

PRESEK

List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652

Letnik **17** (1989/1990)

Številka 6

Strani 326–330

Milena Strnad:

PRAŠTEVILA NEKOČ IN DANES - Kar so osnovni delci v fiziki in elementi v kemiji, so praštevila v teoriji števil

Ključne besede: matematika.

Elektronska verzija: <http://www.presek.si/17/966-Strnad.pdf>

© 1990 Društvo matematikov, fizikov in astronomov Slovenije

© 2009 DMFA – založništvo

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

MATEMATIKA

PRAŠTEVILA NEKOČ IN DANES

“Kar so osnovni delci v fiziki in elementi v kemiji, so praštevila v teoriji števil”

Na vprašanje “Kaj so *praštevila*?” zna odgovoriti vsak učenec, ki je končal peti razred osnovne šole: “To so tista naravna števila, ki so večja od 1 in deljiva le z 1 in s samim seboj.” Našteti nekaj manjših praštevil tudi ni težko: 2, 3, 5, 7, 11, 13, 17, 19,... Marsikdo bi še dodal, da se da vsako naravno število, ki ni praštevilo, razcepiti na produkt samih praštevil - *prafaktorjev*. Zato imenujemo ta števila *sestavljena števila*. Tak racep je mogoč le na en način, če se ne menimo za vrstni red prafaktorjev, na primer: $12 = 2 \cdot 2 \cdot 3$, $15 = 3 \cdot 5$, $16 = 2 \cdot 2 \cdot 2 \cdot 2 = 2^4$, $120 = 2^3 \cdot 3 \cdot 5$.

Manj učencev najbrž ve, da je na to vprašanje znal odgovoriti Grk *Evklid* že 350 let pred našim štetjem. Dokazal je tudi, da je praštevil neskončno mnogo. Dokaz in še marsikaj zanimivega o praštevilih, tudi drugačno, a enakovredno definicijo praštevila, najdete v članku B. Lavriča v lanskim 2. številki Preseka.

Matematiki ne bi bili matematiki, če si ne bi postavili še več vprašanj, na primer:

1. Kako naj praštevila ločimo od vseh naravnih števil 1, 2, 3, 4, 5, 6, 7, 8, ... $N - 1$, N ?
2. Ali obstaja aritmetična formula, ki zajame vsa, skoraj vsa ali le nekatera praštevila?
3. S kakšno metodo zanesljivo ugotovimo, ali je neko naravno število praštevilo ali ni?

Na prvo vprašanje je odgovoril že Grk *Eratosten* v drugem stoletju pred našim štetjem. O *Eratostenovem situ* je pisal Presek dvakrat, v omenjenem članku in v 1. številki leta 1973/74. Ta metoda je uporabna le pri dovolj majhnih številih. Pri številih z več kot osmimi ciframi namreč tudi ob pomoči velikih računalnikov z njo ni preprosto ugotoviti, ali gre za praštevilo ali ne.

Drugo vprašanje ima več delnih odgovorov. Omenimo le najznamenitejšega, ki ga je v obliki hipoteze zapisal eden izmed največjih francoskih matematikov *Pierre de Fermat* (slika 1). O njegovem življenju in delu je pisal Presek v 1. številki leta 1975/76.

Fermat je v pismu rojaku *Marinu Mersennu* zatrdil, da so vsa števila - dandanes jim pravimo *Fermatova števila* - z obliko $F_n = 2^{2^n} + 1$ za $n \in \mathbb{N}$ praštevila. Hitro ugotovimo, da Fermatova trditev za $n = 1, 2$ in 3 zares velja: $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, z $F_4 = 65537$ za $n = 4$ pa je nekaj več dela. Resne težave se začnejo že pri $n = 5$ in se z vsakim naslednjim



Slika 1. Pierre de Fermat (1601 do 1665)



Slika 2. Carl Friedrich Gauss (1777 do 1855)

naravnim številom hitro večajo, saj zaporedje Fermatovih števil izredno hitro narašča.

Zato ni čudno, da je Fermatovo hipotezo ovrgel šele leta 1732 znameniti matematik *Leonhard Euler*, ki je dokazal, da število $F_5 = 2^{32} + 1 = 4294967297$ ni praštevilo, ker je deljivo s 641.

Fermatova hipoteza je napeljala druge matematike na pomembna odkritja. Tako je *Karl Friedrich Gauss* (slika 2) po proučevanju Fermatovih števil napisal leta 1801 znamenito delo *Disquisitiones arithmeticae*, ki je temelj moderne teorije števil. V zadnjem, sedemnajstem razdelku knjige je dokazal tesno povezavo med Fermatovimi praštevili in konstrukcijo pravih mnogokotnikov *z ravnilom in šestilom*. Pri tem smemo uporabljati ravnilo le za risanje črt, ne pa za merjenje, in šestilo le za risanje krožnic, ne pa za prenašanje dolžin. Pokazal je, da je na ta način mogoče konstruirati vse pravilne mnogokotnike, katerih število stranic se da zapisati v obliki $2^k p_1 p_2 \dots p_r$, če je k naravno število ali 0 in so $p_1, p_2, \dots, p_r$ Fermatova praštevila. To, da je mogoče z ravnilom in šestilom konstruirati pravilni sedemnajstkotnik ($F_2 = 17$), je Gauss imel za svoje največje matematično odkritje. Želel je celo, da mu mnogokotnik narišejo na nagrobnik. Želje

mu niso izpolnili, pač pa je narisana pravilni sedemnajstkotnik na Gaussovem spomeniku v njegovem rojstnem kraju Braunschweigu.

Na tretje vprašanje poznamo pravilen teoretičen odgovor že iz starih grških časov. Njegovo uporabo pa odkrivajo šele sedaj. Metodo, ki temelji na definiciji praštevila, imenujemo *deljenje s preizkušanjem*. Število N kar po vrsti delimo s števili 2, 3, 4, 5, 6, 7, ... , $(N - 1)$. Kakor hitro je eno izmed njih delitelj števila N , vemo, da je to število sestavljeno. Tako ugotovimo tudi najmanjši delitelj števila N in njegov prvi prafaktor. Po deljenju števila N s tem prafaktorjem dobimo količnik, ki ga zopet delimo s preizkušanjem. Teoretično lahko tako ugotovimo vse prafaktorje sestavljenega števila. V praksi pa je metoda uspešna le, če število N ni preveliko, na primer $150 = 2 \cdot 75 = 2 \cdot 3 \cdot 25 = 2 \cdot 3 \cdot 5^2$.

Metodo deljenja s preizkušanjem izboljšamo tako, da se opremo na Eratostenovo ugotovitev in iz množice vseh možnih deliteljev števila N izločimo vsa tista števila, ki niso praštevila in niso večja od števila $\sqrt{N}$. Zakaj je tako, lahko preberete v knjigi I. Vidava *Rešeni in nerešeni problemi matematike*, DMFA Slovenije. Tak način je ob pomoči dobrega računalnika uporaben pri številih z največ desetimi ciframi. Pri številih z dvajset in več ciframi pa odpove, kot razberemo iz tabele.

Za ugotovitev, ali je dano število z dvajset do tisoč ciframi praštevilo, obstaja več dobrih *računalniških metod*. Ena izmed njih sloni na primer na *Wilsonovem izreku*: p je praštevilo tedaj in samo tedaj, če je število $(p - 1)! + 1$ deljivo s p . Pri tem je $N! = 1 \cdot 2 \cdot 3 \cdot \dots \cdot (N - 1)N$. Toda s temi metodami v splošnem ne moremo velikega sestavljenega števila razstaviti na prafaktorje.

Število cifer	deljenje s preizkušanjem	računalniška metoda
20	2 uri	10 sekund
50	10 let	15 sekund
100	10^{36} let	40 sekund
200	10^{86} let	10 minut
1000	10^{486} let	1 teden

Tabela 1: Čas, ki je potreben, da z računalnikom preverimo, ali je kako število praštevilo

Obstajajo pa metode, s katerimi je mogoče razcepiti Fermatova števila, ki imajo do osemdeset cifer. Tako je *Landry* leta 1880 dokazal, da je število F_6 deljivo z 274177. Leta 1905 sta *Morehead* in *Westeren* pokazala, da je število F_7 z 39 ciframi sestavljeno število. Štiri leta zatem sta to pokazala tudi za število F_8 z 78 ciframi. Dokončen razcep števila F_7 , ki velja za doslej najtežjega, sta šele leta 1971 našla *Brillhart* in *Morrison*. Za ta razcep

je računalnik IBM 360-91 porabil poldrugo uro. Število F_8 sta leta 1981 razcepila z računalnikom UNIVAC 1100/42. Prvi prafaktor s 16 ciframi je računalnik izračunal po dveh urah. Nista pa ugotovila, ali je drugi faktor z 62 ciframi praštevilo ali ne. Da gre za praštevilo, je kmalu zatem ugotovil Williams.

Pokazalo se je, da vsebujejo Fermatova števila od F_9 do F_{13} razmeroma majhne najmanjše prafaktorje, največjega s 13 ciframi vsebuje število F_{13} . Kljub temu, da ta števila niso zelo velika, pa jih doslej še niso uspeli razcepiti. Prav tako še ni znan razcep sestavljenega števila s 148 ciframi, ki pomnoženo s praštevilom 24148333 tvori število F_9 .

Praštevila in šifriranje

Praštevila je mogoče uporabiti pri šifriranju sporočil. Zelo zanesljivo šifro *RSA Public Key System* so si izmislili matematiki *Rivest*, *Shamir* in *Adleman* na osnovi spoznanja, da ni splošne metode, po kateri bi razcepili število z dvesto ciframi na prafaktorja s , denimo, po sto ciframi. Površno rečeno, ustreza šifriranje množenju z dvema velikima prašteviloma, dešifriranje pa razcepu na praštevila. Način je še posebno uporaben zato, ker pri šifriranju ni treba poznati obeh prafaktorjev, ampak samo njun produkt. Pri dešifriranju pa je treba poznati oba prafaktorja. Tako pošiljatelju sporočila ni treba poznati šifre, dovolj je, da jo pozna prejemnik. Zato ta način šifriranja uporabljajo v javnih informacijskih omrežjih, na primer telefonu.

Rekordi

Zelo zanimive podatke o praštevilih vsebuje knjiga P. Ribenboima, *The Book of Prime Number Records*, Springer 1989.

- V Evklidovem dokazu nastopa produkt vseh praštevil, manjših od p , povečan za 1, torej $2 \cdot 3 \cdot 5 \dots p + 1$. V nekaterih primerih je to praštevilo. Sedanj rekord je za $p = 13649$ praštevilo, ki ima 5862 cifre.
- p in $p + 2$ je dvojček praštevil. Za zdaj je rekorder dvojček $107570463 \cdot 10^{2250} \pm 1$.
- Nekatera izmed števil, ki jih sestavljajo same enice. 111...1, so praštevila. Sedanj rekord je praštevilo s 1031 enicami.
- Mersennova števila imajo obliko $2^n - 1$. Mersennovo število $2^{216091} - 1$ s 65050 ciframi je bilo največje znano praštevilo med letoma 1985 in 1989. Ribenboim je v uvodu svoje knjige, ki obravnava resna vprašanja matematike ponekod na zabaven način, zapisal: "Naravnost rečeno, bi se mi zdelo visoko civilizirano, če bi bral, da se je v eni naših krčm razvilo prerivanje iz razgrete razprave o največjem dvojčku praštevil.

Zdaj že vemo, da za vse vrednosti n od 5 do 16 (in še za nekatere druge) Fermatova števila F_n niso praštevila. Domnevajo celo, da so le prva štiri Fermatova števila praštevila, vendar ta hipoteza ni nič trdnejša, kakor je bila Fermatova.

Število cifer največjega znanega praštevila je začelo hitro naraščati, ko so se razvili računalniki. Leta 1952 je imelo največje znano praštevilo 157 cifer, a leta 1978 že 6533 cifer. Leta 1985 je D. Slowinski s sodelavci ugotovil, da je Mersennovo število $2^{216091} - 1$ s 65050 ciframi praštevilo. To praštevilo navaja Ribenboim kot rekordno. Toda poleti 1989 so J. Brown in njegovi sodelavci povečali rekord za 37 cifer. Zdaj ima rekordno praštevilo

$$391581 \cdot 2^{216193} - 1$$

že 65087 cifer. Kdo ve, kako dolgo bo "držalo" rekord?

Dobili so ga takole. Najprej so izbrali 350000 kandidatov. S preizkušanjem so jih delili z nekaj milijardami najmanjših praštevil. Preizkus je prestalo samo 7000 kandidatov. Te so nato obdelali z računalniškimi metodami. Obdelava enega števila z računalnikom je trajala kar osemdeset minut. Ko se je število kandidatov še močnejše razredčilo, so za eno število porabili le še pol ure. Tako so se naposled prepričali, da je zapisano število praštevilo. Take račune delajo računalniške družbe, češ da lahko uporabijo pridobljene izkušnje pri izboljšanju računalnikov. Najbrž pa gre pri tem tudi za tekmovanje.

Milena Strnad