PRESEK
List za mlade matematike, fizike, astronome in računalnikarje

ISSN 0351-6652
Letnik **27** (1999/2000)
Številka 2
Strani 68–71

Ivan Vidav:

KATERA PRAŠTEVILA SO VSOTA DVEH KVADRATOV NARAVNIH ŠTEVIL?

Ključne besede: matematika, teorija števil, praštevila, vsota kvadratov.

Elektronska verzija: http://www.presek.si/27/1393-Vidav.pdf

KATERA PRAŠTEVILA SO VSOTE DVEH KVADRATOV NARAVNIH ŠTEVIL?

Odgovor na to vprašanje je že dolgo znan. Glasi se takole:

Liho praštevilo p delimo s 4. Če dobimo pri tej delitvi ostanek 1, je p vsota dveh kvadratov, če dobimo ostanek 3, p ni vsota dveh kvadratov.

Edino sodo število 2 je vsota dveh kvadratov: $2 = 1^2 + 1^2$.

Za zgled vzemimo praštevila $13, 23, 29$ in 73. Ker je

$$13 = 4 \cdot 3 + 1, \quad 23 = 4 \cdot 5 + 3, \quad 29 = 4 \cdot 7 + 1 \quad \text{in} \quad 73 = 4 \cdot 18 + 1,$$

dajo števila $13, 29$ in 73 pri delitvi s 4 ostanek 1, število 23 pa ostanek 3. Zato 23 ni vsota dveh kvadratov, $13, 29$ in 73 pa so:

$$13 = 2^2 + 3^2, \quad 28 = 2^2 + 5^2, \quad 73 = 3^2 + 8^2.$$

Dokaz navedene trditve najde bralec v vsaki knjigi, ki obravnava teorijo števil, v našem jeziku v knjigi *Teorija števil*, ki jo je napisal prof. Jože Grasselli.

Pred nekaj leti pa je Don Zagier objavil nov zanimiv dokaz, ki ne zahteva nobenega znanja iz teorije števil, zadostuje srednješolska matematika. Namen tega članka je prikazati njegov dokaz.

Naj bo liho praštevilo p vsota dveh kvadratov, torej

$$p = a^2 + b^2.$$

Tu sta a in b naravni števili. Ker je p lih, je eno izmed njiju liho, drugo sodo. Denimo, da je a liho in b sodo število. Potem lahko pišemo $a = 2k + 1$ in $b = 2l$, kjer sta k in l naravni števili. Enakost

$$p = (2k + 1)^2 + 4l^2 = 4(k^2 + k + l^2) + 1$$

pove, da dobimo ostanek 1, če delimo p s 4. Zato p ni vsota dveh kvadratov, kadar je ta ostanek enak 3.

Naravno število, ki da ostanek 1, če ga delimo s 4, lahko zapišemo v obliki $4n + 1$, kjer je n spet naravno število (n je kvocient pri delitvi s 4).

Naj bo zdaj praštevilo p oblike $p = 4n + 1$. Dokazati moramo, da je vsota dveh kvadratov. V ta namen si oglejmo enačbo

$$x^2 + 4yz = p\,. \tag{1}$$

Zanimajo nas njene rešitve v naravnih številih x, y, z. Ali obstajajo? Obstajajo. Ena je kar $x = 1$, $y = n$, $z = 1$. V splošnem premore enačba (1) več rešitev, toda vselej samo končno mnogo. Naravna števila x, y, z, ki ji zadoščajo, so namreč očitno vsa manjša od p.

Zaznamujmo z M množico vseh trojk (x, y, z) naravnih števil, ki ustrezajo enačbi (1). Množica M je, kakor rečeno, končna. Pri $p = 17$ so na primer v njej tele trojke

$$p = 17: \quad M = \{(1, 1, 4), (1, 2, 2), (1, 4, 1), (3, 1, 2), (3, 2, 1)\}.$$

Pripomba. Hkrati s trojko (x, y, z) je tudi trojka (x, z, y) v množici M, saj je $p = x^2 + 4yz = x^2 + 4zy$. Če $y \neq z$, štejemo trojko (x, y, z) in (x, z, y) za različni rešitvi enačbe (1), torej različna elementa množice M.

Še tole omenimo: Denimo, da cela števila x, y, z ustrezajo enačbi (1). Nobeno izmed njih ni enako nič. Res. Če bi bil $x = 0$, bi bilo $p = 4yz$; praštevilo p pa ni deljivo s 4. Če pa bi bilo $y = 0$ ali $z = 0$, bi bil $p = x^2$, toda praštevilo p ni kvadrat.

Denimo, da smo na neki način ugotovili, da je število trojk v množici M liho. Povežimo trojke iz M v pare takole: Trojki (x, y, z) priredimo trojko (x, z, y), se pravi trojko, v kateri smo zamenjali zadnji števili. Torej

$$(x, y, z) \longleftrightarrow (x, y, z).$$

Ker ima množica M liho število trojk, morata biti vsaj v enem od teh parov trojki med seboj enaki. Toda trojki (x, y, z) in (x, z, y) sta enaki samo tedaj, kadar je $z = y$. Zato je v M vsaj ena trojka oblike (x, y, y). Ker trojke zadoščajo enačbi (1), imamo

$$x^2 + (2y)^2 = p.$$

Vidimo, da je p vsota dveh kvadratov (namreč vsota kvadratov naravnih števil x in $2y$), če ima množica M liho število elementov.

Kako bi ugotovili, da je število trojk v množici M vselej liho? Don Zagier je imel tole zamisel: Povežimo trojke iz M v pare na kak drug način, in sicer tako, da bosta trojki v enem in samo enem paru enaki. Če smo tako povezavo našli, je v M liho število trojk.

Zapišimo enačbo (1) v eni izmed naslednjih oblik

$$p = x^2 + 4yz = (x + 2z)^2 + 4z(y - x - z), \tag{2a}$$

$$p = x^2 + 4yz = (x - 2y)^2 + 4(x + z - y)y, \tag{2b}$$

$$p = x^2 + 4yz = (2y - x)^2 + 4y(x + z - y). \tag{2c}$$

Enačba (2a) pove, da je hkrati s trojko (x, y, z) tudi trojka celih števil $(x + 2z, z, y - x - z)$ rešitev enačbe (1). V trojkah množice M so samo naravna števila, tretje število $y - x - z$ nove trojke pa je negativno, če je $y < x + z$ (kakor vemo, ne more biti enako nič). Zato je trojka $(x + 2z, z, y - x - z)$ v množici M le tedaj, kadar je $y > x + z$.

Enačbi (2b) in (2c) pa dasta trojki celih števil $(x - 2y, x + z - y, y)$ in $(2y - x, y, x + z - y)$, ki sta rešitvi enačbe (1). Da bosta ti trojki v M, mora biti $y < x + z$. V prvi trojki mora biti tudi $x > 2y$, v drugi $x < 2y$.

Razdelimo zdaj M na tri podmnožice takole

$$M_1 = \{(x, y, z) \in M\,, \quad x + z < y\}\,,$$
$$M_2 = \{(x, y, z) \in M\,, \quad x + z > y \text{ in } x > 2y\}\,,$$
$$M_3 = \{(x, y, z) \in M\,, \quad x + z > y \text{ in } x < 2y\}\,.$$

Očitno je vsaka trojka množice M v eni in le eni izmed navedenih množic. To se pravi, da je M unija treh disjunktnih množic M_1, M_2, M_3, torej $M = M_1 \cup M_2 \cup M_3$.

Če je trojka (x, y, z) v M_1, je trojka $(x+2z, z, y-x-z)$ v množici M, ker je $y - x - z > 0$. Kateri izmed množic M_1, M_2, M_3 pripada? Pišimo

$$x + 2z = x', \quad z = y', \quad y - x - z = z'.$$

Preprost račun pokaže, da je

$$x' - 2y' = x > 0, \quad x' + z' - y' = y > 0 \quad \text{in} \quad y' = z > 0\,. \qquad (*)$$

Od tod dobimo $x' > 2y'$ in $y' < x' + z'$. Zato je trojka (x', y', z') v M_2.

S podobnim računom ugotovimo, da je trojka $(x - 2y, x + z - y, y)$ v M_1, če je trojka (x, y, z) v M_2.

Videli smo, da je trojka $x' = x + 2z$, $y' = z$, $z' = y - x - z$ v M_2, kadar je (x, y, z) v M_1. Zato je trojki (x', y', z') pripadajoča trojka $(x' - 2y', x' + z' - y', y')$ v M_1. Enačbe $(*)$ povedo, da je ta trojka enaka začetni trojki (x, y, z). Podobno se prepričamo, da pridemo nazaj na prvotno trojko, če poljubni trojki (x, y, z) iz množice M_2 priredimo najprej trojko $(z - 2y, x + z - y, y)$ v M_1, nsto pa le-tej poiščemo ustrezno trojko v M_2.

Naj bo zdaj trojka (x, y, z) v množici M_3. Potem je trojka $(2y - x, y, x + z - y)$ v množici M. Preprost račun pokaže, da je ta trojka spet v M_3. Pišimo $x' = 2y-x$, $y' = y$, $z' = x+z-y$. Takoj ugotovimo, da je trojki (x', y', z') pripadajoča trojka $(2y' - x', y', x' + z' - y')$ kar enaka prvotni trojki (x, y, z).

Povežimo zdaj trojke iz množice M v pare takole:

trojki $(x, y, z) \in M_1$ priredimo trojko $(x + 2z, z, y - x - z)$ v M_2,
trojki $(x, y, z) \in M_2$ priredimo trojko $(x - 2y, x + z - y, y)$ v M_1,
trojki $(x, y, z) \in M_3$ priredimo trojko $(2y - x, y, x + z - y)$ v M_3.

Iz zgoraj povedanega izhaja tole: Če smo priredili trojki (x, y, z) trojko (x', y', z'), pripada vselej trojki (x', y', z') prvotna trojka (x, y, z). S tem predpisom so torej trojke množice M res povezane v pare.

Ali sta lahko v kakšnem paru trojki enaki? Trojke iz M_1 so povezane s trojkami iz M_2, trojke iz M_2 pa s trojkami iz M_1. Ker M_1 in M_2 nimata skupnih trojk, sta tu v vsakem paru povezani trojki različni. Naj bo zdaj trojka (x, y, z) v M_3. Če se ujema s pripadajočo trojko $(2y-x, y, x+z-y)$, ki je tudi v M_3, mora biti $2y - x = x$, $y = y$ in $x + z - y = z$. Te enačbe so izpolnjene natanko tedaj, kadar je $y = x$, to je pri trojki (x, x, z). Ker je trojka (x, x, z) rešitev enačbe (1), velja

$$x(x + 4z) = p\,. \tag{3}$$

Toda p je praštevilo, x in z pa sta naravni števili in je zato $x + 4z > x$. Edina možnost, da ustrežemo enačbi (3), je ta, da postavimo $x = 1$ in $x + 4z = p$. Od tod imamo $z = (p - 1)/4$. Ker je p oblike $4n + 1$, je kvocient $(p - 1)/4$ enak n, se pravi naravno število. Tako smo ugotovili: Edino trojka $(1, 1, \frac{p-1}{4}) \in M$ se ujema s pripadajočo trojko v paru, v vseh drugih parih sta trojki različni. To pa pomeni, da je v množici M liho število trojk. Ker je bilo p poljubno praštevilo oblike $4n+1$, smo dokazali:

Vsako praštevilo oblike $4n + 1$ je vsota dveh kvadratov.

Na koliko načinov je praštevilo $p = 4n + 1$ izrazljivo z vsoto dveh kvadratov? Če je $p = a^2 + b^2$, kjer sta a in b naravni števili, je tudi $p = b^2 + a^2$. V teh dveh zapisih sta samo sumanda zamenjana. Velja tole:

Če se ne oziramo na vrstni red sumandov, se da praštevilo $p = 4n + 1$ zapisati kot vsota dveh kvadratov samo na en način.

Naravno število je namreč sestavljeno (ni praštevilo), če je na dva različna načina izrazljivo z vsoto dveh kvadratov. Dokaz tega dejstva najde bralec v članku *Kako ugotovimo, da je naravno število sestavljeno, preden ga razstavimo?* Članek je izšel v Preseku, letnik 25 (1997/98), str. 130–136.

Ivan Vidav