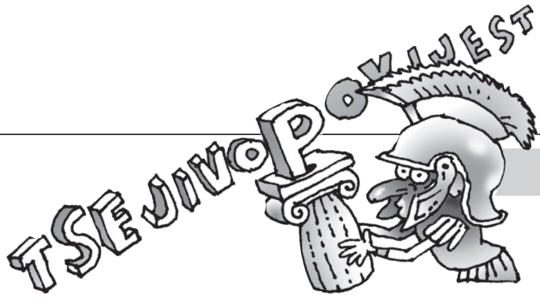
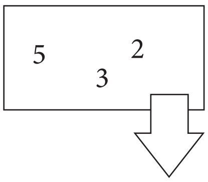


Matea Gusić, Varaždin

ZAKON PROSTIH BROJEVA

Što li su to brojevi morali napraviti da ih matematičari počaste „prostim” nazivom? Prošećemo li se kroz povijest matematike, lako ćemo uočiti da su prosti brojevi zaslužni za izluđivanje mnogih ljudi, ne samo matematičara. Bez obzira na to, naziv nisu dobili radi nepristojnosti, nego radi jednostavnosti. Naime, prosti su brojevi prirodni brojevi veći od jedan koji, osim sebe i jedinice, nemaju drugih prirodnih djelitelja. Ako ne želimo miješati dijeljenje u ovu brojevnu priču, reći ćemo da su to prirodni brojevi veći od jedan koji se ne mogu zapisati kao umnožak manjih prirodnih brojeva. Tako, primjerice, broj 6 nije prost jer ga možemo zapisati kao umnožak brojeva 2 i 3, a njegov sljedbenik 7 jest prosti broj. Njihova važnost nije u skladu s jednostavnim nazivom koji nose, naime, prosti su brojevi glavna tema Osnovnog teorema aritmetike, koji je baza „kraljice matematike”, kako ju je od milja zvao veliki Carl Friedrich Gauss, „teorije brojeva”. Teorem, koji kaže da se svaki prirodan broj veći od jedan može na jedinstveni način zapisati kao umnožak prostih brojeva, još je 300 godina prije Krista poznavao Euklid koji ga je zapisao u svojim „Elementima”.

Već su stari Grci uočili da određivanje prostih brojeva neće biti jednostavan posao. Odličnu metodu smislio je Euklidov vršnjak, grčki matematičar Eratosten. Algoritam je jednostavan: zapišemo redom prirodne brojeve veće od 1 (primjerice prvih 100), zaokružimo prvi prosti broj, dvojku (jer je djeljiva samo sa sobom i jedinicom), zatim křižamo redom sve višekratnike broja 2, zatim zaokružimo drugi prosti broj 3 i križamo sve njegove višekratnike. Postupak nastavljamo dok nam svi zapisani brojevi nisu ili zaokruženi ili prekriženi. Algoritam podsjeća na sito koje propušta kroz sebe sve osim prostih brojeva, pa se naziva *Eratostenovim sitom*. Euklid nije imao sito nego stroj. On je zamislio da ima stroj koji „hrani” prostim brojevima, a stroj mu vraća nove na način da ih redom množi, te dobivenom umnošku pribroji 1.



$2 \cdot 3 \cdot 5 + 1 – 31$

Euklidov stroj u kojem se nalaze tri prosta broja (2, 3, 5) i iz kojeg izlazi novi prosti broj 31.

Kao što je već napisano, brojni su se matematičari zapleli u mrežu prostih brojeva. Dok su se jedni zaludili traženjem idućeg u nizu prostih brojeva, drugi su se spotakli o brojna svojstva koja im pripadaju. Spomenut ćemo dva velika imena, po jedno iz svake kategorije.

Prije četiri stoljeća francuski svećenik Marin Mersenne proučavao je posebnu vrstu prostih brojeva koje danas upravo po njemu nazivamo Mersenneovim brojevima. Radi se o prostim brojevima koje dobijemo tako da množimo

Matka 96.indd 254 2.5.2016. 21:47:19

broj 2 sam sa sobom više puta, a zatim oduzmemo jedinicu. Tako su, primjerice, 7 (= 2 · 2 · 2 – 1) i 31 (= 2 · 2 · 2 · 2 · 2 – 1) primjeri Mersenneovih brojeva. Potraga za Mersenneovim brojevima još je aktualna. Posljednji takav broj pronađen je početkom ove, 2016. godine, a zapis mu sadrži 22 338 618 znamenaka.

Ime Christiana Goldbacha bit će zauvijek povezano s prostim brojevima. Naime, prije tri stoljeća ovaj je diplomat s posebnim interesom za matematiku izrekao sudbonosnu slutnju: *Je li ili nije istina da svaki paran broj veći od 3 može biti zapisan kao zbroj dvaju prostih brojeva?* Slutnja je uz pomoć računala provjerena i za velike parne brojeve, štoviše, pokazano je da zbroj ne mora biti jedinstven. Tako parni broj 30 možemo zapisati kao zbroj prostih brojeva 11 i 19, ali i kao zbroj prostih brojeva 7 i 23. Nažalost, koliko god „daleko" provjeravali, uvijek postoji mnoštvo još većih parnih brojeva, među kojima se možda može naći neki za koji slutnja neće vrijediti. Matematičari i matematički fanatici stoljećima pokušavaju dokazati ovu slutnju za čije je matematički ispravno rješenje ponuđena novčana nagrada. Činjenica da to do današnjeg dana nikome nije pošlo za rukom lansiralo je ovu slutnju u društvo najpoznatijih i najstarijih neriješenih matematičkih problema[1].

Za kraj ću vam postaviti pitanje. Jeste li primijetili kako su prosti brojevi iz svoga kruga izbacili jedinicu? Jeste li se pitali zašto 1 nije prosti broj? Zar za nju ne vrijedi da je djeljiva samo sa sobom? Nije to uvijek bilo tako. Naime, Grci su jedinicu zanemarili jer je navodno nisu smatrali brojem. Za vrijeme srednjega vijeka i renesanse, matematičari su odlučili dopustiti jedinici da se pridruži društvu prostih brojeva. Početkom 20. stoljeća ipak je odlučeno da jedinica mora istupiti iz toga skupa. Jedan od razloga svakako je taj što s jedinicom kao prostim brojem jedinstvenost u tzv. osnovnom teoremu aritmetike ne bi vrijedila. Primjerice: prirodan broj 14 mogao bi se zapisati kao umnožak prostih brojeva 2 i 7, ali također i kao umnožak brojeva 1, 2 i 7. Niti Eratostenovo sito ne bi funkcioniralo jer bismo nakon zaokruživanja jedinice prekrižili sve njezine višekratnike, odnosno sve ostale prirodne brojeve. Također, prosti brojevi imaju točno dva djelitelja, jedinicu i samog sebe. Jedinica bi se, sa samo jednim djeliteljem, i po tome razlikovala od ostatka prostih brojeva. Radi očuvanja mira među svojstvima prostih brojeva jedinica je morala odstupiti.

[1]Goldbachova slutnja i pompa vezana uz njezino (ne)dokazivanje tema je matematičkog trilera „Stric Petros i Goldbachova slutnja" Apostolosa Doxiadisa.