

PRESEK

List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652

Letnik **16** (1988/1989)

Številka 2

Strani 82-89, 117

Boris Lavrič:

O PRAŠTEVILIH

Ključne besede: matematika, teorija števil, praštevila.

Elektronska verzija: <http://www.presek.si/16/928-Lavric.pdf>

© 1988 Društvo matematikov, fizikov in astronomov Slovenije

© 2010 DMFA - založništvo

Vse pravice pridržane. Razmnoževanje ali reproduciranje celote ali posameznih delov brez poprejšnjega dovoljenja založnika ni dovoljeno.

O PRAŠTEVILIH

Dogovorimo se, da bomo tu z besedo število razumeli naravno število, torej element množice $\mathbb{N} = \{1, 2, 3, \dots\}$. Ukvarjali se bomo namreč le z naravnimi števili. Brž ko želimo bolje spoznati njihove lastnosti, se srečamo s pomembno družino števil, ki jim rečemo praštevila. Zanje je značilno, da imajo v množici $\mathbb{N}$ natanko po dva delitelja. Število n je torej praštevilo, če je večje od 1 in ni produkt dveh od 1 različnih števil. Druga števila, razen 1, tedaj lahko razstavimo v produkt z manjšima faktorjema in jih zato imenujemo sestavljena števila. Z zaporednim razstavljanjem faktorjev v produkt, če je to potrebno, pridemo do naslednje znane in pomembne ugotovitve:

Vsako naravno število razen števila 1 je produkt samih praštevil.

Dognali bi lahko celo to, da je takšna razstavitev le ena, če ne gledamo na vrstni red faktorjev v njej.

Praštevila so potemtaka osnovni sestavni deli vsakega naravnega števila, zato jim namenimo nekaj več pozornosti.

Zapišimo po velikosti nekaj najmanjših zaporednih praštevil:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, ...

in se za hip pomudimo ob vprašanju, ali je vseh praštevil končno mnogo ali ne. Že znameniti grški matematik *Evklid* se je ubadal s tem problemom in ga tudi rešil. Dokazal je, da je praštevil brez konca, in to tako mojstrsko utemeljil, da bomo ponovili njegov dokaz. Takole teče:

Denimo, da so 2, 3, 5, ..., p zaporedna praštevila, in postavimo $n = 2 \cdot 3 \cdot 5 \cdots p + 1$. Potem n očitno ni deljiv z nobenim od praštevil 2, 3, 5, ..., p . Zato je n bodisi praštevilo ali pa je deljiv s praštevilom, ki je večje od p . V obeh primerih obstaja praštevilo, večje od p , torej praštevil ni končno mnogo.

Veliko težje je zvedeti kaj več o gostoti porazdelitve praštevil v zaporedju vseh naravnih števil. Kljub temu poznamo nekaj pomembnih rezultatov v tej smeri, med katerimi je zelo lep naslednji.

IZREK: Naj bo naravno število n večje od 1. Potem med n in $2n$ obstaja vsaj eno praštevilo.

Dokaz je prezahteven za naš list, iznašel pa ga je ruski matematik *P.L. Čebišev* leta 1850, to je pet let po tem, ko je francoski matematik *J. Bertrand* postavil domnevo, da navedeni izrek velja. Danes vemo, da za $n > 5$ med n in $2n$ obstajata vsaj dve praštevili.

Za svoja dela je Čebišev žel priznanja doma in v tujini, bil je član več akademij, v Franciji pa tudi vitez Legije časti. Med obiski v Parizu je večkrat predaval v Association Française pour l'avancement des sciences. Eno njegovih predavanj, *O krojenju oblek*, je privabilo res številno in, lahko si mislimo, izbrano poslušalstvo, snovalce in nosilce modnih krikov. Po prvem stavku so se kot en mož dvignili in zapustili dvorano. Čebišev je predavanje začel takole: Zaradi enostavnosti privzemimo, da ima človeško telo obliko krogle. V resnici je šlo za nalogo iz diferencialne geometrije, kako iz kosa ravnine (blaga) napraviti lupino, ki se bo najbolje prilegala danemu telesu.

Anekdotno smo prepisali iz Križaničeve knjige *Nihalo, prostor in delci*, Slovenska Matica (1982).

Ozrimo se spet na zaporedje vseh praštevil. Hitro opazimo, da si praštevila ne slede enakomerno. Z izjemo para 2, 3 je razlika med sosednjima prašteviloma tega zaporedja vedno sodo število, saj so vsa od 2 različna praštevila liha. Že na kratkem odseku zaporedja vseh praštevil najdemo sosednji praštevili, ki se razlikujeta za 2, 4, 6 ali 8, te razlike pa so neenakomerno posejane. Ponujata se naslednji vprašanji:

1. Kako na preprost način najti vsa praštevila, manjša od danega števila n ?
2. Ali so razlike med sosednjimi praštevili lahko poljubno velike?

Zanimivo je odgovoril na prvo vprašanje grški astronom *Eratosten(es)* že pred približno dva tisoč leti. Stopimo po njegovi poti.

Naravna števila od 2 do n razvrstimo po velikosti v naraščajoče zaporedje in najprej obkrožimo praštevilo 2 ter prečrtamo vse druge večkratnike števila 2. Najmanjše neoznačeno število je zdaj praštevilo 3. Zato obkrožimo 3 in prečrtamo vse tiste njegove večkratnike, ki še niso prečrtani ali obkroženi. Najmanjše neoznačeno število je zdaj praštevilo 5, ki ga obkrožimo in nato prečrtamo vse njegove večje večkratnike. Če nadaljujemo na enak način, bomo obkrožili natanko vsa praštevila do n .

Pravkar opisani postopek imenujemo *Eratostenovo rešeto*. Ni težko videti, da seje precej hitro — brž ko smo obkrožili prvo praštevilo, ki presega $\sqrt{n}$, nam ostanejo neoznačena v zaporedju le še praštevila.

Enostavno konstrukcijo Eratostenovega rešeta, posebno pripravno za praštevila do 120, najdemo v eni od Gardnerjevih knjig iz rekreacijske matematike.

Števila od 1 do 120 zapišemo v pravokotno tabelo 20×6 , kot kaže slika. Nato pri sejanju upoštevamo, da soda števila ležijo v drugem, četrtem in šestem stolpcu, večkratniku števila tri v tretjem (in šestem), petkratniki na vsaki peti "naraščajoči" diagonali, večkratniki števila 7 pa na vsaki sedmi "padajoči"

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
61	62	63	64	65	66
67	68	69	70	71	72
73	74	75	76	77	78
79	80	81	82	83	84
85	86	87	88	89	90
91	92	93	94	95	96
97	98	99	100	101	102
103	104	105	106	107	108
109	110	111	112	113	114
115	116	117	118	119	120



diagonalni, začeniši z drugo. V nekaj potezih nam tako na rešetki ostanejo natančno vsa praštevila, manjša od 127.

Matematik S. Ulam si je na nekem dolgem sestanku preganjal dolgčas s tem, da je na list narisal kvadratno mrežo in vanjo razvrščal po spirali zaporedna naravna števila podobno kot na sliki 1. Nato se je pozabaval z obkroževanjem vseh vpisanih praštevil in presenečen opazil, da se večinoma nahajajo vzdolž nekaterih diagonalnih premic. Blizu središča ta lastnost še ni tako izrazita kot dlje od njega, kjer se tudi ohranja. Ulam je s pomočjo računalnika in znane tabele praštevil uspel v laboratoriju izdelati sliko spirale, na kateri je

prvih 65 000 naravnih števil. Izsek tega vzorca, ki ga imenujemo *Ulamov prt*, je na sliki 2.

65	64	63	62	61	60	59	58	57
66	37	36	35	34	33	32	31	56
67	38	17	16	15	14	13	30	55
68	39	18	5	4	3	12	29	54
69	40	19	6	1	2	11	28	53
70	41	20	7	8	9	10	27	52
71	42	21	22	23	24	25	26	51
72	43	44	45	46	47	48	49	50
73	74	75	76	77	78	79	80	81

Slika 1



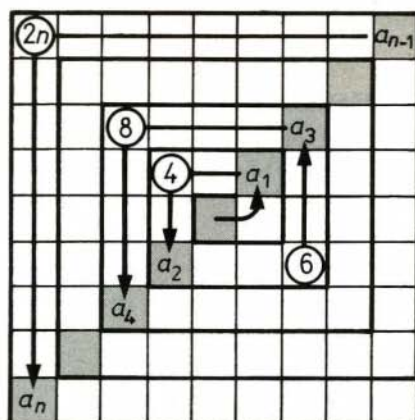
Slika 2

Števila na diagonali prta lahko izrazimo s preprosto formulo, ki jo dobimo takole. Krenimo po spiralni poti iz sredine. Prvo število, ki ga srečamo na "naraščajoči" glavni diagonali, zaznamujmo z a_1 , naslednje z a_2 in tako nadaljujmo (torej je $a_1 = 3$, $a_2 = 7$, $a_3 = 13$, ...). Od središča do a_1 smo napravili en ovinek in prešli dve polji, od a_1 do a_2 smo spet enkrat zavili in prešli štiri polja, nato pa smo od a_2 do a_3 potrebovali šest polj, od a_{n-1} do a_n pa je tedaj pot dolga $2n$ kvadratov. Torej velja zveza $a_n = a_{n-1} + 2n$. Če jo zaporedoma uporabimo za $n, n-1, n-2, \dots$, dobimo:

$$\begin{aligned} a_n &= a_{n-1} + 2n = a_{n-2} + 2(n-1) + 2n = \dots \\ &= a_1 + 2(2 + 3 + \dots + n) = n^2 + n + 1 \end{aligned}$$

in formula je tu: $a_n = n^2 + n + 1$.

Če namesto z 1 v sredini začnemo z m , za števila na diagonali dobimo formulo $a_n = n^2 + n + m$. Pri $m = 17$ in pri $m = 41$ dobimo dve izmed mnogih "formul za praštevila", ki jih je že v 18. stoletju odkril veliki švicarski matematik *Leonhard Euler*. Prva da praštevila za vsak $n \in \{0, 1, 2, \dots, 15\}$, druga (ki je najbolj znana) pa celo za vsak $n \in \{0, 1, \dots, 39\}$. To pomeni, da je diagonala kvadrata velikosti 40×40 na Ulamovem prt, ki se začne v sredini z 41, v celoti zapolnjena s praštevili.



			293								283	281
			233			229	227			223		
				181	179					173		
	239		139	137					131			
			103	101			97			277		
	241				73	71						
			107			53						
			79		43			127				
		191	109	59	41				167			
				47		67						
307	193			61							271	
		149	83			89						
			113					163	269			
		151			157				211			
311	197	199										
	251			257				263				
313			317									

Poslovimo se zdaj od prvega vprašanja in odgovorimo na drugo. V ta namen vzemimo poljubno število $n > 2$, zapišimo $m = 2 \cdot 3 \cdots n$ in si oglejmo zaporedje $m + 2, m + 3, \dots, m + n$. Število $m + 2$ je deljivo z 2, $m + 3$ s 3, ..., $m + n$ pa z n , torej so vsa sestavljena. Razlika med sosednjima prašteviloma (pred in po navedenem zaporedju) je vsaj n , nasploh pa poljubno velika.

Zanimiva je tudi druga skrajnost. Le praštevili 2 in 3 sta sosedni naravni števili, parov praštevil, ki se razlikujeta za dve, pa je več. Rečemo jim pari praštevil dvojčkov. Naštejmo nekaj najmanjših:

3, 5; 5, 7; 11, 13; 17, 19; 29, 31; 41, 43; 59, 61; 71, 73; ...

in povejmo, da je eden največjih znanih dvojčkov par $9.2^{211} - 1, 9.2^{211} + 1$ (števili imata v desetiškem zapisu po 65 cifer).

Je tudi teh parov brez konca, tako kot vseh praštevil? Vprašanje zveni preprosto in je znano pod imenom problem praštevil dvojčkov, odgovora nanj pa do danes še ne poznamo. Uvrščamo ga med najslavnejše nerešene matematične probleme.

Kljub tem težavam o parih praštevil dvojčkov vendarle lahko nekaj pove-mo. Poglejmo spet zaporedje praštevil in označimo pare dvojčkov:

2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47, 53, 59, 61, 67..

Opazili ste, da edino 5 nastopa v dveh parih dvojčkov. Dokažimo, da ima res samo praštevilo 5 to lastnost.

Števila $p, p + 2$ in $p + 4$ pri deljenju s 3 dajo različne ostanke, zato je eno od njih deljivo s 3. Če hočemo, da so vsa tri praštevila, mora biti $p = 3$, odkoder sledi naša trditev.

Podobno doženemo naslednjo lastnost. Če sta prvo in zadnje število trojice $p, p + 1, p + 2$ praštevili (dvojčka) in velja $p > 3$, potem je vmesno število $p + 1$ deljivo s 6. Dokaz prepustimo bralcu. Razen v primeru (3, 5) je par dvojčkov torej vedno oblike $(6k - 1, 6k + 1), k \in \mathbb{N}$.

O tem, kako gosto so posejani pari dvojčkov v zaporedju vseh praštevil, vemo bolj malo. Na začetku zaporedja jih srečamo mnogo, obsežnejša preglednica praštevil pa pokaže, da kasneje pari dvojčkov nastopajo vedno redkeje. Pokažimo, da je med pari zaporednih praštevil neskončno takšnih, ki niso pari dvojčkov.

Res, če je parov praštevil dvojčkov končno mnogo, potem to očitno drži. V nasprotnem primeru pa pogledjmo tiste pare zaporednih praštevil (p, q) , pri katerih so $(p - 2, p)$ pari dvojčkov. Takšnih parov je (po predpostavki) neskončno in očitno, razen pri $p = 5$, nobeden ni par dvojčkov.

S tem smo trditev dokazali, toda žal nam pove bore malo. Vsaj to bi še radi vedeli, če je praštevil, ki niso vključena v pare dvojčkov, tudi neskončno mnogo. Če bi jih bilo le končno število, potem bi morale biti parov praštevil

dvojčkov brez konca (vseh praštevil je neskončno), s tem pa "rešen" problem praštevil dvojčkov. Toda ta je še nerešen, zato jih je končno mnogo. Je to res dokaz? Seveda ne.

Za tehten odgovor na vprašanje, ki smo si ga postavili, bomo potrebovali kanček znamenitega Dirichletovega izreka.

IZREK: Naj bosta a in b tuji naravni števili. Potem je v množici $\{ak + b; k \in \mathbb{N}\}$ neskončno praštevil.

Dokaz tega izreka, ki ga je nemški matematik *P.G. Lejeune–Dirichlet* objavil leta 1837, je težak in ni elementaren. Kasneje so ga drugi poenostavili, toda tudi najpreprostejši znani dokaz je še vedno zelo zapleten in krepko presega Presekov okvir. Za nekatere posebne primere, npr. $a = 4$, $b = 3$ ali $a = 6$, $b = 5$, je izrek vendarle mogoče preprosto dokazati. Ob tem se ne bomo zadrževali, pač pa se lotimo zadane naloge.

Preverimo, da nobeno število oblike $21k + 5$, $k \in \mathbb{N}$, ne more biti udeleženo v paru praštevil dvojčkov. Res, za dve manjše število $21k + 3$ je deljivo s 3, za dve večje število $21k + 7$ pa je deljivo s 7. Obe sta večji od 7 in zato ne moreta biti praštevili. Po Dirichletovem izreku (za $a = 21$ in $b = 5$) je med števili $21k + 5$, $k \in \mathbb{N}$, neskončno praštevil, ki po prejšnjem ne pripadajo parom dvojčkov. Z enako lastnostjo se odlikujejo še mnoga druga zaporedja.

Naloga je rešena, naš izlet v svet praštevil pa sklenimo s preglednico praštevil (z označenimi pari dvojčkov) in s kopico vprašanj.

2	31	73	127	179	233	283	353	419	467	547	607	661	739	811	877
3	37	79	131	181	239	293	359	421	479	557	613	673	743	821	881
5	41	83	137	191	241	307	367	431	487	563	617	677	751	823	883
7	43	89	139	193	251	311	373	433	491	569	619	683	757	827	887
11	47	97	149	197	257	313	379	439	499	571	631	691	761	829	907
13	53	101	151	199	263	317	383	443	503	577	641	701	769	839	911
17	59	103	157	211	269	331	389	449	509	587	643	709	773	853	919
19	61	107	163	223	271	337	397	457	521	593	647	719	787	857	929
23	67	109	167	227	277	347	401	461	523	599	653	727	797	859	937
29	71	113	173	229	281	349	409	463	541	601	659	733	809	863	941

1. Katera od števil 101, 1001, 10001 in 100001 so praštevila?
2. Ali obstaja tak $n \in \mathbb{N}$, da so n , $2n + 1$ in $5n - 1$ hkrati praštevila?
3. H.E. Dudeney je leta 1907 ugotovil, da ima od (tedaj) znanih praštevil le 11 v desetiškem zapisu samo enke. Dokazal je, da so števila $a_k = \underbrace{11 \dots 1}_k$,

kjer je $3 \leq k \leq 18$, vsa sestavljena, in objavil vprašanje, če je katero od števil a_k , $k > 18$, praštevilo. Eden od bralcev je kmalu ugotovil, da je že a_{19} praštevilo. Tudi a_{23} je praštevilo, ni pa znano, če je med števili a_k neskončno praštevil. In navsezadnje še naloga. Dokaži, da velja sklep: Če je a_n praštevilo, je tudi n praštevilo.

4. Dokaži, da sta enakovredni trditvi:
 - a) Parov praštevil dvojčkov je končno mnogo.
 - b) Le končno mnogo števil iz množice $\{n^2 - 1 : n \in \mathbb{N}\}$ ima natanko štiri delitelje v $\mathbb{N}$.
5. Dokaži, da produkt praštevil dvojčkov pri deljenju s 36 da ostanek 35, če le ni to par (3, 5).
6. Poišči med zaporedji $\{ak + b : k \in \mathbb{N}\}$, kjer sta na voljo tuji naravni števili a in b , neskončno takih, ki ne vsebujejo nobenega praštevila iz parov dvojčkov.

Odgovore in rešitve najdete na strani 117.

Boris Lavrič

O PRAŠTEVILIH – Rešitev s str. 88

1. Le 101 je praštevilo.
2. Če n ni deljiv s 3, je vsaj eno od števil $2n + 1$ in $5n - 1$ deljivo s 3 in zato sestavljeno. Torej mora biti $n = 3$, vendar tudi v tem primeru vsa tri števila niso praštevila.
3. Denimo, da je k sestavljeno število. Tedaj velja: $k = m \cdot n$ ($m > 1, n > 1$) in zato

$$\underbrace{11 \dots 1}_k = \underbrace{11 \dots 1}_n \cdot \underbrace{10 \dots 010 \dots 0 \dots 10 \dots 01}_n$$

4. Število $n^2 - 1 = (n - 1)(n + 1)$ ima točno štiri delitelje le, če je $(n - 1, n + 1)$ par praštevil dvojčkov.
5. Vsak par dvojčkov, različen od (3, 5), je oblike $(6k - 1, 6k + 1)$, $k \in \mathbb{N}$, torej je produkt obeh praštevil enak $36k^2 - 1$.
6. Naj bo $b > 3$ poljubno liho število in $a = (b - 2)(b + 2)$. Potem sta števili a in b tuji, števili $ak + b - 2$ in $ak + b + 2$ pa sestavljeni za vsak $k \in \mathbb{N}$.

Boris Lavrič