8. 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 GALILEEM, FERMATEM, PASCALEM a dalšími. Stal se centrem významné pařížské vědecké komunity, z níž se časem vyvinula Francouzská akademie (1660).

Marin Mersenne

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*. Následující Mersennova prvočísla 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 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 IVAN MICHEJEVIČ PERVUŠIN (1827 -- 1900), 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

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

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 to je 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.

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!

TABULKA MERSENNOVÝCH PRVOČÍSEL

	p	cifer M_p	cifer P_p	rok	objevil
1	2	1	1	-	-
2	3	1	2	-	-
3	5	2	3	-	-
4	7	3	4	-	-
5	13	4	8	1456	?
6	17	6	10	1588	Cataldi
7	19	6	12	1588	Cataldi
8	31	10	19	1772	Euler
9	61	19	37	1883	Pervušin
10	89	27	54	1911	Powers
11	107	33	65	1914	Powers
12	127	39	77	1876	Lucas
13	521	157	314	1952	Robinson
14	607	183	366	1952	Robinson
15	1279	386	770	1952	Robinson
16	2203	664	1327	1952	Robinson
17	2281	687	1373	1952	Robinson
18	3217	969	1937	1957	Riesel
19	4253	1281	2561	1961	Hurwitz
20	4423	1332	2663	1961	Hurwitz
21	9689	2917	5834	1963	Gillies
22	9941	2993	5985	1963	Gillies
23	11213	3376	6751	1963	Gillies
24	19937	6002	12003	1971	Tucker
25	21701	6533	13066	1978	Noll, Nickel
26	23209	6987	13973	1979	Noll
27	44497	13395	26790	1979	Nelson, Slowinski
28	86243	25962	51924	1982	Slowinski
29	110503	33265	66530	1988	Colquitt, Welsh
30	132049	39751	79502	1983	Slowinski
31	216091	65050	130100	1985	Slowinski
32	756839	227832	455663	1992	Slowinski, Gage
33	859433	258716	517430	1994	Slowinski, Gage
34	1257787	378623	757263	1996	Slowinski, Gage
35	1398269	420921	841842	1996	GIMPS
36	2976221	895932	1791864	1997	GIMPS
37	3021377	909526	1819050	1998	GIMPS
38	6972593	2098960		1999	Hajratwala,GIMPS
39?	13466917	4053946		2001	Cameron, GIMPS
40?	20996011	6320430		2003	GIMPS

Do dnešního dne již bylo nalezeno celkem 40 Mersennových prvočísel (viz předcházející tabulku všech dosud známých Mersennových prvočísel).

Jak „dlouhé“ je poslední z těchto prvočísel? Při desetibodovém písmu, což je běžná velikost knižních publikací, to činí 29 728 metrů.

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. Velký 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 909 526 cifer, takže další bariérou se stalo nalezení tzv. **megaprvočísla**, které bude mít více milion cifer. I tato bariéra však již v r. 1998 padla. Protože však skok od 38. Mersennova čísla k dalšímu je nápadně velký, je možné, že některé Mersennovo číslo bylo vynecháno. Proto jsou u posledních dvou čísel v tabulce uvedeny otazníky.