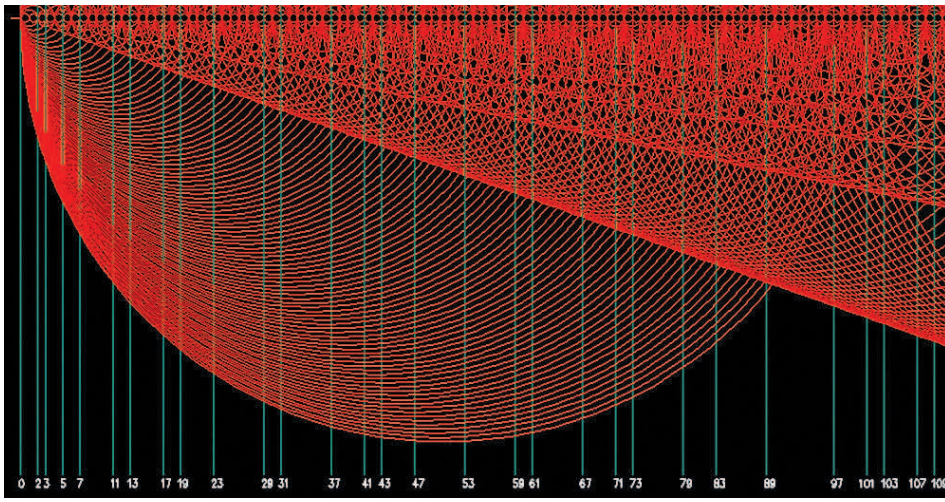
Prosti brojevi

Davor Klobučar, Osijek



Matematičari su do današnjeg dana uzalud pokušavali otkriti neki red u slijedu prostih brojeva, i imamo razloga vjerovati da je to misterij u koji ljudski um nikada neće prodrijeti.
(Leonhard Euler)

Uvod. Proste brojeve susreću učenici već u osnovnoj školi, ali njima se bave i srednjoškolci i studenti. Pa i matematičari znanstvenici ponekad s ovim brojevima imaju posla. Postoje, naime, brojne pretpostavke o svojstvima prostih brojeva koje još uvijek nisu dokazane. Čak i na ono trivijalno pitanje: "Je li zadani broj n prost ili nije?" često nemamo odgovora bez pomoći računala, a ponekad ni s njima.

Definicija. *Prost broj* (ili *prim-broj*) je takav broj koji ne možemo ni s čime zanimljivim podijeliti, odnosno nikako rastaviti na umnožak dvaju prirodnih brojeva, osim na prilično nezanimljiv umnožak jedinice i njega samoga. Prosti brojevi su redom: $2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41,$ itd.

Prirodne brojeve koji nisu prosti zovemo *složeni brojevi*. Svi prosti brojevi su neparni, osim broja 2. Slično bismo mogli reći i da nisu djeljivi s 3, osim samog broja 3, niti su djeljivi s 5, osim samog broja 5. Broj 1 ne sudjeluje u ovoj priči. On nije ni prost, ni složen.

Faktorizacija. Prosti se brojevi pojavljuju u faktorizaciji prirodnih brojeva (u njihovu rastavljanju na proste faktore). Složeni broj n može se prikazati kao produkt drugih dvaju prirodnih brojeva (koji nisu 1 ili n). Jasno je da su oba ta broja manja od n. Ovi pak, ako su i sami složeni, mogu se dalje rastavljati na još manje brojeve i tako sve dok ne dođemo do kraja, kad su svi faktori prosti. Ako se neki faktor pojavljuje više puta, onda ga u ispisu rezultata prikažemo toliko puta. A može i samo jednom, ali s odgovarajućim eksponentom.

Npr. $30 = 2 \cdot 3 \cdot 5$, $16 = 2^4$, $71 = 71$ (jer je prost), $6936 = 2^3 \cdot 3 \cdot 17^2$.

Ova intuitivno jasna stvar spada u *osnovni teorem aritmetike*, koji još tvrdi i da je ova faktorizacija jedinstvena ako se zanemari poredak tih istih faktora.

Koliko ih ima? Tisućama godina ljudi su si postavljali bezbrojna pitanja i zadatke u vezi s prostim brojevima. Teško je zamisliti područje matematike gdje su pitanja tako kratka i svakome razumljiva, a

odgovori često toliko teški da ih ni do danas nismo pronašli!

Možda najstarije pitanje glasi: ima li prostih brojeva beskonačno mnogo? Ili postoji jedan koji je najveći, a više nijedan broj nakon njega nije prost? Na ovo pitanje odgovor je poznat, a dao ga je već grčki matematičar Euklid oko 300. godine pr. Kr.

Odgovor je da prostih brojeva ima beskonačno mnogo. Euklid je pošao od pretpostavke da ih ima konačan broj. Pa kad ih je konačno mnogo, onda možemo zamisliti da smo ih sve pomnožili i dobili neki vrlo velik broj P. Tom broju možemo dodati 1, dakle dobivamo broj $Q = P + 1$. Budući da Q ne spada u tih "konačno mnogo" prostih brojeva, onda on nije prost. Stoga se on može podijeliti s nekim od prostih brojeva. Ali s druge strane moramo priznati da Q nije djeljiv ni s jednim od "konačno mnogo" prostih brojeva jer je tako definiran da uvijek daje ostatak 1. A ako nije djeljiv ni s čime, onda je on po definiciji ipak prost. Dolazimo do kontradikcije – da mora biti prost, a nije. Stoga je polazna pretpostavka bila kriva. Prostih je brojeva beskonačno mnogo.

Potraga za najvećim. Koji je najveći poznati prosti broj?

Prema internetskoj enciklopediji Wikipediji sredinom 2013. godine bio je to broj $2^{57\,885\,161} - 1$. On ima $17\,425\,170$ znamenaka, a otkrila ga je 25. siječnja 2013. grupa dobrovoljaca koji su odrađivali posao po dijelovima na većem broju računala. Kako je nastala ta grupa? Američki informatičar George Woltman je 1996. pokrenuo projekt GIMPS za pronalaženje prostih brojeva među Mersennovim brojevima i napisao softver za tu svrhu. (Mersennovi brojevi su svi brojevi oblika $2^n - 1$ i neki su od njih prosti.) Samo u prvoj godini u taj se projekt uključilo preko 1000 ljudi. Tijekom prvih 16 godina otkrili su 14 Mersennovih prostih brojeva, od kojih su 11 bili u trenutku otkrića rekorderi među prostim brojevima uopće.

U svojoj knjizi *Matematika naša svagdašnja* (Element, 2012.) naveo sam kako je GIMPS otkrio Mersennov broj s $12\,978\,189$ znamenaka, no taj je podatak sada zastario. Ali taj prethodni broj spominjem jer su njegovi otkrivači za njega dobili nagradu od 100 000 dolara! Naime, američka nevladina organizacija Electronic Frontier Foundation (EFF), koja se bavi zaštitom prava i sloboda na internetu, ponudila je tu nagradu onome tko pronađe prost broj s barem 10 milijuna znamenaka. (Prije toga je EFF raspisao i nagradu za prost broj s milijun znamenaka u iznosu od 50 000 dolara, a i tu je nagradu osvojila ista grupa GIMPS godine 1999.) Nove nagrade za 100 milijuna i za milijardu znamenaka još uvijek čekaju na dobitnika. Iznosi su 150 000 i 200 000 dolara. Možda da pokušate?

Što reći o veličini tog "rekordera" iz 2013.? U slučaju da stranica teksta ima 40 redaka sa 70 znamenaka u retku, za ispisivanje tog broja trebala bi knjiga od $6\,223$ stranice. Svaki komentar je suvišan.

Bezobrazni susjedi. Mogu li dva susjedna broja biti prosta? Uočimo da je jedan od njih uvijek paran, dakle djeljiv s 2. Jedini paran prost broj je 2. Zato su "prosti susjedi" samo 2 i 3.

Ali dva susjedna neparna broja već mogu biti prosta, npr. 11 i 13, 29 i 31, 71 i 73. Nije, međutim, ni dandanas poznato ima li takvih "blizanaca" beskonačno mnogo ili nema. Usput rečeno, među brojevima manjim od milijarde ima takvih parova $3\,424\,506$.

A mogu li čak *tri* uzastopna neparna broja biti prosti? Ne mogu jer bi uvijek jedan od njih bio djeljiv s 3. Provjerimo! Ako već prvi broj n nije djeljiv s 3, onda on daje ostatak 1 ili 2. Ako je ostatak 1, tada bi sljedeći neparni $(n+2)$ imao ostatak $1+2 = 3$, dakle 0, pa je djeljiv s 3. Ako je ostatak od n bio 2, tada treći neparni broj $(n + 4)$ ima ostatak $2 + 4 = 6$, dakle djeljiv je s 3. U svakom slučaju točno je jedan broj djeljiv s 3, pa nisu svi prosti.

Divno razmišljanje, ali prebrzo! Ipak smo previdjeli jednu sitnicu: postoji broj koji je djeljiv s 3, a svejedno je prost! To je sam broj 3. A njegova dva neparna sljedbenika su 5 i 7, koji su, kao za inat, također prosti! Ali $(3,\ 5,\ 7)$ je jedini takav slučaj. Ako ste pomislili na $(1,\ 3,\ 5)$, pogriješili ste jer 1 nije prost!

Fino društvo. Drugo je zanimljivo pitanje postoji li takvih 100 uzastopnih brojeva da su među njima svi složeni, a nijedan prost?

Postoji, a evo i primjera. Uzmimo $n = 101!$ (tj. produkt prvih 101 prirodnih brojeva). Takav n djeljiv je s 2, 3, 4, 5,... pa sve do 101.

Niz $n+2$, $n+3$, $n+4$, $n+5$ itd. sve do $n+100$, $n+101$ jest stotina uzastopnih brojeva koji su svi redom složeni brojevi! Kako to? Jednostavno. Npr., $n+2$ djeljiv je s 2 jer su oba člana sume djeljiva s 2. Na isti je način i $n+3$ djeljiv s 3, $n+4$ s 4, $n+5$ s 5 i na koncu $n+101$ s 101. Jednakom logikom dokazuje se i da je moguće naći 200 ili 500 ili bilo koliko uzastopnih prirodnih brojeva koji su svi složeni.

Generator prostih brojeva. Ljudi su se odavno pitali ima li nekakva formula u koju bi se uvrštavao proizvoljan prirodan broj, a da dobiveni rezultat uvijek bude prost. Na taj bi se način mogao generirati proizvoljno velik prost broj. Ali za sve jednostavne formule brzo se našao kontraprimjer, tj. prirodan broj za koji je rezultat složen. A neke su složenije formule još nerazjašnjene jer je njihovo izračunavanje previše teško. Danas ne poznamo nijednu pouzdanu formulu za generiranje prostih brojeva koja bi se pritom mogla koliko-toliko lako izračunavati. Pogledajmo neke primjere poznate iz povijesti:

Svi plus jedan. Iz dokaza da je prostih brojeva beskonačno mnogo moglo bi se naslutiti da je produkt prvih n prostih brojeva uvećan za jedan uvijek prost. I zaista, početak je bio obećavajuć. Za $n = 1$ imamo samo jedan prost broj, onaj prvi, a to je 2. Dodajemo mu 1 i dobijemo prosti broj 3. Za $n = 2$ imamo $2 \cdot 3 + 1 = 7$, a on je prost. Za $n = 3$ imamo $2 \cdot 3 \cdot 5 + 1 = 31$, također prost, kao i za $n = 4$, kada dobivamo $2 \cdot 3 \cdot 5 \cdot 7 + 1 = 211$. Rezultat je prost i za $n = 5$ kada imamo $2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 = 2\,311$. I baš kad smo pomislili da nam dobro ide, dolazi $n = 6$ i rezultat $30\,031$ koji je produkt $59 \cdot 509$, pa ova formula nije ono što smo htjeli.

Fermatovi brojevi. Pierre de Fermat (oko 1601.–1665.) bio je francuski matematičar. Po njemu su dobili ime tzv. Fermatovi brojevi koje označujemo i definiramo ovako: $F(n) = 2^{2^n} + 1$, gdje je n prirodan broj. On je naslutio da su svi oni prosti brojevi, jer su prosti $F(1) = 2^2 + 1 = 5$, $F(2) = 2^4 + 1 = 17$, $F(3) = 2^8 + 1 = 257$ i $F(4) = 65\,537$. Ali već sljedeći broj $F(5) = 4\,294\,967\,297$ tako je velik da je Fermat morao odustati od traženja njegovih djelitelja (faktora). Stoljeće poslije Euler je otkrio da je $F(5)$ djeljiv sa 641. (Ta se djeljivost može pokazati i direktnim računom jer $F(5)$ nije tako velik broj, ali za vježbu bi se to moglo dokazati i pomoću osnovnih svojstava kongruencija.)

A što se tiče sljedećih Fermatovih brojeva, do godine 2010. poznato je da su složeni svi od $F(5)$ do $F(32)$, pri čemu za neke znamo kompletan rastav na proste faktore, a za neke samo djelomično. Za $F(20)$ i $F(24)$ znamo čisto teoretski da su složeni, ali ne znamo nijedan od njihovih faktora!

Eulerovih 40. Leonhard Euler (1707.–1783.) primijetio je zanimljiv niz:

$$P(n) = n^2 - n + 41\,.$$

Za sve prirodne brojeve $n < 41$ je $P(n)$ prost broj! Zaista, $P(1) = 41$, $P(2) = 43$, $P(3) = 47$, $P(4) = 53$, $P(5) = 61$ (preskočili smo prosti broj 59), $P(6) = 71$ itd. Ali $P(41) = 41^2$, što je djeljivo s 41. Dakle, vrlo jednostavna formula, običan polinom, i to samo drugog stupnja, a koji se "dobro držao" za čak prvih 40 prirodnih brojeva!

Polinom nije generator. Formula koja generira same proste brojeve nikako ne može biti jedan polinom, što se lako dokazuje. Pretpostavimo da imamo takav polinom $F(x)$. Onda bi bilo $F(1) = p$, gdje je p neki prost broj. Tada bi bilo $F(1 + p)$, $F(1 + 2p)$ i uopće bilo koji $F(1 + kp)$ djeljiv s p. Zašto? Zato jer je $F(x)$ polinom, pa uvrštavanjem $x = 1 + kp$ i dizanjem tog x na razne potencije opet dobijemo $F(1)$, ali sada uvećan za neku sumu potencija čiji svaki član sadrži p. Kako su oba dijela $F(1 + kp)$ djeljiva s p, onda je i $F(1 + kp)$ djeljiv s p. Ako je p bio prost, a tvrdimo da je $F(1 + kp)$ također prost i pri tome djeljiv s p, onda mora biti $F(1 + kp) = p$. Ali tim putem bismo za svaki prirodni k dobivali uvijek istu vrijednost p, pa bi onda polinom $F(x) - p$ imao beskonačno mnogo nul-točaka. To je nemoguće, osim ako je to nul-polinom, odnosno da je $F(x)$ konstanta, i to prosta. To je trivijalan slučaj koji nikoga ne zanima, i zato pravih polinoma koji generiraju proste brojeve nema.

Opasni brojevi! Znate li zašto je nezgodno ako bombona u vrećici ima prost broj? Zato što će

među djecom koja ih dobiju na dar redovito izbiti svađa. Naime, koliko god djece bilo u društvu, nikako ih neće moći pravedno podijeliti! Osim ako je djece jednako koliko i bombona...

Eratostenovo sito. Bilo bi nepravedno ovdje preskočiti grčkog matematičara i astronoma Eratostena (276. pr. Kr.–195. pr. Kr.) koji je uspio izračunati opseg zemaljske kugle, i to u vrijeme kad još mnogi nisu ni vjerovali da je Zemlja okrugla. On je smislio i postupak za sistematizirano dobivanje velike količine prostih brojeva koji zovemo *Eratostenovo sito*.

Postupak ide ovako. Zapišimo redom sve prirodne brojeve od 2 pa do nekog velikog broja, recimo do 1000. Uzmemo najmanji broj od njih, a to je 2, proglasimo ga prostim i zaokružimo. Nakon toga redom križamo njegove višekratnike, dakle 4, 6, 8, 10, 12 (i tako sve do 1000) jer oni ne mogu biti prosti. Postupak se ponavlja – sada gledamo najmanji slobodni broj na popisu (koji nije prekrižen niti zaokružen), a to je 3. Njega zaokružimo i proglasimo prostim, a križamo redom njegove višekratnike 6, 9, 12, 15, 18... sve do kraja. Ne smeta ako su neki već i prije bili prekriženi (npr. 6 i 12), a svakako ćemo zahvatiti i neke koji dotad nisu bili. S popisa očitamo novi prvi slobodni broj, a to je 5. I tako se postupak ponavlja dok god ima neoznačenih brojeva na popisu. Zaokruženi brojevi daju točan skup svih prostih brojeva do 1000, ili dokle smo već htjeli.

Gustoća prostih brojeva. Znamo da prostih brojeva ima beskonačno mnogo i da su raspoređeni vrlo neobično. Ipak postoji zanimljiv asimptotski zakon koji kaže da kad prirodni broj n raste u beskonačnost, onda je količina prostih brojeva koji su manji od n (oznaka $\pi(n)$) sve bliže i bliže vrijednosti $\frac{n}{\ln n}$. Uzmemo li proizvoljan broj između 1 i n, vjerojatnost da je on prost iznosi oko $\frac{1}{\ln n}$.

Pogledajmo na primjerima kako ova formula funkcionira! Za $n = 1000$ imamo 168 prostih brojeva, a formula ih predviđa 145, dakle 23 manje ili oko $13.7\ \%$ manje. Za $n = 1\,000\,000$ ih ima $78\,498$, a formula predviđa $72\,382$ ili $7.8\ \%$ manje. A za stvarno golem broj $n = 10^{24}$ je rezultat za $1.8\ \%$ manji od pravog. Vidimo da je ova asimptotska formula poput pravde u životu: spora, ali dostižna!

Formulu je 1793. godine naslutio petnaestogodišnji Carl Friedrich Gauss, budući matematički velikan, a isti onaj koji je kao desetogodišnjak zbunio svog učitelja hitrim zbrajanjem brojeva od 1 do 100. Nezavisno od njega je 1798. Adrien-Marie Legendre (le'žandr) došao do iste formule. U svom drugom izdanju "Théorie des nombres" iz 1808. dao je Legendre poboljšanu ocjenu $\pi(n) \approx \frac{n}{\ln n - 1.08366}$. Ona za $n = 1000$ predviđa 172 prosta broja, tj. samo 4 više ili $2.38\ \%$, a za $n = 1\,000\,000$ predviđa $78\,543$, tj. 45 ili $0.05\ \%$ više!

Dirichletov teorem o aritmetičkim nizovima. Ovaj teorem zove se ponekad i Dirichletov teorem o prostim brojevima. Ako imamo dva relativno prosta prirodna broja a i d, onda u aritmetičkom nizu a, $a + d$, $a + 2d$, $a + 3d$... postoji beskonačno mnogo prostih brojeva. Ne kaže se koji su to, niti ima li i složenih brojeva beskonačno mnogo. A i dokaz je prilično složen pa ga ne navodim. Sjetimo se kako je Euklid utvrdio da prostih brojeva i inače ima beskonačno mnogo. Ovaj teorem je "jači" jer beskonačno mnogo prostih brojeva pronalazi ne samo u čitavom skupu $\mathbf{N}$ (poput Euklida), nego i u njegovom podskupu koji ima oblik aritmetičkog niza! Pa makar taj niz bio i veoma rijedak, poput niza $a_n = 1 + 1\,000\,000 \cdot n$.

Legendreova hipoteza. Za svaki prirodni broj n postoji bar jedan prost broj između n^2 i $(n + 1)^2$. Ovo ni dandanas nije dokazano.

Goldbachova hipoteza. Svaki paran prirodan broj veći od 2 može se prikazati kao suma dvaju prostih brojeva. Npr. $4 = 2 + 2$, $6 = 3 + 3$, $8 =$

$5+3$, $10 = 7+3$, $12 = 7+5$, $14 = 11+3$ itd. Imamo čak i neke duplikate i triplikate: $20 = 13+7 = 17+3$, odnosno $30 = 7+23 = 11+19 = 13+17$. Ovu je pretpostavku postavio još njemački matematičar Christian Goldbach godine 1742. u pismu Euleru. Slavni Euler nije je mogao dokazati, a nedokazanom je ostala i do dandanas. Zahvaljujući računalima provjereni su svi parni brojevi do $1.609 \cdot 10^{18}$ (stanje u 2012.) i za njih je pretpostavka točna.

Ideja za rješavatelje: provjerite pretpostavku za brojeve do milijun, a usput nađite i koji se broj može prikazati kao takva suma na najviše različitih načina!

Postoji i "slabija" varijanta Goldbachove hipoteze: ona sluti da se svaki *neparni* broj veći od 5 može prikazati kao zbroj *triju* prostih brojeva. Nedavno je objavljen tekst koji navodno dokazuje ovu slabiju varijantu.

Dijeljenje "šakom i kapom". Kako odrediti je li neki zadani n prost?

Za početak, uvijek ga možemo pokušati podijeliti s nekoliko tipičnih brojeva. Dok je n malen broj, to može funkcionirati. Ali kako ustanoviti je li broj poput $n = 124\,567\,931$ prost ili nije? Djeljivost s 2, 3, 5, 7, 11 možemo isprobati, ali ovaj broj s njima nije djeljiv. Nema druge nego pokušavati s raznim brojevima dok ne nađemo čime se može podijeliti, ili dok ne iscrpimo sve moguće djelitelje. Samo, koji su to svi mogući djelitelji, tj. kada možemo s pokušajima dijeljenja prestati i broj proglasiti prostim?

Najprije treba provjeriti je li broj n djeljiv s 2. Kad smo ustanovili da nije, više ne moramo pokušavati dijeliti ga s ostalim parnim brojevima. Dakle, dijelit ćemo s 3, 5, 7... i ostalim neparnim brojevima, i to redom. Dijelimo li na papiru, možemo preskočiti dijeljenje s 9 (jer smo već pokušali s 3, pa nije išlo) ili dijeljenje s 35 (jer smo prije toga pokušali dijeliti s 5, pa čak i sa 7, ali nije išlo). Dakle, ne moramo dijeliti sa složenim brojevima jer smo sigurno prije toga već pokušali dijeliti s njihovim faktorima. Ali kad dijeljenje prepuštamo računalu, ono ne može "znati iz iskustva" da je neki potencijalni djelitelj složen broj. On mora probati dijeliti i s njim jer mu je to brže nego da ispituje još i njegovu složenost. Zato bismo računalu dali da dijeli najprije s parnim 2, a zatim redom s neparnima 3, 5, 7, 9, 11, 13 itd.

Glavno je pitanje kada s dijeljenjima treba stati. Obično ljudima najprije padne na pamet da trebaju potencijalni djelitelji rasti tako dugo dok ne dostignu broj n, a onda stati. Uistinu, svi mogući faktori od n moraju od njega biti manji. Ali to je jako neučinkovit kriterij zaustavljanja, jer za npr. prost broj blizu $10\,000$ treba provesti oko $5\,000$ dijeljenja! (Nije ih $10\,000$ jer gledamo samo neparne djelitelje.) Kad na ovo ukažete ljudima, sjete se da je dovoljno dijeliti do pola, tj. do $5\,000$ ($2\,500$ dijeljenja). Jer ako je broj veći od polovice n, s čime bismo ga uopće mogli množiti pa da rezultat bude n? Već ako ga množimo s 2, umnožak će premašiti n, a da i ne govorimo o množenju faktorom većim od 2.

Ovo se može i dalje usavršavati. Naime, označimo $x = \sqrt{n}$, pri čemu nije nužno da x bude prirodan broj. Znamo da je $n = x \cdot x$. Ako se n može prikazati još i kao umnožak neka druga dva faktora a i b, što možemo znati o njima? Jednostavno: ako je jedan od njih manji od x, onda drugi mora biti veći od x. Ili, ako je jedan veći, drugi mora biti manji. U svakom slučaju neki je od njih manji ili jednak broju $x = \sqrt{n}$. Dakle, dovoljno je dijeliti zadani n s 2 i zatim sa svim neparnim brojevima redom počevši od 3, pa sve dok nismo nadmašili $\sqrt{n}$. Ako nađemo da je n djeljiv s nečim, onda smjesta stanemo i broj proglasimo složenim. Ako nismo ništa našli, a nadmašili smo $\sqrt{n}$, stanemo i proglasimo n prostim.

Koliko ovo iznosi za brojeve blizu $10\,000$? Imamo $\sqrt{10\,000} = 100$, dakle oko 50 neparnih djelitelja, a ne 2500 ili čak 5000. Vidimo da smo dobrim promišljanjem ovog problema skratili vrijeme računanja mnogo puta!

Fermatov test. U prethodnom je odlomku opisana metoda pokušaja i pogrešaka za određivanje je li broj prost ili složen. Štoviše, ona kod složenih brojeva daje i jedan od njihovih faktora. Pritom brojevi veličine nekoliko milijardi nisu problem za današnja računala, čak ni za ona personalna. Ta riječ je o nekih $50\,000$ dijeljenja koja se izvedu u par sekundi. Buduća računala će biti još i brža, tako

da će vrijeme računanja biti prihvatljivo i za znatno veće brojeve.

Matematičare će ipak i dalje zanimati neki ekstremno veliki brojevi, bilo iz čisto teorijskih razloga, bilo iz nekih praktičnih (npr. kriptografija – šifriranje i dešifriranje tajnih poruka). Potrebne su stoga naprednije metode ispitivanja složenosti i eventualne faktorizacije zadanog broja. Na tom području već su postignuti zanimljivi rezultati pa ću ovdje prikazati ponešto od toga.

Poznat je francuski matematičar Pierre de Fermat iz 17. stoljeća, kao i čuveni *Veliki Fermatov teorem* ili *Posljednji Fermatov teorem*. On kaže da ne postoje tri prirodna broja a, b i c takva da je $a^n + b^n = c^n$ za neki prirodni eksponent $n > 2$.

Nas će ovdje više zanimati drugi, tzv. *mali Fermatov teorem*, kao osnova za testiranje složenosti brojeva. On kaže: ako je p prost broj i a bilo kakav broj koji nije višekratnik od p, tada je izraz $a^{p-1} - 1$ djeljiv s p. Drukčije zapisano, $a^{p-1} \equiv 1 (\mathrm{mod}\ p)$.
Za probu uzmimo prost broj $p = 7$ i $a = 2$. Trebalo bi biti $2^6 - 1$ djeljivo sa 7. Zaista, 7 dijeli 63. Ali što ako za broj p ne znamo unaprijed je li prost ili nije? Tada možemo pretpostaviti da jest i odabrati neki proizvoljni a koji nije višekratnik od p i provjeriti je li $a^{p-1} - 1$ djeljiv s p. Ako se dogodi da nije djeljiv, onda p ne može biti prost broj.

Primijetite da je ovakav rezultat pravi mali fenomen! Naime, uz malo sreće saznali smo da je p složen, a da uopće nemamo pojma ni o jednom njegovom faktoru!

AKS-test. Fermatov test iz prethodnog odlomka ima dvije dobre osobine. On je univerzalan – može se primjenjivati na bilo koji prirodan broj (za razliku od nekih testova koji su namijenjeni samo za Mersenove brojeve ili za neki drugi skup). Osim toga je i bezuvjetan. Neki drugi testovi imaju uvjete – da bi bili ispravni, mora biti točna jedna Riemanova hipoteza, a ona još nije dokazana, premda je po svoj prilici točna.

Fermatov test ima i dvije loše osobine. Ona glavna jest da on ne daje za sve brojeve potpuno pouzdan odgovor. Odgovor je pouzdan samo za većinu složenih brojeva. Za proste i za neke specijalne složene brojeve odgovor je "možda", čak i "gotovo sigurno", ali to nam nije dovoljno. Druga mu je mana količina računanja za vrlo velike zadane brojeve. Ona u općem slučaju nije polinomijalna u odnosu na broj znamenaka zadanog broja.

Prvi test koji ima sve četiri poželjne osobine (univerzalnost, bezuvjetnost, pouzdanost i polinomijalno vrijeme) otkriven je 2002. u Indiji i zove se AKS-test prema inicijalima trojice njegovih autora. To su Manindra Agrawal, Neeraj Kayal i Nitin Saxena s Tehnološkog instituta u Kanpuru. Prvi je bio profesor koji je radio na doktorskoj radnji sa sasvim drukčijim ciljem, a druga dvojica studenti koji su njegove ideje razvili dalje i opazili nove mogućnosti. Naposljetku su sva trojica prikazala AKS u konačnom obliku.

Njihov je rad naišao na mnoge nagrade i odušev-ljenje u svijetu. Njemačka Wikipedija navodi kao ilustraciju popularnosti da je *web*-stranica s njihovim radom imala samo u prvom tjednu oko 2 milijuna posjeta! Ali i relativna jednostavnost ideje se dojmila matematičkog svijeta. Toliko da se izvjesni P. Leyland zapitao: "Što smo još (od jednostavnih stvari u čitavoj matematici) propustili primijetiti?" AKS-test je ipak složeniji od Fermatova, pa se njime ovdje nećemo detaljnije baviti.

Obogatiti se bez muke? Ljudi vas u životu više cijene ako imate novca nego ako znate matematiku. Žalosno, ali istinito. No to nije razlog da odbacite ovu znanost. Naime, evo prilike da povežete matematiku s novcem! Već je spomenuto u ovom članku da je raspisana visoka nagrada onome koji pronađe prost broj s barem milijardu znamenaka. Pa ćemo sada to zajedno i pokušati!

Neka je n broj koji se sastoji od točno milijardu znamenaka "1". On je neparan, dakle nije djeljiv s 2. Je li djeljiv s 3? Suma znamenaka mu je milijarda, a nju s 3 ne možemo podijeliti. Zato n nije djeljiv s 3. Očito se ne da podijeliti ni s 5. Izgleda nam je krenulo!

Djeljivost sa 7 provjeravamo tako da broj podijelimo u grupe od po 3 znamenke, počevši zdesna. Nakon toga tim grupama naizmjenično dodijelimo predznake $+$ ili $-$. Svejedno je s kojim predznakom počinjemo pa zato npr. prvu grupu ostavimo pozitivnom, drugoj dodamo minus, treća ostaje

pozitivna, četvrta negativna itd. Kad sve te grupe zbrojimo, pogledamo je li rezultat djeljiv sa 7. Ako jest, onda je i početni broj djeljiv sa 7, inače ne. Sada uzmimo grupe u "velikom paketu" od po 2 komada, tj. podijelimo broj n na velike grupe od po 6 znamenki zdesna. Kako su u igri same znamenke "1", svaka velika grupa bit će 111111. Unutar ove šestorke traženi je zbroj jednak $111 - 111 = 0$. I tako sve do lijevog kraja broja n.

Doduše, prva lijeva grupa ne mora imati svih 6 znamenaka. Zaista, $1\,000\,000\,000 : 6 = 166\,666\,666$ uz ostatak 4. Dakle, ostaje s lijeve strane "stršiti" broj 1111, koji daje male grupe 1 i 111, a njihova razlika 110 (ili -110) nije djeljiva sa 7. Stoga niti n nije djeljiv sa 7. Osjećate li već miris velikog novca?

Sljedeći kandidat za proste djelitelje je 11. Postupamo slično kao kod djeljivosti sa 7, samo ne alterniramo grupe od 3, nego od 1 znamenke. Svaka "velika" grupa sada ima 2 znamenke i uključuje jednu "plus jedinicu" i jednu "minus jedinicu" pa joj je suma 0. Milijarda je djeljiva s 2 pa se n sastoji samo od takvih velikih grupa, a ukupna suma je 0, što je djeljivo s 11. Zato je i cijeli broj n djeljiv s 11. Zaboravite nagradu!

Mogli smo reći i ovako: broj n ima sumu znamenaka na parnim pozicijama $500\,000$, a ista je suma i na neparnim. Razlika tih dviju suma je 0, pa je djeljiva s 11, a to onda vrijedi i za sam n. Općenito, svaki broj koji ima zapis od bilo kakve parne količine jedinica djeljiv je s 11.

Napomena! Možemo djeljivost s 11 dokazati i direktnim dijeljenjem n s 11 na isti onaj način kako smo dijelili na papiru u osnovnoj školi. Naime, prva lijeva znamenka od n je 1, što pri dijeljenju s 11 daje 0 i ostatak 1. Spuštamo sljedeću znamenku i dobijemo 11, a to daje kvocijent 1 i ostatak 0. Sada smo opet u početnoj situaciji, samo s 2 znamenke manje! Dakle, dvije po dvije znamenke daju ostatak 0, a da bi čitav n bio djeljiv s 11, potrebno je jedino da ukupan broj znamenaka bude paran, kao što u ovom slučaju i jest.

Ovo se može generalizirati. Budući da je milijarda djeljiva i s 5, onda je n djeljiv i s $11\,111$ (pet jedinica!). Djeljiv je i s $1\,111\,111\,111$ (deset jedinica) i sl. A to se sve vidi iz dobrog starog "ručnog" dijeljenja!

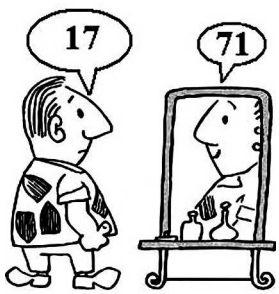
Ako se i dalje nadate lakoj zaradi, kako vam se čini novi broj n s $1\,000\,000\,001$ znamenaka "1"? On nije djeljiv ni s jednim od brojeva 2, 3, 5, 7 i 11. Pa kako onda dalje? Jednostavno, kao u prethodnom primjeru, pokušajmo naći neki p koji je faktor broja $1\,000\,000\,001$, a potom podijeliti n s brojem sastavljenim od p znamenaka "1". Vidimo da je $1\,000\,000\,001$ djeljiv sa 7 jer imamo $-1 + 0 - 0 + 1 - 0 + 0 - 1 + 0 - 0 + 1 = 0$, pa je n djeljiv s $1\,111\,111$ (broj od 7 jedinica).

Napomena! Budući da je $10^9 + 1$ suma dvaju 9-tih potencija, djeljiva je s $10 + 1$, tj. s 11. Stoga broj n možemo podijeliti i s brojem od 11 znamenki "1".

Sve u svemu, niste se obogatili u novcu, ali jeste u znanju!

Prosti brojevi i fantazija. U knjizi "Strast za matematikom" (Clifford A. Pickover, Izvori, 2012.) nalazi se mnoštvo zabavnih matematičkih činjenica. Mnoge od njih nemaju praktičnu korist, nego su čista rekreacija. Evo nekoliko iz područja prostih brojeva.

• Budući da se prost broj na engleskom kaže *prime number* ili samo *prime*, netko je predložio da se obrnuto pisanom riječi *emirp* nazove svaki prost broj koji pročitan naopačke opet daje prost broj. Npr. 17 je *emirp* jer kad se obrnuto čita, dobije se 71 koji je prost. Prvih nekoliko *emirpa* su u skupu $\{13, 17, 31, 37, 71, 73, 79, 97, 107, 113, ..., 1597...\}$. Očigledno ovakvi brojevi dolaze u parovima – ako je neki broj *emirp*, takav je i njegov obrnuti broj.



Ja bih otišao korak dalje – prost broj poput 11 koji je palindrom (tj. kad se obrnuto čita jednak samom

sebi) nazvao bih *savršeni emirp*. A ako bismo *emirp* prevodili na hrvatski, ne bismo li trebali reći *tsorp*?

• Još su u 17. stoljeću matematičari primijetili da su sljedeći brojevi prosti: 31, 331, 3331, $33\,331$, $333\,331$, $3\,333\,331$ i $33\,333\,331$. Logičkom indukcijom (ne onom matematičkom) zaključili su da će svi brojevi takvog oblika biti prosti. Ali ništa od toga, već prvi sljedeći – onaj s 8 trojki – nije prost: $333\,333\,331 = 17 \cdot 19\,607\,843$.

• Čitamo li redom znamenke broja π, dobivamo sve veće i veće cijele brojeve. Ima li među njima prostih? Ima, naravno, to su npr. već 3 i 31. A dalje?
Najveći poznati primjer je
$31\,415\,926\,535\,897\,932\,384\,626\,453\,832\,795\,028\,841$
koji sadrži prvih 38 znamenaka od π i prost je. Kako navodi autor spomenute knjige, njegov kolega Mark Ganson tražio je i dalje, sve do 3000 znamenaka, ali uzalud.

• Uzmimo prost broj a, načinimo kvadrate njegovih znamenaka i te kvadrate zbrojimo. Ako je rezultat b također prost, onda za početni broj a možemo reći da je *otac* broja b. Barem je to tako nazvao izvjesni Terry Trotter, inače umirovljeni nastavnik matematike.

Npr. 23 je otac od 13 jer je $2^2 + 3^2 = 13$. Ili 191 je "otac" od 83 jer je $1^2 + 9^2 + 1^2 = 83$. A taj 83 je ćaća – oprostite – otac od 73. Ne znam smijemo li reći da je 191 *djed* od 73, ali postoji još takvih nizova predaka, npr. $1499 \to 179 \to 131 \to 11 \to 2$. A rekordna duljina niza je 6 i otkrio ga je opet onaj spomenuti Mark Ganson. Niz glasi:

$$28\,999\,999\,999 \to 797 \to 179 \to 131 \to 11 \to 2.$$

Ako bismo se i dalje išli "zafrkavati" s ovim brojevima, nezaobilazna primjedba bila bi da broj 179, kako se vidi u spomenutim nizovima, ima čak dva oca! To su 1499 i 797. No dobro, otac je tu, kakavtakav, ali gdje je majka? Kako je definirati? Kao razliku "otac minus sin"?

Bolje da se vratimo na ozbiljnije teme. Mene bi, recimo, najviše zanimalo: jesu li svi takvi nizovi padajući? Navedeni primjeri jesu. Ali pogledajmo broj 17. Od njega se dobije $1^2 + 7^2 = 50$, dakle veći broj od njega, samo što taj novi broj nije prost. Ali u slučajevima kad jest prost, niz možda uvijek pada.

Prosti brojevi u prirodi? Kad bismo iz svemira primili radijske signale koji se sastoje od raznih prostih brojeva redom, to bi sigurno bili umjetni signali koje su poslala inteligentna živa bića. Ali ipak postoji i jedna prirodna pojava koja ima veze s prostim brojevima!

"Cikade" su jedna porodica kukaca u koje spadaju i naši cvrčci. Njihov životni put je uglavnom ovakav: ženke polažu jajašca u neke biljke, iz toga se izlegu ličinke koje padaju na zemlju i ukopaju se u nju, čak i do pola metra dubine. Tamo se ličinke hrane korijenjem i u dobroj sigurnosti provode svoje vrijeme razvoja u odraslu cikadu. Nakon određenog vremena izlaze na površinu i u preostalom kratkom životu se opet razmnožavaju.

Zanimljivo da neke vrste cikada iz zemlje izlaze tek nakon 13, odnosno 17 godina. Objašnjenja ovih brojeva ima raznih, ali matematičko je najuvjerljivije. Naime, razni grabežljivci (prirodni neprijatelji odraslih cikada) imaju svoje periode razmnožavanja. Ali koji god periodi bili, ova dva prosta broja (13 i 17) nisu djeljiva s njima. Stoga cikade s takvim periodima imaju najveće šanse za preživljavanje. S vremenom su se te vrste raširile, a druge propadale. Da je to točno, pokazuju i računalno generirani modeli ove biološke situacije.