# Prosti brojevi blizanci

*Matija Kazalicki*[1]

## Yitang Zhang

*Slika 1. Yitang Zhang*

Dana 17. travnja 2013. matematički svijet je uzburkala objava američkog matematičara kineskog porijekla Yitanga Zhanga o otkriću vezanom uz poznati neriješeni problem iz teorije brojeva – slutnju o prostim brojevima blizancima. Ta slutnja tvrdi da postoji beskonačno mnogo parova prostih brojeva čija je razlika točno dva. Zhangu, tada malo poznatom pedesetosmogodišnjem predavaču na sveučilištu u New Hamphsireu, pošlo je za rukom nešto što se svim njegovim puno poznatijim kolegama činilo nemoguće – dokazao je specijalan slučaj Elliott-Halberstamove slutnje što je rezultiralo probojem u razumijevanju distribucije prostih brojeva. Posebno, Zhang je dokazao da postoji beskonačno mnogo parova prostih brojeva čija je razlika manja od sedamdeset milijuna.

Zhangova karijera ni po čemu nije bila tipična. Rodio se 1955. u Šangaju. Od ranog djetinjstva je pokazivao velik interes za matematiku, tako je s devet godina sam pronašao dokaz Pitagorinog teorema. Tijekom kulturne revolucije, dok su škole bile zatvorene, zajedno je sa svojom majkom poslan na selo gdje je na farmi bio primoran uzgajati povrće. Nakon kulturne revolucije, 1978., s navršene dvadeset tri godine upisuje studij na sveučilištu u Pekingu gdje završava studij matematike kao jedan od najboljih studenata. Svoje usavršavanje nastavlja na sveučilištu Purdue, gdje je i doktorirao 1991. Tržište rada u Americi početkom devedesetih nije bilo naklonjeno matematičarima – čak i neki ponajbolji studenti nakon završetka studija nisu mogli naći posao u znanosti. Razlog je u velikom priljevu izvrsnih matematičara iz "istočnog bloka" nakon raspada Sovjetskog saveza. Kako uz sve to Zhang nije imao dobar odnos sa svojim mentorom koji mu nije htio napisati pismo preporuke, nakon doktorata je godinama radio kao računovođa, dostavljač hrane pa onda i kao prodavač u restoranu Subway. Zhang nije odustao od matematike te se 1999. zapošljava kao predavač na sveučilištu New Hampshire (radno mjesto predavača tipično dolazi s velikim nastavnim opterećenjem koje onda ostavlja malo vremena za znanstveni rad). Tamo je ostao sve do 2014. kada postaje profesor na Kalifornijskom sveučilištu u Santa Barbari. Za svoj rad je 2014. dobio prestižnu stipendiju zaklade MacArthur kao i Coleovu nagradu – najznačajniju iz teorije brojeva.

## Slutnja o prostim brojevima blizancima

Prosti brojevi su još od antičkih dana zaokupljali pažnju matematičara tako da je još u 3. st. pr. Kr. Euklid u devetoj knjizi svojih Elemenata dokazao da prostih brojeva ima beskonačno mnogo. Razumijevanje prostih brojeva otežava to što je njihova definicija

[1] Izvanredni je profesor na Zavodu za algebru i osnove matematike na Matematičkom odsjeku Prirodoslovno-matematičkog fakulteta Sveučilišta u Zagrebu; e-pošta: mkazal@math.hr

"indirektna" – kažemo da je prirodan broj $n$ prost ako nije djeljiv s niti jednim prirodnim brojem većim od jedan i manjim od $n$. Zbog toga smo za precizniju tvrdnju o veličini skupa prostih brojeva (Teorem o prostim brojevima) trebali čekati 1896. kada su Jacques Hadamard i Charles Jean de la Vallée Poussin koristeći ideje Bernharda Riemanna (Riemannova zeta funkcija) dokazali da je $\pi(x)$, broj prostih brojeva manjih od $x$, asimptotski jednak funkciji $\dfrac{x}{\ln x}$. Za funkciju $f(x)$ kažemo da se asimptotski ponaša kao funkcija $g(x)$ ako je $\lim\limits_{x\to\infty}\dfrac{f(x)}{g(x)}=1$. Ugrubo, mogli bi reći da je vjerojatnost da je slučajno odabran veliki prirodan broj $x$ prost, jednaka $\dfrac{1}{\ln x}$ ili ekvivalentno da je prosječan razmak između prostog broja $p$ i prvog idućeg jednak $\ln p$.

Preciznija pitanja o razmacima između susjednih prostih brojeva su se pokazala još težima. Francuski matematičar Alphonse de Polignac je 1849. postavio tvrdnju da se svaki paran prirodan broj beskonačno puta javlja kao razlika između dva uzastopna prosta broja. Zato brojeve koji zadovoljavaju ovu slutnju nazivamo de Polignacovim brojevima. Posebno, slutnja o prostim brojevima blizancima tvrdi da je dva de Polignacov broj. Nije bilo poznato postoje li uopće takvi brojevi sve do 2013. kada je Zhang dokazao da postoji barem jedan de Polignacov broj koji je manji od sedamdeset milijuna.

## Što je točno Zhang dokazao?

Zhangove ideje, kao što to obično i bude u matematici, nisu nastale u izolaciji nego su se nadovezale na važan raniji rad Goldstona, Pintza i Yildirima iz 2005. Već smo ranije rekli da je razmak $p_{n+1}-p_n$ između $n$-tog i $(n+1)$-vog prostog broja u prosjeku $\ln p_n$. Goldston, Pintz i Yildirim su pokazali da je taj razmak često i puno manji, tj. da je $\liminf\dfrac{p_{n+1}-p_n}{\ln p_n}=0$, gdje $p_n$ označava $n$-ti prost broj. No, možda i važnije, oni su pokazali da su razmaci između prostih brojeva usko povezani s distribucijom prostih brojeva u aritmetičkim nizovima.

Prema Dirichletovom teoremu o prostim brojevima u aritmetičkim nizovima znamo da svaki aritmetički niz oblika $a_n=b+nq$, gdje su $b$ i $q$ relativno prosti prirodni brojevi, sadrži beskonačno mnogo prostih brojeva. No, isto tako znamo da su prosti brojevi ravnomjerno raspoređeni po klasama ostataka modulo $q$ – broj prostih brojeva manjih od $x$ koji se nalaze u nizu $a_n$ je asimptotski jednak $\dfrac{\pi(x)}{\phi(q)}=\dfrac{x}{\phi(q)\ln x}$. Ovdje je $\phi(n)$ Eulerova $\phi$-funkcija koju za prirodan broj $n$ definiramo kao broj prirodnih brojeva manjih od $n$ koji su relativno prosti s $n$ (npr. $\phi(p)=p-1$ za prost broj $p$), tako da je broj klasa ostataka modulo $q$ koje su relativno proste s $q$ jednak $\phi(q)$. Primjerice, postoje dvije klase ostataka modulo 4 koje su relativno proste sa 4, brojevi oblika $4k+1$ i $4k+3$.

Za ilustraciju, možemo sada zamisliti da proste brojeve $2<p<x$ redom stavljamo u $\phi(q)$ kutija s obzirom na to koji ostatak $p$ daje pri dijeljenju s $q$. Prema prethodno rečenom, za veliki $x$, sve te kutije bi trebale imati približno jednak broj elemenata, ali razlike između individualnih kutija će postojati i unaprijed ne možemo puno reći o njima. Enrico Bombieri i Askold Ivanovič Vinogradov su sredinom 1960-ih ravnomjerenost popunjavanja kutija (za sve $q$-ove) opisali jednim brojem $0<\theta\leqslant 1$ – što je $\theta$ veći to se kutije ravnomjernije popunjavaju. Pritom su dokazali (u poznatom Bombieri-Vinogradovom teoremu) da je $\theta\geqslant\dfrac{1}{2}$.

Vratimo se sad na proste brojeve blizance i rad Goldstona, Pintza i Yildirima. Oni su pokazali da će i najmanja generalizacija Bombieri-Vinogradovog teorema (tj. tvrdnja da je $\theta > \frac{1}{2}$) implicirati postojanje de Polignacovog broja. Zhang je dokazao da je $\theta \geqslant \frac{1}{2} + \frac{1}{584}$ iz čega je slijedilo da postoji de Polignacov broj manji od 70 milijuna.

Peter Elliott i Heini Halberstam su 1968. g. naslutili da je $\theta = 1$, odnosno da su prosti brojevi "idealno" raspoređeni po aritmetičkim nizovima. U slučaju da je Elliott-Halberstamova slutnja točna, iz rada Goldstona, Pintza i Yildirima bi slijedilo da postoji beskonačno mnogo parova prostih brojeva čija je razlika manja ili jednaka 16.

## Eratostenovo sito i generalizacije

Za proučavanje raznih problema vezanih uz distribuciju prostih brojeva uglavnom se koriste metode analitičke teorije brojeva – metode teorije sita. Povijesno, te metode su motivirane (iako to često nije očito) Eratostenovim sitom, algoritmom za traženje prostih brojeva nazvanom po grčkom matematičaru Eratostenu.

Pretpostavimo da želimo odrediti sve proste brojeve manje od 100. Krenemo od najmanjeg prostog broja 2 i s liste svih prirodnih brojeva manjih od 100 izbrišemo (prosijemo) sve brojeve koji su djeljivi s 2. Najmanji preostali broj u listi veći od 2 (u ovom slučaju je to 3) je prost te u sljedećem koraku brišemo sve njegove višekratnike. Postupak ponavljamo sve dok ne dođemo do prvog prostog broja većeg od $10 = \sqrt{100}$. Tada su svi preostali brojevi u listi prosti.

Budući da su metode teorije sita koje je Zhang koristio u svom radu tehnički prekomplicirane za ovaj članak, mi ćemo neformalno ilustrirati neke osnovne ideje te teorije tako što ćemo Eratostenovo sito primijeniti na problem određivanje broja blizanaca.

Malo općenitije, neka $\Psi(x,z)$ označava broj parova brojeva $(n, n+2)$, za $n+2 \leqslant x$ takvih da niti $n$ niti $n+2$ nemaju niti jedan prost djelitelj manji od $z$. Tada je $\Psi(x,\sqrt{x})$ jednak broju parova prostih blizanaca manjih ili jednakih $x$ jer je prirodan broj manji od $x$ prost ako i samo ako nema niti jedan prost djelitelj manji od $\sqrt{x}$. Ta funkcija se standardno označava s $\pi_2(x)$.

Broj $\Psi(x,z)$ možemo izraziti na sljedeći način. Označimo s $\mathcal{A} = \{n \in \mathbb{N} : n+2 \leqslant x\}$. Element $n \in \mathcal{A}$ (odnosno par $(n, n+2)$) ćemo "obrisati" ako postoji prost broj $p < z$ za koji vrijedi da $p \mid n$ ili $p \mid n+2$, tj. ako je $n \equiv 0,\ -2 \pmod{p}$. Za prost broj $p$ označimo s $\mathcal{A}_p = \{n \in \mathcal{A} : n \equiv 0,\ -2 \pmod{p}\}$ – to je skup parova koje "brišemo" iz skupa $\mathcal{A}$ kad ga prosijavamo s prostim brojem $p$. Nakon što prođemo kroz sve proste brojeve manje od $z$ dobivamo da je broj preostalih elemenata u skupu $\mathcal{A}$ jednak

$$\Psi(x,z) = \#\Big(\mathcal{A} \setminus \bigcup_{p<z} \mathcal{A}_p\Big),$$

gdje je # oznaka za broj elemenata skupa. Ako za $d \in \mathbb{N}$ označimo s $\mathcal{A}_d = \bigcap_{p \mid d} \mathcal{A}_p$ onda prema formuli uključivanja i isključivanja imamo

$$\Psi(x,z) = \#\mathcal{A} - \sum_{p_1 \mid P_z} \#\mathcal{A}_{p_1} + \sum_{p_1,p_2 \mid P_z} \#\mathcal{A}_{p_1p_2} - \sum_{p_1,p_2,p_3 \mid P_z} \#\mathcal{A}_{p_1p_2p_3} + \cdots,$$

gdje je $P_z = \prod_{p<z} p$, a $p_i$-ovi su međusobno različiti prosti brojevi. Koristeći Möbiusovu $\mu$-funkciju

$$\mu(n) = \begin{cases} 0, & \text{ako } n \text{ nije kvadratno slobodan,} \\ (-1)^k, & \text{ako je } n \text{ produkt } k \text{ različitih prostih brojeva,} \end{cases}$$

taj izraz možemo elegantnije zapisati

$$\Psi(x,z) = \sum_{d|P_z} \mu(d) \#\mathcal{A}_d.$$

Broj višekratnika od $p$ manjih ili jednakih $x$ je jednak $\left\lfloor \frac{x}{p} \right\rfloor$, pa slijedi da je $\#\mathcal{A}_p$ jednak $2\left\lfloor \frac{x}{p} \right\rfloor$ ili $2\left\lfloor \frac{x}{p} \right\rfloor + 1$. Slično, budući da je $\mathcal{A}_d = \bigcap_{p|d} \mathcal{A}_p$, slijedi $2^{\omega(d)} \left\lfloor \frac{x}{d} \right\rfloor \leqslant \#\mathcal{A}_d \leqslant 2^{\omega(n)} \left\lfloor \frac{x}{d} \right\rfloor + 2^{\omega(d)}$, gdje je $\omega(d)$ broj različitih prostih djelitelja od $d$. Iz $\left\lfloor \frac{x}{d} \right\rfloor \leqslant \frac{x}{d} < \left\lfloor \frac{x}{d} \right\rfloor + 1$, slijedi da postoje brojevi $R_d$, $0 \leqslant R_d < 2^{1+\omega(d)}$, takvi da je $\#\mathcal{A}_d = \frac{2^{\omega(d)} x}{d} + R_d$.

Tada je

$$\Psi(x,z) = x \sum_{d|P_z} \frac{2^{\omega(d)} \mu(d)}{d} + \sum_{d|P_z} \mu(d) R_d.$$

Želimo razumjeti ponašanje ove funkcije za velike $x$ (idealno uz $z = \sqrt{x}$). Na prvi član ovog izraza gledamo kao na glavni član – onaj koji određuje asimptotsko ponašanje funkcije, dok na drugi kao na "grešku" – očekujemo (nadamo se) da će drugi član biti zanemariv u odnosu na prvi za velike $x$. To je istina ako je $z$ jako mali u odnosu na $x$, ali nažalost nije istina za $z = \sqrt{x}$ – taj slučaj zahtijeva upotrebu sofisticiranijih metoda. No, unatoč tome, analizom glavnog člana dobit ćemo heuristički uvid u ponašanje funkcije $\Psi(x, \sqrt{x})$ koji se onda uz malo truda može pretvoriti u gornju ogradu za funkciju $\pi_2(x)$.

Polazna točka naše analize je identitet (koji je jednostavna posljedica jedinstvene faktorizacije cijelih brojeva)

$$\sum_{d|P_z} \frac{2^{\omega(d)} \mu(d)}{d} = \prod_{p<z} \left(1 - \frac{2}{p}\right).$$

Trebat će nam i sljedeća tvrdnja iz analize čiji dokaz ostavljamo čitatelju za vježbu.

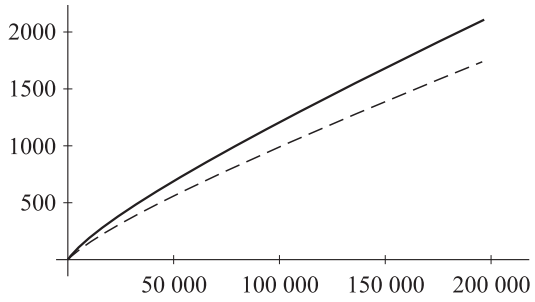
**Zadatak 1.** *Dokažite da je za sve* $x \in \mathbb{R}$, $1 - x \leqslant e^{-x}$.

Iz prethodnog zadatka slijedi

$$\prod_{p<z} \left(1 - \frac{2}{p}\right) \leqslant \prod_{p<z} e^{-\frac{2}{p}} = e^{-2\sum_{p<z} \frac{1}{p}}.$$

Nije teško dokazati da je $\sum_{p<z} \frac{1}{p} > \ln\ln z - 1$ (za dokaz pogledajte primjer 1.6 u [1]), pa zaključujemo da je glavni član manji od $xe^{-2\ln\ln z + 2} < \frac{10x}{(\ln z)^2}$. Uvrštavanjem $z = \sqrt{x}$ dobivamo da je glavni član funkcije $\Psi(x, \sqrt{x})$ manji od $\frac{Cx}{(\ln x)^2}$ za neku konstantu $C > 0$.

U 1915. Viggo Brun je koristeći analizu sličnu našoj (on je koristio Brunovo sito) dokazao da je broj parova blizanaca $\pi_2(x)$ manji od $\dfrac{Cx}{(\ln x)^2}$ za neku konstantu $C > 0$. Iz te ocjene lako slijedi da suma recipročnih vrijednosti brojeva blizanaca $\sum \dfrac{1}{p}$ konvergira. Recimo još da Hardy-Littlewoodova slutnja predviđa da se funkcija $\pi_2(x)$ asimptotski ponaša kao $2 \cdot C_2 \dfrac{x}{(\ln x)^2}$, gdje je $C_2 = \prod_{p \geqslant 3} \left(1 - \dfrac{1}{(p-1)^2}\right) \approx 0.6601618158\ldots$ konstanta prostih brojeva blizanaca (pogledajte sliku 2).




*Slika 2. Grafovi funkcija* $\pi_2(x)$ *i* $\dfrac{2C_2x}{(\ln x)^2}$ *(iscrtkano).*

## Nastavak priče

*Slika 3. James Maynard*

Zhangova priča ima neočekivani nastavak. U listopadu iste godine, slično kao i Zhang, pojavio se niotkuda još jedan matematičar i poboljšao Zhangov rezultat koristeći drugačije, jednostavnije i još općenitije metode. James Maynard, koji je malo prije nego što je Zhang objavio svoj rezultat dovršio svoj doktorat na Oxfordu, radio je na potpuno drugačijem pristupu problemu blizanaca, preko višedimenzionalnih sita. Taj njegov pristup je bio inspiriran još jednim člankom Goldstona i Yildirima iz 2003. Tom metodom je uspio Zhangovu ogradu spustiti sa 70 milijuna na 600. Nedugo nakon toga Terence Tao je pokrenuo projekt "masovne" suradnje Polymath8b (na projektu je sudjelovalo desetak matematičara uključujući Maynarda) s ciljem dodatnog smanjenja Zhangove ograde (prethodni projekt Polymath8 je smanjio konstantu na 5414 – to je bilo prije Maynardovog rada). Kombinirajući Zhangovu i Maynardovu metodu uspjeli su smanjiti ogradu na 246. Ta ograda se do danas nije mijenjala. Također su pokazali da je moguće uz pretpostavku poopćene Elliott-Halberstamove slutnje ogradu spustiti do 6 (Maynard je ranije pokazao da standardna Elliott-Halberstamova slutnja spušta ogradu do 12), tako da će za razrješenje slutnje o prostim brojevima blizancima biti potrebna neka radikalno drugačija ideja.

## Literatura


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

[2] D. MACKENZIE, *Prime Clusters and Gaps: Out-Experting the Experts*, in D. Mackenzie, B. Cipra: What's happening in the mathematical sciences, volume 10 (2015).