Eduard Fuchs

Co ještě nevíme o přirozených číslech (3) aneb O hledání velkých prvočísel

Učitel matematiky, Vol. 7 (1999), No. 3, 129–136

Persistent URL: http://dml.cz/dmlcz/150985

CO JEŠTĚ NEVÍME O PŘIROZENÝCH ČÍSLECH (3)

aneb

O hledání velkých prvočísel

EDUARD FUCHS

6. Proč vůbec hledáme velká prvočísla

Víme, že prvočísel je sice nekonečně mnoho, jak jsme však uvedli již v první části tohoto seriálu, nejen že neznáme žádnou formuli, která by nám postupně umožňovala počítat všechna prvočísla, ale nemáme k dispozici dokonce ani formuli $f(n)$, která by v přirozených číslech nabývala postupně (navzájem různých) prvočíselných hodnot, byť ne nutně všech. (Problémy spojené s hledáním takové formule jsme viděli v minulém pokračování v odstavci o Fermatových prvočíslech.)

Je však zřejmé, že hledání stále větších a větších prvočísel bylo pro matematiky od dávnověku intelektuální výzvou. Nemá smyslu se ptát, „k čemu bylo toto hledání dobré". K čemu je „dobré" malování obrazů, hraní šachů či zdolávání velehor? Konáme mnoho činností jen proto, že jsme **lidé** obdařeni intelektem a emocemi, kteří cítí — alespoň někteří z nás — vnitřní potřebu poznávat nepoznané, zdolávat nezdolané a sdělovat jiným své vidění světa, své myšlenky a obohacovat se navzájem. Každý z nás, kdo svůj život více či méně spojil s matematikou, proto dobře rozumí i v této oblasti pohnutkám našich předchůdců.

A jak už nám historie mnohokrát ukázala, ideje a teorie, které se zpočátku zdály jen intelektuální hříčkou bez hlubšího významu a bez praktického využití, se dříve či později ukázaly přínosné a často nepostradatelné v oborech, o nichž v době jejich vzniku nebylo a nemohlo být ani potuchy. Tak našla teorie grup užití ve fyzice či krystalografii, teorie kvaternionů v kosmonautice a mohli bychom jmenovat mnoho dalších příkladů. Podobný osud čekal i na zdánlivě zcela neužitečné hledání velkých prvočísel, která

dnes nacházejí zásadní využití například v testování hardwaru a softwaru či v intenzívně se rozvíjející kryptografii.

O některých postupech matematiků dřívějších období, kdy ještě nebyla k dispozici výpočetní technika, se můžeme jen dohadovat. Již mnohokrát jsme se zmínili o některých obdivuhodných výsledcích Fermata a Eulera. Fermat vyslovil, většinou bez důkazů, řadu pozoruhodných hypotéz, které o století později Euler dokázal. Mezi takové příklady patří například hypotéza, že *každé prvočíslo tvaru* $4n+1$ $(n \in \mathbb{N})$, *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

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

Hledání velkých prvočísel však v dobách, kdy ještě nebyla k dispozici výpočetní technika, rozhodně nebylo snadnou záležitostí. Vzhledem k tomu, že pro výpočet prvočísel není známa žádná zákonitost, začala být v průběhu staletí studována prvočísla jistých tvarů ve víře, že mezi nimi budou adepti na nově objevená prvočísla.

V prvních dvou pokračováních jsme se již zmínili o tzv. **Mersennových** a **Fermatových** prvočíslech[1]. Kromě nich jsou studovány ještě například následující skupiny prvočísel:

- **faktoriálová prvočísla** tvaru $n! \pm 1$,
- **eukleidovská prvočísla** tvaru $2 \cdot 3 \cdot 5 \cdots p + 1$,
- **prvočísla Sophie Germain**[2], což jsou taková lichá prvočísla p, že $2p+1$ je rovněž prvočíslo,
- **Cullenova prvočísla** tvaru $n \cdot 2^n + 1$,
- **Woodallova prvočísla** tvaru $n \cdot 2^n - 1$ aj.

[1]Připomeňme, že Mersennova prvočísla jsou prvočísla tvaru $2^p - 1$, Fermatova prvočísla mají tvar $2^{2^p} + 1$.

[2]Sophie GERMAIN (1776 – 1831), francouzská matematička a filosofka. Podrobněji o ní viz v tomto čísle článek H. Durnové, str. 146.

O žádné z uvedených skupin dodnes nevíme, kolik provočísel obsahuje, zda je konečná nebo nekonečná. Nejméně nadějná se jeví Fermatova prvočísla, o nichž jsme hovořili podrobně v minulém pokračování a mezi nimiž nebylo od 17. století objeveno žádné další.

Ve všech uvedených skupinách jsou však pomocí počítačů objevována stále další prvočísla. Pro zajímavost uveďme stav platný v době uzávěrky tohoto čísla, tj. v březnu 1999.

Všechna níže uvedená čísla byla objevena v roce 1998, pouze rekordman v kategorii eukleidovských prvočísel byl nalezen již v r. 1993:

- faktoriálové prvočíslo $6\,917! - 1$, které má 23 560 cifer
- eukleidovské prvočíslo $2 \cdot 3 \cdot 5 \cdots 24\,029 + 1$
- prvočíslo Sophie Germain $72\,021 \cdot 2^{23\,630} - 1$, které má 7 119 cifer
- Cullenovo prvočíslo $481\,899 \cdot 2^{481\,899} + 1$ o 145 072 cifrách
- Woodallovo prvočíslo $151\,023 \cdot 2^{151\,023} - 1$, které má 45 468 cifer.[3]

Všechny tyto výsledky však samozřejmě bylo možno získat pouze za zcela zásadní pomoci výkonných počítačů. Vraťme se tedy ještě krátce do epochy, kdy počítače k dispozici ještě nebyly. V té době byl pokrok v této oblasti velmi obtížný a pomalý. Již v minulém pokračování jsme uvedli, že největší prvočíslo ve své době nalezl Euler. Ten v r. 1772 dokázal, že prvočíslem je číslo

$$2^{31} - 1 = 2\,147\,483\,647.$$

tj. 31. Mersennovo prvočíslo

[3]Pro úplnost a pro ilustraci, jak rychle se v současnosti vyvíjejí poznatky v této oblasti, uveďme zlepšení jednoho výsledku z první části našeho seriálu. Na str. 6 jsme uvedli, že *nejdelší známá aritmetická posloupnost po sobě jdoucích prvočísel* má 7 členů. Od té doby byla nalezena 7. 11. 1997 posloupnost osmi takových čísel a v r. 1998 nalezl Manfred Toplic z Klagenfurtu v Rakousku dokonce posloupnost o 9 a posléze i 10 členech. Nejdelší dnes známá aritmetická posloupnost po sobě jdoucích prvočísel je tedy tvořena čísly 100 996 972 469 714 247 637 786 655 587 969 840 329 509 324 689 190 041 803 603 417 758 904 341 703 348 882 159 067 729 719 + $k \cdot 210$, $k = 0, 1, \ldots, 9$.

Další pokrok přišel až po téměř 100 letech, když v r. 1867 našel LANDRY prvočíslo

$$\frac{2^{59}-1}{179\,951} = 3\,203\,431\,780\,337.$$

Již v r. 1876 však nalezl LUCAS[4] prvočíslo $2^{127}-1$, které má dokonce 39 cifer. Poslední pokrok v „předpočítačovém" věku byl učiněn v r. 1951, kdy FERRIER našel prvočíslo $\frac{2^{148}+1}{17}$, které má 44 cifer.

Již v témže roce však bylo nalezeno pomocí počítače další prvočíslo o 79 cifrách a definitivně tak skončila éra samostatných počtářů, kteří pracovali v nejlepším případě s mechanickým počitadlem. Současně bylo čím dál jasnější, že nejvhodnějšími kandidáty na hledání velkých prvočísel jsou tzv. *Mersennova prvočísla*, o nichž jsme se již několikrát zmínili. Tato čísla dnes hrají ve sledované problematice centrální roli; proto se o nich zmíníme podrobněji.

7. Mersennova prvočísla

Francouzský fyzik, matematik a teolog Marin MERSENNE (1588 – 1648) studoval na jezuitské koleji současně s Descartem a poté na pařížské Sorbonně (1609 – 1611). Po studiích vstoupil do kláštera. Dopisoval si s mnoha učenci, například s Galileim, Fermatem, Pascalem a dalšími. Stal se centrem významné pařížské vědecké komunity, z níž se časem vyvinula Francouzská akademie (1660).

V Mersennově době bylo známo, že když n **není** prvočíslo, nemůže být prvočíslem ani číslo $2^n - 1$. S obráceným tvrzením je to však podstatně komplikovanější. Pro prvočíslo n číslo $2^n - 1$ **může**, avšak — jak lze lehce ukázat — **nemusí** být prvočíslem.

Z důvodů, které za chvíli uvidíme, je dnes obvyklé nazývat čísla $M_n = 2^n - 1$ *Mersennovými čísly*. Některá z Mersennových

[4]François Edouard Anatole LUCAS (1842 – 1891), francouzský matematik.

prvočísel znali již staří Řekové:

$$M_2 = 3,\ M_3 = 7,\ M_5 = 31,\ M_7 = 127,\ M_{13} = 8\,191.$$

Již v souvislosti s dokonalými čísly v první části jsme uvedli, že v r. 1603 dokázal CATALDI, že prvočísly jsou čísla M_{17} a M_{19}.

V r. 1644 vyslovil Mersenne hypotézu, že pro $n < 258$ 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.)

Již jsme uvedli, že čísla M_{31} (Euler 1772) a M_{127} (Lucas 1876) jsou opravdu prvočísla. V r. 1883 odvodil PERVUŠIN[5], že Mersenne zapomněl na index 61; číslo M_{61} je také prvočíslem.

První chybu v Mersennově seznamu objevil v r. 1903 americký matematik Frank Nelson COLE (1861 – 1926), který na říjnovém zasedání *American Mathematical Society* v New Yorku předvedl, že

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

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

Později se ještě ukázalo, že v Mersennově seznamu chybějí prvočísla M_{89} a M_{107} a nepatří tam složené číslo M_{257}. Přestože tedy Mersennova hypotéza byla v řadě případů nesprávná, nemění to nic na skutečnosti, že právě tato čísla se ukázala jako mimořádně vhodná při snahách o nalezení velkých prvočísel.

Svou roli zde sehrává řada okolností. Především samozřejmě skutečnost, že těchto prvočísel je zřejmě „relativně dost", alespoň v tom smyslu, že je nestihl například osud Fermatových prvočísel. Pro počítačovou éru se však mimořádně užitečnou a příznivou ukázala ještě další skutečnost.

Již Lucas v roce 1870 odvodil test prvočíselnosti Mersennových čísel, který ještě zjednodušil v roce 1930 LEHMER. Tento test spočívá v následujícím tvrzení.

[5]Ivan Michejevič PERVUŠIN (1827 – 1900), ruský matematik.

TABULKA MERSENNOVÝCH PRVOČÍSEL

	p	cifer M_p	rok	objevil
1	1	1	-	-
2	3	1	-	-
3	5	2	-	-
4	7	3	-	-
5	13	4	1456	?
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi
8	31	10	1772	Euler
9	61	19	1883	Pervušin
10	89	27	1911	Powers
11	107	33	1914	Powers
12	127	39	1876	Lucas
13	521	157	1952	Robinson
14	607	183	1952	Robinson
15	1 279	386	1952	Robinson
16	2 203	664	1952	Robinson
17	2 281	687	1952	Robinson
18	3 217	969	1957	Riesel
19	4 253	1 281	1961	Hurwitz
20	4 423	1 332	1961	Hurwitz
21	9 689	2 917	1963	Gillies
22	9 941	2 993	1963	Gillies
23	11 213	3 376	1963	Gillies
24	19 937	6 002	1971	Tucker
25	21 701	6 533	1978	Noll, Nickel
26	23 209	6 987	1979	Noll
27	44 497	13 395	1979	Nelson, Slowinski
28	86 243	25 962	1982	Slowinski
29	110 503	33 265	1988	Colquitt, Welsh
30	132 049	39 751	1983	Slowinski
31	216 091	65 050	1985	Slowinski
32	756 839	227 832	1992	Slowinski, Gage
33	859 433	258 716	1994	Slowinski, Gage
34	1 257 787	378 623	1996	Slowinski, Gage
35	1 398 269	420 921	1996	GIMPS
?	2 976 221	895 932	1997	GIMPS
?	3 021 377	909 526	1998	GIMPS

Lucas-Lehmerův test. *Položme* $S(n) = 4$, $S(n+1) = S(n)^2 - 2$. *Nechť* p *je liché prvočíslo. Pak je* M_p *prvočíslem právě tehdy, když dělí číslo* $S(p-1)$.

Onou příznivou skutečností, o níž jsme se výše zmínili, je fakt, že tento test je mimořádně vhodný pro programování, neboť umožňuje relativně rychlé prověřování, jak ještě uvedeme.

Vývoj po roce 1951, kdy se tedy do hledání prvočísel zapojily počítače — byť z dnešního hlediska pomalé a nevýkonné — rychle gradoval. Když bylo v r. 1957 nalezeno prvočíslo M_{3217}, které má 969 cifer, bylo s napětím očekáváno, kdy padne bariéra 1000 cifer; takto velkým prvočíslům se začalo říkat **titánská**. Tato hranice padla v r. 1961, kdy HURWITZ nalezl první titánské prvočíslo M_{4423}, které má 1332 cifer.

A vývoj se nezastavil a překonával všechna očekávání. Když pracovníci *University of Illinois* v r. 1963 nalezli na počítači ILLIAC 2 v pořadí již 23. Mersennovo prvočíslo $M_{11\,213}$, které má 3376 cifer, opatřovali poštu matematického ústavu speciálním razítkem, které do celého světa oznamovalo, že $2^{11\,213} - 1$ je prvočíslo! (Viz obr. 1)

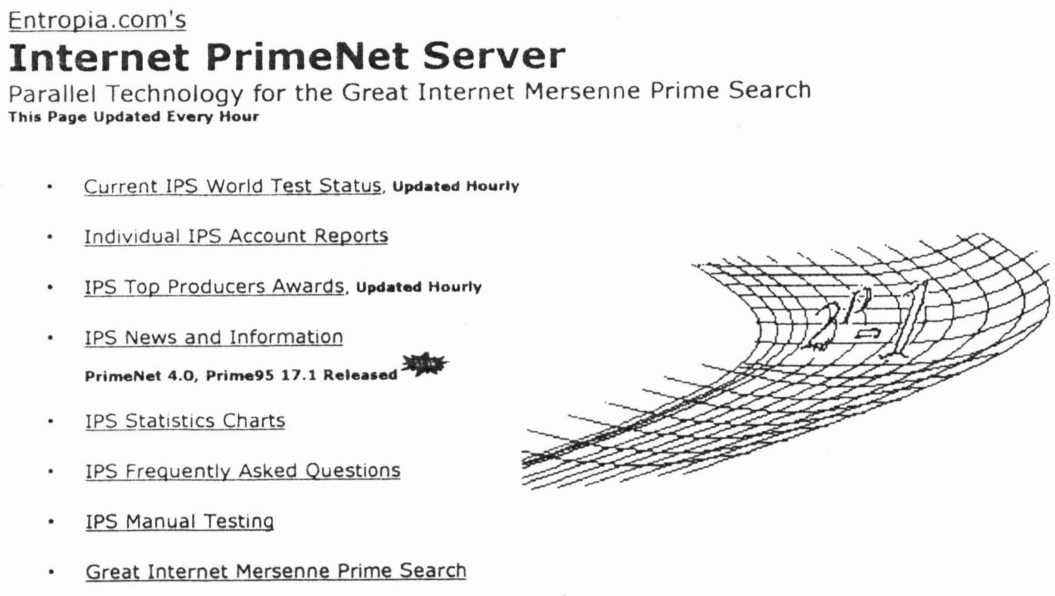
obr. 1

Do dnešního dne již bylo nalezeno celkem 37 Mersennových prvočísel (viz tabulku všech dosud známých Mersennových prvočísel na str. 134). Významnou roli v tomto procesu sehrává v posledních letech nadnárodní skupina GIMPS (the **G**reat **I**nternet **M**ersenne **P**rime **S**earch), která sdružuje několik tisíc nadšenců z celého světa, kteří společně pracují na projektu vyhledávání dalších prvočísel. Poslední úspěch tato skupina zaznamenala 27. ledna 1998, kdy její člen, devatenáctiletý student kalifornské univerzity Roland CLARKSON, nalezl po několikadenní práci svého osobního

počítače 37. Mersennovo prvočíslo $M_{3\,021\,377}$. Jeho výpočet prověřil dne 30. 1. 1998 na superpočítači Cray jeden z intelektuálních vůdců celé skupiny David SLOWINSKI, který se významně podílel na objevení mnoha prvočísel. Toto prozatím největší prvočíslo má 909 526 cifer, takže zřejmě stojíme před další bariérou: očekává se nalezení tzv. **megaprvočísla**, které bude mít více milion cifer.

Abychom si mohli učinit alespoň částečný obrázek o velikosti prvočísel, o nichž hovoříme, uveďme alespoň jeden údaj: kdybychom chtěli číslo $M_{3\,021\,377}$ vysázet ve velikosti 10 bodů, což je velikost písma tohoto textu, bylo by dlouhé 8 556 metrů a zabralo by při 35 řádcích na stránce celkem 2 445 stran.

Na závěr ještě stručnou poznámku k tabulce Mersennových prvočísel. Na posledních dvou řádcích je v prvním sloupci, který udává pořadí, otazník. Dosud se totiž neví, zda mezi 35. a dalším Mersennovým prvočíslem nejsou nějaká další. „Mezera" mezi nimi je totiž nápadně velká a všichni adepti v ní dosud nebyli prověřeni.


Entropia.com's

Internet PrimeNet Server

Parallel Technology for the Great Internet Mersenne Prime Search

This Page Updated Every Hour

- Current IPS World Test Status, **Updated Hourly**
- Individual IPS Account Reports
- IPS Top Producers Awards, **Updated Hourly**
- IPS News and Information
  PrimeNet 4.0, Prime95 17.1 Released
- IPS Statistics Charts
- IPS Frequently Asked Questions
- IPS Manual Testing
- Great Internet Mersenne Prime Search

Úvod internetovské stránky o prvočíslech na adrese
`http://entropia.com/primenet/status.shtml`