1.
O prirodnim brojevima

"Prirodne brojeve stvorio je Bog, sve ostalo je ljudsko djelo."
(Kronecker)

Skup prirodnih brojeva izgleda nam stvarno "prirodno", a koliko još tajni skriva! Taj skup

$$\mathbf{N} = \{1, 2, 3, 4, \ldots, n-1, n, n+1, \ldots\} \tag{1}$$

je beskonačan. Iza svakog prirodnog broja n dolazi prirodan broj $n+1$, što nas dovodi do pojma tzv. potencijalne beskonačnosti koju danas priznaju skoro svi matematičari. Da li se skup $\mathbf{N}$ može shvatiti u totalitetu, u ukupnosti? Ta tzv. aktualna beskonačnost još je i danas predmet razmatranja.

Da je skup $\mathbf{N}$ beskonačan uočili su i stari Grci riječima: "Mnogo ima zrnaca pijeska u moru i mnogo je kapljica kiše palo na zemlju, ali ima brojeva većih i od tog broja". Mi možemo zamisliti i ispisivati sve veće i veće prirodne brojeve. Predodžbu o njihovoj veličini ubrzo ćemo izgubiti. Navedimo neke zanimljivosti:

a) Edingtonov broj svih elektrona u Svemiru iznosi $E = 10^{76}$, no taj je broj beznačajan prema broju svih različitih šahovskih partija koji iznosi

$$S = 10^{18900}.$$

b) Zanimljivo je pitanje: Koji se najveći broj može napisati s tri devetke? U odgovoru ćemo se koristiti i našim znanjem o potencijama, a i relacijom za n faktorijela

$$n! = 1 \cdot 2 \cdot 3 \cdot \ldots \cdot (n-1) \cdot n. \tag{2}$$

Uzevši u obzir **a)** i **b)** dobivamo ovaj niz rastućih prirodnih brojeva:

$$999 < 99^9 < \text{E} < (9^9)^9 < 9^{99} < 999! < S < 9^{9^9}.$$

Red veličina ovih *brojeva divova* je redom

$$10^3 < 10^{19} < 10^{76} < 10^{78} < 10^{87} < 10^{2\,565} < 10^{18\,900} < 10^{369\,000\,000},$$

a dobivamo ih pomoću logaritama; pri tome smo **999!** napisali kao

$$\frac{1\,000!}{1\,000}$$

a **1000!** smo računali pomoću Stirlingove formule (približno)

$$n! = n^n e^{-n}\sqrt{2n\pi}. \tag{3}$$

Tu je $e = 2,718\ldots$ (baza prirodnih logaritama), a $\pi = 3.14\ldots$.

2.
Primbrojevi

2.1. Uvod

"Matematika je kraljica nauke, a aritmetika (teorija brojeva) je kraljica matematike."
(K. F. Gauss)

"Kraljica je sve manje, a i kraljevanje je sve teže."
(V. Devidé)

Izdvojimo iz skupa prirodnih brojeva $\mathbf{N}$ skup prostih ili primbrojeva, tj. sve one prirodne brojeve koji su djeljivi samo sa 1 i sa samim sobom

$$P = 2, 3, 5, 7, 11, 13, 17, \ldots \tag{4}$$

Ostale prirodne brojeve zvat ćemo složenima, a neka broj 1 nije ni prim ni složen, jer nema dva različita djelitelja.

Skup P krije još mnoge tajne. Navedimo neke:

t1) Ne znamo napisati po volji veliki prim broj, npr. prvi prim broj koji je veći od 9^{9^9}, nego danas računalima moramo redom ispitivati brojeve $9^{9^9}+2$ pa onda $9^{9^9}+4$ i mukotrpnim računom ustanoviti da li su oni prim ili složeni.

t2) Nije otkrivena formula koja daje sve prim brojeve. Uočimo funkciju

$$f(n) = n^2 + n + 41 \ldots \tag{5}$$

Nađimo redom

$$\begin{aligned} f(0) &= 41 \\ f(1) &= 43 \\ f(2) &= 47 \\ f(3) &= 53 \\ f(4) &= 61 \end{aligned}$$

Dobili smo pet prim brojeva $41, 43, 47, 53, 61$. Lako se uvjeravamo da su svi brojevi od $f(0)$ do $f(39)$ prim, ali $f(40) = 41^2$ je složen. Dakle ta formula ne daje sve prim brojeve. Slično relacija

$$f(n) = n^2 + n + 17$$

daje primbrojeve za sve n od 1 do 15, a relacija

$$f(n) = 2n^2 + 29$$

daje primbrojeve za sve n od 1 do 28. Bilo je još drugih bezuspješnih pokušaja da se nađe formula koja daje primbrojeve za svaki n.

t3) Ne znamo da li tzv. parova primbrojeva blizanaca kao što su 3, 5 ili 5, 7 ili 41, 43 ima konačno ili beskonačno mnogo. Drugim riječima do danas nije poznato da li se broj 2 može na beskonačno mnogo načina predstaviti kao razlika dva uzastopna prosta broja. Do broja 30 000 000 ima 152 892 takvih parova blizanaca.

Ako redom ispitujemo sve veće i veće primbrojeve, uočit ćemo da su oni u skupu prirodnih brojeva sve rjeđi. Npr. izmjeđu 200 i 210 nema nijednog primbroja. Da li možda negdje ne prestaju tj. da li postoji najveći primbroj? Ta slutnja nije opravdana jer je Euklid (4. st. pr. n. e.) dokazao:

Poučak 1. Ne postoji najveći primbroj.

Dokazi. Pretpostavimo suprotno, tj. neka je p najveći primbroj. Pomnožimo sve primbrojeve od 2 do p i dodajmo jedinicu.

$$2 \cdot 3 \cdot 5 \cdot 7 \ldots p + 1 = p_1 \tag{6}$$

Sada je prirodni broj p_1 ili prim ili složen. Ako je p_1 prim, on je veći od p, tj. p nije najveći prim broj. Ako je p_1 složen, tada on mora biti djeljiv sa nekim od primbrojeva $2, 3, 5, 7, \ldots, p$. No iz relacije (6) vidi se da p_1 nije djeljiv ni sa jednim od primbrojeva $2, 3, 5, 7, \ldots, p$ jer je ostatak kod djeljenja uvijek 1. Prema tome mora postojati primbroj p_2 veći od p, s kojim se složen broj p_1 može podijeliti bez ostatka, pa p opet nije najveći primbroj. Time je dokaz završen.

Iz dokaza Poučka 1. vidi se i postupak dobivanja sve većih i većih prim brojeva. Naime, iz relacije (6) ili je p_1 primbroj veći od p ili postoji primbroj (veći od p) s kojim je p_1 djeljiv. Dakle za svaki primbroj p možemo naći novi prim broj veći od p.

Kummer je dao novu formulaciju dokaza Poučka 1:

Poučak 1'. Pretpostavimo da postoji samo konačno mnogo primbrojeva

$$p_1 < p_2 < \ldots < p_i.$$

Neka je $N = p_1 \cdot p_2 \cdot \ldots \cdot p_i > 2$. Neka je najprije prirodni broj $N-1$ složen, pa kao produkt primbrojeva ima primdjelitelj p_i zajedno sa N; prema tome p_i dijeli N i $N-1$, dakle i njihovu razliku, tj. p_i dijeli $N-(N-1)=1$ što je nemoguće.

Neka je sada broj $N-1$ prim. Budući da je $N = p_1 \cdot p_2 \cdot \ldots \cdot p_i$ slijedi da je sada primbroj $N-1 > p_i$, tj. p_i nije najveći primbroj. Dakle je skup primbrojeva $2, 3, 5, 7, 11 \ldots$ beskonačan. Kummerov dokaz se svodi na Euklidov.

Ribenboim je u svom djelu "Book of Prime Number Records" osim Kummerovog dokaza navodi još desetak dokaza teorema o beskonačnosti skupa primbrojeva. Samuel Yates definira *primbrojeve titane* kao primbrojeve koji imaju više od 1 000 znamenaka. Kada je u 1984. uveo taj pojam bilo je poznato samo 110 takvih primbrojeva; danas ih znamo 150 puta više.

Yates je uveo i pojam *primbrojeva giganata*. To su primbrojevi sa najmanje 10 000 znamenaka.

Zahvaljujući računalima danas znamo za vrlo velike proste brojeve. Godine 1947. najveći poznati prosti broj bio je $2^{127}-1$ (ima 33 znamenke), 1961. godine to je bio broj $2^{3217}-1$ (969 znamenke). Poslije 1961. pronađen je još veći primbroj $2^{19937}-1$ (6 001 znamenke). Godine 1978. poslije trogodišnjeg ispitivanja, studenti Laura Nickel i Kurt Nol s Harwardskog sveučilišta u Kaliforniji otkrili su uz pomoć računala primbroj $2^{21701}-1$ (6 533 znamenke). Do njega su došli pošto su načinili 5 različitih programa za računalo.

2.2. Eratostenovo sito

Primbrojeve možemo dobiti pomoću skupa prirodnih brojeva

$$\mathbf{N} = \{1, 2, 3, 4, 5, \ldots, \} \tag{7}$$

na sljedeći način:

Uočimo prvi primbroj 2 i izbacimo iz skupa sve njegove višekratnike $4, 6, 8, 10, \ldots$. Zatim uzmemo sljedeći primbroj iza 2, tj. broj 3 i također izbacimo sve višekratnike toga broja. Postupak nastavimo i sa sljedećim primbrojevima $5, 7, 11, 13, \ldots$ po volji daleko. Tada će u skupu $\mathbf{N}$ ostati osim broja 1 neprecrtani primbrojevi $2, 3, 5, 7, 11, \ldots$ dok su ostali propali kao kroz neko sito, tzv. Eratostenovo sito (Eratosten (275.–195. pr. n. e.)).

Danilo Blanuša našao je sljedeću jednostavnu geometrijsku interpretaciju Eratostenovog sita. Zamislimo u Descartesovim koordinatnom sustavu skup A točaka $\left(0, \frac{1}{m}\right)$, $m = 1, 2, 3, \ldots$ i skup B točaka $(n+1, 0)$, $n = 1, 2, 3, \ldots$. Svaku točku skupa A spojimo pravcem sa svakom točkom skupa B. Tada je skup apscisa sjecišta spomenutih pravaca s pravcem $y = -1$ upravo skup složenih brojeva.

Dokaz. Koristeći jednadžbu pravca kroz dvije točke $\left(0, \frac{1}{m}\right)$ i $(n+1, 0)$ slijedi

$$y - y_1 = \frac{y_2 - y_1}{x_2 - x_1}(x - x_1) \tag{8}$$

$$\frac{x}{n+1} + my = 1 \tag{9}$$

Pravac (9) siječe pravac $y = -1$ u točkama apscice

$$x = (m+1)(n+1). \tag{10}$$

Broj x je složen jer su m i n prirodni brojevi.

Obratno. Ako je x složen, tad je (10) tj. $x = (m+1)(n+1)$, m, n iz N, dakle je x apscisa sjecišta pravaca koji spaja točke $\left(0, \frac{1}{m}\right)$ i točke $(n+1, 0)$ sa pravcem $y = -1$.

2.3. Primbrojevi blizanci

Deset prvih parova uzastopnih prim brojeva je

$$\begin{array}{ccccc} 3,5, & 5,7, & 11,13, & 17,19, & 29,31, \\ 41,43, & 59,61, & 71,73, & 101,103, & 107,109. \end{array}$$

H. Tietze je dao tablicu prvih blizanaca manjih od 300 000 i veći broj u svakom paru. Ima ih 2 994.

Selmer i Nesheim dali su prirodne brojeve n za koji su $6n+1$ i $6n-1$ prim blizanci i manji od 200 000.

D. H. i E. Lehmer našli su da postoji 152 892 parova prim blizanaca manjih od 30 000 000. Najveći od tih parova je par

$$10^{12}+9\,649 \quad \text{i} \quad 10^{12}+9\,651.$$

Kraće to možemo zapisati kao

$$10^{12}+9\,650\pm 1.$$

Poput prim blizanaca moglo bi se razmatrati i pitanje složenih blizanaca. Za svaki složeni prim broj k naći sve složene brojeve $k-2$? Golomb piše o tom problemu. W. A. Golubew se pitao da li za svaki $n \in \mathbf{N}$ postoji bar jedan par blizanaca između n^3 i $(n+1)^3$?

Red recipročnih vrijednosti primbrojeva parova blizanaca je konačan ili konvergentan (Brun). "Elementarni" dokaz Brunova teorema je u knjizi E. Landaua. Zbroj toga reda pod (11) odredio je E. S. Selmer.

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)+\left(\frac{1}{29}+\frac{1}{31}\right)+\ldots \quad (11)$$

Red recipročnih vrijednosti svih primbrojeva je divergentan.

$$\sum_{k=2}^{\infty}\frac{1}{p_k}=\frac{1}{2}+\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\ldots+\frac{1}{31}+\frac{1}{37}+\frac{1}{41}+\ldots \quad (12)$$

Dokaz slijedi iz nejednakosti

$$\sum_{k=2}^{n}\frac{1}{p_k}>\frac{1}{36}\ln\ln(n+1) \quad (13)$$

$n=3,4,5,\ldots$.

Deset najvećih poznatih prim blizanaca.

Prim par	Broj znamenaka	Otkrili	Kada
$242\,206\,083 \cdot 2^{3880} \pm 1$	11 713	Indlekofer i Jarai	XI./ 1995.
$570\,918\,348 \cdot 10^{5120} \pm 1$	5 129	Dubner	X./ 1995.
$697\,053\,813 \cdot 2^{16352} \pm 1$	4 932	Indlekofer i Jarai	1994.
$6\,797\,727 \cdot 2^{15328} \pm 1$	4 622	Tony Forbes	1995.
$169\,223\,232 \cdot 10^{4020} \pm 1$	4 030	Dubner	1993.
$4\,655\,428\,828 \cdot 10^{3429} \pm 1$	3 439	Dubner	1993.
$1\,706\,595 \cdot 2^{11235} \pm 1$	3 389	Amdahl Six	1989.
$1\,706\,459 \cdot 2^{8529} \pm 1$	2 571	Dubner	1993.
$1\,171\,452\,282 \cdot 10^{2490} \pm 1$	2 500	Dubner	1991.
$571\,305 \cdot 2^{7701} \pm 1$	2 324	Amdahl Six	1989.

2.4. Neke napomene o prim brojevima

Ideja o prim blizancima može se poopćiti na prim trojke, prim četvorke i mnogo općenitije na prim k–torke. Tony Forbes posjeduje popis rekordno velikih prim k–torki.

Svi problemi koje smo ovdje razmatrali spadaju u granu matematike koju zovemo teorija brojeva. Takvih problema ima još mnogo. Neke ćemo navesti kasnije. Osim riješenih i neriješenih ima i djelomično riješenih (nepotpuno riješenih). Općenito možemo neriješene probleme svrstati u dvije grupe. U jednoj grupi su problemi kod kojih je poznat način kojim se može doći do njihovog potpunog rješenja, a jedina teškoća je u tome što zasad nismo u stanju izvršiti, zbog njihove obimnosti, potrebne operacije, čak ni velikim računalima. Svi ostali neriješeni problemi pripadaju u drugu grupu. Neznamo čak ni način na koji bi se oni mogli riješiti.

Da bismo ispitali da li je neki prirodni broj n prim moramo ga dijeliti redom sa svim primbrojevima manjim od $\sqrt{n}$. Npr. ako želimo ustanoviti da li je broj 211 prim, trebamo ga dijeliti sa $2, 3, 5, 7, 11$ i 13. S idućim primbrojem 17 ne moramo broj 211 dijeliti jer je $17 > \sqrt{211}$.

Veliki ruski matematičar P. L. Čebišev (1821.–1894.) je dokazao: "Između prirodnih brojeva n i $2n$ postoji najmanje jedan primbroj". Npr. između 17 i 34 primbrojevi su 19, 23, 29 i 31.

Zanimljivo je da uprkos nepravilnoj raspodjeli primbrojeva unutar svih prirodnih brojeva, možemo napisati npr. 100 uzastopnih složenih brojeva. To su npr. brojevi $101!+2$, $101!+3$, ..., $101!+101$. Naime,

$$\begin{aligned} 101!+2 &\text{ djeljiv je sa } 2 \\ 101!+3 &\text{ djeljiv je sa } 3 \\ &\ldots\ldots\ldots\ldots \\ 101!+100 &\text{ djeljiv je sa } 100 \\ 101!+101 &\text{ djeljiv je sa } 101 \end{aligned}$$

Prema tome svi su uzastopni prirodni brojevi od $101!+2$ do $101!+101$ složeni, a ima ih 100, što smo željeli pokazati. Analogno možemo dobiti i 1 000 uzastopnih složenih prirodnih brojeva, dakle i po volji (ali konačno mnogo) uzastopnih složenih prirodnih brojeva.

2.5. Zakon raspodjele primbrojeva

Stoljećima su se matematičari zanimali za raspodjelu (distribuciju) skupa primbrojeva unutar skupa svih prirodnih brojeva. Tek su 1896. godine J. Hadamard (1865.–1963.) i C. J. de laVallee Poussin (1866.–1962.) nezavisno jedan od drugoga dokazali zakon raspodjele primbrojeva.

Neka je x prirodan broj, a broj $\pi(x)$ neka je broj svih primbrojeva manjih ili jednakih x. Npr. $\pi(20)=8$, jer ima 8 primbrojeva manjih od 20. To su $2,3,5,7,11,13,17,19$. Tok funkcije $\pi(x)$ je vrlo nepravilan i nezakonit, jer su primbrojevi nepravilno posijani među prirodnim brojevima. Ima, naime, primbrojeva koji se minimalno razlikuju, a ima ih koji su daleko jedan od drugog. Npr. prosti brojevi 2 309 i 2 311 razlikuju se jedan od drugog za 2, a između primbrojeva 370 261 i 370 373 nalaze se samo složeni brojevi. Ali za vrlo velike prirodne brojeve x vrijedi da je produkt $\pi(x)$ i $\ln x$ približno jednak x ili preciznije

$$\lim_{x\to\infty} \frac{\pi(x)\ln x}{x} = 1. \tag{14}$$

Tu je $\ln x$ prirodni logaritam od x i $\ln x \approx 2.30 \log x$. Granična vrijednost (14) iskazuje spomenuti zakon raspodjele primbrojeva.

Za ilustraciju tog zakona imamo i sljedeću tablicu:

x	$\pi(x)$	$\frac{x}{\ln x}$	$\frac{\pi(x)\ln x}{x}$
10^3	168	145	1.159
10^6	78 498	72 382	1.084
10^9	50 847 478	48 254 942	1.053

Zakon raspodjele primbrojeva iskazan relacijom (14) Hadamard i De laVallee Poussin izveli su na osnovu Riemannovih rezultata o zeta funkciji, pa ćemo nešto reći o vezi te zanimljive funkcije i primbrojeva.

Fenomen zeta funkcije privlačio je matematičare cijelo stoljeće. Ta je funkcija jedinstven primjer specijalne funkcije, koja je, iako definirana na približno jednostavan način, otkrivala svoja svojstva vrlo polako i povremeno, tek pod pritiskom najsnažnijih teorema o analitičkim funkcijama; još je interesantnije što je zeta funkcija do 1961. godine sačuvala svoju glavnu tajnu — distribuciju nula u kritičnoj pruzi, i izazvala duboke reperkusije na matematičko stvaranje u toku cijelog jednog vijeka (1859.–1959.).

To je paradoksalna crta u prirodi ove funkcije, koja joj u isto vrijeme daje veo neke tajanstvenosti.

Riemannova zeta funkcija $\zeta(s)$, gdje je $s = x + iy$ kompleksna varijabla, $(i = \sqrt{-1})$ definirana je za $s > 1$ Dirichletovim redom

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} = 1 + \frac{1}{2^s} + \frac{1}{3^s} + \dots . \tag{15}$$

Fundamentalna uloga primbrojeva u teoriji brojeva iskazana je tzv. osnovnim teoremom aritmetike:

Svaki prirodan broj veći od 1 može se jednoznačno prikazati kao produkt primbrojeva. Npr. $540 = 2^2 3^2 5$. Aritmetički ekvivalent osnovnog teorema aritmetike čuveni je Eulerov identitet.

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_{p} \left(1 - \frac{1}{p^s}\right)^{-1} \tag{16}$$

Desna strana je beskonačni produkt

$$\left(1 - \frac{1}{2^s}\right)^{-1} \left(1 - \frac{1}{3^s}\right)^{-1} \left(1 - \frac{1}{5^s}\right)^{-1} \dots ,$$

a nazivnici su primbrojevi $2, 3, 5, \dots$. Varijabla $s = x + iy$, $x > 1$. Identitet (16) ukazuje na vezu zeta funkcije i prostih brojeva.

Onog trenutka kad je Euler postavio taj identitet, zeta funkcija počela je igrati fundamentalnu ulogu u teoriji prostih brojeva. Pokušaji da se ta teorija oslobodi sudbinske veze sa zeta funkcijom neznatno su uspjeli.

Potpuno i strogo rješenje teškog problema koji smo nazvali zakon raspodjele primbrojeva čekalo je na teoriju zeta funkcije koju je Riemann (1826.–1866.) prvi shvatio kao funkciju kompleksne varijable. U Riemannovim novim idejama da problematiku teorije brojeva ispituje analitičkim sredstvima, ležao je ključ za rješenje predhodnog teorema.

Poslije dokaza zakona o ditribuciji primbrojeva, definitivno se smatralo da se on ne može dokazati elementarno, tj. bez upotrebe zeta funkcije i teorije kompleksnih funkcija. Zato je Selbergov i Erdösev elementarni dokaz 1949. izazvao senzaciju. Upotreba zeta funkcije u teoriji brojeva uvela je u ovu sredstva matematičke analize. Iz takvog spajanja rodila se nova metoda u teoriji brojeva — analitička metoda. Zakon raspodjele naslućivali su već Gauss (1777.–1855.), Legendre (1752.–1833.), Riemann (1826.–1866.), Dirichlet (1805.–1859.) i Čebišev (1821.–1894.).

Iz relacije (14) slijedi da su "skoro svi" prirodni brojevi složeni. Do tog zaključka došao je već Euler kad je naveo poučak da

$$\frac{\pi(x)}{x} \to 0, \quad (x \to \infty).$$

U 16. vijeku Cataldi je napisao tablicu primbrojeva manjih od 750. U Fermatovo vrijeme ta je tablica bila najveća poznata (1640.). U Eulerovo vrijeme (1738.) to je bila Branckerova (do 100.000). U Legendrovo doba (1798.) to je bila Felkerova, do 408 000.

Raspodjela primbrojeva je vrlo nepravilna. Lehmer primjećuje da nema primbrojeva između 20 831 323 i 20 831 533 u razmaku od 210. U drugu ruku, Kraitchik ističe da su prirodni brojevi $1\,000\,000\,000\,060 \pm 1$ oba prim (prim blizanci). Jednostavna formula $\pi(n)$ niti je poznata, niti se može očekivati.

Nije poznat laki dokaz relacije (14). Prošao je čitav vijek od slutnje do samog dokaza — to je mjerilo teškoće tog dokaza. Teorem prvenstveno spada u analizu. Teorija brojeva igra u dokazu samo malu ulogu. Zbog limesa jasno je da neki sadržaji analize moraju ulaziti u dokazivanje teorema (14), ali udio analize je neočekivan (iznenađujući).

Teorem (14) može se dati u više oblika zamjenom $\frac{n}{\ln n}$ funkcije bilo kojom funkcijom koja je asimptotska s njom npr.

Poučak 2.

$$\pi(n) \approx \frac{n}{\ln n - 1}.$$

Poučak 3.

$$\pi(n) \approx \int_2^n \frac{dx}{\ln n}.$$

Te tri verzije su jednako istinite.

Pitanje. Koja je funkcije zdesna najbolja aproksimacija ?

P. Čebišev je 1848. dao teoreme 2. i 3. bez dokaza. C. F. Gauss piše J. F. Enckeu 1849. da je on (Gauss) otkrio teorem 3. u dobi od 16 godina 1793. Dalje Gauss kaže:"Kad je 1811. bila objavljena tablica primbrojeva do 1 020 000, ja sam bio oduševljen primbrojilac."

Sad ćemo navesti neke tablice najvećih primbrojeva, a kasnije ćemo se još zabaviti s primbrojevima, posebno sa Mersenneovim primbrojevima.

2.6. Jedanaest najvećih primbrojeva

13. studenog 1996. tim Joela Armengauda, Georgea Woltmana i dr. otkrio je novi rekordni primbroj $2^{1398269} - 1$.

To je tzv. 35–i poznati Mersennev primbroj (mogu postojati manji ukoliko svi prijašnji manji eksponenti nisu provjereni).

Armengaud je otkrio ovaj primbroj koristeći program koji je napisao Woltman. Armengaud je jedan od nekoliko stotina pojedinaca uključenih u GIMPS-u (Great Internet Mersenne Prime Search — Veliko istraživanje Mersenneovih primbrojeva putem Interneta) koje je pokrenuo Woltman početkom 1996. godine. GIMPS nudi kompletnu programsku podršku kao i izvorni kod programa za vlasnike osobnih računala koji žele istraživati velike primbrojeve jednako kao i bazu podataka za osiguranje ranga provjera.

David Slowinski je provjerio primalitet gornjeg broja. On je našao većinu ranijih rekordnih primbrojeva. Cjelokupni decimalni zapis ovog broja od 420 921 znamenaka dostupan je i u obliku teksta i u sažetom obliku (zip datoteka).

Popis 11 najvećih primbrojeva (do 1996.)

Prim	Broj znamenaka	Otkrili	Kada
$2^{1398269}-1$	420 921	Armegand, Woltman i dr.	1996.
$2^{1257787}-1$	378 632	Slowinski i Gage	1996.
$2^{859433}-1$	258 716	Slowinski i Gage	1994.
$2^{756839}-1$	227 832	Slowinski i Gage	1992.
$397\,581\cdot 2^{216193}-1$	65 087	Amdahl Six	1989.
$2^{216091}-1$	65 050	Slowinski	1985.
$3\cdot 2^{157169}-1$	47 314	Jeffrey Young	1995.
$9\cdot 2^{149143}+1$	44 898	Jeffrey Young	1995.
$9\cdot 2^{147073}+1$	44 275	Jeffrey Young	1995.
$9\cdot 2^{145247}+1$	43 725	Jeffrey Young	1995.
$2^{132049}-1$	39 751	Slowinski	1983.

2.7. Deset najvećih poznatih faktorijela i primorial primbrojeva (do 1993)

Definicija: Označimo sa $n\#$ produkt svih primbrojeva koji su manji ili jednaki od prirodnog broja n. Npr. $5\# = 2\cdot 3\cdot 5 = 30$. Ako su brojevi oblika $n\#+1$ ili $n\#-1$ prim, nazvat ćemo ih *primorial prim*. Evo spomenute tablice:

Prim	Broj znamenaka	Otkrili	Kada
$3610!-1$	11 277	Caldwell	1993.
$3507!-1$	10 912	Caldwell	1993.
$24029\#+1$	10 387	Caldwell	1993.
$23801\#+1$	10 273	Caldwell	1993.
$18523\#+1$	8 002	Dubner	1989.
$15877\#-1$	6 845	Caldwell i Dubner	1992.
$13649\#+1$	5 862	Dubner	1987.
$1963!-1$	5 614	Caldwell i Dubner	1992.
$13033\#-1$	5 610	Caldwell i Dubner	1992.
$11549\#+1$	4 951	Dubner	1986.
$1477!+1$	4 042	Dubner	1984.

2.8. Deset najvećih poznatih primbrojeva Sophie Germain (do 1995.)

To su neparni primbrojevi p za koji je $2p + 1$ također prim. Tako su nazvani po matematičarki Sophie Germain, kad je ona dokazala prvi slučaj Fermatovog posljednjeg teorema ($x^n + y^n = z^n$ nema rješenje za $n > 2$; teorem je sada potpuno dokazan) za eksponente djeljive sa takvim primbrojevima. Evo spomenutog popisa:

Prim	Broj znamenaka	Otkrili	Kada
$8\,069\,496\,435 \cdot 10^{5072} - 1$	5 082	Dubner	1995.
$470\,943\,129 \cdot 2^{16352} - 1$	4 932	Indlekofer i Ja'rai	1995.
$157\,324\,389 \cdot 2^{16352} - 1$	4 931	Indlekofer i Ja'rai	1995.
$5\,415\,312\,903 \cdot 10^{4526} - 1$	4 536	Dubner	1994.
$1\,468\,358\,892 \cdot 10^{4003} - 1$	4 013	Dubner	1994.
$15\,614\,233\,635 \cdot 10^{3529} - 1$	3 540	Dubner	1994.
$47\,013\,511\,545 \cdot 10^{2999} - 1$	3 010	Dubner	1993.
$1\,746\,052\,308 \cdot 10^{2581} - 1$	2 591	Dubner	1993.
$21\,063\,042 \cdot 10^{2110} - 1$	2 118	Dubner	1993.
$2\,926\,924 \cdot 10^{2032} + 1$	2 039	Dubner	1992.