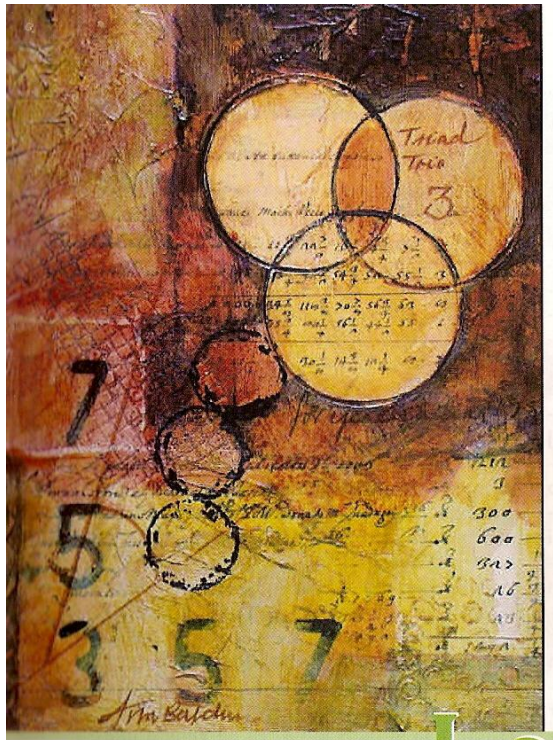


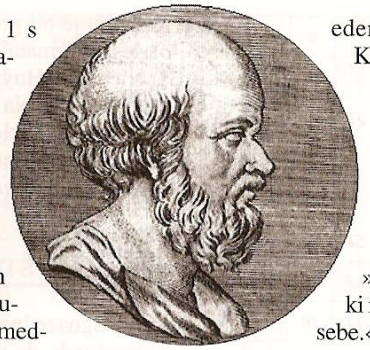
Iskanje velikih praštevil že nekaj časa ni več zgolj domena superračunalnikov in učenjakov z debelimi naočniki. V lov se lahko vključi vsakdo, ki ima doma spodoben računalnik s procesorjem Pentium 4 priključen na medmrežje – in to vse leto ter 24 ur na dan.

Lov na 44. Mersennovo praštevilo

Vera in Gregor Pavlič

Vsesplošni lov na velika praštevila ali GIMPS (angl. Great Internet Mersenne Prime Search) se je začel pred 10 leti. Sprožil ga je George Woltman z brezplačnim programom na internetu in zaposlil na tisoče osebnih računalnikov, ki neprekinjeno »meljejo« po več mesecev ter na koncu morda uspejo – ali pa tudi ne. Program na internetnem naslovu (objavljen je v okvirčku na koncu članka) temelji na algoritmu, ki ga je leta 1990 napisal Richard Crandall, izvrsten znanstvenik, zaposlen pri družbi Apple. Uspelo mu je podvojiti hitrost množenja velikih števil, ki se je izkazala za uspešno tudi pri drugih problemih. Hkrati s tem je odkril in patentiral poseben sistem enkripcije oz. šifriranja (angl. Fast Elliptic Encryption system), ki ga družba Apple danes uporablja za hitro šifriranje in dešifriranje. George Woltman je Crandallov algoritem priredil za računalniški strojni jezik ter sprožil odmeven in uspešen projekt. GIMPS ima središče v Orlandu na Floridi in ga propagirajo učitelji od osnovnih šol do univerz, da bi učence in študente navdušili za matematične raziskave.

Lastnika najnovejše trofeje projekta GIMPS sta dr. Curtis Cooper in dr. Steven Boone z državne univerze v Missouriju, ki sta 15. decembra lani odkrila 43. Mersennovo praštevilo $2^{30.402.457} - 1$ s kar 9.152.052 števkami. Zaradi bližine magičnega števila 10 milijonov števk je postalo iskanje naslednjega Mersennovega praštevila še zanimivejše in (po ameriško) ustrezno »finančno podprto«. Za nagrado 100.000 ameriških dolarjev se najbrž ne bo trudilo le okrog 1500 članov mednarodnega internetnega društva *mersennforum.org*, čeprav iskanje spominja na iskanje šivanke v kopici sena. Glede na izkušnje imajo prav člani tega društva velike možnosti, saj so od leta 1996 našli devet Mersennovih praštevil – v povprečju po eno na leto (večina najditeljev je bila iz ZDA, po eden pa iz Francije, Nemčije, Kanade in Anglije).



Eratosten (275–194 pr. Kr.)

Praštevil je neskončno mnogo.

Dokaz tega izreka je eden pomembnejših v teoriji števil, hkrati pa toliko preprost, da se ga učijo že gimnazijci v prvem letniku. Temelji na dveh možnostih, ki se izključujeta.

Dokazovanje začnemo s predpostavko, da je praštevil končno mnogo – recimo k. Če jih je končno, jih lahko preštejemo in razvrstimo po velikosti $p_1, p_2, p_3, \ldots, p_k$. Potem tvorimo število N, ki je za 1 povečan produkt vseh naštetih praštevil: $N = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1$. To število je ali sestavljeno ali praštevilo. Če bi veljala druga možnost, smo že prišli do protislovja, saj smo začeli s predpostavko, da je praštevil končno mnogo in vemo, da je p_k največje med njimi, število N pa je očitno večje. Edina možnost, ki nam ostane, je, da je N sestavljeno število. Če to drži, mora biti deljivo vsaj z enim od praštevil $p_1, p_2, p_3, \ldots, p_k$. Tu pa spet pride to težav, saj pri deljenju števila N s katerim koli znanim praštevilom izmed $p_1, p_2, p_3, \ldots, p_k$ ostane 1. Tudi ta možnost nas je pripeljala v brezizhoden položaj, zato sklepamo, da je bila predpostavka napačna in da velja ravno obratno: če praštevil ni končno, jih je neskončno. S tem je izrek dokazan.

PRAŠTEVILA

Praštevila vznemirjajo svet že poltretje tisočletje. Njihova definicija se glasi: »Praštevila so naravna števila, ki imajo samo dva delitelja: 1 in sebe.« Vsa druga naravna števila, ki so večja od 1, imajo več kot dva delitelja in se imenujejo sestavljena števila. Tako definicijo sta z neznatno razliko v zaporedju besed postavila slavna grška učenjaka Aristotel in Evklid. Slednji je tudi dokazal, da je praštevil neskončno mnogo. Vsa praštevila, manjša od ne prevelikega naravnega števila, pa je znal poiskati Eratosten. Metoda se po njem imenuje Eratostenovo rešeto in je zelo preprosta.

V nadaljevanju si oglejmo, kako najdemo praštevila do 100. Najprej napišemo vsa naravna števila od 1 do 100. Ko prečrtamo vsa soda števila oziroma vse večkratnike števila 2 (prvo praštevilo), se seznam prepolovi. Prvo neprečrtano število je 3 in je naslednje praštevilo. Nato prečrtamo vse večkratnike števila 3, pri čemer se seznam spet znatno skrajša. Enako storimo pri naslednjih praštevilih 5 (prečrtamo števila 25, 35, 55, 65, 85 in 95), 7 (prečrtamo števila 49, 77 in 91) in 11. Če smo vsaj malo vešči poštevanke, vidimo, da je prečrtavanja konec in da so vsa neprečrtana števila praštevila. Pravilo, ki sledi iz te kratke vaje, se glasi: za iskanje praštevil do naravnega števila n je treba izvesti Eratostenov postopek do (na celo število zaokroženega) števila $\sqrt{n}$.

MERSENNOVA PRAŠTEVILA

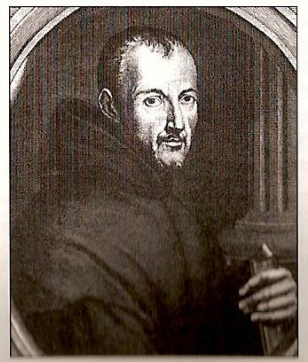
Marin Mersenne se je rodil leta 1588 v majhnem francoskem mestu Oizé v delavski družini. Že kot otrok je kazal neverjetno željo po učenju, zato so ga starši kljub pomanjkanju poslali v šole. Pri šestnajstih je zaprosil za sprejem v jezuitsko šolo, ki je sprej-

1	2	3	4	5	6	7	8	9	10
11	12	13	14	15	16	17	18	19	20
21	22	23	24	25	26	27	28	29	30
31	32	33	34	35	36	37	38	39	40
41	42	43	44	45	46	47	48	49	50
51	52	53	54	55	56	57	58	59	60
61	62	63	64	65	66	67	68	69	70
71	72	73	74	75	76	77	78	79	80
81	82	83	84	85	86	87	88	89	90
91	92	93	94	95	96	97	98	99	100

Praštevila do 100

mala študente ne glede na njihov finančni položaj. Naključje je hotelo, da je isto šolo obiskoval tudi 8 let mlajši genij Réné Descartes, čeprav se takrat po vsej verjetnosti nista poznala in sta postala prijatelja šele precej kasneje. Na nadaljevanje študija se je odpravil v Pariz in se po enem dnevu bivanja pri redovnikih frančiškanih – navdušen nad videnim – odločil stopiti v njihov red. Ko je leta 1611 zaključil študij teologije in filozofije na College Royale in na Sorboni, je postal član reda in bil leto kasneje posvečen v duhovnika. S prvo zadolžitvijo je postal učitelj teologije in filozofije mladih pripravnikov v samostanu v Neversu, po dveh letih pa predstojnik samostana Place Royale v Parizu, kjer je ostal do smrti leta 1648.

Mersenna je od otroških let zanimala matematika in z njo se je ves čas tudi ukvarjal. Leta 1623 je izdal prvi dve razpravi iz teologije, v katerih je med drugim pred napadi drugih teologov branil Galileija in Aristotela. Svoje globoko prepričanje, da teologija brez znanosti, posebno matematike, ne more napredovati, je opisal v knjigi *La vérité des sciences* (Resnica znanosti). V tem času je že postal glavni dopisovalec mnogih znanih matematikov – lahko bi rekli, da je bil predhodnik intraneta za Descartesa, Fermata, Huygensa, Pella, Galileija, Torricellija, Huygensa, Robervala, Gassendija in druge. Na začetku se je največ ukvarjal s krivuljo cikloido, kasneje pa s praštevili oblike $2^p - 1$, kjer je p praštevilo. Po njem se imenujejo *Mersennova praštevila*.



Marin Mersenne (1588–1648)

POPOLNA ŠTEVILA

Mnogo srednjeveških matematikov je bilo prepričanih, da so vsa števila oblike $2^p - 1$ pri praštevilskem p praštevila. Mersenne je v razpravi *Cogitata Physica-Mathematica* (1644) postavil trditev, da so števila oblike $n = 2^p - 1$ praštevila, če je $p = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127$ in 257, v vseh drugih 44 primerih praštevil do 257 pa sestavljena števila. Šele leta 1947 je bilo dokončno jasno, da se je zmotil le v 5 primerih (števili 67 in 257 ne pripeljeta do praštevil, tri števila 61, 89 in 107, ki pripeljejo do praštevilskoti števila n, pa je zgrešil). Zagovorniki Mersenna sodijo, da je bilo število 67 le slabo zapisano število 61 in da je bilo pomot v resnici manj.

Mersennova praštevila so povezana tudi s popolnimi števili, ki jih je proučeval že Pitagora. To so števila, ki so enaka vsoti svojih pravih deliteljev. Prva štiri taka števila, ki so jih poznali že v antiki, so:

$6 = 1 + 2 + 3,$
$28 = 1 + 2 + 4 + 7 + 14,$
$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248$
$8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064$

Pri iskanju splošne formule je Evklid prišel do naslednjega pravila: vsoto prvih treh potenc števila 2 (ki je praštevilo $1 + 2 + 4 = 7$) pomnožimo z zadnjim 4 in dobimo $7 \cdot 4 = 28$.

Pravilo deluje tudi v naslednjih primerih (le da seštejemo vedno po eno potenco več):

$1 + 2 + 4 + 8 + 16 = 31,$
$31 \cdot 16 = 496.$

p (eksponent)	Število števk	Leto	Odkritelj
1	$2, 2^2 - 1$	1	–	–
2	$3, 2^3 - 1$	1	–	–
3	$5, 2^5 - 1$	2	–	–
4	$7, 2^7 - 1$	3	–	–
5	13	4	1456	anonymous
6	17	6	1588	Cataldi
7	19	6	1588	Cataldi
8	31	10	1772	Euler
9	61	19	1883	Pervushin
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	1281	1961	Hurwitz
20	4.423	1332	1961	Hurwitz
21	9.689	2917	1963	Gillies
22	9.941	2993	1963	Gillies
23	11.213	3376	1963	Gillies
24	19.937	6002	1971	Tuckerman
25	21.701	6533	1978	Noll in Nickel
26	23.209	6987	1979	Noll
27	44.497	13395	1979	Nelson in Slowinski
28	86.243	25962	1982	Slowinski
29	110.503	33265	1988	Colquitt in Welsh
30	132.049	39751	1983	Slowinski
31	216.091	65050	1985	Slowinski
32	756.839	227832	1992	Slowinski in Gage
33	859.433	258716	1994	Slowinski in Gage
34	1.257.787	378632	1996	Slowinski in Gage
35	1.398.269	420921	1996	Armengaud (GIMPS)
36	2.976.221	895932	1997	Spence (GIMPS)
37	3.021.377	909526	1998	Clarkson (GIMPS)
38	6.972.593	2098960	1999	Hajratwala (GIMPS)
39	13.466.917	4053946	2001	Cameron (GIMPS)
40	20.996.011	6320430	2003	Shafer (GIMPS)
41	24.036.583	7235733	2004	Findley (GIMPS)
42	25.964.951	7816230	2005	Nowak (GIMPS)
43	30.402.457	9152052	2005	Cooper in Boone (GIMPS)

Ker velja, da je $1 + 2 + 4 + \ldots + 2^{k-1} = 2^k - 1$, se izrek na splošno glasi takole: »Če je število $2^k - 1$ praštevilo (oz. Mersennovo praštevilo), potem je $2^{k-1} \cdot (2^k - 1)$ popolno število.« Hkrati z novim, 43. Mersennovim praštevilom poznamo sedaj tudi 43. popolno število $2^{30.402.456} \cdot (2^{30.402.457} - 1)$; to zares velikansko število ima kar 18.304.103 števke.

Najbrž je že marsikdo pomislil, čemu se je vredno toliko ukvarjati s praštevili, ali pa, da vse skupaj že spominja na igračkanje. Morda je to še veljalo za Pitagoro in njegovo družbo 500 let pr. Kr., ki so delovanje sveta razlagali s števili. Od takrat naprej pa so se poklicni in amaterski matematiki zelo resno ukvarjali s to podmnožico naravnih števil, odkrili celo vrsto njihovih čudovitih lastnosti in postavili na kupe hipotez, od katerih veliko še ni potrjenih. Šele v 20. stoletju se je pokazalo, da so praštevila tudi uporabna: brez njih ne gre v kriptografiji pri kodiranju z javnim ključem oziroma kodiranju RSA.

KODIRANJE RSA

Kodiranje RSA so leta 1977 iznašli Ronald Rivest, Adi Shamir in Leonard Adleman (po začetnicah njihovih priimkov se kodirni ključ tudi imenuje). Danes ga dnevno uporabljajo milijoni ljudi

Primer poteka kodiranja RSA

Oseba A bi rada poslala osebi B sporočilo, npr. številko 71 omarice na železniški postaji. Proces se začne tako, da oseba B izbere dve (veliki) praštevili, recimo p = 11 in q = 13. Njun produkt je 143 in to število javno objavi. Potem izračuna produkt (p – 1) · · (q – 1) = 120 in izbere število e, ki je tuje številu 120, denimo e = 7. Tudi število e je javno. Sedaj mora rešiti enačbo z dvema neznankama (imenuje se tudi Diofantska enačba) 7 d – 120 y = 1 in kot rešitev dobi števili d = 103 in y = 6. Število 103 je skrivno dekodirno število.

Oseba A pozna število, ki ga mora zakodirati, in javni števili 143 in 7. Število zakodira tako, da izračuna ostanek pri deljenju števila 71^7 s številom 143. To število je 124 in ga pošlje osebi B.

Za dekodiranje števila 124 mora oseba B izračunati ostanek pri deljenju števila 124^{103} s številom 143 in s tem dobi poslano skrivno število 71.

Računanje seveda opravi računalnik s pomočjo posebnega programa, in če poznate osnove kongruenčnega računa, si lahko ogledate postopek od zadnjega konca:

$71^7 = 143\,k + 124$

$71^7 = (11 \cdot 13 \cdot q) + 124 \equiv 0 + 124 \pmod{11}$

$(71^7)^{103} \equiv 124^{103} \pmod{11}$

$7 \cdot 103 = 1 + 120 \cdot 6$

$(71^7)^{103} = 71^{7 \cdot 103} = 71^{1 + 120 \cdot 6} =$
$= 71 \cdot 71^{120 \cdot 6} = 71 \cdot (71^{72})^{10}.$

Ker velja D(11,71) = 1, dobimo po malem Fermatovem izreku: $n^{p-1} \equiv 1 \pmod{p}$

$(71^{72})^{10} \equiv 1 \pmod{11}$

$124^{103} \equiv (71^7)^{103} \equiv 71 \cdot (71^{72})^{10} \equiv 71 \cdot 1 =$
$= 71 \pmod{11}$

$124^{103} - 71 \equiv 0 \pmod{11},$

torej 11 deli število $124^{103} - 71$, pa tudi 13 deli to število. In ker sta 11 in 13 tuji, tudi njun produkt deli to število, torej je ostanek pri deljenju števila 124^{103} s 143 enak 71.

Sedaj je tudi lažje razumeti, zakaj so velika praštevila tako pomembna. Za kodiranje potrebujemo dve dovolj veliki praštevili, in čeprav je kodirni ključ znan, v določenem času (npr. mesec dni), še tako dober računalnik s še tako dobrim programom ne more iz njunega produkta poiskati obeh faktorjev. Po enem mesecu pa oblikujejo kodo z drugima dvema velikima praštevilomi – in »kriptosvet« se vrti naprej.

pri e-poslovanju, e-poštnih sporočilih, e-kupovanju, e-bančništvu itd. Kako pomembno je tovrstno kodiranje, pove tudi podatek, da so podjetje Data Security, ki se je ukvarjalo s promocijo in prodajo storitev RSA, že pred leti prodali za 400 milijonov dolarjev. S praštevili se torej da tudi pošteno zaslužiti.

V teoriji praštevil so doslej postavili že zelo veliko trditev in jih prav tako zelo veliko tudi rešili. Kljub temu ostajajo nekatere še nerešene, stalno pa nastajajo nove. Ena najstarejših nerešenih je *Golbachova domneva*. Leta 1742 je pruski matematik Christian Golbach poslal Leonhardu Eulerju (ŽIT 2003/9, str. 66), tedanji matematični avtoriteti, pismo s trditvijo: »Vsako sodo naravno število, ki je večje od 2, lahko zapišemo kot vsoto dveh praštevil (ki sta lahko tudi enaki; op. avt.).«

$4 = 2 + 2$
$6 = 3 + 3$
$8 = 3 + 5$
$10 = 3 + 7 = 5 + 5$
$12 = 5 + 7$
$14 = 3 + 11 = 7 + 7$

Čeprav so se z iskanjem dokaza ukvarjali in se še ukvarjajo najslavnejši matematiki Euler, Hardy, Littlewood, Vinogradov, Chen, Estermann in drugi, in je angleški založnik Tony Faber za uspešen dokaz v letu 2000 razpisal nagrado milijon dolarjev, se ni oglasil še nobeden. Kot se je pokazalo že mnogokrat, so dokazi na videz preprostih trditev v teoriji števil najtežji: v našem primeru je rešitev po vsej verjetnosti povezana z generalizirano Riemannovo hipotezo, eno najbolj slavnih ugank matematičnega sveta.

Z rešitvijo Golbachove domneve je najbrž povezana tudi rešitev vprašanja o številu praštevilskih dvojčkov. To so pari praštevil oblike p in $p + 2$, za katere domnevajo, da jih je neskončno mnogo. Kako trd boj bijejo matematiki, dokazuje zgodba o ameriškem matematiku Richardu Arenstorfu, ki je maja 2004 na 38 straneh objavil domnevno rešitev tega problema, že čez en teden pa je Michel Balazard z univerze v Bordeauxu na strani 35 v pomožnem izreku našel napako. Najbrž še vedno ugotavljajo, ali je mogoče napako popraviti oz. nadomestiti izrek z drugim pomožnim izrekom, ali pa je napaka usodna.

7	2
11	11
929	101
98689	10301
9989899	1003001
999727999	100030001
99999199999	10000500001
9999987899999	1000008000001
999999787999999	100000323000001
99999999299999999	10000000500000001
999999992999999999	100000008000000001

palindromna piramidna praštevila

188888881	111181111	323232323
19999999	111191111	727272727
355555553	777767777	919191919
platojska praštevila	8-cifrna praštevila	izmenična praštevila
123484321	120343021	765404567
345676543	354767453	987101789
345686543	759686957	987646789
gorata praštevila	delno zaporedna praštevila	dolinska praštevila

PALINDROMNA PRAŠTEVILA

Palindromna praštevila so praštevila, ki se berejo enako z desne in leve in so različica palindromnih stavkov, kot npr. »PERICA REŽE RACI REP«, »SATOR AREPO TENET OPERA ROTAS« (ŽIT 2006/4, str. 47) in še malo bolj črn »ALI SE BO GORDANA NA DROG OBESILA« ter obešenjaški »ATA KIDNI S SINDIKATA«.

Nekaj prvih palindromnih praštevil si sledi takole: 2, 3, 5, 7, 11, 101, 131, 151, 181, 191, 313, 353, 373, 383, 727, 757, 787, 797, 919, 929, 10301, 10501, 10601, 11311, itd. Od novembra 2004 največje znano palindromno praštevilo (zapisano v potenčni obliki) je $10^{130022} + 3761673 \cdot 10^{65008} + 1$ nič ne pove o tem, ali jih je neskončno ali končno mnogo. Zato bo treba na odgovor na to vprašanje še počakati. Posebno zanimivo je, da so nekatera praštevila nepalindromi v desetiškem zapisu, v dvojiškem pa so palindromi:

17	31	73	107	127	257	313	443	1193
10001	11111	1001001	1101011	1111111	100000001	100111001	110111011	10010101001

Primer zase je praštevilo

1023456987896543201,

prav tako zanimivo praštevilo, ki ni palindrom, pa je

12345678901234567891.

Ker se reševanje več odprtih praštevilskih problemov vleče že stoletja, nekateri strokovnjaki menijo, da se lahko zgodi, da bo njihova rešitev povezana s kakšno preprosto metodo, ki vrhunskim matematikom še ni prišla na misel, lahko pa bi morda kakšnemu razsvetljenemu amaterju. Zato kar veselo na delo!

Po drugi strani imajo veselje s temi števili tudi zanesenjaki amaterji, ki med njimi iščejo posebne vzorce in posebnosti. Mednje spadajo palindromna piramidna števila in številne podvrste palindromnih praštevil s slikovitimi imeni.

http://...

www.mersenne.org (vse o tekmovanju GIMPS)
primes.utm.edu/mersenne/index.html (Mersennova praštevila)
www-groups.dcs.st-and.ac.uk/~history/HistTopics/Perfect_ numbers.html (popolna števila)
en.wikipedia.org/wiki/Goldbach%27s_conjecture (o Golbachovi domnevi)
www.jimloy.com/number/twin.htm (praštevilski dvojčki)
numbers.computation.free.fr/Constants/Primes/twin.html (praštevilski dvojčki)
members.cox.net/mathmistakes/palindromes.htm (palindromna števila)