Konstrukcije v teoriji števil

Jan Pantner (jan.pantner@gmail.com)

30. oktober 2025

Kazalo

Uvod **3**

1 Praštevila **4**

2 Razne konstrukcijske ideje **7**
2.1 Optimistično razmišljanje 7
2.2 Indukcija 8
2.3 Pellova enačba 9

Literatura **10**

Uvod

Zapiski so nastali kot dodatek k predavanju, ki sem ga imel 23. novembra. 2022 v okviru priprav na mednarodna matematična tekmovanja v šolskem letu 2022/2023 in vsebujejo rešitve nekaterih nalog. V prihodnjih letih so bili rahlo posodobljeni.

Za razumevanje zapiskov je potrebno poznati indukcijo in osnove teorije števil. Pogledamo si nekaj uporabnih strategij za reševanje konstrukcijskih nalog. V prvem delu je na primerih prikazano kako lahko uporabimo lastnosti praštevil, v drugem delu pa je prikazanih še nekaj drugih uporabnih strategij.

Bralcu predlagam, da, preden prebere rešitev katerekoli naloge, najprej poskusi nalogo rešiti sam. Enako velja tudi za dokaze trditev in izrekov.

V primeru kakšne dileme oziroma vprašanja me lahko brez oklevanja kontaktirate na jan.pantner@gmail.com. Zelo verjetno se v zapiskih nahaja tudi kakšna napaka. Če jo opazite, prosim, da mi to sporočite.

1 Praštevila

Praštevila so pogosto ključnega pomena pri reševanju nalog, povezanih s teorijo števil. V tem razdelku si bomo pogledali nekaj njihovih lastnosti in kako jih lahko uporabimo pri tvorjenju konstrukcij.

Naloga 1.1

Dokažite, da je praštevil neskončno mnogo.

Dokaz. Predpostavimo, da je praštevil končno. Naj bodo $p_1, \ldots, p_n$ vsa praštevila. Poglejmo si število

$$N = \prod_{i=1}^{n} p_i + 1.$$

Število N ni deljivo z nobenim od $p_1, \ldots, p_n$, torej obstaja neko drugo praštevilo, ki deli N, kar pa je v protislovju s tem, da so $p_1, \ldots, p_n$ vsa praštevila. □

Praštevil je torej neskončno mnogo. Zgornjo konstrukcijo je prvi opisal Evklid že približno tri stoletja pred našim štetjem.

Naloga 1.2

Naj bo n naravno število. Dokažite, da obstaja n zaporednih sestavljenih števil.

Rešitev. Ključna ideja je, da razmišljamo o fakultetah, saj v bistvu vsebujejo n zaporednih naravnih števil. Torej, za $i < n$ je število $n! + i$ deljivo z i. Če je $i > 1$, potem $n! + i$ očitno ne more biti praštevilo.

Mogoče bi kdo naprej pomislil, da je rešitev $n! + 1, n! + 2, \ldots n! + n$, vendar to ni nujno res, saj je lahko $n! + 1$ praštevilo (npr. $3! + 1$). S to konstrukcijo smo torej dokazali samo obstoj $n - 1$ zaporednih sestavljenih števil. To lahko brez večjega problema popravimo, če vzamemo $(n + 1)! + 2, \ldots, (n + 1)! + n + 1$. □

Naloga nam med drugim pove nekaj o redkosti praštevil, in sicer da je razlika med zaporednima praštevilomi lahko poljubno velika.

Enostavno se je prepričati tudi, da so vsa praštevila, z izjemo 2 in 3, oblike $6k \pm 1$ za neko naravno število k. Bolj zanimivi vprašanji sta, če je praštevil oblike $6k - 1$ in oblike $6l + 1$ enako, in ali obstaja neskončno praštevilskih dvojčkov, to je takšnih praštevil p, da je tudi $p + 2$ praštevilo. Odgovor na prvo vprašanje nam bo podal Dirichletov izrek, drugo vprašanje pa je že vrsto let eno od velikih odprtih vprašanj v teoriji števil, znano kot domneva o praštevilskih dvojčkih.

Naloga 1.3

Naj bo n naravno število. Dokaži, da obstaja $k \in \mathbb{N}$, da za vsak $m \geq k$ velja, da obstaja m zaporednih naravnih števil med katerimi je natanko n praštevil.

Rešitev. Prepuščena bralcu. □

Izrek 1.4: Dirichlet

Naj bosta n in m tuji si naravni števili. Aritmetično zaporedje $(an+b)_{n=0}^{\infty}$ vsebuje neskončno mnogo praštevil.

Dokaz zgornjega izreka presega nivo, ki je predviden na srednješolskih tekmovanjih, v njem so na primer uporabljene Dirichletove L-funkcije. Na tekmovanjih lahko trdimo, da je izrek splošno znan. Poglejmo si primer uporabe.

Naloga 1.5

Naj bosta a in b naravni števili. Pokažite, da obstaja neskončno mnogo naravnih števil n, ki jih ni mogoče zapisati kot $3ab+a+b$.

Rešitev. Iščemo takšna naravna števila n, da enačba $n = 3ab+a+b$ nima rešitve.

Takšne enačbe se pogosto splača faktorizirati. V tem primeru lahko uporabimo znan trik in dobimo

$$n = 3ab+a+b \iff 3n+1 = (3a+1)(3b+1).$$

Ker sta a in b naravni števili, sta oba oklepaja na desni strani enačbe večja od 1. Torej je leva stran, to je $3n+1$, sestavljeno število. To pomeni, da če bi bilo $3n+1$ praštevilo, enačba ne bi imela rešitve.

Dirichletov izrek nam pove, da v zaporedju $(3n+1)_{n=0}^{\infty}$ obstaja neskončno mnogo praštevil, torej obstaja neskončno mnogo n-jev, ki jih ne moremo zapisati v obliki $3ab+a+b$, kjer sta a in b naravni števili. □

Naloga 1.6

Ali obstaja takšna neskončna množica naravnih števil, da vsota poljubnih nekaj njenih elementov ni popolna potenca?

Število je popolna potenca, kadar so v njegovem praštevilskem razcepu vsi eksponenti enaki. Iščemo torej števila, ki imajo različne eksponente v praštevilskem razcepu. Najenostavnejši primer takšnega števila je $p^k q^{k+1}$, kjer sta p ter q praštevili in k naravno število.

Rešitev. Odgovor je pritrdilen. Poglejmo si množico $\{2^n \cdot 3^{n+1} \mid n \in \mathbb{N}\}$. Vsota nekaj elementov iz te množice bo vedno oblike $2^x 3^{x+1} \cdot Y$, kjer je število Y tuje številu 6. To ni popolna potenca, saj sta v praštevilskem razcepu eksponenta od 2 in od 3 različna. □

Naloga 1.7: RMM 2015/1

Ali obstaja zaporedje naravnih števil $(a_n)_{n=1}^{\infty}$, v katerem sta elementa zaporedja a_n in a_m tuja natanko tedaj, kadar $|m-n|=1$?

Rešitev. Števili sta si tuji natanko tedaj, kadar nimata skupnega praštevilskega faktorja. To dejstvo bo naša glavna motivacija.

Predstavljajmo si števila kot (multi)množice njihovih praštevilskih deliteljev (na primer $42 = 2 \cdot 3 \cdot 7 \mapsto \{2,3,7\}$). Iščemo torej zaporedje množic praštevil (P_n), kjer velja $P_i \cap P_j = \emptyset$ natanko tedaj, kadar sta i in j zaporedni naravni števili.

Recimo, da določimo $P_1 = \{2\}$. Potem lahko določimo $P_2 = \{3\}$. Sedaj mora slediti $2 \in P_3$ in $2 \in P_4$, vendar potem $P_3 \cap P_4 \neq \emptyset$. Torej mora P_1 vsebovati vsaj dva elementa. Še več, to nas motivira, da na vsakem koraku dodamo dva nova elementa (torej praštevili, ki se še nista pojavili).

Določimo torej $P_1 = \{2,3\}$ in $P_2 = \{5,7\}$. Potem lahko določimo $P_3 = \{2,11,13\}$ in $P_4 = \{3,5,17,19\}$. Zdaj lahko, ker $2,7,11 \notin P_4$, za P_5 vzamemo 2 iz P_1, 7 iz P_2 in 11 iz P_3, torej imamo $P_5 = \{2,7,11,24,29\}$. Torej v množice, ki sledijo P_3, alternativno dodajamo 2 in 3, podobno v množice, ki sledijo P_4, alternativno dodajamo 5 in 7. Idejo lahko predstavimo s sledečo tabelo.

	P_1	P_2	P_3	P_4	P_5	P_6	P_7	
iz $\mathbb{P}$	$2,3$	$5,7$	$11,13$	$17,19$	$23,29$	$31,37$	$47,53$	
iz P_1			2	3	2	3	2	
iz P_2				5	7	5	7	$\cdots$
iz P_3					11	13	11	
iz P_4						17	19	
$\vdots$							$\ddots$	

Ker je praštevil neskončno mnogo, takšna konstrukcija res obstaja, niti se ni težko prepričati, da res ustreza pogojem naloge. □

2 Razne konstrukcijske ideje

2.1 Optimistično razmišljanje

Naloga 2.1

Naj bosta a in b različni naravni števili, večji od 1.

1. Najdite neskončno mnogo parov (a, b), da ab deli $a^2 + b^2 - 1$.
2. Določite vse celoštevilske vrednosti, ki jih lahko zavzame izraz

$$\frac{a^2 + b^2 - 1}{ab}.$$

Rešitev. Če za začetek pogledamo primer $n = 2$, dobimo $2b \mid b^2 - 3$ in opazimo, da $b = 3$ ustreza pogoju. Še več, če pogledamo po modulu b, dobimo, da je $b = 3$ celo edina rešitev za ta primer.

Če smo po srcu optimisti in se zavedamo, da je $b = 3 = 2 + 1 = a + 1$, lahko pomislimo, da mogoče par $(a, a + 1)$ ustreza tudi v splošnem. Izkaže se, da je to res, saj velja

$$a^2 + b^2 - 1 = a^2 + (a + 1)^2 - 1 = 2a^2 + 2a = 2a(a + 1) \equiv 0 \pmod{a(a + 1)}.$$

Torej smo našli neskončno mnogo parov (a, b), da ab deli $a^2 + b^2 - 1$. Optimizem se je res izplačal!

Za drugi del naloge uganemo, da je možna vrednost vsako naravno število. Ker sta imenovalec in števec vedno pozitivna, ni mogoče dobiti nepozitivnih celih števil.

Najprej lahko poskusimo razširiti zgornjo konstrukcijo v $(a, b) = (a, a + k)$. Enostavno lahko preverimo, da to ne deluje. Zakaj ne?

V zgornjem primeru, $k = 1$, se je k okrajšal z -1 iz izraza $a^2 + b^2 - 1$. To nas motivira, da mogoče poskusimo $(a, b) = (a, ka - 1)$. Dobimo

$$\frac{a^2 + (ka - 1)^2 - 1}{a(ka - 1)} = \frac{(k^2 + 1)a - 2k}{ka - 1} = k + \frac{a - k}{ka - 1}.$$

Želimo, da bi $ka - 1$ delilo $a - k$. Najenostavnejša stvar, ki jo lahko naredimo, je da poskusimo $a - k = 0$. Preverimo, da to res deluje. Imamo konstrukcijo $(a, b) = (k, k^2 - 1)$, ki nam pokaže, da lahko dobimo poljubno naravno število. □

Nauk zgornje naloge je, da se včasih splača preizkusiti tudi najpreprostejše vzorce. Če nek vzorec deluje v prvem primeru in spodleti v drugem, poskusite ugotoviti, kako se primera razlikujeta in razumeti, zakaj je prišlo do napake. Potem obstaja solidna možnost, da lahko napako odpravite (tako kot smo rešitev prvega dela zgornje naloge prilagodili, da je rešila tudi drugi del).

Seveda pa v splošnem na žalost ni nikakršne garancije, da nas bo takšno poskušanje pripeljalo do rešitve, ampak še vedno se pogosto splača poskusiti!

Naloga 2.2: IMO Shortlist 2014 N4

Naj bo $n > 1$ naravno število. Dokažite, da obstaja neskončno mnogo celih števil $k \geq 1$, da je število

$$\left\lfloor \frac{n^k}{k} \right\rfloor$$

liho.

Rešitev. Če je n liho, lahko preprosto vzamemo $k = n^t$ za poljuben $k \in \mathbb{N}$.

Bolj zanimiv je primer, ko je n sodo število. Poglejmo najprej $n = 2$. Če eksperimentiramo z majhnimi k-ji, ugotovimo, da je 12 najmanjše število, ki zadošča. Ker je $12 = 2^2 \cdot 3$, pomislimo na $k = n^2(n+1)$. Dobimo

$$N = \left\lfloor \frac{n^{n^2(n+1)}}{n^2(n+1)} \right\rfloor = \left\lfloor \frac{n^{n^2(n+1)-2}}{n+1} \right\rfloor = \frac{n^{n^2(n+1)-2} - 1}{n+1},$$

kjer zadnja enakost sledi, ker velja

$$n^{n^2(n+1)-2} \equiv (-1)^{n^2(n+1)-2} \equiv 1 \pmod{n+1}. \qquad \heartsuit$$

Ker sta imenovalec in števec liha, je N liho.

Našli smo število, ki zadošča za vsak sodi n. Kako jih dobimo neskončno mnogo? Opazimo, da enačba $\heartsuit$ drži tudi, če 2 zamenjamo s poljubnim sodim številom. Torej, če vzamemo $k = n^{2t}(n+1)$, dobimo

$$\left\lfloor \frac{n^{n^{2t}(n+1)}}{n^{2t}(n+1)} \right\rfloor = \left\lfloor \frac{n^{n^{2t}(n+1)-2t}}{n+1} \right\rfloor = \frac{n^{n^{2t}(n+1)-2t} - 1}{n+1},$$

ki je še vedno liho. Torej imamo, za poljubni $k \in \mathbb{N}$ in za sod n, konstrukcijo $k = n^{2t}(n+1)$. $\square$

2.2 Indukcija

Indukcija je pogosto enostaven način za tvorjenje konstrukcij. Recimo, da imamo konstrukcijo za n, potem je mogoče, da ji lahko samo nekaj dodamo in dobimo konstrukcijo za $n+1$.

Naloga 2.3: USAMO 2003/1

Naj bo n naravno število. Dokažite, da obstaja n-mestno število, deljivo s 5^n, ki ima same lihe števke.

Rešitev. Če pogledamo primere za prvih nekaj naravnih števil, lahko hitro najdemo sledeče konstrukcije:

Na tej točki opazimo, da smo pri prehodu na naslednje konstrukcije v bistvu samo dodajali eno števko na začetek prešnje. To nam namigne, da bi nalogo lahko mogoče rešili z indukcijo.

n	konstrukcija
1	5
2	75
3	375
4	9375

Predpostavimo, da obstaja število X_n, ki ima natanko n števk, ki so vse lihe, in velja $5^n \mid X_n$. Iščemo liho števko Y, za katero velja $5^{n+1} \mid Y \cdot 10^n + X_n$. Ta pogoj je ekvivalenten pogoju $5 \mid Y \cdot 2^n + \frac{X_n}{5_n}$ oziroma

$$Y \cdot 2^n + \frac{X_n}{5^n} \equiv 0 \pmod 5.$$

Torej lahko preprosto vzamemo

$$Y \equiv (2^n)^{-1} \frac{-X_n}{5^n} \pmod 5.$$

To nam sicer še ne zagotovi, da je Y liha števka, vendar ji lahko v primeru, da je soda, enostavno prištejemo 5 in postane liha. □

2.3 Pellova enačba

Komur Pellova enačba še ni poznana, si lahko o njej prebere v [2, Poglavje 4.8]. Tukaj bomo uporabili samo osnovna dejstva.

Naloga 2.4

Najdite neskončno mnogo trojic (a, b, c) naravnih števil, kjer so a, b in c zaporedni členi aritmetičnega zaporedja in kjer so števila $ab+1$, $bc+1$ in $ca+1$ popolni kvadrati.

Ker so a, b, c zaporedni členi aritmetičnega zaporedja, uporabimo substitucijo $(a, b, c) \mapsto (x - d, x, x + d)$. Pogoj o popolnih kvadratih se potem glasi

$$\begin{aligned} x^2 - xd + 1 &= X^2, \\ x^2 + xd + 1 &= Y^2, \\ x^2 - d^2 + 1 &= Z^2. \end{aligned}$$

Leve strani želimo zapisati kot kvadrate. Poskusimo z $x \mapsto 2w$ in dobimo

$$\begin{aligned} 4w^2 - 2wd + 1 &= (w - d)^2 + 3w^2 + d^2 + 1, \\ 4w^2 + 2wd + 1 &= (w + d)^2 + 3w^2 + d^2 + 1, \\ 4w^2 - d^2 + 1 &= w^2 + wu^2 - d^2 + 1, \end{aligned}$$

kjer nam je člen $-2wd$ bil motivacija, da smo prvi člen napisali v obliki $(w - d)^2 + \ldots$ in podobno drugi člen. Potem pa smo opazili, da se odvečni skupni člen prvih dveh enačb

pojavi tudi v tretji. Optimistično nastavimo $3w^2 - d^2 + 1 = 0$. Če nam to uspe za neskončno mnogo parov (w, d), smo končali. Slednje nam garantira Pellova enačba.

Torej, naša konstrukcija je, da izberemo poljubna (w, d), da velja $w^2 - 3u^2 = 1$ in potem $(a, b, c) = (2u - v, 2u, 2u + v)$.

Naloga 2.5

Pokažite, da obstaja neskončno mnogo naravnih števil n, da je $n!$ deljivo z $n^2 + 1$.

Glavna ideja je, da določimo $n^2+1 = dm^2$ in zagotovimo $dm^2 \mid n!$, saj smo potem končali. Motivacija za takšen pristop je, da je lažje gledati deljivost s produktom kot deljivost z vsoto.

Imamo torej negativno Pellovo enačbo $n^2 - dm^2 = -1$, za katero vemo, da, če ima eno rešitev, jih ima neskončno mnogo. Izberemo takšen d, da zagotovimo rešitve. Hitro lahko najdemo primer $2^2 - 5 \cdot 1^2 = -1$, torej $d = 5$ ustreza.

Če bi želeli $5m^2 \mid n!$, bi lahko naivno poskusili dokazati $n > 5m^2$, kar pa žal ni res. Zadošča pa, da najdemo dva večkratnika m, ki sta manjša od n, ker potem $m^2 \mid n!$ in, ker obstaja neskončno rešitev lahko zagotovimo $n > 5$. Očitno $m, 2m < \sqrt{5} \cdot m = \sqrt{n^2 + 1} < n + 1$, torej $m, 2m \leq n$, kar smo želeli.

Literatura

[1] Cody Johnson. *Constructions*. 2016. URL: https://www.math.cmu.edu/~ctj/Articles/constructions.pdf (pridobljeno 21. 10. 2022).

[2] Aditya Khurmi. *Modern Olympiad Number Theory*. 2020. Pogl. 9, str. 233–254. URL: https://www.academia.edu/44512122/Modern_Olympiad_Number_Theory.