ACTA MATHEMATICA SPALATENSIA
Series didactica
Vol.1 (2018) 41-50

O distribuciji prostih brojeva

Zrinka Franušić, Nikola Pavlinić

Sažetak

Prosti brojevi su jednostavan matematički pojam uz koji se vežu mnoga otvorena pitanja. U radu ćemo *ponoviti* važna svojstva prostih brojeva i *dotaknuti se* nekih neriješenih problema, posebice onih vezanih uz distribuciju prostih koja nas vode čak do velike Riemannove slutnje.

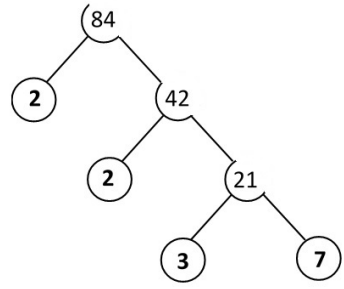
Ključni pojmovi: prost broj, testiranje prostosti, Teorem o prostim brojevima, Riemannova slutnja

1 Što su prosti brojevi?

Prosti ili **prim** brojevi jedan su od fundamentalnih pojmova u matematici. Učenici se s tim pojmom susreću već u 5. razredu osnovne škole i nauče da je svaki prirodan broj veći od 1 **prost broj** ako nema djeljitelja većeg od 1 i manjeg od sebe samog. Još kažemo da je broj prost ako su mu jedini djelitelji 1 i on sam. Prirodan broj veći od 1 koji nije prost naziva se **složen broj**, stoga broj 1 nije niti prost niti složen. Svaki složen broj može se prikazati kao umnožak prostih. Na primjer, $84 = 2 \cdot 2 \cdot 3 \cdot 7$. Posebno je zgodno rastav složenog broja na proste faktore vizualizirati stablom faktorizacije kao na Slici 1.

Gledajući stablo faktorizacije pada nam na pamet usporedba između složenih (*sastavljenih*) brojeva i *molekula*, te prostih (*nerastavljivih*) brojeva i *atoma*. To svojstvo da svaki prirodan broj veći od 1 možemo prikazati kao umnožak prostih brojeva, pri čemu uzimamo da se faktorizacija prostog broja sastoji samo od njega samog, i to na *jedinstven* način, izuzetno je važno i dano je u tvrdnji koja se naziva *Osnovni teorem aritmetike*.

Ovaj rad je potpomogla Hrvatska zaklada za znanost projektom br. 6422.



Slika 1: Stablo faktorizacije

Teorem 1 (Osnovni teorem aritmetike)**.** *Faktorizacija svakog prirodnog broja n većeg od* 1 *na proste faktore je jedinstvena do na poredak prostih faktora.*

Prirodno pitanje koje nam se dalje nameće jest koliko je velik skup prostih brojeva. Odgovor na to pitanje znali su još i stari Grci. Naime, u 9. knjizi Euklidovih *Elemenata* (3. st. pr. Kr.) nalazimo iskaz i jednostavan dokaz tvrdnje o brojnosti skupa prostih brojeva.

Teorem 2 (Euklid)**.** *Prostih brojeva ima beskonačno mnogo.*

Dokaz. Pretpostavimo suprotno, tj. da je skup prostih brojeva konačan. Neka su su $p_1 = 2 < p_2 = 3 < \ldots < p_r$ svi prosti brojevi. Broj $n = p_1 p_2 \cdots p_r + 1$ očito je veći od 1 i nije djeljiv niti s jednim od brojeva $p_1, \ldots, p_r$. Stoga postoji prost broj q, $q \neq p_1, \ldots, p_r$, koji dijeli broj n. Dakle, pronašli smo prost broj q koji ne pripada skupu $\{p_1, \ldots, p_r\}$ što je kontradikcija s pretpostavkom te zaključujemo da je skup prostih brojeva beskonačan. □

Postoji još mnogo drugih dokaza gornjeg teorema koji su zasnovani na tvrdnjama iz različitih matematičkih grana kao što su matematička analiza, topologija, itd., a za njih su zaslužni poznati matematičari poput Eulera, Goldbacha, Furstenberga, Kummera. Na primjer, Euler kao argument da je skup svih prostih brojeva $\mathcal{P}$ beskonačan koristi činjenicu da je red

$$\sum_{p \in \mathcal{P}} \frac{1}{p}$$

divergentan. Naime, može se dokazati da je $\sum_{p \leq y, p \in \mathcal{P}} \frac{1}{p} > \ln \ln y - 1$ za svaki realan broj $y \geq 2$, iz čega direktno slijedi da je red divergentan.

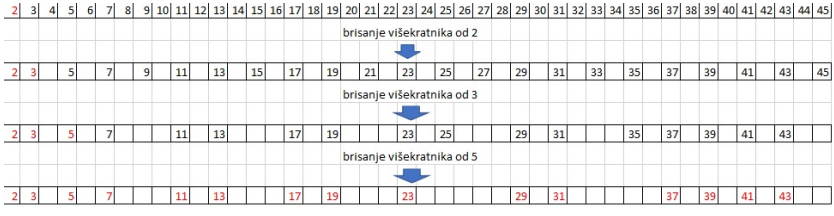
2 Ispitivanje prostosti

Sljedeći problem kojeg je razumno razmotriti jest onaj kako provjeriti je li dani prirodan broj n prost ili složen. Pristupimo li po definiciji, trebat će ispitati ima li broj n nekog prostog djelitelja manjeg od n. Lako se može pokazati da je dovoljno provjeriti postoji li prost djelitelj manji od $\sqrt{n}$. Naime, vrijedi sljedeća tvrdnja.

Propozicija 1. *Neka je n složen broj. Tada postoji prost djelitelj od n koji je manji ili jednak od $\sqrt{n}$.*

Dokaz. Pretpostavimo da je $n = p \cdot k$, gdje je p najmanji prost faktor od n. Tada je $k \geq p$ pa je $n \geq p^2$, odnosno $\sqrt{n} \geq p$. □

Stoga bi u svrhu ispitivanja prostosti bilo korisno imati listu prostih brojeva manjih od nekog zadanog prirodnog broja n. Ako je n "dovoljno malen" postoji vrlo učinkovit algoritam pomoću kojeg možemo kreirati takvu listu - tzv. *Eratostenovo*[1] *sito*. To je postupak u kojem s liste brojeva od 2 do n brišemo najprije sve prave višekratnike broja 2 - najmanjeg prostog broja. Uočimo da su ti obrisani brojevi složeni jer su djeljivi s 2 i strogo veći od 2. Najmanji "neobrisan" broj veći od 2 je 3 - sljedeći prost broj. Zatim s liste brišemo sve prave višekratnike broja 3 i zaključujemo da je sljedeći prost broj 5. Ponavljajući postupak, na listi će nakon konačno mnogo koraka ostati samo prosti brojevi.



Slika 2: Eratostenovo sito za određivanje prostih brojeva ≤ 45

Na Slici 2 "prosijani" su svi prosti brojevi manji od 45 i to u samo 3 koraka. Zbog Propozicije 1 jasno je da će u koraku "brisanja višekratnika od p", p^2 biti prvi pobrisani višekratnik (jer su oni manji već pobrisani

[1] Eratosten, starogrčki matematičar, 3. st. pr. Kr.

u prethodnim koracima). U našem primjeru, kako je $45 < 7^2$, nakon brisanja višekratnika od 5 ostaju samo prosti brojevi. Prije korištenja računala na ovaj način bili su popisani svi prosti brojevi manji od 10^7.

Ako želimo ispitati je li neki *jako velik* broj n prost, metoda dijeljenja sa svim prostim brojevima manjim ili jednakim od $\sqrt{n}$ je vrlo neefikasna prvenstveno zbog toga jer proste brojeve manje ili jednake od $\sqrt{n}$ nije moguće naći u nekom "razumnom" vremenu. Stoga se danas koriste različiti testovi prostosti koji se dijele na vjerojatnosne i determinističke. Razlog nastajanju mnogih algoritama koji ispituju je li neki broj prost ili ne je jednim dijelom u ljudskoj želji za pronalaženjem sve većih prostih brojeva ali i zbog njihove konkretne primjene u ICT-u (informacijsko - komunikacijskim tehnologijama). Naime, sigurnost nekih sustava za kriptiranje informacija upravo leži u težini faktorizacije brojeva koji su produkt dva (velika) tajna prosta broja.

Najveći poznati prost broj u ovom trenutku je $2^{77\,232\,917} - 1$ (siječanj 2018.), broj koji u decimalnom zapisu ima 23 249 425 znamenaka. Za predodžbu o veličini toga broja, napomenimo da bi nam za zapis bilo potrebno 12 917 kartica teksta. (Kartica predstavlja mjernu jedinicu za izračunavanje količine teksta u dokumentu a sastoji se od $1800 = 60 \cdot 30$ znakova.) Ovaj gigantski prost broj spada u tzv. *Mersenneove proste brojeve*, tj. u proste brojeve oblika $2^p - 1$ gdje je p prost broj. Najsvježiji podatci o pronalascima velikih prostih bojeva mogu se naći na stranicama projekta nazvanog GIMPS (Great Internet Mersenne Prime Search). On obuhvaća volontere i entuzijaste diljem svijeta koji sudjeluju u potrazi za velikim prostim Mersenneovim brojevima (https://www.mersenne.org/).

Postoje još mnogi drugi zanimljivi oblici prostih brojeva kao što su $n! \pm 1$ i $n\sharp \pm 1$, pri čemu $n\sharp$ označava umnožak svih prostih brojeva manjih ili jednakih n. Brojevi takvih oblika su zanimljivi jer za njih postoje efikasni deterministički testovi prostosti. Nadalje, posebnu primjenu u kriptografiji javnog ključa imaju i prosti brojevi p takvi da je $2p + 1$ isto prost, npr. $p = 11$ i $2p + 1 = 23$. Oni su nazvani *Sophieini prosti* u čast Marie-Sophie Germain[2].

3 Teorem o prostim brojevima

Lako smo ustanovili da prostih brojeva ima beskonačno mnogo, no postavlja se pitanje postoji li neka pravilnost u njihovom pojavljivanju. Odgovor na pitanje krije se iza naslova ovog odjeljka, Teorem o prostim brojevima, iza kojeg stoji *priča* o distribuciji prostih brojeva.

Već na relativno malom uzorku opažamo (vidi Sliku 2) da postoje susjedni prosti brojevi koji su vrlo blizu jedan drugog, kao na primjer 5

[2]Marie-Sophie Germain, francuska matematičarka, 1776. – 1831.

i 7, 11 i 13, 17 i 19, 29 i 31, itd. Dva uzastopna neparna broja koja su prosta nazivaju se *prosti brojevi blizanci*. Poznata slutnja kaže:

Slutnja 1. *Postoji beskonačno mnogo prostih brojeva blizanca.*

Najveći poznati par prostih brojeva blizanaca je $2996863034895 \cdot 2^{1\,290\,000} \pm 1$, pronađen u rujnu 2016. godine (prema [7]), a svaki od brojeva ima 388 342 znamenke. Zanimljivost vezana uz Slutnju 1 jest i u tome što je poznato da red

$$\sum_{p,p+2\in\mathcal{P}} \left(\frac{1}{p} + \frac{1}{p+2}\right),$$

gdje je $\mathcal{P}$ skup svih prostih brojeva, konvergira (tzv. *Brunov* [3] *teorem*). Ovo bi značilo da, ako je Slutnja 1 istinita, skup svih prostih brojeva blizanaca čini jedan "mali beskonačan" skup.

S druge strane uzastopni prosti brojevi mogu biti i prilično udaljeni što možemo zaključiti iz sljedeće tvrdnje.

Propozicija 2. *Za svaki prirodan broj n postoji n uzastopnih složenih brojeva.*

Dokaz. Uvjerimo se da je

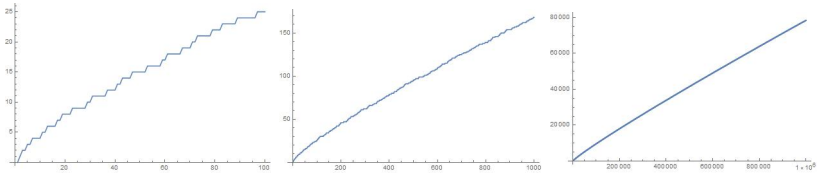
$$(n+1)!+2,\ (n+1)!+3,\ \ldots,(n+1)!+n,\ (n+1)!+n+1$$

niz od n složenih brojeva. Zaista, $2|(n+1)!+2$, $3|(n+1)!+3$, ..., $n+1|(n+1)!+n+1$. □

Nakon ovoga što smo vidjeli u prethodnim razmatranjima jasno nam je da ne možemo očekivati da će prosti brojevi pojavljivati u nekom pravilnom ritmu. Čak i činjenice da se u prvih sto prirodnih brojeva nalazi 25 prostih, u intervalu $\langle 10^7 - 100, 10^7\rangle$ njih 9, dok se u intervalu $\langle 10^7, 10^7 + 100\rangle$ nalaze samo 2 prosta broja, mogu na prvi pogled djelovati obeshrabrujuće. Ipak, *distribucija* prostih brojeva je na neki način pravilna.

Broj prostih brojeva koji su manji ili jednaki od nekog danog realnog broja x označava se s $\pi(x)$. Na Slici 3 prikazani su grafovi funkcije $x \mapsto \pi(x)$ na tri intervala $[0, 100]$, $[0, 1\,000]$ i $[0, 1\,000\,000]$. Na prvoj slici lijevo se lijepo vidi stepeničasta struktura grafa funkcije π, što je sasvim očekivano. No, na posljednjoj slici graf funkcije π izgleda gladak iz razloga što se na njemu stepeničasta struktura ne primijeti golim okom. Ono što nas zanima jest je li moguće tu prekidnu funkciju π, odnosno,

[3] Viggo Brun, norveški matematičar, 1885. – 1978.



Slika 3: Grafovi funkcije $x \mapsto \pi(x)$ za $x \leq 10^2, 10^3, 10^6$

nazovimo ju, *skalinadu prostih brojeva* zamijeniti nekom glatkom funkcijom koja bi ju dobro aproksimirala. Smatramo da je potraga za tom *glatkom aproksimacijom* počela prije dva stoljeća kad je mladi Gauss[4] eksperimentalno otkrio jednu takvu glatku funkciju. Godine 1791., u dobi od samo 14 godina, Gauss je dobio knjigu koja je sadržavala logaritme brojeva manjih od 10^7 i tablicu svih prostih brojeva do 10 009 te uskoro uočio da bi se $\pi(x)$ mogao dobro aproksimirati kvocijentom

$$\frac{x}{\ln x} = f(x),$$

gdje je s $\ln x$ označen prirodni logaritam broja x. Umjesto funkcije f broj prostih brojeva manjih od nekog x može se aproksimirati i pomoću funkcije g dane s

$$g(x) = \frac{x}{2 \cdot (\text{broj znamenaka od } \lfloor x \rfloor)},$$

pri čemu je $\lfloor x \rfloor$ najveće cijelo od x (tj. najveći cijeli broj koji nije veći od x). Zaista, broj znamenaka od $\lfloor x \rfloor$ u bazi 10 je najmanji cijeli broj (strogo) veći od $\log \lfloor x \rfloor$ i $\ln x = \ln 10 \cdot \log x$ pa se $f(x) = \frac{x}{\ln x}$ ugrubo može aproksimirati s $g(x)$.

Dosta kasnije, 1849. godine, u svom pismu njemačkom astronomu J. F. Enckeu, Gauss je predložio još jednu bolju aproksimaciju funkcijom Li koja je dana s

$$Li(x) = \int_2^x \frac{dt}{\ln t},$$

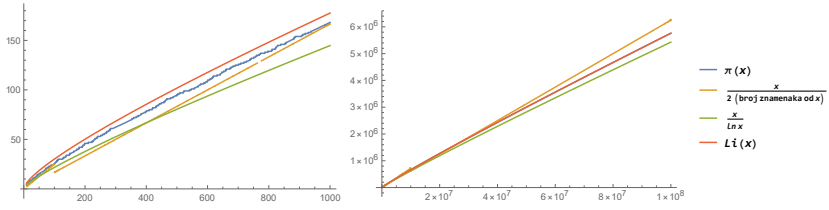
a poznata pod nazivom *logaritamsko integralna funkcija* ili *logaritamski integral*. Međutim Gauss svoj rezultat nije obavio (objavljen je posthumno 1863.). U Tablici 1 prikazane su konkretne vrijednosti funkcija aproksimacija $g(x) = \frac{x}{2 \cdot (\text{broj znamenaka od } \lfloor x \rfloor)}$, $f(x) = \frac{x}{\ln x}$ i $Li(x) = \int_2^x \frac{dt}{\ln t}$ te apsolutne pogreške njihovih aproksimacija.

Prethodna zapažanja eksperimentalne prirode dio su zakonitosti raspodjele prostih brojeva, odnosno funkcije π, koju objašnjava tvrdnja

[4] Johann Carl Friedrich Gauss, njemački matematičar, 1777. – 1855.

x	$\pi(x)$	$g(x)$	$f(x)$	$Li(x)$	err_g	err_f	err_{Li}
9	4	4.5	4.1	4.7	0.5	0.1	0.7
99	25	24.8	21.5	28.9	0.2	3.5	3.9
999	168	166.5	144.6	176.4	1.5	23.4	8.4
9 999	1229	1249.9	1085.6	1245.0	20.9	143.4	16
99 999	9592	9999.9	8685.8	9628.7	407.9	906.2	36.7
999 999	78498	83333.3	72382.3	78626.4	4835.3	6115.7	128.4

Tablica 1: Aproksimacije od $\pi(x)$ i njihove apsolutne pogreške



Slika 4: Aproksimacije od $\pi(x)$

poznata pod nazivom *Teorem o prostim brojevima* ili kratko PNT (od engl. Prime Number Theorem):

Teorem 3 (Teorem o prostim brojevima)**.**

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

Tvrdnja Teorema 3 opisuje tzv. asimptotsko ponašanje funkcije π i kaže da je π *asimptotski jednaka* ili *asimptotski ekvivalentna* funkciji f što se kratko zapisuje kao

$$\pi(x) \sim f(x).$$

Isto vrijedi i za funkciju $Li(x)$ jer je

$$\lim_{x\to\infty} \frac{\frac{x}{\ln x}}{\int_2^x \frac{dt}{\ln t}} = \{\text{L'Hôspitalovo pravilo}\} = \lim_{x\to\infty} \frac{\frac{\ln x - 1}{\ln^2 x}}{\frac{1}{\ln x}} = \lim_{x\to\infty} \frac{\ln x - 1}{\ln x} = 1.$$

Teorem 3 dokazali su 1896. godine Jacques Hadamard i Charles Jean de la Vallée-Poussin, neovisno jedan o drugome, oslanjajući se na Riemannovu[5] ideju o povezanosti prostih brojeva s tzv. Riemannovom zeta-funkcijom kompleksne varijable, ζ, o kojoj ćemo ukratko nešto reći u sljedećem odjeljku.

[5]Bernhard Riemann, njemački matematičar, 1826. – 1866.

4 Riemannova slutnja

Teorem 3 govori o asimptotskoj aproksimaciji funkcije $x \mapsto \pi(x)$ funkcijom $x \mapsto \frac{x}{\ln x}$ što je ekvivalentno tvrdnji da je n-ti prost broj p_n asimptotski jednak $n \ln n$, tj. $p_n \sim n \ln n$, no ne kaže ništa o pogrešci te aproksimacije.

Slutnja 2. *Za svaki $\varepsilon > 0$, postoji $n_0 \in \mathbb{N}$ takav da je*

$$|\pi(n) - Li(n)| < n^{\frac{1}{2}+\varepsilon},$$

za sve $n \in \mathbb{N}$, $n > n_0$.

Iskazana slutnja kaže da je greška aproksimacije broja svih prostih brojeva manjih ili jednakih od nekog prirodnog broja n, $\pi(n)$, pomoću $Li(n)$ u suštini $\sqrt{n}$. Nadalje, ova slutnja koliko god na prvi pogled izgleda jednostavno, ona to nipošto nije. Štoviše, ekvivalentna je jednom od najpoznatijih otvorenih problema u matematici – *Riemannovoj slutnji. Riemannova zeta-funkcija* $s \mapsto \zeta(s)$ se definira pomoću apsolutno konvergentnog reda

$$\zeta(s) = \sum_{i=1}^{\infty} \frac{1}{n^s},$$

za sve kompleksne brojeve s čiji je realni dio veći od 1. Sam je Riemann pokazao da je ovu funkciju moguće analitički proširiti na sve kompleksne brojeve s, $s \neq 1$. Može se pokazati da funkcija ζ ima nultočke u $s = -2, -4, -6, \ldots$ što su tzv. *trivijalne nultočke* zeta-funkcije. Sva istraživanja u vezi Riemannove zeta-funkcije u posljednjih stotinjak godina, uglavnom su se bavila problemom lociranja skupa njenih netrivijalnih nultočaka pri čemu je glavni cilj dokazati sljedeću glasovitu slutnju koju je dao sam Riemman.

Slutnja 3 (Riemannova slutnja)**.** *Sve netrivijalne nultočke Riemannove zeta-funkcije ζ nalaze se na pravcu* $\operatorname{Re} s = \frac{1}{2}$.

Još uvijek se malo zna o skupu nultočaka Riemannove zeta-funkcije. Do sada je pokazano da se netrivijalne nultočke moraju nalaziti unutar tzv. *kritične pruge* $0 < \operatorname{Re}(s) < 1$.

Bez dubljeg poniranja u problem distribucije prostih brojeva, za slutnje 2 i 3 na prvi pogled možemo reći kako nemaju ništa zajedničkog. Ipak, proste brojeve i funkciju ζ veže sljedeća formula

$$\zeta(s) = \prod_{p \in \mathcal{P}} \frac{1}{1 - p^{-s}},$$

gdje je $\mathcal{P}$ skup svih prostih brojeva, a naziva se *Eulerova produktna formula*.

Postoje još mnoge slutnje povezane s prostim brojevima i njihovom distribucijom (Goldbachova slutnja, slutnje o Mersennovim brojevima, o Fermatovim brojevima, o Sophieinim brojevima, itd.). Neke od njih su vrlo lako shvatljive, čak i osnovnovnoškolcima, dok druge razumiju samo znanstvenici. Mi smo istaknuli samo dvije, vrlo lako razumljivu o prostim brojevima blizancima (Slutnja 1) i vrlo tešku Riemannovu (Slutnja 3). Na kraju možemo zaključiti kako o prostim brojevima, tom elementarnom matematičkom pojmu, znamo još vrlo malo i kako oni predstavljaju gotovo neiscrpan izvor za istraživački rad. Koliko posla nas čeka najbolje je iskazao David Hilbert[6] koji je rekao: - Ako se probudim nakon tisuću godina, moje prvo pitanje bi bilo: *Je li dokazana Riemannova slutnja?*

Literatura

[1] A. Dujella, *Uvod u teoriju brojeva* (skripta), https://web.math.pmf.unizg.hr/~duje/utb/utblink.pdf

[2] J. C. Lagarias, *An Elementary Problem Equivalent to the Riemann Hypothesis*, http://www.math.lsa.umich.edu/~lagarias/doc/elementaryrh.pdf

[3] B. Mazur, W. Stein, *Prime Numbers and the Riemann Hypothesis*, Cambridge University Press, 2016.

[4] B. Širola, *Distribucija prim brojeva i Riemannova zeta-funkcija; prvi dio*, math.e, br. 13, http://e.math.hr/zeta/index.html

[5] Prime number, https://en.wikipedia.org/wiki/Prime_number#Formulas_for_primes

[6] Riemann hypothesis, https://en.wikipedia.org/wiki/Riemann_hypothesis

[7] The Largest Known Primes, http://primes.utm.edu/primes/page.php?id=122213

[6] David Hilbert, njemački matematičar, 1862. – 1943.

Zrinka Franušić
Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, Matematički odsjek, Bijenička cesta 30, Zagreb
E-mail adresa: fran@math.hr

Nikola Pavlinić
student, Sveučilište u Zagrebu, Prirodoslovno-matematički fakultet, Matematički odsjek, Bijenička cesta 30, Zagreb
E-mail adresa: nikola.pavlinic@yahoo.com