Mersenneovi brojevi

U maloj vijesti (članak je na sljedećoj stranici) objavljenoj 5. rujna 1996. u visokotiražnom dnevniku *New Herald Tribune* javlja se o otkriću prostog broja $2^{1\,257\,787} - 1$ koji *ima* 378 632 *znamenke. Ispis tog broja popunjava 12 novinskih stranica*.

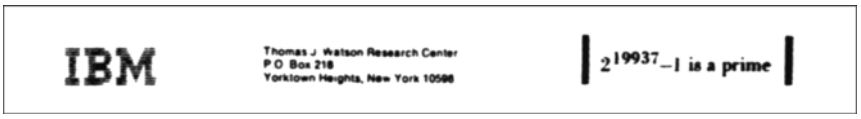
No već su i ranije slična dostignuća uzbuđivala svijet pa im je davan uistinu velik publicitet. Tako je primjerice 1963. godine u Sjedinjenim Američkim Državama kreiran poštanski pečat na kojem stoji zapis da je broj $2^{11\,213} - 1$ prost. A na memorandumu velikog proizvođača računala IBM–a neko je vrijeme stajalo zapisano da je broj $2^{19\,937} - 1$ prost.

Riječ je o *Mersenneovim brojevima*. To su prosti brojevi oblika

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

Francuski svećenik Marin Mersenne (1588. – 1648.) u svojoj knjizi *Cogita Physico–Mathematica* iznio tvrdnju da je broj $2^n - 1$ za $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ prost, a za sve druge prirodne brojeve manje od 257 da je složen. Kasnije su provjere pokazale kako je Mersenne pogriješio, brojevi m_{67} i m_{257} nisu prosti, a prosti su brojevi m_{61}, m_{89} i m_{107}.

Do danas je poznato 38 Mersenneovih brojeva. Potpun popis može se naći na adresi `www.mersenne.org.`, a mi u donjoj tablici navodimo nekoliko posljednjih.



n	broj znamenki	godina	otkrio
1 257 787	378 632	1996	Slowinski i Gage
1 398 269	420 921	1996	Armengaud i Woltman
2 976 221	895 932	1997	Spence i Woltman
3 021 377	909 526	1998	Clarkson
6 972 593	2 098 960	1999	Hajratwala i dr.

Prime Time: 378,632 Digits In a Number

The Associated Press

EAGAN, Minnesota — Computer scientists crunching numbers at the outer limits of numeration say they have stumbled onto the largest-known prime number.

Primes are whole numbers, such as 3, 5, 17, 23, that are evenly divisible only by one and themselves. This one, at 378,632 digits, would fill up 12 newspaper pages in standard type.

Mathematicians would express the number as two to the 1,257,787th power minus one. To work it out, take 2, multiply it by itself 1,257,786 times, and subtract one.

A Cray Research team discovered this largest prime number while testing one of the company's latest supercomputers in Chippewa Falls, Wisconsin.

The Greek mathematician Euclid proved that there is an infinite number of primes, but they do not occur in a predictable sequence and there is no formula for generating them.

''Finding these special numbers is a true 'needle in a haystack' exercise, but we improve our odds by using tremendously fast computers and a clever program,'' said David Slowinski, a Cray scientist.

Mr. Slowinski and a fellow researcher, Paul Gage, developed the program, which is used as a quality assurance test on supercomputer systems, that found the number.

Apart from testing supercomputers and fascinating mathematicians, large prime numbers are used extensively in cryptography.

Provjere je li neki broj oblika $2^n - 1$ Mersenneov ili nije nisu nimalo jednostavne. Naime, broj 2^n vrlo brzo raste pa je neophodno u provjerama koristiti kompjutore. No neki stariji rezultati su uistinu impresivni. Primjerice, francuski matematičar Edouard Lucas (1842. – 1891.), dokazao je 1876. da je broj

$$m_{127} = 170\,141\,183\,460\,469\,231\,731\,687\,303\,715\,884\,105\,727$$

prost broj. Pritom je razvijao metode kojima bi se postupak provjere što više pojednostavnio, pa Lucasa danas smatraju pionirom modernog numeričkog računa. Važan je rezultat kako broj $2^n - 1$ uopće može biti prost samo ako je n prost.

Uz traganje za Mersenneovim brojevima vezan je niz zgodnih detalja. Tako su, primjerice Laura Nickel i Curt Noll (slika dolje), dvoje osamnaestogodišnjih studenata Kalifornijskog sveučilišta u Haywardu, otkrili (naravno, uz pomoć računala) da je $2^{21\,701} - 1$ prost broj. Taj broj sastoji se čak od 6 533 znamenke. Devetnaestogodišnji Amerikanac Ronald Clarkson je 1998. na svom kućnom PC–u otkrio Mersenneov broj $m_{3\,021\,377}$ u čijem je zapisu 909 526 znamenki. Dojam o veličini toga broja može se steći ako se kaže da bi za njegov zapis bila potrebna knjiga od oko 500 stranica.

I na kraju, na spomenutoj internet adresi *The Electronic Frontier Foundation* nudi nagradu od 100 000 USD onome tko prvi otkrije prost broj s barem 10 000 000 znamenki. Natječaj je raspisan u okviru projekta GIMPS (*Great Internet Mersenne Prime Search*).