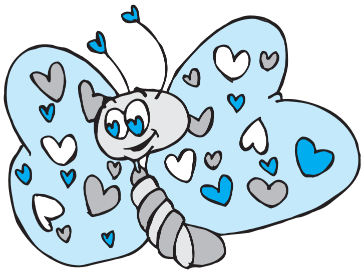
Top ten



Najveći prosti brojevi

Postoji li najveći prosti broj? Ne postoji! Tu je činjenicu još davno dokazao Euklid. Dokaz je danas dostupan svakom nadarenijem petnaestogodišnjaku i ponekad se može naći i u gimnazijskim udžbenicima.

Određivanje što većeg prostog broja desetljećima zaokuplja matematičare, ali i ne samo njih. Jer nema zapravo lakog puta kojim bi se provjerilo je li neki dovoljno velik broj prost ili ne. Nekad je taj posao svakako bio teži nego što je to danas kad postoje moćna elektronička računala.

Koji je najveći poznati prosti broj?

Od 14. studenog 2001. rekord pripada mladom studentu iz Ontarija Michaelu Cameronu. On je dokazao da je broj $2^{13\,466\,917}-1$ prost. Michaelovom osobnom računalu (800 MHz AMD T-Bird) za pronalazak rekorda bila su potrebna 42 dana. Broj ima 4 053 946 znamenki te bi njegov ispis zahtijevao više od 2000 stranica. Duljina toga broja ispisanog u niz bila bi veća od 10 kilometara. Da bi se taj broj pročitao naglas, trebalo bi ga čitati gotovo pola godine, čitajući dnevno osam sati. Da je nađeni broj uistinu prost, provjerio je Paul Victor na Compaq Alpha računalu (667 MHz) a provjera je trajala tri tjedna.

Samo nekoliko mjeseci prije negoli je našao rekordni broj, Michael se, kao jedan od 120 000 individualaca, uključio u svjetski projekt poznat pod nazivom GIMPS (Great Internet Mersenne Prime Search). Kad je 1998. svoj rekord postavio 19-godišnji Ronald Clarkson, u isti je projekt bilo uključeno manje od 5 000 volontera. GIMPS je 1996. godine pokrenuo George Woltman, programer iz Orlanda u Sjedinjenim Američkim Državama. On je napisao i prve programe te je vlasnicima osobnih računala pružio potpuno slobodan pristup svojem softwareu za traženje velikih prostih brojeva. Zanimljivo je da mnogi nastavnici u SAD koriste GIMPS kako bi svoje učenike motivirali za učenje matematike.

Trenutno rekordni broj koji je pronašao Michael Cameron jest *Mersenneov broj*. **Mersenneovi brojevi** su prosti brojevi oblika $2^p - 1$. O njima smo objavili kraći zapis u MŠ-u broj 11, str. 38.

Najveći "obični" prosti broj je broj

$$10^{5\,019} + 3^2 \cdot 7^5 \cdot 11^{11},$$

ima 5 020 znamenki a pronađen je u rujnu 2001. godine. Paul Underwood, David Broadhurst, Bouk de Water i Paul Leyland tvrde (bilo je to 30. rujna 2002.) da su dokazali kako je broj $2^{64\,695} - 32\,769$ (ima 19 476 znamenki) prost, ali formalno još to nisu objavili.

Matematičari i dalje tragaju za novim rekordima. Oni to rade i uz neke druge zadatke vezane uz proste brojeve.

Jedan od njih je odrediti najveći par blizanaca. **Blizancima** zovemo dva prosta broja čija je razlika jednaka 2. To su dakle prosti brojevi p i $p+2$. Pretpostavlja se, ali je još pod upitnikom, da postoji beskonačno mnogo prostih blizanaca.

Najveći poznati par prostih blizanaca za sada je $33\,218\,925 \cdot 2^{169\,690} \pm 1$ (51 090 znamenki) a pronašli su ga 2002. godine Papp i Gallot.

Sofie Germain prost broj[1] je neparan prost broj za koji je i broj $2p+1$ također prost. Najveći do danas poznati takav broj je $1\,213\,822\,389 \cdot 2^{81\,131} - 1$ i ima 24 432 znamenke. Rekord pripada Michaelu Angelu, Dirku Augustinu i Paulu Joblingu, a potječe iz kolovoza 2002.

Na našoj "duplerici" naći ćete TOP TEN listu rekorda za proste brojeve. Želite li doznati još i više o ovakvim rekordima, posjetite internet stranice na adresi `http://www.utm.edu/research/primes/largest.html`

POSTOJI NEIZMJERNO MNOGO PRIMBROJEVA

Pretpostavimo naprotiv da ih ima samo konačan broj, naime, $p_1, p_2, \ldots, p_r$. *Promatrajmo broj*

$$n = p_1 p_2 \ldots p_r + 1.$$

Taj broj je očito veći od svih tih primbrojeva, a nije djeljiv ni s kojim od njih jer dioba uvijek daje ostatak 1. Ako je n primbroj, on je veći, dakle različit od $p_1, p_2, \ldots, p_r$, *tj. to nisu svi primbrojevi. Ako je n složen broj, onda prema T1*[2] *postoji rastav u primfaktore. No ti primfaktori ne mogu biti* $p_1, p_2, \ldots, p_r$ *jer s njima n nije djeljiv. Ima dakle još drugih primbrojeva. Došli smo u proturječje s pretpostavkom i teorem je dokazan.*

Ovaj dokaz potječe još od Euklida.

D. Blanuša, *Viša matematika, I. dio, prvi svezak*, Tehnička knjiga, Zagreb, 1963.

[1] Sofie Germain (1776. – 1831.), francuska matematičarka
[2] Svaki se složeni broj može prikazati kao produkt primbrojeva.