Eduard Fuchs

Co ještě nevíme o přirozených číslech (2) aneb Od dokonalých čísel k Fermatovým prvočíslům

Učitel matematiky, Vol. 7 (1999), No. 2, 65–74

Persistent URL: http://dml.cz/dmlcz/150972

CO JEŠTĚ NEVÍME O PŘIROZENÝCH ČÍSLECH (2)

aneb

Od dokonalých čísel k Fermatovým prvočíslům

EDUARD FUCHS

3. Dokonalá čísla

Již starořečtí matematikové znali čtyři pozoruhodná čísla, která je fascinovala. Byla to čísla 6, 28, 496 a 8 128. V čem spočívala jejich pozoruhodnost?

Každé z těchto čtyř čísel je rovno součtu všech svých vlastních dělitelů. (Připomeňme si, že vlastní dělitel čísla n je každý dělitel menší než n.) Skutečně,

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

Tato vlastnost musela doslova uchvátit zejména *pýthagorejce*[1], kteří číslům připisovali mocné a někdy doslova mystické vlastnosti. Čísla s popsanou vlastností proto nazvali **dokonalá**.

První, skutečně mimořádně důležitý výsledek o těchto číslech, odvodil již kolem roku 300 př. n. l. EUKLEIDÉS v *Základech*, o nichž jsme se zmiňovali již v minulé části tohoto miniseriálu. V IX. knize, části XXXVI, dokázal následující tvrzení:

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

---

[1] Řecký filosof PÝTHAGORÁS ze Samu (asi 560 - asi 480 př.n.l.) prohlásil číslo za základ a podstatu světa. Učení pýthagorejců, filosofické školy, kterou založil, bylo tajné a předávalo se jen ústně. Řád světa podle nich vzniká spojováním protikladů v určitých číselných poměrech a jen dodržování těchto poměrů zaručuje harmonii. Pro úplnost dodejme, že známou *Pýthagorovu větu* znali již v Babylonii dávno před Pýthagorem.

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

$$1+2+4+8+\cdots+2^n = 2^{n+1}-1,$$

můžeme Eukleidův výsledek zformulovat takto: *je-li* $M_n = 2^n - 1$ *prvočíslo*[2], *je číslo* $P_n = M_n \cdot (2^{n-1})$ *dokonalé.* V právě zavedeném označení tedy můžeme říci, že již v antice byla známa dokonalá čísla P_2, P_3, P_5 a P_7.

Uvedená čtyři čísla uvádí ve své učebnici *Arithmétiké eisagógé* (tj. *Úvod do matematiky*) i NÍKOMACHOS z Gerasy, řecký filosof z první poloviny 2. století n. l. Tuto učebnici komentoval zhruba o 150 let později IAMBLICHOS z Chalkidy (asi 270 – 330), který ještě 800 let po pýthagorejcích připisoval číslům různé magické vlastnosti.

Protože čísla 6, 28, 496 a 8128 mají postupně 1, 2, 3 a 4 cifry, vyslovil hypotézu, že pro každé přirozené n existuje právě jedno dokonalé číslo o n cifrách a na posledním místě se pravidelně střídají číslice 6 a 8.

První část Iamblichovy hypotézy je nesprávná, což koneckonců není překvapující. Vycházela totiž z výhradné preference dekadického zápisu čísel, ačkoliv z čistě matematického hlediska není žádný důvod, proč desítkovou soustavu preferovat proti 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 (v dekadickém zápisu) buďto dvojčíslím 28 nebo cifrou 6, před níž stojí liché číslo. Číslice 6 a 8 se však pravidelně nestřídají.

Již ve středověkých rukopisech je zmiňováno páté dokonalé číslo 33 550 336 (= P_{13}), není však známo, kdo je objevil[3]. Další dvě dokonalá čísla, šesté a sedmé, našel v r. 1603 PIETRO CATALDI (1552 – 1626); jejich hodnoty jsou 8 589 869 056 (= P_{17})

[2]Označení M_n souvisí s tím, že prvočísla tohoto tvaru se nazývají *Mersennova.* O důvodech se více dozvíme v příštím pokračování.

[3]Někdy je jeho objevení připisováno J. MÜLLEROVI (1436 – 1476), známému pod jménem REGIOMONTANUS.

a 137 438 691 328 (= P_{19}). Všechna tato čísla přitom byla tvaru, který uváděl Eukleidés, přestože ten dokázal pouze **dostatečnost** výše uvedené podmínky. Že tyto výsledky byly zákonité, dokázal až v 18. století, dva tisíce let po Eukleidovi, Euler, který odvodil, že **sudá** dokonalá čísla jsou právě čísla popsaná Eukleidem.

Sám Euler našel další, již osmé dokonalé číslo $P_{31} = 2^{30} \cdot M_{31}$. Toto číslo bylo dlouho považováno za největší dokonalé číslo, které bylo možno odhalit[4]. Ještě například v roce 1814 napsal anglický matematik 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, jaké kdy bude objeveno.*

Nalezení podstatně větších dokonalých čísel umožnil až nástup výpočetní techniky ve 20. století. O tom však budeme podrobněji hovořit v kapitole o hledání velkých prvočísel.

Ještě jsme však nevysvětlili jednu věc. Všechna prozatím popisovaná dokonalá čísla byla **sudá**. Jak je to tedy s **lichými** dokonalými čísly?

Odpověď je dosti překvapivá: **nevíme!** Jejich existence je jedním z dosud nevyřešených problémů a o nalezení důkazu jejich existence či neexistence panuje dosti velká skepse. Je pouze známa řada dílčích výsledků, typu:

Liché dokonalé číslo — pokud existuje — musí být větší než 10^{200}, *musí mít alespoň 8 prvočíselných dělitelů, z nichž aspoň jeden musí být větší než* 300 000; *je-li menší než* $10^{9\,118}$, *musí být dělitelné 6. mocninou některého prvočísla,* atd.

4. Spřátelená čísla

S dokonalými čísly úzce souvisí tématika tzv. **spřátelených čísel**. Proto se o nich stručně zmíníme.

[4]Přesněji řečeno, Eulerovým cílem bylo dokázat, zda číslo M_{31} je prvočíslo. (O důvodech těchto snah budeme podrobně hovořit později.) Dokonalé číslo P_{31} pak bylo „vedlejším produktem“ tohoto snažení.

Přirozená čísla a, b se nazývají *spřátelená*, jestliže součet vlastních dělitelů každého z nich je roven druhému z těchto čísel. 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 a 110 , vlastní dělitelé čísla 284 jsou 1, 2, 4, 71 a 142 a přitom 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 Pýthagorás. Ani Iamblichos však ještě nevěděl, zda existují nějaká jiná spřátelená čísla a neznal ani žádnou metodu, jak je případně hledat. Zásadní krok v tomto směru učinil až arabský matematik, fyzik a astronom THABIT ibn Qurra (asi 836 – 901), který podrobně studoval a popsal Eukleidovy poznatky 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

$$2^n \times a \times b \quad a \quad 2^n \times c$$

spřátelená.

Přes důmyslnost Thabitovy formule však není nalezení dalších dvojic podle ní vůbec jednoduché, neboť to vyžaduje současné nalezení tří prvočísel předepsaného tvaru. Thabit sám ostatně žádnou další dvojici nenalezl. To se podařilo až jinému arabskému matematikovi, ibn al-BANNOVI, který objevil dvojici 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 geniálního Pierra Fermata (1601 – 1665), o němž budeme blíže hovořit v dalším odstavci. Ten o této dvojici v roce 1636 napsal Marinu Mersennovi (1588 – 1648), o němž se ještě zmíníme v příštím pokračování.

O pouhé dva roky později nalezl René Descartes (1595 – 1650) třetí dvojici: 9 363 584 a 9 437 056. Z Thabitovy formule ji obdržíme pro $n = 7$.

Thabitově formuli přitom **nevyhovují všechny dvojice** spřátelených čísel. 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 již několikrát zmiňovaný L. Euler. Nalezl více než 60 dvojic těchto čísel a jeho teoretické výsledky dodnes tvoří základ dalších zkoumání. V průběhu 17. a 18. století bylo postupně nalezeno mnoho dalších dvojic spřátelených čísel. Vesměs však tato čísla byla velká — řádově v milionech či miliardách. Proto bylo pro matematickou veřejnost značným překvapením, když šestnáctiletý italský školák Niccolò Paganini v roce 1866 nalezl dvojici překvapivě „malých" spřátelených čísel: 1 184 a 1 210.

V současnosti jsou spřátelených dvojic známy tisíce včetně **všech** těch, jejichž menší člen nepřesahuje jeden milion. Na Internetu lze prakticky denně nalézt zprávu o rozšíření počtu těchto dvojic, včetně například dvojice

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

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 však tvořeny soudělnými čísly a není

známo, zda existuje dvojice **nesoudělných** spřátelených čísel. Víme pouze, že v kladném případě by jejich součin musel být větší než 10^{67}.

Ve všech dosud známých dvojicích jsou obě čísla sudá nebo obě lichá. Neví se však, zda takové jsou všechny dvojice. U dvojic sudých čísel nemůže být žádný člen dělitelný 3, známé dvojice lichých čísel jsou naopak zásadně násobky 3, není však dokázáno, zda tomu tak musí být vždy. Čtenáři se tedy mohoou pokusit o nalezení dvojice „sudo-lichých" spřátelených čísel. Třeba budou mít podobné štěstí jako v minulém století N. Paganini.

5. Fermatova prvočísla

PIERRE FERMAT (1601 – 1665) byl jedním z matematických géniů 17. století. Celý život prožil v jihofrancouzském Toulouse a jeho nejbližším okolí, nikdy dokonce ani nenavštívil Paříž, ačkoliv si s tamější vědeckou komunitou dopisoval. Nebyl dokonce ani povoláním matematik, těch ostatně bylo v té době nemnoho. Nevíme ani, zda jeho nejbližší okolí za jeho života tušilo, že jedna ze zálib ctihodného soudního rady, pana P. de Fermat, jak byl někdy též titulován, ho zařadí mezi nejvýznamnější světové matematiky všech dob. S největší pravděpodobností spíše oceňovalo jeho vynikající klasické vzdělání, dokonalou znalost latiny, řečtiny, italštiny a španělštiny; tyto jazyky znal natolik dobře, že v nich psal i verše a na překlady z řečtiny byl vyhlášeným expertem.

Rekapitulujeme-li jeho matematické výsledky, musíme se zmínit o tom, že dosáhl významných výsledků v **matematické analýze**, jimiž připravoval půdu k založeni infinitesimálního počtu o několik desetiletí později; že společně s Descartem položil základy **analytické geometrie** a že je považován za zakladatele **teorie čísel**[5]. Fermatova intuice a jasnozřivost byla opravdu mimořádná. (Jedním z nejznámějších dokladů je tzv. **Velká Fermatova věta**, tj. tvrzení, že rovnice $x^n + y^n = z^n$ nemá pro $n > 2$

[5]O Fermatových výsledcích v tomto oboru viz blíže například v článku Karla Lepky: *Malá Fermatova věta*, Učitel matematiky **5**(1997),143-150.

netriviální celočíselné řešení. Důkaz této věty byl po staletích marného snažení proveden až v r. 1995.)

O to zajímavější je následující případ, v němž se Fermat spletl, a to naprosto zásadně. Jak k tomu došlo?

Fermat studoval dokonalá čísla, o nichž jsme hovořili v §3. Jak již víme, souvisejí tato čísla bezprostředně s Mersennovými prvočísly, tj. prvočísly tvaru $2^n - 1$. Není tedy překvapující, že si Fermat položil otázku, kdy jsou prvočísly čísla podobného tvaru: $2^n + 1$. Fermat vyslovil následující hypotézu:

čísla tvaru $F_m = 2^{2^m} + 1$ pro $m = 0, 1, 2, \ldots$ *jsou prvočísla.*

Jak na tuto hypotézu Fermat přišel? Platí následující evidentní tvrzení, které Fermat bezesporu znal (nebo si je odvodil):

Je-li p *přirozené a* $q > 1$ *liché, platí*

$$2^{pq} + 1 = (2^p + 1)(2^{p(q-1)} - 2^{p(q-2)} + \cdots - 2^p + 1).$$

Odtud okamžitě plyne, že číslo tvaru $2^n + 1$ může být pro $n > 1$ prvočíslem pouze tehdy, když exponent n nemá lichého prvočinitele, tj. je tvaru 2^m. Fermat navíc spočítal pět prvních čísel F_m:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537$$

a zjistil, že jsou to vesměs prvočísla. Formulace výše uvedené hypotézy se tedy zdá naprosto logická.

Fermat sám několikrát ve své korespondenci[6] uvádí, že obecný důkaz této hypotézy se mu sice nepodařilo nalézt, věnoval však problematice tolik úsilí a provedl tolik namáhavých výpočtů, že je o pravdivosti této hypotézy zcela přesvědčen.

[6]Své výsledky Fermat — až na čestné výjimky — nepublikoval a zachovaly se jen v jeho četné korespondenci nebo jako vpisky do literatury, kterou studoval. Za zachování většiny výsledků tak vděčíme Fermatovu synovi Samuelovi (rovněž soudnímu radovi v Toulouse), který se po otcově smrti vydání jeho díla intenzívně věnoval.

Fermat tedy umírá v domnění, že jeho hypotéza je pravdivá, že všechna čísla F_m jsou prvočísla. Další vývoj byl zajímavý a v mnoha ohledech poučný.

Fermatovo dílo, alespoň v oblast teorie čísel, upadalo po jeho smrti v zapomnění; zřejmě předběhl dobu a matematika nebyla na rozvoj této disciplíny připravena. Až o necelé století později se o definitivní zrod teorie čísel zasloužil největší matematik 18. století, LEONHARD EULER. Ten řadu Fermatových výsledků znovuobjevil, v mnohém na Fermata navázal a jako první zasáhl do historie Fermatových čísel F_m, když v r. 1832 dokázal, že **číslo F_5 je složené!** Nalezl totiž faktorizaci

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

Tím byla samozřejmě Fermatova hypotéza vyvrácena, nebylo však ani zdaleka jasné, jak je to s dalšími čísly F_m. (V dalším budeme *Fermatovým prvočíslem* rozumět číslo F_m, které je prvočíslem.)

Zájem o Fermatova prvočísla výrazně vzrostl koncem 18. století, kdy německý matematik CARL FRIEDRICH GAUSS (1777 – 1855) odvodil následující překvapující souvislost Fermatových prvočísel s pravidelnými mnohoúhelníky:

Pravidelný mnohoúhelník je eukleidovsky konstruovatelný právě tehdy, když počet jeho vrcholů je roven číslu

$$n = 2^k p_1 p_2 \cdots p_k \ ,$$

kde $p_1, p_2, \ldots, p_k$ jsou navzájem různá Fermatova prvočísla.

Odtud okamžitě vyplývá, že pravidelné n-úhelníky jsou eukleidovsky konstruovatelné například pro $n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \ldots$ a nejsou eukleidovsky konstruovatelné například pro $n = 7, 9, 11, 13, 14, \ldots$.

Protože Fermatových prvočísel bylo v onu chvíli známo pouze 5 (a jak uvidíme, tento počet se dodnes nezvýšil), bylo podle Gausse možno dokázat existenci eukleidovské konstrukce pouze

pro $2^5 - 1 = 31$ pravidelných mnohoúhelníků s **lichým** počtem vrcholů.

Další krok v poznávání Fermatových čísel se podařilo udělat až za 150 let po Eulerovi, v roce 1880, kdy F. LANDRY dokázal, že F_6 je součinem dvou prvočísel:

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

Ani další číslo tedy nesplňovalo Fermatovu předpověď!

A vývoj byl i nadále k Fermatově hypotéze neúprosný. V r. 1897 dokázal FELIX KLEIN (1849 – 1925), že číslo F_7 je složené, nenašel však žádného dělitele. V roce 1909 dokázali analogický výsledek pro číslo F_8 J.C. MOREHEARD a A.E. WESTERN.

Faktorizaci čísla F_7 se podařilo nalézt až v r. 1970:

$$F_7 = (2^9 \cdot 116\,503\,103\,764\,643 + 1)(2^9 \cdot 11\,141\,971\,095\,088\,142\,685 + 1),$$

dělitele čísla F_8 nalezli BRENT a POLLARD až v roce 1981; je jím číslo 1 238 926 361 552 897.

Abychom mohli docenit jak obtížné bylo uvedené výsledky získat, stačí si uvědomit, jak rychle posloupnost $(F_m)_{m=0}^{\infty}$ Fermatových čísel roste.

Podívejme se, jak bychom zjišťovali „standardními“ metodami, zda je například F_m prvočíslo. Víme, že k tomu stačí dělit číslo F_m všemi prvočísly, která nepřevyšují číslo $\sqrt{F_m}$. Jak dlouho bychom tedy prověřovali například číslo F_8?

Celá část čísla $\sqrt{F_8}$ má 39 cifer, takže lze vcelku snadno odvodit, že před číslem $\sqrt{F_8}$ je cca

$$\frac{10^{38}}{38 \cdot \ln 10} \doteq 10^{36}$$

prvočísel. Vzhledem k tomu, že rok má cca $3.2 \cdot 10^7$ sekund, potřebovali bychom při miliardě dělení za sekundu k provedení potřebných výpočtů přibližně $3 \cdot 10^{19}$ let. Jen pro porovnání: stáří vesmíru odhadujeme na cca $15 \cdot 10^9$ let.

Pokusme se — pod dojmem právě uvedených odhadů — alespoň představit, jakými metodami mohl polský matematik WACŁAW SIERPIŃSKI (1882 – 1969) v roce 1962, bez využití výpočetní techniky, dokázat, že číslo F_{1945} není prvočíslo. Dekadický zápis tohoto čísla zcela jistě nikdy nikdo nenapíše, protože počet jeho číslic je 10^{582}.

Ještě neuvěřitelnější je fakt, že v r. 1983 W. KELLER odvodil, že číslo $F_{23\,471}$ je dělitelné číslem $5 \cdot 2^{23\,473} + 1$. Toto Fermatovo číslo má více než $10^{7\,000}$ cifer. (**Pozor**: velikost posledního čísla si nesmíme plést s číslem $10^{7\,000}$. Toto číslo má „jen“ 7 001 cifer.)

Nyní již můžeme uzavřít historii probírané Fermatovy hypotézy. Zdá se, že Fermat se v tomto případě mýlil naprosto fatálně. **Všechna** dosud prozkoumaná Fermatova čísla, kromě prvních pěti, **jsou složená**. Dodnes sice není dokázáno, že žádné další Fermatovo prvočíslo neexistuje, mnohé však tomu nasvědčuje.

Téměř šokující je přitom skutečnost, že teoreticky se Fermat vlastně **vůbec neměl splést**. Z výsledků, které sám odvodil a dokázal, totiž plynulo, že číslo F_5, které posléze rozložil Euler, může mít prvočíselné dělitele pouze tvaru $64n + 1$ a číslo 641, o němž Fermat bezpochyby i zpaměti věděl, že je prvočíslem, je opravdu dělitelem.

Zdá se téměř neuvěřitelné, že tento fakt Fermat, který byl v praktických výpočtech mimořádně zběhlý a i mnohem větší čísla faktorizoval prakticky obratem, mohl přehlédnout. A přitom, jak jsme již uvedli, sám napsal, že výpočtům v tomto směru věnoval mnoho úsilí! Jediné vysvětlení je, že se prostě při pokusu o faktorizaci čísla F_5 spletl a svůj výpočet již nikdy neprověřoval.

Kdyby této Fermatovy pravděpodobné chyby nebylo, nikdy by nezformuloval onu hypotézu. Vývoj teorie čísel by možná v některých ohledech byl jiný. Ona osudná chyba však rozhodně nesnižuje Fermatovu genialitu a možná paradoxně přispěla k mnoha zajímavým objevům v této oblasti.

Pokračování příště