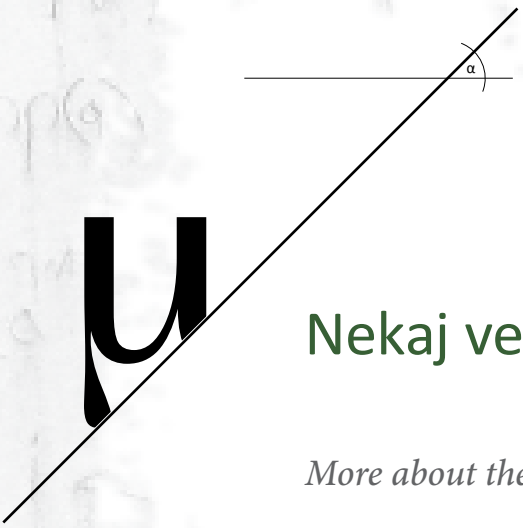

# Nekaj več o praštevilih

*More about the prime numbers*

**Kristijan Breznik**
Mednarodna fakulteta
za družbene in poslovne
študije, Celje
**Janko Marovt**
Ekonomsko-poslovna
fakulteta, Maribor

Σ Izvleček

Praštevila imajo v matematiki posebno mesto, zato so, in so bila tudi v preteklosti, zelo dobro proučevana. V delu bomo podali nekaj znanih problemov, trditev in domnev, ki so povezana s praštevili. Večina problemov je zelo enostavno zastavljenih, seveda pa to ne pomeni, da so tudi rešitve enostavne.

**Ključne besede:** teorija števil, praštevila, sestavljena števila.

*Σ Abstract*

*Prime numbers have a special place in mathematics and for that reason they have been very well researched. We present some well known problems, statements and conjectures related to prime numbers. Most of the problems are formulated in a simple way, but that doesn't mean that their solutions are simple.*

***Key words**: number theory, prime numbers, composite numbers.*

## α Uvod

Matematika je kraljica znanosti, teorija števil pa je kraljica matematike. Tako je nekoč trdil in zapisal slavni nemški matematik Johann Carl Friedrich Gauss (1777–1855).

Ker je teorija števil zelo stara matematična veda, so matematiki na tem področju odkrili veliko zanimivega, vendar pri tem naleteli tudi na veliko problemov. V delu bomo podali nekaj znanih primerov, domnev in izrekov iz teorije števil. Nekateri primeri so že dokazani ali ovrženi, nekateri so še vedno odprti, prav vsi pa bodo tako ali drugače povezani s praštevili. Praštevila zavzemajo v teoriji števil prav posebno vlogo. Njihove lastnosti s pridom izkoriščajo v kriptografiji in teoriji kodiranja. Nekaj osnovnih idej uporabe si lahko pogledamo v [4] in [5].

Učenci se srečajo s praštevili že v osnovni šoli in nato praviloma svoje znanje o njih nadgradijo v prvem letniku srednje šole. Delo pred vami je lahko predvsem smiselna dopolnitev k predpisani učni snovi, lahko pa je tudi motivacija za vpeljavo snovi o praštevilih. Osnovnošolsko razumevanje matematičnih pojmov presega le zadnje poglavje o praštevilskem izreku.

V uvodu poglejmo še nekaj lastnosti praštevil, ki so bralcu verjetno že dobro znane, vendar si bo lahko vseeno malo osvežil spomin. V vsakem nekoliko boljšem srednješolskem učbeniku lahko najdemo enostaven dokaz, da je vseh praštevil neskončno mnogo. Prvi dokaz o tem je bil najden že v Evklidovih Elementih, ki so nastali še pred našim štetjem. Precejšen korak k temu, kako hitro narašča število praštevil (o čemer govori zadnje poglavje), je napravil Euler, ki je dokazal, da je vsota recipročnih vrednosti praštevil

$$\frac{1}{3}+\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\cdots$$

divergentna. Posledično vrsta recipročnih vrednosti vseh naravnih števil, imenovana tudi harmonična vrsta, prav tako divergira.

## β Goldbachova domneva

Ena najbolj znanih in najstarejših še odprtih domnev v povezavi s teorijo števil je Goldbachova domneva. Leta 1742 je manj znani pruski matematik Cristian Goldbach (1690–1764) pisal pismo Eulerju (1707–1783), ki je bil takrat avtoriteta na matematičnem področju, v katerem mu je omenil svojo domnevo, da lahko vsako liho naravno število večje od 5 zapiše kot vsoto treh praštevil. Izvirno pismo si lahko pogledamo na spletnem naslovu [6]. Euler je v odgovoru to izjavo malce dopolnil, in danes je ta problem znan kot

**Goldbachova domneva:** Vsako sodo naravno število, večje od 2, je vsota dveh praštevil.

Domneva, zapisana v zgornji obliki, je v matematiki znana kot krepka Goldbachova domneva. Problem, zapisan v izvirni obliki, kot ga je Eulerju v pismu predstavil Goldbach, pa je znan kot šibka Goldbachova domneva. Seveda bi iz dokaza krepke Goldbachove domneve takoj sledilo, da velja tudi šibka Goldbachova domneva. Namreč, če lahko vsako sodo število, večje od 2, zapišemo kot vsoto dveh praštevil, potem z dodajanjem števila 3 dobimo vsa liha naravna števila večja od 5.

Poglejmo nekaj konkretnih primerov zapisa sodega naravnega števila, večjega od dve, kot vsote dveh praštevil, torej krepke Goldbachove domneve:

$4 = 2 + 2$
$6 = 3 + 3$
$8 = 3 + 5$
$10 = 3 + 7 = 5 + 5$
$12 = 5 + 7$
$14 = 3 + 11 = 7 + 7$
$16 = 3 + 13 = 5 + 11$
$18 = 5 + 13 = 7 + 11$

Nekatera večja soda naravna števila lahko zapišemo kot vsoto dveh praštevil tudi na več načinov, recimo

$$42 = 5 + 37 = 11 + 31 = 13 + 29 = 19 + 23.$$

Problem je na videz zelo preprost, vendar ga matematikom vse do danes ni uspelo razrešiti. Kljub temu v matematičnih krogih prevladuje mišljenje, da je Goldbachova domneva pravilna. Pri preverjanju domneve si matematiki zadnje čase pomagajo z vedno zmogljivejšimi računalniki. Z njimi so do julija leta 2008 domnevo že preverili za vsa soda naravna števila, ki so manjša od $10^{18}$. Pokazano je bilo celo nekoliko več, namreč da lahko vsa soda naravna števila, večja od 6 in manjša od $33 \cdot 10^6$, zapišemo kot vsoto dveh tujih si praštevil. Toda še tako zmogljiv računalnik odpove pri preverjanju domneve za prevelika števila.

Stroga matematična dokazovanja pa gredo ravno v nasprotno smer. Matematiki želijo dokazati, da od nekega števila naprej domneva velja za vsa soda naravna števila. Razlog je v tem, da bi potem za ostala manjša soda naravna števila domnevo preverili neposredno z računom ali s pomočjo vedno zmogljivejših računalnikov. Poglejmo nekaj rezultatov, ki so se približali dokazu pravilnosti Goldbachove domneve. V tridesetih letih prejšnjega stoletja je bilo pokazano, da lahko vsako sodo število zapišemo kot vsoto največ 300.000 praštevil, kar pa je seveda še zelo daleč od vsote dveh praštevil. Pred nekaj leti so rezultat precej popravili, namreč dokazali so, da je vsako sodo naravno število vsota največ šestih praštevil (Goldbachova domneva govori o dveh praštevilih). Za največji korak proti dokazu Goldbachove domneve štejemo delo kitajskega matematika Jinga Runa Chena, ki je leta 1966 dokazal, da lahko vsako sodo naravno število zapišemo kot vsoto praštevila in števila, ki je produkt največ dveh praštevil [1].

Leta 2000 je bilo ponujenih milijon dolarjev tistemu, ki bi mu uspelo dokazati Goldbachovo domnevo v dveh letih. Na žalost nihče ni prijavil dokaza, kar verjetno pomeni, da bo Goldbachova domneva ostala pretrd matematični oreh še kar nekaj časa.

Med poukom lahko v razredu Goldbachovo domnevo uporabimo kot zanimivost, lahko pa učence zaposlimo s preverjanjem te domneve za nekatera manjša soda naravna števila in tako hkrati preverjamo njihovo vedenje o praštevilih.

## γ Praštevilski dvojčki

Praštevilski dvojček je praštevilo, za katerega obstaja praštevilo, ki se od njega razlikuje za 2. Najmanjši praštevilski dvojček tvorita števili 3 in 5. Naslednji pari praštevilskih dvojčkov so 5 in 7, 11 in 13, 17 in 19 itd. V povezavi s praštevilskimi dvojčki še vedno obstaja odprta naslednja domneva.

**Domneva o praštevilskih dvojčkih:** Praštevilskih dvojčkov je neskončno mnogo.

Čeprav se je veliko matematikov trudilo dokazati to preprosto domnevo, dokaza do danes še niso našli. Poglejmo, kaj se je pomembnega dogajalo v povezavi z njo. Leta 1849 je francoski matematik de Polignac podal splošnejšo domnevo. Trdil je, da za poljubno naravno število k obstaja neskončno mnogo parov praštevil $p$ in $p'$, da je $p' - p = 2k$ V posebnem primeru, ko je $k = 1$, dobimo ravno prej omenjeno domnevo o praštevilskih dvojčkih. Tudi primera, ko je $k = 2$ in $k = 3$, sta dobila svoji imeni. Pri $k = 2$ govorimo o

bratranskih praštevilih, pri $k = 3$ pa o sexy praštevilih (poimenovanje izhaja iz latinske besede sex, ki pomeni šest). Na primer 7 in 11 sta bratranski praštevili, števili 7 in 13 pa bi naj bili sexy praštevili. Podobno kot za praštevilske dvojčke tudi za bratranska in sexy praštevila matematikom ni uspelo pokazati, da jih je neskončno. V resnici domneva ostaja odprta za vsa naravna števila $k$.

Matematiki so se precej ukvarjali ne samo z dokazovanjem praštevilske domneve, temveč tudi s samim iskanjem praštevilskih dvojčkov. Do zdaj je bil najuspešnejši Francoz Eric Vautier, ki je v začetku leta 2007 našel do zdaj največji praštevilski dvojček. To sta števili $2003663613 \cdot 2^{195000} + 1$ in $2003663613 \cdot 2^{195000} - 1$. Ti dve naravni števili imata v desetiškem zapisu natanko 58711 števk. Za ilustracijo velikosti teh dveh praštevil lahko povemo, da bi z njunim zapisom skoraj napolnili ves 60-listni zvezek velikega formata.

Pomemben rezultat v povezavi s praštevilskimi dvojčki, ki pa je dokazan, je Brunov izrek. Ta nam pove, da vsota obratnih vrednosti praštevilskih dvojčkov konvergira. Z drugimi besedami povedano, obstaja vsota izraza

$$\left(\frac{1}{3}+\frac{1}{5}\right)+\left(\frac{1}{5}+\frac{1}{7}\right)+\left(\frac{1}{11}+\frac{1}{13}\right)+\left(\frac{1}{17}+\frac{1}{19}\right)\cdots$$

in je končno število. Omenjeno vsoto imenujemo Brunova konstanta, ki znaša $B \approx 1{,}92160\ldots$ Že uvodoma smo povedali, da vsota vseh recipročnih vrednosti praštevil divergira, torej ni končno število. To pomeni, da je praštevilskih dvojčkov *precej manj* kot praštevil, vendar jih je še zmeraj lahko neskončno mnogo.

## δ Bertrandova domneva

Čeravno jo matematiki še danes imenujejo Bertrandova domneva, bi to težko zagovarjali, saj je ta trditev v celoti dokazana. Tudi Bertrandova domneva je, podobno kot druge tukaj omenjene trditve, zelo preprosto zastavljena.

**Bertrandova domneva:** Med poljubnim naravnim številom, večjim od 1, in njegovim dvakratnikom je vsaj eno praštevilo.

Izraz Betrandova domneva se je ohranil iz zgodovinskih razlogov. Francoski matematik Joseph Bertrand (1822–1900) je to domnevo dokazal za vsa naravna števila, manjša od treh milijonov, za preostala pa je le domneval, da ta trditev drži. Svojo domnevo je sicer s pridom uporabljal pri matematičnem raziskovanju. Za manjša naravna števila lahko tudi mi domnevo preverimo z neposrednim računom. Med 2 in 4 je praštevilo število 3. Podobno je med 3 in 6 praštevilo 5 ter med 4 in 8 sta celo dve praštevili, 5 in 7 itd. Seveda pa to ni dovolj, da bi lahko potrdili veljavnost domneve za vsa naravna števila.

Prvi, ki je to domnevo v resnici dokazal, je bil ruski matematik Pafnutij Čebišov (1821–1894), in sicer mu je to uspelo sredi devetnajstega stoletja. Nekateri zato menijo, da bi Bertrandovo domnevo lahko imenovali tudi izrek Čebišova. Kot zanimivost lahko omenimo, da je precej krajši dokaz več let pozneje predstavil madžarski matematik Paul Erdos (1913–1996), eden največjih sodobnih matematikov, ki so se ali se še ukvarjajo s teorijo števil. S kratkim dokazom te domneve je potrdil svojo nadarjenost, saj je bil takrat šele osemnajstletni študent. Dokaz Bertrandove domneve, ki temelji na Erdosovem razmišljanju, lahko najdemo na spletnem naslovu [7]. Oba omenjena matematika, Čebišov in

Erdos, sta veliko prispevala moderni teoriji števil in ju bomo v nadaljevanju še omenjali.

Seveda se matematiki pozneje niso zadovoljili le z dokazom te domneve in so si postavljali nova vprašanja, povezana z njo. Med drugim so dokazali tudi izboljšano Bertrandovo domnevo, ki pravi, da je med poljubnim naravnim številom $n > 3$ in številom $2n - 2$ vsaj eno praštevilo. Če vzamemo za $n = 4$, potem je $2n - 2 = 6$ in med 4 in 6 je praštevilo 5. Podobno je med 5 in $2 \cdot 5 - 2 = 8$ praštevilo 7 itd. Seveda je bilo pričakovati, da bodo slej kot prej odkrili tudi kakšen pretrd oreh. Tako obstaja še vedno neodgovorjeno naslednje vprašanje: Ali za poljubno naravno število $n$, večje od 1, velja, da je med $n^2$ in $(n+1)^2$ vsaj eno praštevilo? Tega seveda ni težko preveriti za prvih nekaj naravnih števil. Med $2^2 = 4$ in $(2+1)^2 = 9$ najdemo praštevili 5 in 7. Med 9 in 16 je prav tako nekaj praštevil. Problem nastane pri večjihnaravnih številih, za katera tega vprašanja ni mogoče preveriti niti s pomočjo najzmogljivejših računalnikov.

## ε Fermatova in Mersennova praštevila

Francoski matematik Pierre S. de Fermat (1601–1665) je znan predvsem po Fermatovem zadnjem izreku in Fermatovem malem izreku. Nas bo bolj zanimala

**Fermatova domneva:** Števila oblike $F_n = 2^{2^n} + 1$ so praštevila za vsako nenegativno celo število n.

Za n = 0, 1, 2, 3, 4 res po vrsti dobimo praštevila 3, 5, 17, 257 in 65537. Praštevilom take oblike, Fermatu v čast, danes pravimo Fermatova praštevila, vsem številom oblike $2^{2^n} + 1$, pa kar Fermatova števila. Fermatova domneva je bila relativno hitro ovržena. Leta 1732 je že prej omenjeni Euler pokazal, da je $F_5 = 641 \cdot 6700417$ in je tako sestavljeno število. Pozneje jim je uspelo pokazati, da so Fermatova števila za $6 \le n \le 16$ sestavljena števila. Kljub prizadevanjem jim do danes ni uspelo najti nobenega drugega Fermatovega praštevila, razen petih, prej omenjenih. Hitro pa lahko pokažemo naslednje: če je praštevilo res oblike $2^m + 1$, potem je število m zagotovo potenca števila 2. Dokaz s protislovjem je zelo kratek in vsebuje razcep dvočlenika. Poglejmo si ga.

Denimo, da število m ni potenca števila 2. Potem je m zagotovo deljivo z nekim lihim naravnim številom, recimo $k$, večjim od 1, kar lahko zapišemo:

$$2^m + 1 = \left(2^{\frac{m}{k}}\right)^k + 1 = \left(2^{\frac{m}{k}} + 1\right) \cdot \left(\left(2^{\frac{m}{k}}\right)^{k-1} - \left(2^{\frac{m}{k}}\right)^{k-2} + \cdots - 2^{\frac{m}{k}} + 1\right)$$

To pa že pomeni, da je število $2^m + 1$ sestavljeno število in trditev je dokazana.

Fermatov rojak in sodobnik je bil Marin Mersenne (1588–1648). Njegova domneva se je glasila tako:

**Mersennova domneva:** števila oblike $M_n = 2^n - 1$ so praštevila za $n$ = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127 in 257 ter sestavljena števila za preostala pozitivna naravna števila, manjša od 257.

Števila oblike $2^n - 1$ imenujemo Mersennova števila, in če so hkrati praštevila, jim pravimo Mersennova praštevila. Kot bomo videli v naslednjem poglavju, jih pogosto srečamo. Hitro opazimo potrebni pogoj za Mersennova praštevila. Število oblike $2^n - 1$ je praštevilo le, če je tudi število $n$ praštevilo. V nasprotnem primeru, torej če je n sestavljeno število, lahko zapišemo $n = k \cdot m$, kjer sta $k$ in $m$ neki naravni števili. Dobimo

$$2^n - 1 = 2^{mk} - 1 = \left(2^m\right)^k - 1 = \left(2^m - 1\right) \cdot \left(\left(2^m\right)^{k-1} + \left(2^m\right)^{k-2} + \cdots + 2^m + 1\right)$$

Tako je v tem primeru tudi $2^n - 1$ sestavljeno število.

Mersennova števila nastopajo tudi drugje. Znano je, recimo, dejstvo, da je za optimalno rešitev matematičnega problema Hanojskih stolpičev z n diski potrebnih natanko $M_n$ korakov. Najdemo jih tudi v računalništvu. Nepredznačeno *n*-bitno število lahko uporabimo za zapis števil do $M_n$.

Vrnimo se k Mersennovi domnevi. Matematiki so potrebovali približno tri desetletja, da jim jo je uspelo preveriti. Ugotovljeno je bilo, da je Mersenne v svoji domnevi zagrešil pet napak. Med praštevila je uvrstil števili $M_{67}$ in $M_{257}$, ki sta sestavljeni števili, in med praštevili izpustil $M_{61}, M_{89}$ in $M_{107}$. Sicer ni znano, kako je Mersenne prišel do svojih sklepov, vendar je moral biti, kljub petim napakam, zavidljivo spreten.

Pri iskanju Mersennovih praštevil so matematiki veliko uspešnejši kot pri iskanju Fermatovih praštevil. Znanih je že 46 Mersennovih praštevil. Na spletu poteka projekt iskanja teh praštevil, imenovan Great Internet Mersenne Prime Search (GIMPS) [9]. V okviru tega projekta so našli tudi do zdaj največje Mersennovo praštevilo. Največje do danes poznano praštevilo je število $2^{43112609}$ -1, ki ima v decimalnem zapisu natanko 12978189 števk. Odkrili so ga avgusta leta 2008, seveda s pomočjo računalnikov. Če bi ga hoteli zapisati, bi ob normalni pisavi v desetiškem sistemu potrebovali več kot petdeset velikih 60-listnih zvezkov! Iz njegovega zapisa vidimo tudi, da spada med Mersennova praštevila. Nasploh spadajo do danes največja znana praštevila med Mersennova praštevila. Kot vidimo, so Mersennova praštevila dokaj dobro raziskana, toda kljub temu se je pojavilo enostavno vprašanje, na katerega še ni bilo odgovora: Ali je neskončno mnogo Mersennovih praštevil?

## ζ Praštevilski izrek

Morda najpomembnejši, zagotovo pa z najbogatejšo in spletk polno zgodovino med vsemi tukaj omenjenimi izreki in domnevami, je praštevilski izrek. Ta nam odgovori na vprašanje, koliko je *približno* praštevil na nekem konkretnem delu naravnih števil. S pomočjo praštevilskega izreka lahko, recimo, odgovorimo na vprašanje, koliko je *približno* praštevil med prvimi milijontimi naravnimi števili. Poudarek je na besedi *približno*, število praštevil se v resnici asimptotično približuje vrednosti izraza v praštevilskem izreku. Asimptotično približevanje pa presega težavnost tega članka in zato se bomo zadovoljili z besedo *približno*. O asimptotičnem približevanju si lahko več preberemo v [3]. Seveda je bralcu poznan že vsaj en način, kako poiskati praštevila med prvimi nekaj naravnimi števili. Iz množice naravnih števil najprej izločimo število 1 in nato vsa soda naravna števila, razen števila 2. Nato izločimo vse večkratnike števila 3, razen samega števila 3. Nadaljujemo in izločamo vse večkratnike naravnih števil, ki še niso bila izločena. Ta postopek je poznan pod imenom Eratostenovo sito. Njegova glavna pomanjkljivost je, da je precej dolgotrajen, vendar nam po drugi strani najde prav vsa praštevila.

Poglejmo zdaj, kaj pravi praštevilski izrek.

**Praštevilski izrek:** Med prvimi n naravnimi števili je približno n/ log n praštevil.

Z log n je označen naravni logaritem števila n. S pomočjo praštevilskega izreka izračunamo, da je med prvimi milijon naravnimi števili približno 72382 praštevil. V resnici jih je 78498. Pravo moč dobi praštevilski izrek šele za zelo velika števila.

Prva matematika, ki sta to domnevala neodvisno drug od drugega, sta bila Adrien-Marie Legendre (1752–1833) in na začetku omenjeni Gauss. Izrek je bil z analitičnimi metodami pokazan konec devetnajstega stoletja. Pri tem sta Jacques Salomon Hadamard (1865–1963) in de la Vallée Poussin (1866–1962) uporabila analitične metode, vključno z znano Riemannovo zeta funkcijo. O tem si lahko več preberemo v [3].

Zanimivejše je bilo dogajanje okrog elementarnega dokaza praštevilskega izreka. Elementarni dokaz pomeni, da v njem ne uporabljamo zahtevnih analitičnih metod in izrekov. Pred približno sto leti so imeli matematiki še zelo malo upanja, da bodo kmalu našli dokaz te vrste. Sredi prejšnjega stoletja sta se prej omenjeni Erdos in Atle Selberg (1917–2007), norveško-ameriški matematik, zelo približala dokazu. Nato sta se sprla in dokaz dokončala vsak zase [8]. Selberg je leta 1950 za svoje delo na elementarnem dokazu praštevilskega izreka dobil celo Fieldsovo medaljo, ki je najvišje matematično priznanje.

**Redakcijska opomba**: Članek je objavljen izjemoma, kljub temu, da v njem ni pomembnejše navezave na pouk. Prepričani smo, da bodo učitelji iz vsebine prispevka znali izluščiti gradivo za preiskovalne naloge, za motiviranje učencev, za delo z nadarjenimi itd….

## ζ Viri in literatura


1. T. M. Apostol, Introduction to Analytic Number theory, Springer (1976).
2. J. Bračič, Uvod v analitično teorijo števil. Podiplomski seminar iz matematike 26, DMFA – založništvo (2003).
3. A. Jurišić, J. Tonejc, Pametne kartice in varnost, Monitor, Letnik 11, št. 6 (2001), str. 66–75.
4. A. Jurišić, J. Tonejc, Pametne kartice. Del 2, Zasebno življenje javnih ključev, Monitor, Letnik 11, št. 7–8 (2001), str. 44–51.
5. Pridobljeno s spletnega mesta: http://www.math.dartmouth.edu/_euler/correspondence/letters/OO0765.pdf.
6. Pridobljeno s spletnega mesta: http://www.nd.edu/_dgalvin1/pdf/bertrand.pdf.
7. Pridobljeno s spletnega mesta: http://www.math.columbia.edu/_goldfeld/ErdosSelbergDispute.pdf.
8. Spletno mesto: http://www.mersenne.org/.