Osječki matematički list 17 (2017), 139-150

Bertrandov postulat

Andrijana Ćurković*, Borka Jadrijević†, Marina Simić‡

Sažetak

Joseph Bertrand je 1845. godine naslutio da uvijek postoji prost broj između n i $2n$. Ta tvrdnja je danas poznata kao *Bertrandov postulat*. Bertrand je svoju slutnju provjerio za $n < 3 \cdot 10^6$, ali nije ju dokazao. To je prvi napravio Pafnuti Čebišev 1850. godine.

U ovom radu izložit ćemo dokaz Bertrandova postulata kojeg je dao Paul Erdös u svom prvom objavljenom članku 1932. godine. Dokaz je elementaran i koristi samo nekoliko jednostavnih svojstava binomnih koeficijenta. Osim toga, dat ćemo i vezu Bertrandova postulat s nekim čuvenim tvrdnjama i slutnjama povezanim s prostim brojevima.

Ključne riječi: *Bertrandov postulat, prosti brojevi, binomni koeficijent, Teorem o prostim brojevima, Goldbachova slutnja*

Bertrand's postulate

Abstract

Joseph Bertrand, in 1845, conjectured that for all positive integers n there exists a prime number between n and $2n$. This statement is known as *Bertrand's postulate*. Bertrand verified his conjecture for $n < 3 \cdot 10^6$, but he did not prove it. The conjecture was proved in 1850 by Pafnuty Cherbyshev. In this paper we present the proof published by Paul Erdös in his first article in 1932. The proof is elementary and uses only a few simple properties of binomial coefficients. In addition, we will see how Bertrand's postulate is related to some famous assertions and conjectures concerning prime numbers.

Keywords: *Bertrand's postulate, prime numbers, binomial coefficient, Prime Number Theorem, Goldbach's conjecture*

*Prirodoslovno-matematički fakultet, Sveučilište u Splitu, email: andrijana@pmfst.hr
†Prirodoslovno-matematički fakultet, Sveučilište u Splitu, email: borka@pmfst.hr
‡studentica, Prirodoslovno-matematički fakultet, Sveučilište u Splitu

1 Uvod

Euklid je u svojim *Elementima*, još oko 300. godine pr. Kr., pokazao da je niz prostih brojeva 2, 3, 5, 7, ... beskonačan. Pitamo se, možemo li nešto reći o međusobnoj udaljenosti brojeva u tom nizu? Lako se vidi da veličina tih udaljenosti nije ograničena. Kako bi to pokazali, dovoljno je za svaki prirodan broj k pronaći k uzastopnih složenih brojeva, što upravo znači da za svaki prirodan broj k postoje dva susjedna prosta broja koja su udaljena za barem $k+1$. U tu svrhu, za prirodan broj k označimo s $N = 2 \cdot 3 \cdot 5 \cdots p$ umnožak svih prostih brojeva manjih od $k+2$ i promotrimo k brojeva

$$N+2,\ N+3,\ N+4, \ldots,\ N+k,\ N+k+1.$$

Primijetimo da niti jedan od ovih brojeva nije prost. Naime, svaki i, $2 \leq i \leq k+1$, ima prost faktor q_i koji je manji od $k+2$. Kako je taj q_i prost faktor i od N, onda q_i dijeli $N+i$, što znači da je $N+i$ složen jer je $q_i < N+i$. Prema ovom, za naprimjer $k = 14$, znamo da niti jedan od sljedećih četrnaest uzastopnih brojeva

$$30\,032,\ 30\,033,\ 30\,034, \ldots, 30\,045$$

nije prost. S druge strane ipak možemo naći gornju granicu za udaljenosti u nizu prostih brojeva. Ta granica može se formulirati na sljedeći način: *udaljenost do prvog sljedećeg prostog broja ne može biti veća od broja od kojeg smo započeli traženje*. Ovu tvrdnju je, kao slutnju, iskazao francuski matematičar Joseph Bertrand 1845. godine, a danas ju nazivamo *Bertrandov postulat* iako se, jer je tvrdnja dokazana, radi o teoremu. Preciznije, tvrdnja glasi:

Joseph Bertrand (1822.–1900.) francuski matematičar koji je dao doprinos u teoriji vjerojatnosti, termodinamici i diferencijalnoj geometriji

Teorem 1.1 (Bertrandov postulat). Za svaki $n \geq 1$, postoji prost broj p takav da je $n < p \leq 2n$.

Bertrand je svoju slutnju provjerio za $n < 3 \cdot 10^6$, ali nije ju dokazao. Tvrdnju je prvi dokazao Pafnuti Čebišev 1850. godine. Puno jednostavniji dokaz dao je indijski matematički genij Srinivasa Ramanujan, a Paul Erdös je, u svom prvom članku [2] objavljenom 1932. godine (kad je imao 19 godina), dao predivan elementaran dokaz koji ne koristi ništa drugo nego nekoliko jednostavnih svojstava binomnih koeficijenta.

Ovdje ćemo dati Erdösev dokaz Bertrandova postulata (također vidjeti [1, 3, 4]) te pokazati kako dvije osnovne leme upotrijebljene u dokazu vrlo brzo daju jednu aproksimaciju od $\pi(x)$ – broja svih prostih brojeva manjih ili jednakih od broja x, što je slabija verzija poznatog Teorema o prostim brojevima. Pokazat ćemo i kako, uz pretpostavku da vrijedi čuvena Goldbachova slutnja, Bertrandov postulat ima vrlo kratak, elementaran dokaz.

Isto tako, vidjet ćemo i kako se, uz pomoć Bertrandova postulata, može pokazati da se elementi skupa $\{1, \ldots, 2n\}$ uvijek mogu grupirati u n parova takvih da je suma elemenata u svakom paru prost broj.

2 Erdösev dokaz

Osnovni teorem aritmetike kaže da je zapis prirodnog broja m u obliku

$$m = \prod_{p \leq m,\, p-prost} p^{k(m,p)}, \quad k(m,p) \in \mathbb{N}_0, \tag{1}$$

odnosno njegov rastav na proste faktore, jedinstven do na poredak faktora. Primijetimo da u (1) imamo produkt po konačno mnogo prostih brojeva p, te da je $k(m,p) = 0$ ako i samo ako p ne dijeli m, a ako p dijeli m, onda je $p^{k(m,p)}$ najveća potencija od p koja dijeli m.

Erdösev dokaz Bertrandova postulata temelji se na nekoliko pomoćnih tvrdnji koje govore o svojstvima rastava na proste faktore binomnog koeficijenta $\binom{2n}{n}$ te o ocjenama tog binomnog koeficijenta.

Od sada pa nadalje s $\lfloor x \rfloor$ označavat ćemo najveći cijeli broj manji ili jednak x, a zbog jednostavnosti kod zapisa oblika $\prod_{p \leq x}$ podrazumijevat ćemo da je to produkt samo po prostim brojevima p manjim ili jednakim x.

Započnimo dokaz Legendreovim teoremom o rastavu na proste faktore broja $n!$.

Lema 2.1 (Legendreov teorem). *Uz oznake kao u* (1)*, rastav od $n!$ na proste faktore je oblika*

$$n! = \prod_{p \leq n} p^{k(n!,p)},$$

pri čemu je

$$k(n!,p) = \sum_{t=1}^{r} \left\lfloor \frac{n}{p^t} \right\rfloor,$$

a $r = r(n,p)$ broj za koji vrijedi $p^r \leq n < p^{r+1}$. Drugačije rečeno, broj $n!$ je djeljiv samo s prostim faktorima p koji su manji ili jednaki n i $n!$ sadrži prost broj p kao faktor točno $\sum_{t=1}^{r} \left\lfloor \frac{n}{p^t} \right\rfloor$ puta.

Dokaz. Očito, za prost broj p vrijedi: p dijeli $n!$ ako i samo ako je $p \leq n$. Nadalje, ako $n!$ zapišemo kao produkt oblika $n! = 1 \cdot 2 \cdot \cdots \cdot n$, onda je točno $\left\lfloor \frac{n}{p} \right\rfloor$ faktora od $n!$ djeljivo s p što znači da $n!$ sadrži p kao faktor barem $\left\lfloor \frac{n}{p} \right\rfloor$ puta. Nadalje, u istom zapisu, $\left\lfloor \frac{n}{p^2} \right\rfloor$ faktora od $n!$ je djeljivo i s p^2, što znači

da se p pojavljuje kao faktor još $\left\lfloor \frac{n}{p^2} \right\rfloor$ puta, itd. Nastavljamo do $\left\lfloor \frac{n}{p^r} \right\rfloor$, gdje je $r = r(n,p)$ broj za koji vrijedi $p^r \leq n < p^{r+1}$, jer je $\left\lfloor \frac{n}{p^{r+1}} \right\rfloor = 0$. Stoga je $k(n!,p)$ upravo $\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \cdots + \left\lfloor \frac{n}{p^r} \right\rfloor = \sum_{t=1}^{r} \left\lfloor \frac{n}{p^t} \right\rfloor$. □

Uz prethodno uvedene oznake, dokažimo sljedeću tvrdnju.

Lema 2.2. *Neka prost broj p dijeli $\binom{2n}{n}$. Tada je $p^{k(\binom{2n}{n},p)} \leq 2n$. Ako je dodatno $p > \sqrt{2n}$, onda je $k(\binom{2n}{n},p) = 1$.*

Dokaz. Kako p dijeli $\binom{2n}{n}$, onda je $k(\binom{2n}{n},p) \geq 1$, a prema Legendreovom teoremu (lema 2.1) imamo

$$\begin{aligned} k\left(\binom{2n}{n},p\right) &= k((2n)!,p) - 2k(n!,p) \\ &= \sum_{i=1}^{r(2n,p)} \left\lfloor \frac{2n}{p^i} \right\rfloor - 2 \sum_{i=1}^{r(n,p)} \left\lfloor \frac{n}{p^i} \right\rfloor \\ &= \sum_{i=1}^{r(2n,p)} \left(\left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor \right). \end{aligned} \tag{2}$$

Ovdje smo koristili činjenicu da je $\left\lfloor \frac{n}{p^i} \right\rfloor = 0$ za $r(n,p) < i \leq r(2n,p)$. Svaki od dobivenih pribrojnika je najviše jednak 1 jer je to cijeli broj koji zadovoljava

$$\left\lfloor \frac{2n}{p^i} \right\rfloor - 2\left\lfloor \frac{n}{p^i} \right\rfloor < \frac{2n}{p^i} - 2\left(\frac{n}{p^i} - 1\right) = 2.$$

Stoga iz (2) dobivamo

$$1 \leq k\left(\binom{2n}{n},p\right) \leq r(2n,p) = \max\{r : p^r \leq 2n\} \tag{3}$$

pa je $p^{k(\binom{2n}{n},p)} \leq p^{r(2n,p)} \leq 2n$.

Ako je $p > \sqrt{2n}$, onda je $p^2 > 2n$, odnosno $\max\{r : p^r \leq 2n\} = 1$, pa u (3) imamo $1 \leq k(\binom{2n}{n},p) \leq 1$, što povlači $k(\binom{2n}{n},p) = 1$. □

Sljedeća lema o djeljivosti binomnog koeficijenta odabranim prostim brojem je ključna tvrdnja Erdöseva dokaza Bertrandova postulata.

Lema 2.3. *Neka je $n \geq 3$ prirodan broj i p prost broj za koji vrijedi $\frac{2}{3}n < p \leq n$. Tada p ne dijeli $\binom{2n}{n}$.*

Dokaz. Iz $3p > 2n \geq 2p$ slijedi da su p i $2p$ jedini višekratnici od p manji ili jednaki $2n$. Budući da je $p > \frac{2}{3}n \geq 2$, odnosno $p \neq 2$, broj $2p$ nije djeljiv s p^2. Stoga je brojnik od

$$\binom{2n}{n} = \frac{1 \cdot 2 \cdots 2n}{1 \cdot 2 \cdots n \cdot 1 \cdot 2 \cdot n}$$

djeljiv s p^2, ali ne i s p^3. S druge strane, kako je $p \leq n < \frac{3}{2}p < 2p$, nazivnik ima točno dva faktora p pa slijedi tvrdnja. □

Pokažimo sada dvije tvrdnje koje će nam dati dovoljno dobru gornju i donju ogradu za binomni koeficijent $\binom{2n}{n}$.

Lema 2.4. *Za sve prirodne brojeve n vrijedi*

$$\frac{2^{2n}}{2n} \leq \binom{2n}{n}.$$

Dokaz. Ako je $n = 1$, tvrdnja je očito zadovoljena. Pretpostavimo da je $n > 1$. Zapis binomnog koeficijenta

$$\binom{2n}{n} = \frac{2 \cdot 3 \cdots (2n-1) \cdot 2n}{1 \cdot 2 \cdots n \cdot n!}$$

može biti pojednostavljen dijeljenjem produkta parnih brojeva u brojniku s $n!$, pa donju ogradu dobivamo tako da ocijenimo svaki neparan broj u brojniku s prvim prethodnim parnim brojem. Na ovaj način imamo

$$\binom{2n}{n} = 2^n \cdot \frac{3 \cdot 5 \cdots (2n-1)}{n!} > 2^n \cdot \frac{2 \cdot 4 \cdots (2n-2)}{1 \cdot 2 \cdots (n-1) \cdot n} = 2^n \cdot \frac{2^{n-1}}{n} \quad (4)$$

iz čega slijedi tvrdnja. □

Teorem 2.1. Za sve realne brojeve $x \geq 2$ vrijedi

$$\prod_{p \leq x} p \leq 4^x.$$

Dokaz. Dovoljno je tvrdnju dokazati za prirodne brojeve $k \geq 2$ jer ako je istinita za prirodne brojeve, onda za proizvoljni realni broj $x \geq 2$ imamo

$$\prod_{p \leq x} p = \prod_{p \leq \lfloor x \rfloor} p \leq 4^{\lfloor x \rfloor} \leq 4^x.$$

Tvrdnju za prirodne brojeve $k \geq 2$ možemo dokazati indukcijom. Tvrdnja teorema očito vrijedi za $k = 2$. Neka je $k \geq 3$ prirodan broj. Pretpostavimo da tvrdnja teorema vrijedi za sve prirodne brojeve manje od k i dokazujemo da je tvrdnja istinita za k. Ako je k paran, tvrdnja je očita budući da pretpostavka $k \geq 3$ povlači

$$\prod_{p \leq k} p = \prod_{p \leq k-1} p \leq 4^{k-1} \leq 4^k.$$

Neka je k neparan broj oblika $k = 2n + 1$. Tada promatrani produkt možemo napisati kao produkt dva faktora

$$\prod_{p \leq 2n+1} p = \prod_{p \leq n+1} p \cdot \prod_{n+2 \leq p \leq 2n+1} p.$$

Prosti brojevi između $n + 2$ i $2n + 1$ (uključujući rubove) su djelitelji binomnog koeficijenta $\binom{2n+1}{n}$ budući da je ovo prirodan broj oblika

$$\binom{2n+1}{n} = \frac{(n+2)(n+3)\cdots(2n+1)}{1 \cdot 2 \cdots n}.$$

Naime, ovi prosti brojevi su djelitelji brojnika, a nisu djelitelji nazivnika jer je svaki od faktora u nazivniku manji od tih prostih brojeva. Prema tome, produkt prostih brojeva između $n + 2$ i $2n + 1$ je manji ili jednak ovom binomnom koeficijentu pa je dovoljno odrediti gornju granicu za taj binomni koeficijent. Koristeći ideju dokaza ocjene u (4), ali sada ocjenom neparnih brojeva prvim sljedećim parnim brojem, dobivamo

$$\begin{aligned}\binom{2n+1}{n} &= \frac{2 \cdot 3 \cdot 4 \cdots 2n \cdot (2n+1)}{(1 \cdot 2 \cdot 3 \cdots n)(n+1)!} = 2^n \cdot \frac{3 \cdot 5 \cdot 7 \cdots (2n+1)}{2 \cdot 3 \cdots (n+1)} \\ &< 2^n \cdot \frac{4 \cdot 6 \cdots (2n+2)}{2 \cdot 3 \cdots (n+1)} = 4^n.\end{aligned}$$

Koristeći pretpostavku indukcije i gornju nejednakost imamo

$$\prod_{p \leq 2n+1} p = \prod_{p \leq n+1} p \cdot \prod_{n+2 \leq p \leq 2n+1} p < 4^{n+1} \cdot \binom{2n+1}{n} < 4^{n+1} \cdot 4^n = 4^{2n+1},$$

čime je tvrdnja dokazana i za neparan broj $k = 2n + 1$. □

Sad možemo dokazati Bertrandov postulat.

Dokaz teorema 1.1. Prvo ispitujemo vrijedi li Bertrandov postulat za $n \leq 4000$. Nije potrebno provjeriti svih 4000 slučajeva, već se samo uvjeriti da je u nizu brojeva

$$2,\ 3,\ 5,\ 7,\ 13,\ 23,\ 43,\ 83,\ 163,\ 317,\ 631,\ 1259,\ 2503,\ 4001$$

svaki član prost broj te manji od dvostrukog prethodnog člana („Landauov trik“). Naime, ako za neki prost broj p postoji prost broj q u intervalu $(n, 2n]$, onda je taj prost broj q i iz svakog intervala oblika $(m, 2m]$, za $m = p+1, \ldots, q-1$. Prema tome, svaki interval oblika $(n, 2n]$, za $n \leq 4000$ sadrži jedan od 14 gornjih prostih brojeva.
Sad ćemo ocijeniti binomni koeficijent $\binom{2n}{n}$ dovoljno pažljivo da zaključimo: ako ne postoji prost broj p takav da je $n < p \leq 2n$, onda je n „dovoljno malen“. Za $n \geq 3$, koristeći lemu 2.4 za donju granicu, dobijemo

$$\frac{4^n}{2n} \leq \binom{2n}{n} = \prod_{p \leq \sqrt{2n}} p^{k(\binom{2n}{n}, p)} \cdot \prod_{\sqrt{2n} < p \leq 2n} p^{k(\binom{2n}{n}, p)}. \tag{5}$$

Ocijenimo sada faktore na desnoj strani od (5). Po lemi 2.2 vrijedi

$$\prod_{p \leq \sqrt{2n}} p^{k(\binom{2n}{n}, p)} \leq \prod_{p \leq \sqrt{2n}} 2n \leq (2n)^{\sqrt{2n}}. \tag{6}$$

S druge strane, po lemi 2.3 imamo

$$\prod_{\sqrt{2n} < p \leq 2n} p^{k(\binom{2n}{n}, p)} = \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p^{k(\binom{2n}{n}, p)} \cdot \prod_{n < p \leq 2n} p^{k(\binom{2n}{n}, p)}.$$

Iz prethodne jednakosti i leme 2.2 dobivamo

$$\prod_{\sqrt{2n} < p \leq 2n} p^{k(\binom{2n}{n}, p)} \leq \prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \cdot \prod_{n < p \leq 2n} p, \tag{7}$$

a prema teoremu 2.1 vrijedi

$$\prod_{\sqrt{2n} < p \leq \frac{2}{3}n} p \leq \prod_{p \leq \frac{2}{3}n} p \leq 4^{\frac{2}{3}n}. \tag{8}$$

Sada koristeći ocjene (6), (7) i (8), iz nejednakosti (5) slijedi

$$\frac{4^n}{2n} \leq (2n)^{\sqrt{2n}} \cdot 4^{\frac{2}{3}n} \cdot \prod_{n < p \leq 2n} p. \tag{9}$$

Pretpostavimo sada da ne postoji prost broj p takav da je $n < p \leq 2n$, tj. da je produkt $\prod_{n<p\leq 2n} p$ u (9) jednak 1. Tada (9) povlači

$$4^{\frac{1}{3}n} \leq (2n)^{1+\sqrt{2n}}. \tag{10}$$

Uočimo da za sve $a \geq 2$ vrijedi $a + 1 < 2^a$, odakle je

$$2n = \left(\sqrt[6]{2n}\right)^6 < \left(\lfloor \sqrt[6]{2n} \rfloor + 1\right)^6 < 2^{6\lfloor \sqrt[6]{2n} \rfloor} < 2^{6\sqrt[6]{2n}}. \tag{11}$$

Za $n \geq 50$ je $18 < 2\sqrt{2n}$, pa iz (10) i (11) slijedi

$$4^n \leq (2n)^{3(1+\sqrt{2n})} < 2^{\sqrt[6]{2n}(18+18\sqrt{2n})} < 2^{20\sqrt[6]{2n}\sqrt{2n}} = 2^{20(2n)^{2/3}}.$$

Ovo povlači da je $(2n)^{\frac{1}{3}} < 20$, pa je $n < 4000$. Stoga zaključujemo da i za $n \geq 4000$ vrijedi $\prod_{n<p\leq 2n} p \neq 1$, što znači da postoji prost broj p takav da je $n < p \leq 2n$. □

3 Komentari, slutnje, posljedice

Iako su prosti brojevi osnovni „multiplikativni blokovi" od kojih su „izgrađeni" prirodni brojevi, mnoge tvrdnje povezane s njima, premda imaju vrlo jednostavan i razumljiv iskaz, ili imaju vrlo komplicirane dokaze ili se još uvijek radi o nedokazanim slutnjama. Spomenut ćemo ovdje neke od tih tvrdnji, a koje imaju vezu s Bertrandovim postulatom.

Kao posljedicu Bertrandova postulata imamo sljedeći teorem L. E. Greenfielda i S. J. Greenfielda [5] koji kaže da se prirodni brojevi manji ili jednaki od nekog parnog broja mogu svrstati u parove tako da je suma brojeva u svakom paru prost broj. Točnije, imamo:

Teorem 3.1 (Greenfield, Greenfield). *Za svaki prirodan broj n postoji particija skupa $\{1, \ldots, 2n\}$ oblika*

$$\{\{a_1, b_1\}, \{a_2, b_2\}, \ldots, \{a_n, b_n\}\}$$

takva da je $a_i + b_i$ prost broj za sve $1 \leq i \leq n$.

Dokaz. Dokaz provodimo indukcijom po n. Za $n = 1$ tvrdnja je očita. Pretpostavimo da za $n > 1$ tvrdnja vrijedi za sve $k < n$. Po Bertrandovom postulatu postoji prost broj p koji zadovoljava $2n < p \leq 4n$. Broj $4n$ nije prost, pa je $p = 2n + m$ za neki $1 \leq m < 2n$, gdje je m očito neparan. Uparimo $2n$ s m, $2n - 1$ s $m + 1$ i tako nastavljamo uparivati sve do $n + \frac{m+1}{2}$

s $n + \frac{m-1}{2}$ (ovo je valjan par jer je m neparan). Na ovaj način smo za skup $\{m, \ldots, 2n\}$ dobili particiju

$$\{\{2n, m\}, \{2n-1, m+1\}, \ldots \{n + \frac{m+1}{2}, n + \frac{m-1}{2}\}\}$$

s traženim svojstvom. Kako je m neparan i $m < 2n$, zaključujemo da je $m - 1 = 2k$, za neki $k < n$, pa po pretpostavci indukcije postoji particija skupa $\{1, \ldots, m-1\}$ s istim svojstvom. Unija ovih dviju particija je particija skupa $\{1, \ldots, 2n\}$ s traženim svojstvom. Time je tvrdnja teorema dokazana. □

Gornja tvrdnja iskazom podsjeća na čuvenu *Goldbachovu slutnju (*eng. *Goldbach's Conjecture*, kraće GC), jednu od najpoznatijih i najstarijih nedokazanih slutnji u matematici koju je postavio C. F. Goldbach u pismu L. Euleru 1742. godine, a koja glasi:

Slutnja 3.1 (Goldbachova slutnja). Svaki paran broj veći ili jednak 4 može se zapisati kao suma dva prosta broja.

Pregledavanjem starih i novih tekstova iz teorije brojeva, H. J. Ricardo i Y. Tanaka su 2005. godine u [6] neovisno primijetili da nije uočeno da se, uz uvjet da vrijedi Goldbachova slutnja, kratko i jednostavno može dokazati Bertrandov postulat.

Teorem 3.2 (Ricardo, Tanaka). Ako vrijedi Goldbachova slutnja, onda za svaki prirodan broj $n > 1$ postoji prost broj p takav da je $n < p < 2n$.

Dokaz. Kako je $n > 1$, onda je $2n$ paran broj veći ili jedank 4, pa je prema GC, $2n = p_1 + p_2$ za neke proste brojeve p_1 i p_2. Pretpostavimo da su p_1 i p_2 oba manja od n. Tada je $p_1 + p_2 < 2n$, što je kontradikcija. Stoga je barem jedan p_i veći ili jednak n, odnosno imamo $n \leq p_i < 2n$. Ako je n složen broj, onda je $p_i \neq n$ pa imamo $n < p_i < 2n$. S druge strane, ako je n prost, onda je $n+1$ složen, pa prema GC, postoje prosti brojevi p_1' i p_2' takvi da je $2(n+1) = p_1' + p_2'$, gdje je barem jedan p_i' (recimo p_2') strogo veći od $n+1$ pa onda i od n. Sada imamo $n < p_2' < 2n + 2$. Ako je $p_2' = 2n + 1$, onda je $p_1' = 1$, što je u kontradikciji s pretpostavkom da je p_1' prost. Isto tako ne može biti $p_2' = 2n$ jer je $2n$ složen broj. Dakle, $n < p_2' < 2n$. □

Ako je s $\pi(x)$ označen broj prostih brojeva manjih ili jednakih od broja x, onda se Euklidov teorem, koji kaže da prostih brojeva ima beskonačno, može zapisati kao $\lim_{x \to +\infty} \pi(x) = +\infty$, dok Bertrandov postulat glasi:
Za svaki prirodan broj n je

$$\pi(2n) - \pi(n) \geq 1. \tag{12}$$

Gauss je prvi posvetio pozornost broju $\pi(x)$. Budući da je uočio da su vrijednosti od $\pi(x)$ dobro aproksimirane s $x/\ln x$, 1792. godine (u svojoj petnaestoj godini) naslutio je da vrijedi

$$\lim_{x\to+\infty} \frac{\pi(x)}{\frac{x}{\ln x}} = 1. \tag{13}$$

J. Hadamard i C. de la Vallée-Poussin 1896. godine su neovisno dokazali (13) rabeći neke nove komplicirane tehnike teorije funkcija kompleksne varijable. Rezultat (13), koji se još zapisuje kao

$$\pi(x) \sim \frac{x}{\ln x}, \tag{14}$$

je postao poznat kao *Teorem o prostim brojevima* (eng. *Prime Number Theorem*, kraće PNT). Iako su 1948. godine A. Selberg i P. Erdös dokazali PNT elementarno, bez korištenja funkcija kompleksne varijable, njihov, a i svi ostali dokazi poznati danas, komplicirani su i dugi.

Pokažimo sada vezu Teorema o prostim brojevima i Bertrandova postulata. Prema (14) imamo

$$\pi(2n) - \pi(n) \sim \frac{2n}{\ln 2n} - \frac{n}{\ln n} = \frac{n}{\ln 2n}\left(2 - \frac{\ln 2n}{\ln n}\right) = \frac{n}{\ln 2n}\left(1 - \frac{\ln 2}{\ln n}\right).$$

Kako zadnji izraz teži prema $+\infty$ kad $n \to +\infty$, slijedi da je nejednakost (12) ispunjena za sve „dovoljno velike“ n. Iz jedne druge verzije Teorema o prostim brojevima, koja uključuje i ocjenu greške, može se pokazati da je (12) ispunjeno za sve prirodne brojeve n, odnosno da vrijedi Bertrandov postulat.

Pokušavajući dokazati Teorem o prostim brojevima, Čebišev je 1850. godine dokazao njegovu slabiju, tj. aproksimativnu, verziju koja glasi:

Teorem 3.3. Postoje konstante $c, C > 0$ takve da za sve realne brojeve $x \geq 2$ vrijedi

$$c\frac{x}{\ln x} \leq \pi(x) \leq C\frac{x}{\ln x}. \tag{15}$$

Tvrdnja prethodnog teorema se zapisuje kao

$$\pi(x) \asymp \frac{x}{\ln x},$$

a znači da su $\pi(x)$ i $\frac{x}{\ln x}$ „istog reda veličine“.

Premda Čebišev nije uspio dokazati Teorem o prostim brojevima, njegova ocjena broja $\pi(x)$, točnije dobivene konstante c i C u (15), su bile dovoljno dobre da je uspio dokazati Bertrandov postulat.

Na kraju, uvjerimo se da dvije ključne tvrdnje Erdöseva dokaza Bertrandova postulata daju kratak elementarni dokaz teorema 3.3. Dokažimo prvo pomoćnu tvrdnju koja je zapravo posljedica leme 2.2.

Lema 3.1. *Broj različitih prostih brojeva koji dijele* $\binom{2n}{n}$ *je najmanje* $\frac{\log_2 \binom{2n}{n}}{\log_2 2n}$.

Dokaz. Neka su $p_1, \ldots, p_l$ svi različiti prosti brojevi koji dijele $\binom{2n}{n}$. Po lemi 2.2 imamo

$$\binom{2n}{n} = \prod_{i=1}^{l} p_i^{k(\binom{2n}{n}, p_i)} \leq (2n)^l,$$

pa logaritmiranjem slijedi tvrdnja. □

Dokaz teorema 3.3. Dokaz ćemo započeti s gornjom granicom. U intervalu $(\sqrt{x}, x]$ postoji $\pi(x) - \pi(\sqrt{x})$ prostih brojeva i svaki od njih je veći od $\sqrt{x}$. Stoga je

$$\sqrt{x}^{\pi(x)-\pi(\sqrt{x})} < \prod_{\sqrt{x}<p\leq x} p \leq \prod_{p\leq x} p \leq 4^x,$$

gdje zadnja nejednakost vrijedi po teoremu 2.1. Sada logaritmiranjem prethodne nejednakosti slijedi

$$\pi(x) < \frac{4x}{\log_2 x} + \pi(\sqrt{x}) \leq \frac{4x}{\log_2 x} + \sqrt{x}. \tag{16}$$

Za svaki $x > 0$ je $\log_2 \sqrt{x} \leq \sqrt{x}$, tj. $\log_2 x \leq 2\sqrt{x}$, pa za $x > 1$ vrijedi $\sqrt{x} \leq \frac{2x}{\log_2 x}$. Uvrštavanjem u (16) vidimo da druga nejednakost u (15) vrijedi za $C = 6 \ln 2$. Odredimo sada donju ogradu za $\pi(x)$. Uočimo da funkcija $x \mapsto \frac{x}{\log_2 x}$ na segmentu $[2, 4]$ ima maksimum $\frac{2}{\log_2 2} = \frac{4}{\log_2 4} = 2$. Stoga za $2 \leq x \leq 4$ vrijedi

$$\pi(x) \geq 1 = \frac{4}{2\log_2 4} \geq \frac{x}{2\log_2 x}.$$

Nadalje, ta je funkcija rastuća na $[e, +\infty)$ pa za $4 < x \leq 16$ imamo

$$\pi(x) \geq 2 = \frac{16}{2\log_2 16} \geq \frac{x}{2\log_2 x}.$$

Konačno, neka je $x > 16$ i $2n$ najmanji paran broj veći ili jednak x. Tada je $2n - 2 < x \leq 2n$. Broj $2n$ nije prost pa je

$$\pi(2n) \leq \pi(x) + 1. \tag{17}$$

Prosti djelitelji od $\binom{2n}{n}$ su manji ili jednaki $2n$, pa je $\pi(2n)$ veći ili jednak od broja različitih prostih djelitelja od $\binom{2n}{n}$. Stoga po lemi 3.1 imamo

$$\pi(2n) \geq \frac{\log_2 \binom{2n}{n}}{\log_2 2n}. \tag{18}$$

Koristeći nejednakost (17), zatim ocjenu (18), činjenicu da je $\log_2$ rastuća funkcija i ocjenu iz leme 2.4 dobivamo

$$\begin{aligned}\pi(x) \geq \pi(2n) - 1 &\geq \frac{\log_2 \frac{4^n}{2n}}{\log_2 2n} - 1 = \frac{\log_2 4^n - \log_2 2n}{\log_2 2n} - 1 \\ &= \frac{2n}{\log_2 2n} - 2 \geq \frac{x}{\log_2 x} - \frac{16}{2\log_2 16} \geq \frac{x}{2\log_2 x}.\end{aligned}$$

Time je pokazano da prva nejednakost u (15) vrijedi za $c = \ln 2/2$. □

Što se tiče samog Teorema o prostim brojevima, tu je sve rečeno, tj. dokazano. Ali, čini se, da će naprimjer dokaz *Riemannove slutnje*, jednog od glavnih otvorenih problema u matematici, dati značajna poboljšanja kod ocjene greške za Teorem o prostim brojevima, odnosno za vrijednosti konstanti c i C u (15). Isto tako očekuju se i dramatična poboljšanja kod ocjene međusobne udaljenosti prostih brojeva. Posebno, pretpostavlja se da će biti moguće dokazati još jednu poznatu slutnju, a koja je „u duhu" Bertrandova postulata i glasi:

Za svaki prirodan broj n postoji prost broj između n^2 i $(n+1)^2$.

Literatura

[1] M. Aigner, G. M. Ziegler, *Proofs from the book (4th ed.)*, Springer, 2010.

[2] P. Erdös, *Beweis eines Satzes von Tschebyschef*, Acta Sci. Math. (Szeged), 5(1930 -1932), 194–198.

[3] P. Erdös, J. Surányi, *Topics in the theory of numbers*, Springer-Verlag, 2003.

[4] D. Galvin, *Erdös's proof of Bertrand's postulate*, `https://www3.nd.edu/~dgalvin1/pdf/bertrand.pdf`, 2015.

[5] L. E. Greenfield, S. J. Greenfield, *Some Problems of Combinatorial Number Theory Related to Bertrand's Postulate*, J. Integer Seq., Vol. 1 (1998), Art. 98.1.2

[6] H. J. Ricardo, Y. Tanaka, *Goldbach's conjecture implies Bertrand's postulate*, Amer. Math. Monthly, Vol. 112, No. 6 (2005) 492