PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **28** (2000/2001)
Številka 6
Strani 349–351

Primož Potočnik:

NAJVEČJA ZNANA PRAŠTEVILA – nekoč in danes

Ključne besede: novice, zgodovina matematike, teorija števil, praštevila, praštevilski dvojčki, GIMPS.

Elektronska verzija: http://www.presek.si/28/1458-Potocnik.pdf

NAJVEČJA ZNANA PRAŠTEVILA – NEKOČ IN DANES

Čeprav je definicija praštevila enostavna in vsakomur razumljiva, je presenetljivo veliko vprašanj v zvezi z njimi še vedno odprtih. Celo tako preprosta naloga, kot je ugotoviti, ali je dano naravno število praštevilo, je lahko zelo trd oreh. Preprost in dobro znan postopek, Eratostenovo rešeto[1], postane pri ugotavljanju praštevilskosti velikih števil (z denimo nekaj tisoč števkami) zelo zamuden in praktično neuporaben. Prav na dejstvu, da je za velika števila težko preveriti, ali so praštevila ali ne, sloni ena najrazširjenejših metod šifriranja sporočil (glej članek: M. Vencelj, Šifriranje z javnim ključem, Presek, letnik 22, št. 6 (1994-1995), stran 354–357).

Že antični Grki so vedeli, da je praštevil neskončno mnogo. Kljub temu pa prav velikih praštevil niso poznali. Prvo praštevilo omembe vredne velikosti lahko zasledimo pri italijanskem matematiku Pietru Cataldiju[2], ki je leta 1588 pravilno preveril, da sta števili $2^{17} - 1 = 131071$ in $2^{19} - 1 = 524287$ praštevili. Ti dve števili sta zaradi svoje majhnosti ravno še primerni za uporabo Eratostenovega rešeta. Če želimo namreč preveriti, da je dano število n praštevilo, je dovolj preveriti, da n ni deljivo z nobenim praštevilom, ki je manjše ali enako kvadratnemu korenu iz števila n. Cataldiju pa so bila vsa praštevila med 2 in korenom zgornjih dveh števil že znana. Opogumljen s svojim rezultatom je Cataldi domneval, da so tudi števila $2^n - 1$ za $n = 23, 29, 31$ in 37 praštevila. Da je bila njegova domneva napačna pri $n = 23$ in $n = 37$, je dobrih 50 let kasneje dokazal znameniti matematik Fermat. Podobno se je godilo Cataldijevi domnevi pri $n = 29$. Pač pa je imel več sreče pri številu $2^{31} - 1 = 2147483647$. Leta 1772 (torej še dobrih sto let za Fermatom) je Euler namreč s precej spretnosti dokazal, da je to število res praštevilo.

Prvo veliko praštevilo, ki ni oblike $2^n - 1$ (praštevilom oblike $2^n - 1$ pravimo danes Mersennova praštevila – o njih bo govora v eni naslednjih številk Preseka), je leta 1867 našel Landry. Njegovo praštevilo je v resnici praštevilski delitelj števila $2^{59} - 1$ in znaša $(2^{59} - 1)/179951 = 3203431780337$. Do prave revolucije pri iskanju velikih praštevil je prišlo

[1] Eratosten (276–194 pr. n. št.). Rojen je bil v današnji Libiji, nekaj časa je deloval v Atenah, kasneje pa se je preselil v Aleksandrijo v Egiptu, kjer je bil med drugim imenovan za vodjo znamenite aleksandrijske knjižnjice. Tam je tudi umrl.

[2] Pietro Cataldi (1548–1626). Rojen je bil v Bologni. Od 17. leta dalje je poučeval matematiko v različnih krajih Italije, med drugim tudi na univerzi v Perugi. Leta 1584 se je vrnil v Bologno, kjer je poučeval matematiko in astronomijo vse do svoje smrti.

leta 1876, ko je francoski matematik Eduard Lucas[3] odkril domiseln in preprost kriterij, ki preverjanje, katero število oblike $2^n - 1$ je praštevilo, močno olajša. S svojo metodo je dokazal, da je 39-mestno število $2^{127} - 1$ praštevilo. Lucasov rezultat že predstavlja uvod v računalniško dobo iskanja velikih praštevil.

Danes si iskanja velikih praštevil brez pomoči računalnika ne moremo zamisliti. Po zaslugi Lucasovega testa so računalniki posebej uspešni pri iskanju velikih Mersennovih praštevil. Tako je med desetimi največjimi, do sedaj znanimi praštevili, kar sedem Mersennovih. Največja štiri so bila odkrita s pomočjo velikega internetskega iskanja Mersennovih praštevil (GIMPS – Great Internet Mersenne Prime Search), v katerega se lahko vključi vsakdo, ki ima dostop do interneta. O projektu GIMPS lahko bralci Preseka več izvejo na internetskem naslovu `www.mersenne.org`, kaj več o njem pa bomo napisali tudi v Preseku, brž ko bomo v uredništvu zbrali nekaj vtisov sodelujočih.

Poleg iskanja velikih praštevil je zelo zanimivo in težko iskanje t.i. praštevilskih dvojčkov. Pravimo, da praštevili p in q tvorita praštevilski dvojček, če se po absolutni vrednosti razlikujeta za natanko 2. Tako so praštevilski dvojčki: $(3, 5)$, $(5, 7)$, $(11, 13)$, $(17, 19)$, itd. Tako kot za Mersennova praštevila tudi za praštevilske dvojčke še vedno ni znano, ali jih je neskončno mnogo ali ne. To vprašanje sodi med najznamenitejše in najstarejše odprte probleme s področja teorije števil.

Za konec si oglejmo še tabeli šestih največjih, do sedaj znanih, praštevil in praštevilskih dvojčkov.

praštevilo	št. mest	odkritelji	letnica odkritja
$2^{6972593} - 1$	2098960	GIMPS	1999
$2^{3021377} - 1$	909526	GIMPS	1998
$2^{2976221} - 1$	895932	GIMPS	1997
$2^{1398269} - 1$	420921	GIMPS	1996
$2^{1257787} - 1$	378632	Slowinski, Gage	1996
$48594^{65536} + 1$	307140	Scott, Gallot	2000

Tabela šestih največjih praštevil

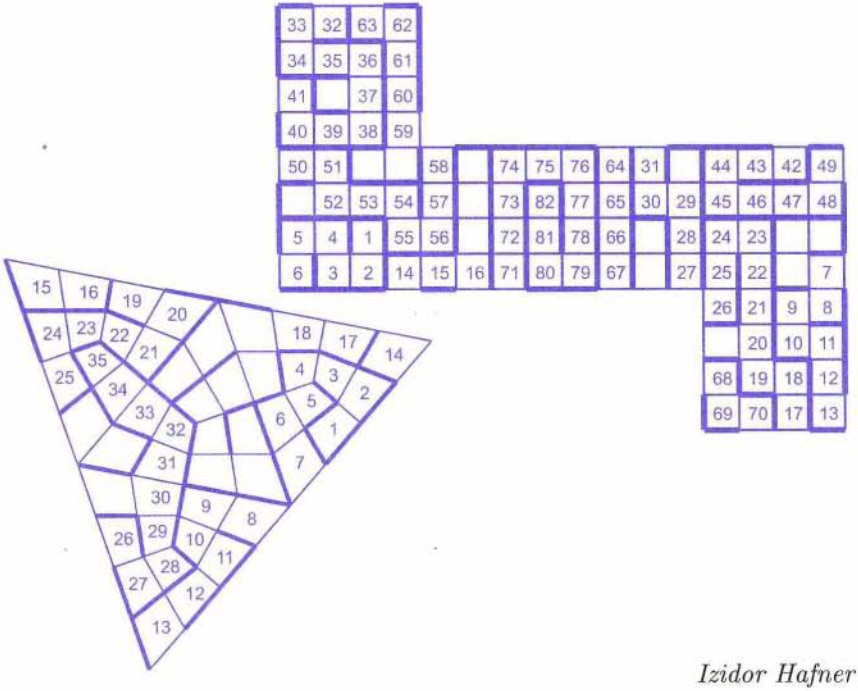
[3] Eduard Lucas (1842–1891). Rojen je bil v Amiensu v Franciji. Med francosko-prusko vojno (1870-1871) je služil v francoski vojski kot topniški častnik. Po francoskem porazu se je zaposlil kot profesor matematike na enem od pariških licejev. Raziskovalno je deloval predvsem na področju teorije števil. Njemu pripisujemo odkritje formule $\sqrt{5}F_n = ((1+\sqrt{5})/2)^n - ((1-\sqrt{5})/2)^n$ za n-ti člen Fibonaccijevega zaporedja F_n.

praštevili	št. mest	odkritelji	letnica odkritja
$1807318575 \cdot 2^{98305} \pm 1$	29603	Underbakke, Carmody, Gallot	2001
$665551035 \cdot 2^{80025} \pm 1$	24099	Underbakke, Carmody, Gallot	2000
$1693965 \cdot 2^{66443} \pm 1$	20008	La Barbera, Jobling, Gallot	2000
$83475759 \cdot 2^{64955} \pm 1$	19562	Underbakke, Jobling, Gallot	2000
$4648619711505 \cdot 2^{60000} \pm 1$	18075	Indlekofer, Jarai, Wassing	2000
$2409110779845 \cdot 2^{60000} \pm 1$	18075	Indlekofer, Jarai, Wassing	2000
$2230907354445 \cdot 2^{48000} \pm 1$	14462	Indlekofer, Jarai, Wassing	1999

Tabela šestih največjih praštevilskih dvojčkov

Primož Potočnik

LABIRINTI NA POLIEDRIH, 2. del – Rešitev s str. 259



Izidor Hafner