

# NEKAJ O PRAŠTEVILIH

LUKA PONIKVAR

POVZETEK. Seznanili se bomo s pojmom praštevila in dokazali kar nekaj zanimivih izrekov. Za konec pa si bomo ogledali še en t.i. "nemogoč" problem.

## 1. O DELJIVOSTI ŠTEVIL IN KONGRUENCAH

**Definicija 1.1** (Deljivost). Celo število  $a$  je *deljivo* s celim številom  $b$ , če se da  $a$  enolično zapisati kot

$$a = kb.$$

Tu je  $k \in \mathbb{Z}$ . V tem primeru se imenuje  $b$  *delitelj* števila  $a$  in  $a$  *večkratnik* števila  $b$ . To dejstvo se piše krajše kot  $b \mid a$ .

**Opomba 1.2.** Seveda je tudi  $k$  delitelj  $a$ -ja in  $a$  večkratnik od  $k$ .

**Definicija 1.3.** Izberimo  $m \in \mathbb{N}$ . Pravimo, da sta števili  $a$  in  $b$  *kongruentni* po modulu  $m$ , če dasta pri deljenju z  $m$  enak ostanek. Enakovredna zahteva je da  $m \mid b - a$ . To pišemo kot

$$a \equiv b \pmod{m}$$

in preberemo: število  $a$  je kongruentno  $b$  po modulu  $m$ .

**Primer 1.4.** Oglejmo si množico  $\mathbb{Z}_9 = \{0, 1, 2, 3, 4, 5, 6, 7, 8\}$ . V to množico uvedemo operaciji seštevanja in množenja po modulu 9. V  $\mathbb{Z}_9$ <sup>1</sup> potekajo zadeve takole:

+	0	1	2	3	4	5	6	7	8
0	0	1	2	3	4	5	6	7	8
1	1	2	3	4	5	6	7	8	0
2	2	3	4	5	6	7	8	0	1
3	3	4	5	6	7	8	0	1	2
4	4	5	6	7	8	0	1	2	3
5	5	6	7	8	0	1	2	3	4
6	6	7	8	0	1	2	3	4	5
7	7	8	0	1	2	3	4	5	6
8	8	0	1	2	3	4	5	6	7

TABELA 1. Tabela za seštevanje v  $\mathbb{Z}_9$

---

<sup>1</sup>Kot lahko opazite v  $\mathbb{Z}_9$  obstajajo rešitve enačbe  $x \cdot y = 0$ , kjer sta  $x, y \neq 0$ . Če boste imeli čas in željo lahko premislite, da je to res natanko tedaj, ko smo v  $\mathbb{Z}_m$ , kjer  $m$  ni praštevilo. Če smo v  $\mathbb{Z}_p$ , enačba  $x \cdot y = 0$  premore le rešitve, kjer je  $x = 0$  ali  $y = 0$ .

·	0	1	2	3	4	5	6	7	8
0	0	0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6	7	8
2	0	2	4	6	8	1	3	5	7
3	0	3	6	0	3	6	0	3	6
4	0	4	8	3	7	2	6	1	5
5	0	5	1	6	2	7	3	8	4
6	0	6	3	0	6	3	0	6	3
7	0	7	5	3	1	8	6	4	2
8	0	8	7	6	5	4	3	2	1

TABELA 2. Tabela za množenje v  $\mathbb{Z}_9$ 

**Definicija 1.5.** Naj bo  $m \in \mathbb{N}$ ,  $m \neq 1$  in  $a$  element v  $\mathbb{Z}_m$ . Elementu  $b$  iz  $\mathbb{Z}_m$  pravimo *inverz elementa  $a$* , če velja  $a \cdot b = 1$ .

**Primer 1.6.** V  $\mathbb{Z}_9$  je 7 inverz elementa 4. Hkrati je seveda tudi 4 inverz elementa 7. Iz tabele razberemo, da imata ta elementa enolično določen inverz. Da to ni le naključje, nam pove naslednji izrek.

**Izrek 1.7** (Inverzi v  $\mathbb{Z}_p$ ). *Naj bo  $p \in \mathbb{P}$ . Vsak<sup>2</sup> element v  $\mathbb{Z}_p$  ima enolično določen inverz.*

*Dokaz.* Dokažimo najprej enoličnost inverza. Denimo, da ima  $a$  dva inverza  $b$  in  $c$ . Računajmo:

$$b = b \cdot 1 = b \cdot (a \cdot c) = (b \cdot a) \cdot c = 1 \cdot c = c.$$

Ostane nam še dokazati, da vsak element ima inverz. Izberimo poljuben  $a$  iz  $\mathbb{Z}_p$ . Ker je  $p$  praštevilo, ne more biti za noben  $b$  iz  $\mathbb{Z}_p$  produkt  $a \cdot b$  večkratnik od  $p$  oz.  $a \cdot b \equiv 0 \pmod{p}$ . Če dokažemo, da imata za različna  $b, c$  iz  $\mathbb{Z}_p$  produkta  $ac$  in  $ab$  različna ostanka po modulu  $p$  je izrek dokazan. Denimo da to ne velja in imata za  $b \neq c$  produkta  $ab$  in  $ac$  enak ostanek po modulu  $p$ . Torej je  $a(b - c) \equiv 0 \pmod{p}$ . To pa je možno le, ko je eden od faktorjev enak 0.  $\rightarrow \leftarrow$   $\square$

<sup>2</sup>Ko se pogovarjamo o množenju enoto za seštevanje (0) ponavadi izključimo iz naše množice.

## 2. PRAŠTEVILA

**Definicija 2.1** (Praštevilo). Naravno število  $p \neq 1$  je *praštevilo*, če sta njegova edina pozitivna delitelja 1 in  $p$ . Množico praštevil označujemo s  $\mathbb{P}$ . Število, ki ni praštevilo in je različno od 1, se imenuje *sestavljeno število*.

**Opomba 2.2.** Pišemo  $\mathbb{P} = \{p \in \mathbb{N} \mid p \text{ praštevilo}\}$

**Izrek 2.3.** Vsako naravno število  $n$  ima enoličen razcep na prafaktorje.

**Izrek 2.4** (Evklid). Množica  $\mathbb{P}$  je neskončna.

*Dokaz.* Dokazovali bomo s pomočjo protislovja. Pa predpostavimo, da ima množica  $\mathbb{P}$  le končno elementov. Torej  $\mathbb{P} = \{p_1, p_2, \dots, p_k\}$ ,  $k \in \mathbb{N}$ . Tvorimo število

$$m = p_1 p_2 \dots p_k + 1.$$

Število  $m$  ni deljivo z nobenim od praštevil  $p_1, p_2, \dots, p_k$  iz  $\mathbb{P}$ .  $\rightarrow \leftarrow$

□

**Definicija 2.5.** Naj bo  $x \in \mathbb{R}$ .  $\pi(x) = \{p \in \mathbb{P} \mid p \leq x\}$ .

**Primer 2.6.** V  $\mathbb{Z}_9$  je 7 inverz elementa 4. Hkrati je seveda tudi 4 inverz elementa 7. Iz tabele razberemo, da imata ta elementa enolično določen inverz. Da to ni le naključje, nam pove naslednji izrek.

**Vaja 2.7.** Poišči praštevila, ki so za 1 manjša od popolnega kvadrata<sup>3</sup>.

**Vaja 2.8.** Poišči vsa praštevila  $p$ , da sta  $p + 10$  in  $p + 14$  tudi praštevili.<sup>4</sup>

**Vaja 2.9.** Dokaži, da je neskončno praštevil oblike  $4k + 3$ .

---

<sup>3</sup>Seveda je vsem jasno, da govorimo o kvadratih naravnih števil.

<sup>4</sup>Namig : Vsako praštevilo različno od 2 in 3 se da zapisati kot  $6k + 1$  ali  $6k - 1$  za nek  $k \in \mathbb{N}$ .

## 3. FERMATOVA ŠTEVILA

**Definicija 3.1** (Fermatovo število). Naj bo  $m \in \mathbb{N}$ . *Fermatovo število* je število oblike  $F_m = 2^{2^m} + 1$ .

$$\begin{aligned} F_0 &= 2^{2^0} + 1 = 2^1 + 1 = 3 \\ F_1 &= 2^{2^1} + 1 = 2^2 + 1 = 5 \\ F_2 &= 2^{2^2} + 1 = 2^4 + 1 = 17 \\ F_3 &= 2^{2^3} + 1 = 2^8 + 1 = 257 \\ F_4 &= 2^{2^4} + 1 = 2^{16} + 1 = 65537 \\ F_5 &= 2^{2^5} + 1 = 2^{32} + 1 = 4294967297 = 641 \cdot 6700417 \end{aligned}$$

**Domneva 3.2.**  $F_m \notin \mathbb{P}$  za  $m \geq 5$

**Trditev 3.3.** 2 različni Fermatovi števili imata disjunktne (različne) prafaktorje.

Te trditve še ne znamo dokazati. Poizkusimo dokazati najprej malce lažji izrek (pomožni izrek se imenuje *lema*), ki nam bo prišel prav pri dokazu trditve ??.

**Lema 3.4.** Za Fermatova števila velja

$$\prod_{k=0}^{n-1} F_k = F_n - 2.$$

*Dokaz.* Dokazovali bomo s pomočjo indukcije. S pomočjo tabele zgoraj se prepričamo, da za  $m = 1$  trditev drži. Sedaj nastopi induksijski korak. Naša induksijska predpostavka bo, da trditev velja za  $m$ . Sedaj dokažimo, da trditev velja za  $m + 1$ .

$$\begin{aligned} \prod_{k=0}^m F_k &= \prod_{k=0}^{m-1} F_k \cdot F_m \\ &\stackrel{\text{I.P.}}{=} (F_m - 2) \cdot F_m \\ &= (2^{2^m} - 1) \cdot (2^{2^m} + 1) \\ &= (2^{2^m})^2 - 1 \\ &= 2^{2 \cdot 2^m} - 1 \\ &= 2^{2^{m+1}} - 1 \\ &= 2^{2^{m+1}} + 1 - 2 \\ &= F_{m+1} - 2 \end{aligned}$$

□

*Dokaz trditve ??.* Vzemimo različni naravni števili  $m, n$ . BŠŠ lahko predpostavimo da je  $n < m$ . Predpostavimo, da imata  $F_n$  in  $F_m$  skupnega delitelja  $d$ :  $d \mid F_n$  in  $d \mid F_m$ . Iz leme ?? sledi, da  $F_n \mid F_m - 2$ , kar nam pove, da  $d \mid F_m - 2$ . Če to zložimo skupaj ugotovimo, da  $d \mid 2$ . Ker sta  $F_n$  in  $F_m$  lihi, sledi  $d = 1$ . □

**Posledica 3.5.**  $\mathbb{P}$  je neskončna.

## 4. VRSTA RECIPROČNIH VREDNOSTI PRAŠTEVIL

Uredimo  $\mathbb{P}$ , da bo veljalo  $p_1 < p_2 < p_3 < \dots$

**Izrek 4.1.** *Vrsta*

$$\sum_{p \in \mathbb{P}} \frac{1}{p} = \sum_{m=1}^{\infty} \frac{1}{p_m}$$

*divergira.*

*Dokaz.* Uporabili bomo dejstvo, da v primeru, ko vrsta

$$\sum_{n=1}^{\infty} a_n$$

konvergira, obstaja indeks  $n_0$ , da velja

$$\sum_{n=n_0+1}^{\infty} a_n < \frac{1}{2}.$$

Denimo torej, da vrsta  $\sum_{m=1}^{\infty} \frac{1}{p_m}$  konvergira. Torej obstaja indeks  $k$ , da velja  $\sum_{m=k+1}^{\infty} \frac{1}{p_m} < 1/2$ .

Imejmo  $p_1, p_2, \dots, p_k$  za mala praštevila in ostala praštevila za velika.

Izberimo  $N \in \mathbb{N}$ . Označimo z  $N_s$  število naravnih števil manjših ali enakih od  $N$ , ki imajo v razcepu na prafaktorje le mala praštevila in z  $N_b$  število naravnih števil manjših ali enakih od  $N$ , ki imajo v razcepu na prafaktorje kakšno veliko praštevilo.

Očitno velja  $N = N_b + N_s$ .

Sedaj bomo ocenili velikost števil  $N_b$  in  $N_s$ .

1.  $N_s$ :

$n \in \mathbb{N}$ , ki ima same male prafaktorje se razpiše na  $n = p_1^{t_1} p_2^{t_2} \dots p_k^{t_k}$ . Tu lahko vse  $t_i$  razpišemo kot  $t_i = 2l_i + s_i$ , kjer je  $s_i \in \{0, 1\}$ . Sledi

$$n = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k} p_1^{2l_1} p_2^{2l_2} \dots p_k^{2l_k} = p_1^{s_1} p_2^{s_2} \dots p_k^{s_k} \left( p_1^{l_1} p_2^{l_2} \dots p_k^{l_k} \right)^2.$$

Označimo  $A := p_1^{l_1} p_2^{l_2} \dots p_k^{l_k}$  in  $B := p_1^{s_1} p_2^{s_2} \dots p_k^{s_k}$

Preštejmo možnosti za  $B$ : Vsak  $s_i$  ima 2 možnosti (0 ali 1s), kar skupaj nanese  $2^k$  možnosti.

Preštejmo možnosti za  $A$ : Ker mora veljati  $A^2 \leq n \leq N$  sledi, da velja  $A \leq \sqrt{N}$

Torej velja  $N_s \leq 2^k \sqrt{N}$ .

1.  $N_b$ :

$$N_b \leq \sum_{m \geq k+1}^* \left\lfloor \frac{N}{p_m} \right\rfloor \leq \sum_{m \geq k+1}^{\infty} \frac{N}{p_m} = N \sum_{m \geq k+1}^{\infty} \frac{1}{p_m} < \frac{N}{2}$$

\*: Izraz na desni prešteje koliko števil manjših ali enakih  $N$  je deljivih s posameznim praštevilo.

Sedaj še izberimo  $N = 2^{2k+2}$  in poiščimo protislovje.

$$N = N_b + N_s < N/2 + 2^k \sqrt{N} = 2^{2k+1} + 2^k 2^{k+1} = 2 \cdot 2^{2k+1} = 2^{2k+2} = N$$

$$N < N \rightarrow \leftarrow$$

□

## 5. PRAŠTEVILSKI DVOJČKI

**Definicija 5.1.** Števili  $p$  in  $p+2$  sta *praštevilski dvojček*, če velja  $p \in \mathbb{P}$  in  $p+2 \in \mathbb{P}$ .

**Odprt problem 5.2.** Praštevilskih dvojčkov je neskončno.

**Opomba 5.3.** Števili  $p$  in  $p+2$  morata biti oblike  $6k-1$  in  $6k+1$ . Edini izjemi sta 3 in 5.

**Izrek 5.4** (Brunov izrek). *Vrsta*

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

*konvergira in njena vsota je približno enaka 2.*

**Definicija 5.5.** Naj bo  $x \in \mathbb{R}$ .  $\pi_2(x) = \{p \in \mathbb{P} \mid p \leq x, p+2 \in \mathbb{P}\}$ .

## 6. KARAKTERIZACIJA PRAŠTEVIL IN PRAŠTEVILSKIH DVOJČKOV

**Izrek 6.1** (Wilsonov izrek). *Naj bo  $m \in \mathbb{N}$  in  $m \neq 1$ .  $m$  je praštevilo natanko tedaj, ko je  $(m-1)! \equiv -1 \pmod{m}$ .*

*Dokaz.* Denimo, da  $m$  ni praštevilo. Torej se razpiše kot  $m = a \cdot b$ . Če sta  $a$  in  $b$  različni števili velja  $(m-1)! \equiv 0 \pmod{m}$ . V primeru ko sta  $a$  in  $b$  enaka ločimo še dve možnosti. če  $a$  in  $b$  nista praštevili lahko pišemo  $m = a_1 \cdot b_1$ , kjer sta  $a_1$  in  $b_1$  različna. V primeru ko sta  $a$  in  $b$  enaki praštevili bomo uporabili dejstvo, da je  $2p < p^2$ .  $p$  in  $2p$  nastopata v  $(m-1)!$  torej je  $(m-1)! \equiv 0 \pmod{m}$ . Primer ko je  $m = 4$  preverimo na roke.

Denimo, da je  $m$  praštevilo. V  $\mathbb{Z}_m$  imajo vsi elementi enolično določen inverz. Kateri elementi so sami sebi inverz? Enačba  $a^2 = 1$  ima v  $\mathbb{Z}_m$  rešitve  $a = 1$  in  $a = -1 = m-1$ . V  $(m-1)!$  se torej izničijo vsi faktorji razen  $m-1$ , ki pa je kongruenten  $-1$ .  $\square$

**Izrek 6.2** (Karakterizacija praštevilskih dvojčkov). *Par  $m, m+2$  je praštevilski dvojček natanko tedaj, ko je  $4((m-1)! + 1) + m \equiv 0 \pmod{m(m+2)}$ .*

## 7. PORAZDELITEV PRAŠTEVIL IN PRAŠTEVILSKIH DVOJČKOV

**Izrek 7.1.** *Za  $x \in \mathbb{R}$  velja*

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

*Oziroma  $\pi(x) \approx \frac{x}{\log(x)}$*

**Opomba 7.2.** V tem besedilu razumemo  $\log(x)$  kot naravni logaritem.

**Izrek 7.3.** *Za  $x \in \mathbb{R}$  velja  $\pi_2(x) \approx \frac{x}{\log(x)^2}$*

**Izrek 7.4.**



## 8. GOLDBACHOVA DOMNEVA IN NEMOGOČI PROBLEM

Kot smo navedli na začetku, se da vsako število, ki je večje od 1 in ni praštevilo zapisati kot produkt praštevil. Vprašanje, ki si ga lahko zastavimo, je slednje: Ali se da vsako število zapisati kot vsota praštevil? Prav gotovo, če se ne oziramo na število sumandov:

$$100 = 2 + 2 + \dots + 2.$$

Tu je v vsoti kar 50 seštevancev. Opazimo, da je vsako sodo število vsota samih dvojk, liho pa vsota trojke in dvojk. Število 100 pa lahko izrazimo tudi takole:

$$100 = 3 + 97 = 11 + 89 = 17 + 83 = 29 + 71 = 41 + 59 = 47 + 53.$$

Vsi sumandi na desni so praštevila. Torej se da 100 zapisati kot vsota dveh praštevil, in sicer kar na šest načinov. Poglejmo, kako je pri najmanjših sodih številih:

$$4 = 2 + 2$$

$$6 = 3 + 3$$

$$8 = 5 + 3$$

$$10 = 5 + 3 = 3 + 7$$

$$12 = 5 + 7$$

Kaj hitro se prepričamo tudi o nadaljnjih neprevelikih sodih številih 12, 14, 16, 18, ..., da se izražajo kot vsota dveh praštevil. Zato se nam upravičeno vsiljuje naslednja domneva.

**Domneva 8.1** (Goldbachova domneva). Vsako sodo število  $\geq 4$  se da zapisati vsaj na en način kot vsota dveh praštevil.

Če nadaljujemo z našo radovednostjo, je očitno naslednje vprašanje: Kaj lahko povemo o lihih številih in vsotah praštevil.

**Domneva 8.2** (Šibka Goldbachova domneva). Vsako število  $\geq 7$  se da zapisati vsaj na en način kot vsota treh praštevil.

**Opomba 8.3.** Iz Goldbachove domneve sledi šibka Goldbachova domneva, narobe pa ne velja.

**Nemogoč problem 8.4.** Peter je izbral dve naravni števili večji od 1. Vsoto teh števil je povedal prijatelju Tonetu, produkt pa Mirku. Tone si ogleda vsoto in telefonira Mirku:

”Ne vidim možnosti, kako bi ti lahko ugotovil vsoto.”

Čez nekaj časa odgovori Mirko:

”Imaš prav. Ne morem določiti vsote.”

Kmalu nato se spet oglasi Tone:

” Vem, kolikšen je produkt.”

Kateri števili je izbral Pete?

*Rešitev.* Imenujmo izbrani naravni števili  $x$  in  $y$ , vsota  $x + y$  naj bo  $V$ , produkt  $xy$  pa  $P$ . Ker sta  $x$  in  $y$  večja od 1, je  $P$  produkt najmanj dveh praštevil. Mirko, ki je poznal  $P$ , je  $P$  razstavil na prafaktorje. Vsoto bi takoj našel, če bi bil  $P$  produkt samo dveh praštevil. Recimo, da bi bilo  $P = 15 = 3 \cdot 5$ . V tem primeru bi Peter izbral števili 3 in 5, vsota pa bi bila 8. Mirko ni mogel določiti vsote zato, ker je  $P$  produkt najmanj treh praštevil. Kako je Tone to vedel? Ogledal si je vsoto  $V$



$n = 1$ . Teda je  $V = 11$  piemolahkan  $V = 11 = 2 + 9 = 3 + 8 = 4 + 7 = 5 + 6$ . Pripadajo produkti  $2 \cdot 9 = 18, 3 \cdot 8 = 24, 4 \cdot 7 = 28$  in  $5 \cdot 6 = 30$ . Ugotovimo, da se da 11 samo na en način zapisati kot vsota  $x + y$  tako, da sumanda  $x$  in  $y$  zadoščata pogoju (iii) namreč 11 je  $5 + 6$ . Torej ima  $V = 11$  tudi lastnost (iv). Iz povedane je razvidno, da edino števili 5 in 6 z vsoto  $V = 11$  in produktom  $P = 30$  zadoščata pogojem (i) do (iv).

## 9. ŠE NEKAJ IZREKOV

**Izrek 9.1** (Dirichlet). . Naj bosta  $a$  in  $b$  tuji si naravni števili. V zaporedju

$$a + b, 2a + b, 3a + b, \dots = \{ak + b \mid k \in \mathbb{N}\}$$

je neskončno praštevil.

**Izrek 9.2** (Bertrand, Čebišev). Za vsako naravno število  $n > 1$  obstaja  $p \in \mathbb{P}$ , za katerega velja  $n < p < 2n$ .

**Izrek 9.3** (mali Fermatov izrek). Naj bo  $p \in \mathbb{P}$ . Za vsako celo število  $a$ , ki je tuje  $p$ , velja

$$a^{p-1} \equiv 1 \pmod{p}.$$

LUKA PONIKVAR, FAKULTETA ZA MATEMATIKO IN FIZIKO, JADRANSKA 19, 1000 LJUBLJANA, SLOVENIJA

Email address: luka.ponikvar1@gmail.com