PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **23** (1995/1996)
Številka 2
Strani 110–113

Borut Zalar:

O PRAŠTEVILIH

Ključne besede: matematika, teorija števil, praštevila.

Elektronska verzija: http://www.presek.si/23/1259-Zalar.pdf

O PRAŠTEVILIH

Že stari Grki so se poleg geometrije veliko ukvarjali tudi s praštevili. Problemi v zvezi s praštevili so največkrat enostavno zastavljeni, a zelo težki za reševanje. Še danes obstaja precej nerešenih problemov kljub številnim novim (neelementarnim) metodam za njihovo reševanje. Ideje, ki izvirajo iz preučevanja praštevil, so bile zelo plodno uporabljene tudi v modernih matematičnih disciplinah, kot sta teorija kolobarjev in algebraična geometrija.

Danes bomo spregovorili nekaj o enostavnejših problemih in metodah, ki so dostopne tudi srednješolcem. Naloge s praštevili so za vas zelo koristne, saj razvijajo sposobnost mišljenja z lastno glavo. Pri teh nalogah namreč ponavadi ne gre za uporabo že naučenih metod, ampak morate sami iznajti tudi metodo reševanja, kar je od vseh opravil človeških možgan nedvomno najtežje.

Kljub temu, da nalog v zvezi s praštevili ni mogoče spraviti v predalčke, bomo poskusili s primeri predstaviti uporabo treh najosnovnejših idej, ki vam večkrat utegnejo koristiti.

1. ideja. Kadar rešujete problem, ki ima kaj opraviti s praštevili, ne pozabite na najosnovnejša dejstva:

(a) Vsa praštevila, razen dvojke, so liha števila.

(b) Nobeno praštevilo, razen trojke, ni deljivo s 3.

(c) Če je p praštevilo in je $p = xy$, potem je $x = 1, y = p$ ali pa $x = p, y = 1$.

(d) Če število n ni praštevilo, ga lahko zapišemo v obliki produkta $n = xy$, kjer sta x, y različna tako od 1 kot od n.

Problem 1. Naj bosta $p > q > 3$ praštevili. Dokaži, da je $p^2 - q^2$ deljivo s 24.

Rešitev. Najprej je očitno, da sta p in q lihi števili, zato lahko pišemo $p = 2n + 1$ in $q = 2m + 1$. Tedaj je število

$$\begin{aligned} p^2 - q^2 &= (4n^2 + 4n + 1) - (4m^2 + 4m + 1) = \\ &= 4(n(n+1) - m(m+1)) \end{aligned}$$

deljivo s 4. Števili $n(n + 1)$ in $m(m + 1)$ sta gotovo sodi, ker je med dvema zaporednima številoma vedno eno sodo in eno liho. To pomeni, da je $p^2 - q^2$ deljivo z 8.

Nadalje je izmed števil $p-1, p, p+1$ natanko eno deljivo s 3. Ker je p praštevilo, različno od 3, p ni deljivo s 3, zato je $(p-1)(p+1) = p^2-1$ deljivo s 3. Podobno je q^2-1 deljivo s 3. Tedaj pa je tudi $p^2-q^2 = (p^2-1)-(q^2-1)$ deljivo s 3 in glede na prejšnji odstavek tudi s 24.

Problem 2. Naj bo p praštevilo. Denimo, da je $8p^2+1$ tudi praštevilo. Koliko je tedaj p?

Rešitev. Najprej poskusimo s $p=2$. Tedaj je $8p^2+1 = 33$, kar ni praštevilo. To pomeni, da lahko predpostavimo, da je p liho število. Pišimo torej $p = 2n+1$. Tedaj je

$$8p^2+1 = 32n^2+32n+9 = 32n(n+1)+9.$$

Če bi bilo eno izmed števil $n, n+1$ deljivo s 3, bi bilo $8p^2+1$ tudi deljivo s 3 in večje od 9, torej bi ne bilo praštevilo. Zato je s 3 deljivo število $n-1$, oziroma $n-1 = 3s$. Če to vstavimo v p, dobimo

$$p = 2n+1 = 2(3s+1)+1 = 6s+3 = 3(2s+1).$$

Ker je p praštevilo, je $s=0$ oziroma $p=3$. Če naredimo preizkus, je $8\cdot 3^2+1 = 73$ res praštevilo.

Problem 3. Za kakšen n sta števili 2^n+1 in 2^n-1 hkrati praštevili?

Rešitev. Število $n=1$ ni rešitev, saj 1 ni praštevilo. Število $n=2$ je rešitev, saj dobimo 3 in 5.

Naj bo zdaj $n>2$. Denimo, da je 2^n-1 praštevilo. Pišimo n v obliki produkta $n = xy$, pri $x \le y$. Tedaj je

$$2^n-1 = (2^x)^y - 1 = (2^x-1)((2^x)^{y-1}+\ldots+2^x+1).$$

Ker je 2^n-1 praštevilo, je $2^x-1 = 1$. Torej je $x=1$ in $y=n$. To pomeni, da n nima netrivialnih deliteljev, zato je n tudi sam praštevilo. Ker je $n>2$, je n liho število. Pišimo ga v obliki $n = 2k+1$. Tedaj je število

$$\begin{aligned} 2^n+1 &= 2\cdot 4^k+1 = 2(3+1)^k+1 = \\ &= 2(3^k+k\cdot 3^{k-1}+\ldots+k\cdot 3+1)+1 = \\ &= 3(2\cdot 3^{k-1}+\ldots+2k)+2+1 \end{aligned}$$

deljivo s 3 in hkrati večje od 3, zato ni praštevilo. Edina rešitev je torej $n=2$.

2. ideja. Včasih je koristno uporabiti dejstvo, da je vsako naravno število mogoče zapisati v obliki produkta potenc praštevil. Vedno imejte v mislih tudi to, da je tak produkt enolično določen, če praštevila uredimo po velikosti.

Problem 4. Naj bo $p = 2^n + 1$ praštevilo. Dokaži, da je n potenca števila 2.

Rešitev. Napišimo n kot produkt potenc praštevil, torej

$$n = 2^k p_2^{k_2} \dots p_n^{k_n}.$$

Ker so praštevila $p_2, \dots, p_k$ liha, je tudi njihov produkt liho število, zato lahko pišemo $n = 2^k(2l+1)$. Tedaj je

$$p = 2^{2^k(2l+1)} + 1 = (2^{2^k} + 1)((2^{2^k})^{2l} - (2^{2^k})^{2l-1} + \dots - 2^{2^k} + 1).$$

Ker je p praštevilo, je $2^{2^k} + 1 = p$, oziroma $l = 0$.

Problem 5. Naj bo D največji skupni delitelj in v najmanjši skupni večkratnik. Dokaži, da je $D(a,b,c)v(ab,bc,ca) = abc$ za poljubna naravna števila a, b, c.

Rešitev. Pišimo

$$a = p_1^{\alpha_1} p_2^{\alpha_2} \dots p_n^{\alpha_n},$$
$$b = p_1^{\beta_1} p_2^{\beta_2} \dots p_n^{\beta_n},$$
$$c = p_1^{\gamma_1} p_2^{\gamma_2} \dots p_n^{\gamma_n}.$$

Jasno je seveda, da so nekateri eksponenti lahko enaki 0. Tedaj je

$$D(a,b,c) = p_1^{\min\{\alpha_1,\beta_1,\gamma_1\}} \dots p_n^{\min\{\alpha_n,\beta_n,\gamma_n\}}.$$

Poleg tega je

$$v(ab,bc,ca) = p_1^{\max\{\alpha_1+\beta_1,\beta_1+\gamma_1,\gamma_1+\alpha_1\}} \dots p_n^{\max\{\alpha_n+\beta_n,\beta_n+\gamma_n,\gamma_n+\alpha_n\}}.$$

Preveriti moramo torej identiteto

$$\alpha + \beta + \gamma = \min\{\alpha,\beta,\gamma\} + \max\{\alpha+\beta, \beta+\gamma, \gamma+\alpha\}.$$

Brez škode za splošnost lahko predpostavimo, da je $\alpha \le \beta \le \gamma$. Tedaj je prvo število na desni enako α, drugo pa $\beta + \gamma$ in enakost res velja.

3. ideja. V matematiki se zelo pogosto uporablja način dokazovanja, ki temelji na naslednjem: Denimo, da moramo dokazati, da iz A sledi B. Tedaj vzamemo, da A velja B pa ne (naredimo torej neko hipotezo), in potem poskušamo pokazati, da nas ta hipoteza vodi v protislovje.

V naslednjem primeru bi šlo naprimer takole: Dokazati moramo, da če ima število p lastnost P, potem je p praštevilo. To poskusimo dokazati tako, da vzamemo, da p ni praštevilo in da ima lastnost P, ter nato poskusimo izpeljati protislovje.

Problem 6. Denimo, da p deli $(p-1)!+1$. Dokaži, da je p praštevilo.

Rešitev. Denimo, da p deli število $(p-1)!+1$ in da ni praštevilo. Potem ima p neki delitelj q, ki je večji od 1 in manjši od p. Toda potem bi q nastopal v produktu $(p-1)! = 1 \cdot 2 \cdot \ldots \cdot (p-1)$ in bi ga seveda delil. V tem primeru seveda q ne more deliti $(p-1)!+1$. Dobili smo torej situacijo, ko q deli p, p deli $(p-1)!+1$, q pa ne deli $(p-1)!+1$. To je očitno protislovje, ki pomeni tudi konec dokaza.

Problem 7. Dokaži, da je praštevil neskončno mnogo. Ta problem je zelo star in so ga znali rešiti že stari Grki.

Rešitev. Pa denimo, da je praštevil končno mnogo, recimo k. Dokazali bomo, da to vodi v protislovje.

Označimo praštevila s $p_1, \ldots, p_k$ in si oglejmo število $N = p_1 p_2 \ldots p_k + 1$. Vsako število je bodisi praštevilo bodisi je deljivo z nekim praštevilom, manjšim od števila samega. Število N ni praštevilo, saj je večje od vseh praštevil $p_1, \ldots, p_k$. Če je deljivo z nekim praštevilom, mora biti deljivo z nekim izmed $p_1, p_2, \ldots, p_k$, saj drugih praštevil ni. Toda tedaj bi p_i delil 1, kar je protislovje.

Problem 8. Dokaži, da je v zaporedju $a_n = 4n+3$ neskončno mnogo praštevil.

Rešitev. Uporabili bomo podoben prijem kot v prejšnji nalogi. Denimo, da je v zaporedju samo končno mnogo praštevil $p_1, p_2, \ldots, p_k$.

Razen dvojke so vsa praštevila liha in zato oblike $4n+1$ ali $4n+3$. Produkt dveh števil oblike $4n+1$ je spet take oblike, zato mora imeti vsako število oblike $4n+3$ vsaj en praštevilski faktor te oblike.

Oglejmo si števili $N = p_1 p_2 \ldots p_k + 2$ ter $M = p_1 p_2 \ldots p_k + 4$. Natanko eno od obeh števil je oblike $4n+3$, drugo pa oblike $4n+1$ (gre za dve zaporedni lihi števili). Denimo, da je N oblike $4n+3$. Tedaj ima N prafaktor oblike $4n+3$, ki je torej člen zaporedja a_n in zato enak enemu izmed praštevil $p_1, p_2 \ldots, p_k$. Če p_i deli N, sledi, da p_i deli 2, kar je nemogoče. Podobno obravnavamo primer, ko je M oblike $4n+3$.

Zdaj ko ste oboroženi z osnovnimi idejami o praštevilih, lahko greste v knjižnico po stare Preseke ali kakšno zbirko nalog in rešujete naloge, ki so v zvezi s praštevili. Pa brez pretiravanja. Nikoli ne pozabite, da matematika ni edina stvar na svetu.

Borut Zalar