Praštevila in njihove lastnosti

Seminar

Sara Bizjak
Fakulteta za matematiko in fiziko
Oddelek za matematiko

April 2018

Kazalo

1 Uvod **3**

2 Množica praštevil **4**
2.1 Največji skupni delitelj 4
2.2 Dokaz osnovnega izreka aritmetike 6

3 Zaporedje praštevil **7**
3.1 Obstaja neskončno praštevil 7
3.2 Praštevila oblike $ax + b$ 9
3.3 Gostota praštevil 10

4 Zanimivosti **13**
4.1 Največja znana praštevila nekoč in danes 13
4.2 Praštevilski dvojčki 13

5 Zaključek **14**

1 Uvod

S praštevili se vsi seznanimo že v zgodnjih letih šolanja, kar priča o tem, da je njihova definicija enostavna in bi morala biti vsakomur razumljiva. Ravno zaradi te preprostosti pa je presenetljivo, koliko vprašanj v zvezi s praštevili je še vedno odprtih. Že samo ugotoviti praštevilnost je lahko precej zahtevno, saj pri številih z nekaj tisoč števkami tudi Eratostenovo rešeto, kot verjetno najenostavnejši postopek, postane prezamudno. Prav zaradi dejstva, da je za velika števila težko preveriti, ali so praštevila ali ne, je ta tema tako zanimiva.

Tudi v tem članku se bomo pobliže seznanili z »večjimi« praštevili, dokazali bomo obstoj neskončnega števila praštevil, nekaj izrekov in kako se praštevila pojavljajo v množici naravnih števil.

2 Množica praštevil

Praštevilo je število, ki ima natanko dva delitelja. Z izjemo števila 2, ki je najmanjše praštevilo, so vsa praštevila liha. 1 ni praštevilo.

Definicija 1 *Praštevilo je naravno število $n > 1$, če število n delita le števili 1 in n.*

Za občutek naštejmo prvih nekaj praštevil:

$$\mathbb{P} = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67, 71, 73, 79, 83, 89, 97, ...\}$$

Vsako naravno število je »sestavljeno« iz praštevil, kar nam pove tudi naslednji izrek, ki ga bomo dokazali kasneje.

Izrek 1 *(Osnovni izrek aritmetike) Vsako naravno število lahko na natanko en način zapišemo kot produkt samih praštevil. Takemu zapisu pravimo tudi razcep števila na prafaktorje in je enoličen do vrstnega reda natančno.*

2.1 Največji skupni delitelj

Za dokaz osnovnega izreka aritmetike bomo potrebovali še nekaj pojmov in premislekov, zato jih posebej navedimo. Ključni korak k dokazu bo razmislek, da če praštevilo deli zmnožek dveh števil, potem deli ali prvo ali drugo število. Za to pa potrebujemo vpeljavo pojma največjega skupnega delitelja.

Definicija 2 *Naj bo* $\gcd(a, b)$ *največji skupni delitelj števil a in b, torej*

$$\gcd(a, b) = \max\{d \in \mathbb{N} : d|a \text{ in } d|b\},$$

razen če sta a in b oba 0*–tedaj velja* $\gcd(0, 0) = 0$.

Zgled 1 *Izračunani največji skupni delitelji:*

- $\gcd(1, 2) = 1$,
- $\gcd(5, 15) = 5$,
- $\gcd(6, 27) = 3$,
- $\gcd(0, a) = \gcd(a, 0) = a$ *za vsak* a.

Lema 1 *Za vsaka $a, b \in \mathbb{Z}$ velja*

$$\gcd(a, b) = \gcd(b, a) = \gcd(\pm a, \pm b) = \gcd(a, b - a) = \gcd(a, b + a).$$

Dokaz: Dokažimo samo enakost $\gcd(a,b) = \gcd(a,b-a)$.
Naj bo d skupni delitelj a in b, torej $d|a$ in $d|b$, torej obstajata taki celi števili c_1 in c_2, da velja $dc_1 = a$ in $dc_2 = b$. Tedaj $b - a = dc_2 - dc_1 = d(c_2 - c_1)$ in takoj sledi, da $d|b-a$. Tako velja $\gcd(a,b) \leq \gcd(a,b-a)$, saj je množica, iz katere jemljemo $\gcd(a,b)$, podmnožica množice za $\gcd(a,b-a)$.
Če a zamenjamo z $-a$ in b zamenjamo z $b-a$, z istim argumentom kot prej, dobimo: $\gcd(a,b-a) = \gcd(-a,b-a) \leq \gcd(-a,b) = \gcd(a,b)$, iz česar sledi $\gcd(a,b) = \gcd(a,b-a)$. □

Zgled 2 *Privzemimo, da smo osnovni izrek aritmetike že dokazali.*
S pomočjo faktorizacije zračunajmo $\gcd(2261, 1275)$. 2261 *lahko zapišemo kot* $7 \cdot 17 \cdot 19$ *in* 1275 *kot* $3 \cdot 5 \cdot 5 \cdot 17$.
Največji skupni delitelj je enak zmnožku skupnih prafaktorjev,
torej $\gcd(2261, 1275) = 17$.

Motivacija: Naj bosta $a, b \in \mathbb{Z}$ in $b \neq 0$. Tedaj obstajata natanko določena $q, r \in \mathbb{Z}$, tako da $0 \leq r < |b|$ in $a = bq + r$.
To nas pripelje do naslednjega algoritma, imenovanega po starogrškem matematiku Evklidu. Prednost Evklidovega algoritma je, da števil ni potrebno razcepiti. Sam postopek je eden najstarejših znanih algoritmov in je znan od približno leta 300 pr. n. št., verjetno pa je bil poznan že 200 let prej, in sicer kot algoritem za določanje največje skupne mere dveh daljic.

Algoritem 1 *Naj bosta* $a, b \in \mathbb{Z}$ *in* $b \neq 0$. *Ta algoritem izračuna* $q, r \in \mathbb{Z}$, *tako da* $0 \leq r < |b|$ *in* $a = bq + r$.

Opomba 1 *Ker smo s tem algoritmom v večini seznanjeni že od prej, ne bomo opisali prav vseh korakov, ampak si bomo ogledali zgled dejanske uporabe.*

Zgled 3 *Oglejmo si kar prejšnji primer, za katerega rešitev poznamo že iz klasičnega faktoriziranja. Izračunajmo torej* $\gcd(2261, 1275)$ *s pomočjo Evklidovega algoritma. Za lažje nadaljevanje označimo* $a = 2261$ *in* $b = 1275$.
Vidimo, da

$$2261 = 1 \cdot 1275 + 986,$$

torej je $q = 1$ *in* $r = 986$. *Za nadaljevanje posodobimo spremenljivke–a postane število* 1275, *b postane število* 986 *(*$b \longmapsto a$ *in* $r \longmapsto b$*) in dobimo:*

$$1275 = 1 \cdot 986 + 289.$$

Z istim postopkom nadaljujemo, dokler $r = 0$.

$$986 = 3 \cdot 289 + 119$$

$$189 = 2 \cdot 119 + 51$$
$$119 = 2 \cdot 51 + 17$$
$$51 = 3 \cdot 17 + 0$$

Ko je $r = 0$, zaključimo in preberemo največji skupni delitelj, ki ga najdemo korak oz. vrstico višje, na mestu r (pobarvan rdeče).
Tudi z Evklidovim algoritmom pridemo do istega rezultata kot prej, in sicer $\gcd(2261, 1275) = 17$.

Naslednjo lemo navedimo brez dokaza.

Lema 2 *Za $a, b, n \in \mathbb{Z}$ velja:*

$$\gcd(an, bn) = \gcd(a, b) \cdot |n|.$$

Lema 3 *Naj bodo $a, b, n \in \mathbb{Z}$ in naj $n|a$ in $n|b$. Tedaj $n|\gcd(a, b)$.*

Dokaz: Ker $n|a$ in $n|b$, obstajata c in d, tako da $a = nc$ in $b = nd$. Po Lemi 2, $\gcd(a, b) = \gcd(nc, nd) = n \cdot \gcd(c, d)$, torej n deli $\gcd(a, b)$. □

Če praštevilo deli produkt dveh števil, potem deli eno izmed števil. To lahko pokažemo z Evklidovim algoritmom in bo kasneje ključ pri dokazovanju osnovnega izreka aritmetike.

Izrek 2 *Naj bo $p \in \mathbb{P}$ in $a, b \in \mathbb{N}$. Če $p|ab$, potem $p|a$ ali $p|b$.*

Dokaz: Če $p|a$, smo končali. Če $p \nmid a$, potem $\gcd(p, a) = 1$. Po Lemi 2, $\gcd(pb, ab) = b$. Ker $p|pb$ in po hipotezi $p|ab$, potem (po Lemi 2) velja: $p|\gcd(pb, ab) = b \cdot \gcd(p, a) = b \cdot 1 = b$. □

2.2 Dokaz osnovnega izreka aritmetike

V prvem delu dokaza bomo pokazali, da lahko vsako število zapišemo kot produkt samih praštevil. Enoličnost faktorizacije (do vrstnega reda natančno), in s tem tudi dokončno osnovni izrek aritmetike, pa bomo dokazali v drugem delu.

Dokaz:
1. del:
Naj bo $n \in \mathbb{N}$. Če $n = 1$, potem je n prazen produkt praštevil. Če je n praštevilo, smo že končali. Sicer n zapišemo kot ab in $a, b < n$. Po indukciji sta tudi a in b produkta praštevil, torej je take oblike tudi n.

2. del:
Denimo, da imamo za število n dve faktorizaciji. Privzamemo, da je $n > 1$. Tedaj obstajajo taka praštevila $p_1, p_2, \ldots, p_m$, da $n = p_1 \cdot \ldots \cdot p_m$. Naj bo $n = q_1 \cdot \ldots \cdot q_n$ drugi zapis števila n kot produkt praštevil. Po Evklidu je lahko $p_1 = q_1$ ali $p_1 | q_2 \cdots q_n$. Po indukciji vidimo, da velja $p_1 = q_i$ za nek i. Tako p_1 in q_i 'okrajšamo' in ponovimo postopek. Vidimo, da sta ti dve faktorizaciji enaki. Enoličnost faktorizacije do vrstnega reda natančno je dokazana. □

3 Zaporedje praštevil

Sedaj bomo odgovorili na sledeča vprašanja:

- Koliko je vseh praštevil?
- Če imamo celi števili a in b podani, koliko je praštevil oblike $ax + b$?
- Kako so praštevila razporejena v množici naravnih števil?

Najprej bomo pokazali, da je praštevil neskončno, potem Dirichletov izrek, nazadnje pa se bomo seznanili s funkcijo $\pi(x)$, ki nam pove, koliko praštevil, manjših od števila x, obstaja.

3.1 Obstaja neskončno praštevil

Motivacija: Poglejmo si spodnjo tabelo. Vsako število na levi strani enačaja je praštevilo. Sicer prav takšen postopek ne deluje v nedogled, deluje pa nekaj zelo podobnega.

$$\begin{aligned} 3 &= 2 + 1 \\ 7 &= 2 \cdot 3 + 1 \\ 31 &= 2 \cdot 3 \cdot 5 + 1 \\ 211 &= 2 \cdot 3 \cdot 5 \cdot 7 + 1 \\ 2311 &= 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11 + 1 \\ &\ldots \end{aligned}$$

Evklid je zapisal: Praštevil je več kot v kateremkoli izbranem seznamu praštevil. Danes bi to lahko povedali na sledeč način.

Trditev 1 *Obstaja neskončno mnogo praštevil.*

Dokaz: Naj bodo $p_1, p_2, \ldots, p_n$ različna praštevila. Naj bo $P = p_1 p_2 \ldots p_n + 1$ in naj bo p praštevilo, ki deli P. Potem p ne sme biti eno izmed praštevil $p_1, p_2, \ldots, p_n$, ker bi sicer število p delilo razliko $P - p_1 p_2 \ldots p_n = 1$, kar pa je nemogoče. Torej je p še eno novo praštevilo in $p_1, p_2, \ldots, p_n$ niso vsa praštevila. Praštevil je torej neskončno. □

Ali po "Evklidovo":
Dokaz: Naj bodo A, B, C izbrana praštevila. Pravim, da je praštevil več kot A, B, C. Vzemimo število, ki ga merijo A, B, C, naj bo to DE, in dodajmo enoto DF številu DE. Potem EF ali je praštevilo ali pa ni.
A_____ B _____C_____
G_____ _____ E_____
_____ _____ D_____
_____F
Najprej naj bo praštevilo, potem smo našli praštevila A, B, C, EF, ki jih je več kot A, B, C. Potem naj EF ne bo praštevilo, torej ga meri neko praštevilo. Naj ga meri praštevilo G. Pravim, da je G različen od vseh A, B, C. Predpostavimo nasprotno. Vemo, da A, B, C merijo DE. Torej tudi G meri DE. Meri pa tudi EF. Zato mora G, ki je število, deliti tudi preostalo enoto DF, kar je protislovje. Tako je G različen od vseh A, B, C. In po hipotezi je praštevilo. Zato smo našli števila A, B, C, G, ki jih je več od izbranih A, B, C. □

Poznamo tudi druge dokaze, ki pokažejo isto stvar. Nekateri taki so Eulerjev, Polyajev, Kummerjev dokaz, pa tudi topološki dokaz. Od teh je zelo zanimiv Eulerjev dokaz, ki ga je predstavil leta 1737. To je bilo namreč prvič, da sta aritmetika in analiza, do tedaj popolnoma ločena pomena proučevanja, začeli delovati skupaj. Od takrat dalje sta teorija števil in analiza neločljivi vedi. Zapišimo še Eulerjev dokaz:

Dokaz: Euler je poznal vsoto geometrijskega zaporedja
$1 + \alpha z + \alpha^2 z^2 + \alpha^3 z^3 + \ldots = \frac{1}{1-\alpha z}$.
Ulomek $\frac{1}{(1-\alpha z)(1-\alpha z)}$ lahko torej zapišemo kot produkt dveh vsot
$(1 + \alpha z + \alpha^2 z^2 + \alpha^3 z^3 + \ldots)$ in $(1 + \beta z + \beta^2 z^2 + \beta^3 z^3 + \ldots)$, zato je enak
$1 + (\alpha + \beta)z + (\alpha^2 + \alpha\beta + \beta^2)z^2 + (\alpha^3 + \alpha^2\beta + \alpha\beta^2 + \beta^3)z^3 + \ldots$
Na ta način je razvil ulomek $\frac{1}{(1-\alpha z)(1-\beta z)(1-\gamma z)(1-\delta z)\ldots}$ v obliko
$1 + Az + Bz^2 + Cz^3 + Dz^4 + \ldots$, kjer je A vsota koeficientov $\alpha, \beta, \gamma, \delta, \ldots$, B je vsota produktov po dveh koeficientih, C vsota produktov po treh koeficientih itd.
Vzemimo z = 1, koeficienti $\alpha, \beta, \gamma, \ldots$ pa naj zavzamejo recipročne vrednosti praštevil $2, 3, 5, 7, \ldots$ Zahvaljujoč osnovnemu izreku aritmetike je Euler tako

dobil neskončno harmonično vrsto $1 + \frac{1}{2} + \frac{1}{3} + \frac{1}{4} + \ldots$, za katero je trdil, da je enaka $\log(\frac{1}{1-x})$ pri $x = 1$.
Prvotni produktni ulomek je tako neskončen, če sprejmemo Eulerjevo nekoliko drzno upravljanje z neskončnimi količinami brez upoštevanja limit, in je enak dolžini seznama praštevil. □

Kljub temu, da je praštevil neskončno, se je smiselno vprašati, katero je največje znano praštevilo. Mersennovo praštevilo je število oblike $2^q - 1$. Največje najdeno praštevilo je

$$2^{74207281} - 1.$$

To število ima več kot 22 milijonov mest

3.2 Praštevila oblike $ax + b$

Oglejmo si praštevila oblike $ax + b$, kjer sta $a > 1$ in b fiksni celi števili in x teče po naravnih številih. Privzamemo, da $\gcd(a, b) = 1$, saj sicer ne bi bilo neskončno praštevil take oblike. Na primer, $2x + 2 = 2(x + 1)$ je praštevilo le, če $x = 0$ in ne za vsak $x \in \mathbb{N}$.

Poglejmo si praštevila oblike $4x - 1$. Zapišimo jih prvih nekaj in obarvajmo tiste, ki so praštevila.

$$3, 7, 11, 15, 19, 23, 27, 31, 35, 39, 43, 47, ...$$

Izrek 3 *Obstaja neskončno praštevil oblike* $4x - 1$.

Dokaz: Naj bodo $p_1, p_2, ..., p_n$ praštevila forme $4x-1$. Naj bo $P = 4p_1p_2...p_n - 1$. Tedaj $p_i \nmid P$. Ni vsako število p, ki deli P, oblike $4x + 1$. Če bi bilo, bi bil tudi P oblike $4x + 1$. Ker je P liho število, je vsak praštevilski delitelj p_i lih, torej obstaja $p|P$ oblike $4x - 1$. Ta postopek lahko ponavljamo v nedogled, torej je množica praštevil oblike $4x - 1$ neskončna. □

Zgled 4 *Naj bo* $p_1 = 3$ *in* $p_2 = 7$. *Tedaj je*

$$P = 4 \cdot 3 \cdot 7 - 1 = 83$$

praštevilo forme $4x - 1$. *Če računamo naprej, je*

$$P = 4 \cdot 3 \cdot 7 \cdot 83 - 1 = 6971$$

praštevilo forme $4x - 1$. *V naslednjem koraku dobimo*

$$P = 4 \cdot 3 \cdot 7 \cdot 83 \cdot 6971 - 1 = 48601811 = 61 \cdot 796751,$$

kjer je $796751 = 4 \cdot 199188 - 1$.

...

Poglejmo si še Dirichletov izrek brez dokaza.

Izrek 4 *Naj bosta a in b taki celi števili, da $gcd(a, b) = 1$. Tedaj obstaja neskončno mnogo praštevil oblike $ax + b$.*

3.3 Gostota praštevil

Videli smo že, da je praštevil neskončno mnogo, torej je vprašanje, koliko je vseh praštevil, nesmiselno. Smiselno pa je vprašanje o gostoti oziroma o deležu praštevil v naravnih številih. Kot je na primer polovica vseh naravnih števil ravno sodih oziroma lihih, poskušamo podobno ugotoviti za praštevila. Vprašajmo se raje, koliko je praštevil manjših ali enakih nekemu naravnemu številu.

Definicija 3 *Definirajmo*

$$\pi(x) = \#\{p \in \mathbb{N} : p \leq x,\ kjer\ p \in \mathbb{P}\}.$$

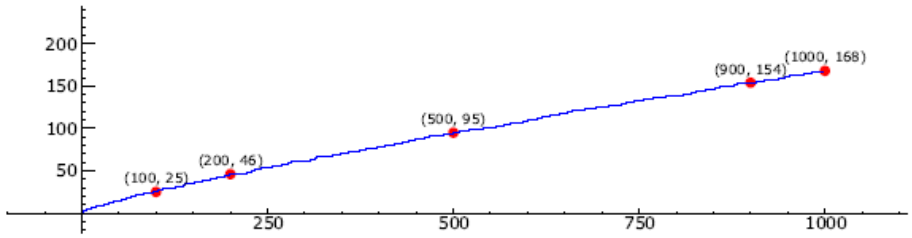
Funkcija $\pi(x)$ je torej moč množice z vsemi praštevili manjšimi ali enakimi x.

Zgled 5 $\pi(6) = \#\{2, 3, 5\} = 3$.

Poglejmo tabelo in graf z vrednostmi $\pi(x)$ *za* $x < 1000$.

x	$\pi(x)$
100	25
200	46
300	62
400	78
500	95
600	109
700	125
800	139
900	154
1000	168

Tabela 1: Vrednosti $\pi(x)$



Slika 1: Graf funkcije $\pi(x)$ za $x < 1000$

Motivacija: Kolikšna je verjetnost, da če naključno izberemo število med 0 in nekim številom x, bo to izbrano število ravno praštevilo? Na to nam odgovori praštevilski izrek, ki v grobem pravi, da je ta verjetnost enaka približno $1/\log(x)$. Torej praštevilski izrek govori o asimptotični porazdelitvi praštevil. Podaja splošni opis, kako so praštevila porazdeljena med pozitivnimi celimi števili. Povzame intuitivno zamisel, da se z večanjem števila x praštevila pojavljajo vse redkeje.

Izrek 5 *Funkcija $\pi(x)$ je asimptotična funkciji $\frac{x}{\log(x)}$, tako da*

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

Vidimo, da Izrek 5 pravzaprav pove, da je $\pi(x)$ približno enako $x/\log(x)$ v smislu, da se relativna napaka tega približka približuje 0, ko gre x preko vsake meje:

$$\lim_{x\to\infty} \frac{\pi(x)}{x} = \lim_{x\to\infty} \frac{1}{\log(x)} = 0,$$

torej za vsak a velja:

$$\lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log(x)-a}} = \lim_{x\to\infty} \frac{\pi(x)}{\frac{x}{\log(x)}} - \frac{a\pi(x)}{x} = 1.$$

Še več, tudi $\frac{x}{\log(x)-a}$ je asimptotična (približno enaka) $\pi(x)$ za vsak a. Če izberemo $a = 1$, vidimo, da je to najboljša možnost (privzeto).

Poglejmo si še tabelo, ki primerja vrednosti $\pi(x)$ in $\frac{x}{\log(x)-1}$ za nekaj vrednosti $x < 10000$.

x	$\pi(x)$	$\frac{x}{\log(x)-1}$ (aproksimacija)
1000	168	169,269029060440816578625 6278
2000	303	302,988873454546387802980 0994
3000	430	428,181931797523704374738 5740
4000	550	548,392209727825326413340 0985
5000	669	665,141878448650217236945 5815
6000	783	779,269888585477862686367 7374
7000	900	891,303565722333997435256 7759
8000	1007	1001,602962794770080754784 281
9000	1117	1110,428422963188172310675 011
10000	1229	1217,976301461550279200775 705

Tabela 2: Primerjava $\pi(x)$ in $\frac{x}{\log(x)-1}$

Kot zanimivost si poglejmo metodologijo dokaza praštevilskega izreka avstralsko-ameriškega matematika Terenca Chi-Shen Taa. V predavanju o praštevilih za širšo javnost je Tao, prejemnik Fieldsove medalje leta 2006, opisal pesniški pristop dokaza praštevilskega izreka s poslušanjem praštevilske glasbe. Začne se z zvočnim valovanjem, ki je glasno pri praštevilih in tiho pri sestavljenih številih–to je von Mangoldtova aritmetična funkcija. Potem se analizira njegove note oziroma frekvence s procesom, sorodnim Fourierjevi transformaciji–to je Mellinova transformacija. Potem se dokaže, kar je težek del, da se določene note v tej glasbi ne morejo pojaviti. Ta izključitev določenih not vodi do praštevilskega izreka. Po Tau ta dokaz vodi do globljega vpogleda v porazdelitev praštevil kot elementarni dokazi.

4 Zanimivosti

4.1 Največja znana praštevila nekoč in danes

Že antični Grki so vedeli, da je praštevil neskončno mnogo, a prav velikih praštevil niso poznali. Prvi praštevili, ki ju že lahko uvrščamo med »večja« praštevila, sta $2^{17} - 1 = 131071$ in $2^{19} - 1 = 524287$, ki ju je leta 1588 pravilno preveril italijanski matematik Pietro Cataldi. Cataldi je poznal praštevila med 2 in korenom zgornjih dveh, torej je moral preveriti samo, da nista deljivi z nobenim manjšim praštevilom. Domneval je, da so tudi števila oblike $2^n - 1$ za $n = 23, 29, 31, 37$ praštevila. Prav je imel le za število $2^{31} - 1$, kar je leta 1772 dokazal Euler. Do prave revolucije pri iskanju velikih praštevil je prišlo leta 1876, ko je francoski matematik Eduard Lucas odkril domiselen in preprost kriterij, ki je prejšnje postopke precej olajšal. Dokazal je, da je 39-mestno število $2^{127} - 1$ praštevilo. Ta rezultat je že predstavljal uvod v računalniško dobo iskanja velikih praštevil. Danes si iskanje velikih praštevil brez pomoči računalnika ne moremo niti predstavljati. Po zaslugi Lucasove ugotovitve so računalniki še posebej uspešni pri iskanju velikih Mersennovih praštevil (praštevila oblike $2^n - 1$). Tako je med največjimi danes poznanimi praštevili največ Mersennovih.

4.2 Praštevilski dvojčki

Poleg iskanja praštevil je zelo zanimivo in težko iskanje t. i. praštevilskih dvojčkov.
Pravimo, da praštevili p in q tvorita praštevilski dvojček, če se po absolutni vrednosti razlikujeta za natanko 2. Tako so praštevilski dvojčki na primer $(3, 5),\ (5, 7),\ (11, 13),\ (17, 19)$...
Razen pri paru $(2, 3)$ je to najmanjša možna razlika med dvema praštevilomi. Vprašanje, ali obstaja neskončno mnogo praštevilskih dvojčkov, je že vrsto let eno od velikih odprtih vprašanj v teoriji števil. Leta 2004 je Richard Arenstorf z Vanderbiltove univerze v Nashvilleu, Tennessee v članku na 38 straneh podal dokaz, da obstaja neskončno mnogo praštevilskih dvojčkov, vendar je mesec dni kasneje Michel Balazard z Univerze v Bordeauxu pokazal na napako in Arenstorf je moral umakniti dokaz.

5 Zaključek

Ker je praštevil neskončno, smo priča vedno novemu lovu na največje znano praštevilo. To iskanje je predvsem zabava za ljudi, ki so jim všeč števila. Za dokazovanje pa je potrebno veliko več znanja, razvijati se morajo tudi tehnologija in algoritmi. Praštevila niso zanimiva le za nas matematike, ampak so uporabna predvsem v računalniških vedah. Zaradi odkrivanja vedno večjih praštevil so računalniški sistemi varnejši, kar temelji na kriptografiji. Kriptografija v osnovi poišče dve dokaj veliki praštevili, ki ju je preprosto zmnožiti. A ko imamo produkt, je težko ugotoviti, katera sta njegova praštevilska faktorja. Varnost temelji na tem, da kdor hoče vdreti v sistem, produkta ne zna razbiti na praštevili, učinkovitih algoritmov, ki pa bi nam na to dali odgovor, še ni.
Glede na uporabo praštevil v vsakdanjem življenju bo to v naslednjih letih še zelo zanimiva tematika.

Literatura

[1] William Stein: Elementary Number Theory: Primer, Congruences, and Secrets, dostopno na https://wstein.org/ent/ent.pdf.

[2] Wikipedia, praštevila.

[3] Revija Presek, list za mlade matematike, fizike, astronome in računalničarje, DMFA-založništvo, 6, 349-351, Letnik 28.

[4] http://www.educa.fmf.uni-lj.si/izodel/sola/2003/ura/valentincic/zaporedje.html.

[5] https://www.rtvslo.si/stevilke/statistika/najvecje-najdeno-prastevilo-ima-vec-kot-22-milijonov-mest/393403.