 = 15 \times 1^4 + 4 \times 2^4.$$

Další známá čísla s touto vlastností jsou 159, 239, 319, 399 a 559.

Pro ostatní mocniny k není dodnes řešení Waringova problému známo. Předpokládá se pouze, že každé přirozené číslo je součtem nejvýše 37 pátých mocnin, nejvýše 73 šestých mocnin a každé dostatečně velké číslo je součtem nejvýše 137 sedmých mocnin.

Riemannova hypotéza

V souvislosti s vlastnostmi funkce $\pi(x)$ jsme se již zmínili o souvislosti funkce

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

s posloupností všech prvočísel.

Zásadním mezníkem v rozvoji moderní teorie prvočísel byl rok 1859, kdy svou práci o vlastnostech funkce ζ publikoval B. RIEMANN. Základní Riemannova myšlenka byla velmi jednoduchá: navrhl studovat funkci $\zeta(s)$ jako funkci **komplexní proměnné**, přičemž tato dnes běžně nazývaná *Riemannova funkce* $\zeta(z)$ je analytickým prodloužením „klasické" funkce $\zeta(s)$, definované pro reálná $s > 1$.

O takto definované funkci $\zeta(z)$ vyslovil Riemann pět hypotéz, z nichž poslední, hypotéza o rozdělení kořenů této funkce, není dodnes přes nesmírné úsilí a přes nasazení výpočetní techniky ani dokázána ani vyvrácena.

Pomocí Riemannových metod, jak jsme již uvedli, byla v roce 1896 dokázána základní věta o prvočíslech.

Podrobnější popis vlastností Riemannovy funkce se vymyká možnostem tohoto textu. Jen pro ilustraci si proto ukažme, jak lze pomocí funkce ζ odvodit jednoduchou a výrazně lepší aproximaci funkce $\pi(x)$ než je již mnohokrát zmiňovaná funkce $\frac{n}{\ln n}$. Touto „lepší" funkcí je například funkce

$$R(n) = 1 + \sum_{k=1}^{\infty} \frac{1}{k \cdot \zeta(k+1)} \cdot \frac{(\ln n)^k}{k!}.$$

V následující tabulce je porovnávána funkční hodnota funkcí $\frac{n}{\ln n}$ a $R(n)$ se skutečnými hodnotami funkce $\pi(n)$.

n	$\frac{n}{\ln n}$	$R(n)$	$\pi(n)$
100 000 000	5 428 681	5 761 552	5 761 455
200 000 000	10 463 629	11 079 090	11 078 937
300 000 000	15 369 409	16 252 355	16 252 325
400 000 000	20 194 906	21 336 185	21 336 326
500 000 000	24 962 408	26 355 517	26 355 867
600 000 000	29 684 688	31 324 622	31 324 703
700 000 000	34 370 013	36 252 719	36 252 931
800 000 000	39 024 157	41 146 248	41 146 179
900 000 000	43 651 379	46 009 949	46 009 215
1 000 000 000	48 254 942	50 847 455	50 847 534

* * *

al-BANNA Ibn (1256-1321), arabský matematik

BARLOW Peter (1776-1868), anglický fyzik a matematik

BERTRAND Joseph Louis Francois (1822-1900), francouzský matematik

CATALDI Pietro Antonio (1552-1626), italský matematik

CAUCHY Augustin Louis (1789-1857), francouzský matematik, jeden z tvůrců moderní matematické analýzy

COLE Frank Nelson (1861-1926), americký matematik

ČEBYŠEV Pafnutij Lvovič (1821-1894), ruský matematik, zakladatel petrohradské matematické školy

DIRICHLET Peter Gustav Lejeune (1805-1859), německý matematik

ERATOSTHENÉS z Kyrény (asi 276 - asi 194 př.n.l.), starořecký matematik a astronom, přítel Archimédův

EUKLEIDÉS z Alexandrie (asi 340- asi 278 př.n.l.), starořecký matematik, autor "Základů"

EULER Leonhard (1707-1783), švýcarský matematik, jeden z nejvýznamnějších matematiků všech dob

FERMAT Pierre de (1601-1665), francouzský matematik, povoláním právník

GAUSS Carl Friedrich (1777-1855), německý matematik, fyzik a astronom

GÖDEL Kurt F. (1906-1978), americko-rakouský matematik a logik

GOLDBACH Christian (1690-1764), německý právník, v matematice samouk

CHURCH Alonzo (1903), americký matematik a logik

HADAMARD Jacques (1865-1963), francouzský matematik

HILBERT DAVID (1862-1943), německý matematik

IAMBLICHOS z Chalkidy (asi 275-330), řecký filosof

LEGENDRE Adrian-Marie (1752-1833), francouzský matematik

LUCAS Francois Eduard Anatole (1842-1891), francouzský matematik

MATIJASEVIČ Jurij Vladimirovič (1947), ruský matematik

MERSENNE Marin (1588-1648), francouzský vědec a organizátor vědeckého života v Paříži

NÍKOMACHOS z Gerasy (1. pol. 2. stol. n.l.), řecký filosof

PERVUŠIN Ivan Michejevič (1827-1900), ruský matemaik

PÝTHAGORÁS ze Samu (asi 560 - asi 480 př.n.l.), starořecký matematik a filozof

RIEMANN Bernhard Georg Friedrich (1822-1866), německý matematik

SIERPINSKI Waclaw Franciszek (1882-1969), polský matematik

ŠNIRELMAN Lev Genrichovič (1905-1938), ruský matematik

THABIT ibn Qurra (836-901), syrský matematik, fyzik a filosof

ULAM Stanislaw Marcin (1909-1984), americký matematik

de la VALLÉE-POUSSIN Charles Jean (1866-1962), belgický matematik

VINOGRADOV Ivan Matvějevič (1891-1983), ruský matematik

Literatura

[1] Davis P.J. - Hersh R., *The Mathematical Experience*, Birkhäuser, Boston 1981.

[2] Dickson L.E., *A History of the Theory of Numbers*, 3vols., Chelsea Publ. Co., New York 1952.

[3] Eukleidés, *Základy*, Jednota českých matematiků a fyziků, Praha 1907.

[4] Fuchs E. a kolektiv, *Světonázorové problémy matematiky IV*, SPN, Praha 1987.

[5] Guy R.K., *Unsolved Problems in Number Theory*, Springer Verlag, New York 1981.

[6] Hellemans A. - Bunch B., *The Timetables of Science*, Simon and Schuster, New York 1988.

[7] Kopanev O., *Z histórie vel'kých prvočísel*, Matematika a fyzika ve škole 16, (1985/86), 289-297.

[8] *Slovník antické kultury*, Svoboda, Praha 1974.

[9] Wells D., *Curious and Interesting Numbers*, Penguin Books, London 1987.