Zadnji Fermatov izrek za $n = 4$

Ajda Frankovič, Jernerj Grlj, Gregor Kikelj
Mentor: Rok Havlas

Matematično raziskovalno srečanje
22. avgust 2016

Povzetek

Fermatov zadnji izrek je kar tri stoletja in pol veljal za najtežji matematični problem, dokler ga ni leta 1995 dokazal angleški matematik Andrew Wiles. V nalogi smo pokazali poseben primer tega izreka, po poti pa smo spoznali nekaj metod iz teorije števil.

1 Uvod

Naslednji izrek je leta 1637 prvi navedel francoski matematik in odvetnik Pierre de Fermat.

Izrek 1 (zadnji Fermatov izrek)**.** *Ne obstaja taka trojica neničelnih celih števil a, b in c, ki bi rešile enačbo*

$$a^n + b^n = c^n$$

za poljubno naravno število $n > 2$.

Očitno je, da ima enačba iz izreka 1 v primerih za $n = 1$ in $n = 2$ neskončno mnogo rešitev. Fermat je v svojem izvodu Diofantove knjige 'Arithmetica' zatrdil, da ima dokaz, vendar je na robu premalo prostora, da bi

ga zapisal. Njegov izvirni latinski zapis se glasi: *"Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet."*

Vse od tedaj so se matematiki trudili dokazati ta Fermatov izrek, ki je kot zadnja njegova odprta domneva postal znan pod imenom zadnji Fermatov izrek. Kot prvemu je šele po 358 letih to uspelo angleškemu matematiku Andrewu Wilesu. Pred tem je bil problem zaradi ogromno neuspelih poskusov dokazov v Guinnessovi knjigi rekordov označen kot "najtežji matematični problem". Da bi dokazali izrek, bi ga morali dokazati za $n = 4$ in za vsa liha praštevila n. Za primer za $n = 4$ je z metodo neskončnega spusta dokazal že Fermat sam. S podobno metodo je Euler dokazal primer za $n = 3$. Primer za $n = 5$ sta leta 1825 dokazala Dirichlet in Legendre. Za $n = 7$ je leta 1839 dokaz našel Lamé. V dvesto letih so tako izrek uspeli dokazati le za praštevila $3, 5$ in 7. Sophie Germain je našla in dokazala pristop, relevanten za vsa praštevila. Tega je kasneje Ernst Kummer uporabil v dokazu za *regularna* praštevila, ki vsebujejo vsa praštevila pod 100, razen $2, 37, 59$ in 67.

Leta 1955 sta japonska matematika Goro Shimura in Yutaka Taniyama opazila povezavo med eliptičnimi krivuljami in modularnimi formami, vendar matematiki v tistem času tega izreka niso in niso mogli dokazati. Leta 1984 je Gerhard Frey opazil povezavo med modularnimi formami in Fermatovim zadnjim izrekom, ki ga je dve leti kasneje s pogojnim dokazom Fermatovega zadnjega izreka v odvisnosti od izreka o modularnosti potrdil Ken Ribet. Z dokazom izreka o modularnosti je kasneje Wiles dokazal Fermatov zadnji izrek in s tem uresničil svoje sanje iz otroštva. Nagrajen je bil z več nagradami, med drugim je leta 2016 prejel tudi prestižno Abelovo nagrado.

V tem članku bomo dokazali Fermatov zadnji izrek v primeru, kjer je $n = 4$. Predhodno pa bomo pokazali nekaj izrekov, ki jih bomo uporabili v dokazu.

2 Pitagorejske trojice

Definicija 1. ***Pitagorejska trojica*** *je trojica neničelnih celih števil x, y in z, ki rešijo enačbo $x^2 + y^2 = z^2$.* ***Primitivna pitagorejska trojica*** *je pitagorejska trojica x, y, z, za katero velja* $\gcd(x, y, z) = 1$.

Recimo, da je $\gcd(x, y, z) = d$. Torej lahko zapišemo $x = dx_1$, $y = dy_1$, $z = dz_1$, tako da velja $\gcd(x_1, y_1, z_1) = 1$. Potem se enačba $x^2 + y^2 = z^2$

preoblikuje v

$$d^2x_1^2 + d^2y_1^2 = d^2z_1^2,$$

kar je ekvivalentno

$$x_1^2 + y_1^2 = z_1^2.$$

Torej je dovolj, da gledamo le primitivne pitagorejske trojice.

Prav tako je dovolj, če gledamo le pitagorejske trojice pozitivnih števil, saj velja $x^2 = (-x)^2$.

Lema 1. *Vsak popoln kvadrat je po modulu* 4 *kongurenten ali* 0 *ali* 1.

Dokaz. Vsako celo število ima po modulu 4 ostanek $0, 1, 2$ ali 3. Torej so vse možnosti za ostanek popolnega kvadrata:

$$(4k)^2 = 16k^2 = 4(4k^2) \equiv 0 \pmod 4,$$

$$(4k+1)^2 = 16k^2 + 8k + 1 = 4(4k^2 + 2k) + 1 \equiv 1 \pmod 4,$$

$$(4k+2)^2 = 16k^2 + 16k + 4 = 4(4k^2 + 4k + 1) \equiv 0 \pmod 4,$$

$$(4k+3)^2 = 16k^2+24k+9 = 4(4k^2+8k)+4\cdot 2+1 = 4(4k^2+8k+2)+1 \equiv 1 \pmod 4,$$

kjer je k neko celo število. Opazimo tudi, da je ostanek po modulu 4 enak 1, če je popolni kvadrat lih in 0, če je poolni kvadrat sod. □

Poglejmo si nekaj primitivnih pitagorejskih trojic:

$$(3,4,5), (5,12,13), (8,15,17), (7,24,25), (20,21,29), (12,35,37), (9,40,41), \ldots$$

Opazimo lahko, da imata manjši števili v vsaki izmed zgornjih trojic različno parnost. Pokažimo to lastnost v lemi.

Lema 2. *Če* (x, y, z) *tvorijo primitivno pitagorejsko trojico, potem sta* x *in* y *različne parnosti.*

Dokaz. Lemo bomo dokazali s protislovjem. Recimo, da sta x in y oba soda. Potem je z sodo število, saj velja $z^2 = x^2 + y^2$. Iz tega sledi, da je $\gcd(x, y, z) \geq 2$, torej trojica (x, y, z) ni primitivna. Poglejmo še, kaj se zgodi, če sta x in y oba liha. Po modulu 4 zaradi leme 1 dobimo $x^2 + y^2 \equiv 1 + 1 = 2 \equiv z^2$, kar ni mogoče zaradi prej omenjene leme. Sledi, da imata x in y različno parnost. □

Naš naslednji cilj je parametrizacija pitagorejskih trojic, saj jih bomo tako kasneje lažje uporabljali za dokaz Fermatovega zadnjega izreka v posebnem primeru $x^4 + y^4 = z^4$. Za dokaz izreka o parametrizaciji potrebujemo še naslednjo lemo.

Lema 3. *Recimo, da so a, b, c in n naravna števila, tako da je* $\gcd(a,b) = 1$ *in* $ab = c^n$. *Potem obstajata taki števili* a_1 *in* b_1, *da velja* $a = a_1^n$ *in* $b = b_1^n$.

Dokaz. Zaradi osnovnega izreka aritmetike za vsako naravno število obstaja praštevilski razcep. Torej lahko napišemo $a = p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{m_1}^{\alpha_{m_1}}$, $b = q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_{m_2}^{\beta_{m_2}}$ in $c = r_1^{\gamma_1} \cdot r_2^{\gamma_2} \cdot \ldots \cdot r_{m_3}^{\gamma_{m_3}}$. Če to vstavimo v izraz $ab = c^n$, dobimo

$$p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot \ldots \cdot p_{m_1}^{\alpha_{m_1}} \cdot q_1^{\beta_1} \cdot q_2^{\beta_2} \cdot \ldots \cdot q_{m_2}^{\beta_{m_2}} = r_1^{\gamma_1 n} \cdot r_2^{\gamma_2 n} \cdot \ldots \cdot r_{m_3}^{\gamma_{m_3} n}.$$

Ker je $\gcd(a,b) = 1$, noben p_i ni enak q_j za vsak $1 \leq i \leq m_1$ in $1 \leq j \leq m_2$. Torej je vsak $p_i^{\alpha_i} = r_l^{n\gamma_l}$ za nek l, $1 \leq l \leq m_3$. Potem je $p_i = r_l$ in $\alpha_i = n\gamma_l$ Iz tega sledi, da $n|\alpha_i$, kar pomeni, da je $\frac{\alpha_i}{n} \in \mathbb{N}$. Torej obstaja naravno število

$$a_1 = p_1^{\frac{\alpha_1}{n}} \cdot \ldots \cdot p_{m_1}^{\frac{\alpha_{m_1}}{n}},$$

za katerega velja $a_1^n = p_1^{\alpha_1} \cdot \ldots = a$. Analogno lahko pokažemo tudi za b. □

Izrek 2 (Izrek o parametrizaciji primitivnih pitagorejskih trojic)**.** *Vse rešitve enačbe* $x^2 + y^2 = z^2$, *ki zadoščajo* $\gcd(x,y,z) = 1$ *in* $x, y, z \in \mathbb{N}$, *kjer je* x *sod so podane s formulami*

$$x = 2st,$$
$$y = s^2 - t^2,$$
$$z = s^2 + t^2,$$

kjer velja $s > t > 0, \gcd(s,t) = 1$ *in* $s, t \in \mathbb{N}$.

Dokaz. Naj bo (x,y,z) poljubna primitivna pitagorejska trojica. Ker je x sod, sta y in z liha. To pomeni, da je $z - y = 2v$ in $z + y = 2u$. Pokazati želimo, da je $\gcd(u,v) = 1$. Recimo, da d deli u in v. Iz tega sledi $2z = 2u + 2v$ oziroma $z = u + v$. Torej d deli z. Prav tako velja $2y = 2u - 2v$ oziroma $y = u - v$, torej d deli tudi y. Prišli smo do protislovja. Zapišimo $z^2 - y^2 = x^2 = 4uv$, oziroma $(\frac{x}{2})^2 = uv$. Iz leme 3 potem sledi, da sta u in v popolna kvadrata. Lahko ju zapišemo kot $u = s^2$ in $v = t^2$, kjer sta s in t naravni števili, večji od 0. Uporabimo ta zapis, da izrazimo $x = 2st$, $y = s^2 - t^2$ in $z = s^2 + t^2$. Pokazati moramo še, da je $\gcd(s,t) = 1$. Privzemimo, da d deli s in t. Iz tega sledi, da d deli hkrati y in z. Prišli smo do protislovja in s tem dokazali želeno lastnost. Pokažimo še, da imata s in t različno parnost. Recimo, da sta oba liha. Potem je y sod. Preverimo še primer, ko sta oba soda. Potem sta y in z soda. Pridemo do protislovja. S tem smo pokazali vse želene lastnosti. □

3 Dokaz Fermatovega zadnjega izreka za n=4

V tem delu bomo dokazali, da Fermatov zadnji izrek nima rešitve za $n = 4$. Še več, dokazali bomo celo, da enačba $x^4+y^4 = z^2$ nima nobene naravnoštevilske rešitve.

Izrek 3. *Enačba $x^4 + y^4 = z^2$ nima rešitve v naravnih številih.*

Dokaz. Ta dokaz bomo naredili s pomočjo metode neskončnega spusta. Privzemimo, da obstajaja neka rešitev te enačbe. Označimo z x_0, y_0, z_0. Brez škode za splošnost lahko privzamemo, da sta si števili x_0 in y_0 tuji. Enačbo $x_0^4+y_0^4 = z_0^2$ lahko zapišemo kot $((x_0)^2)^2+((y_0)^2)^2 = (z_0)^2$. Torej vidimo, da so x_0^2, y_0^2, z_0 primitivna pitagorejska trojica. Privzamemo lahko, da je x_0 sod. Z uporabo izreka 2 o parametrizaciji lahko zapišemo $x_0^2 = 2st, y_0^2 = s^2-t^2, z_0 = s^2 + t^2$, kjer sta s in t, števili, za katri velja $\gcd(s, t) = 1$ in $s > t > 0$. S protislovjem bomo pokazali, da je t sod. Recimo, da je s sod. Ker je y_0 lih, sledi $1 \equiv y_0^2 = s^2 - t^2 \equiv 0 - 1 \equiv 3 \pmod 4$, kar pa ni mogoče, torej smo prišli v protislovje s predpostavko. Torej je s lih. Ker je tudi y_0 lih, mora biti zaradi parnosti t sod. Ker je $\gcd(x_0, y_0) = 1$, je tudi $\gcd(s, t, y_0) = 1$. Torej je tudi (s, t, y_0) primitivna pitagorejska trojica. Ponovno uporabimo izrek 2 o parametrizaciji na tej trojici. Dobimo $t = 2uv$, $y_0 = u^2 - v^2$, $s = u^2 + v^2$, pri čemer sta si u, v tuja in brez škode za splošnost privzamemo $u > v > 0$. Pokazati želimo, da je $\frac{t}{2}$ popoln kvardat. Vemo, da je t sod, zato ga lahko zapišemo kot $t = 2r$. Potem je $x_0^2 = 2st = 4sr$. Razvidno je, da sta si s in r tuja, ker sta si tudi s in t tuja. Napišemo $(x_0/2)^2 = sr$. Iz tega po lemi 3 sledi, da je r popoln kvadrat, in torej je tudi $t/2$ popoln kvadrat. Če zapišemo $t/2 = uv = w^2$, iz tujosti u in v po lemi 3 sledi, da sta u in v popolna kvadrata. Zapišemo $u = x_1^2$ in $v = y_1^2$. Velja $s = u^2 + v^2 = x_1^4 + y_1^4$ in $x_0^2 = 2st = 4uvs$. Dobimo $(x_0/2)^2 = uvs$. Zaradi tujosti uv in s in po lemi 3 sledi, da je s popoln kvadrat. Zato ga lahko zapišemo kot $s = t_1^2$. Dobimo $x_1^4 + y_1^4 = s = t_1^2$. Končno dobimo $0 < t_1 \leq t_1^2 = s \leq s^2 < s^2 + t^2 = t_0$. Uspeli smo konstruirati rešitev t_1, ki je manjša od naše rešitve t_0. Postopek lahko ponavljamo in dobimo neskončno padajoče zaporedije $t_0 > t_1 > t_2 > \ldots$. Ker pa obstaja le končno mnogo naravnih števil, ki so manjša od t_0, zaidemo v protislovje. Sledi da $x^4 + y^4 = z^2$ nima rešitev v celih številih. □

Posledica 1. *Enačba*

$$x^4 + y^4 = z^4$$

nima neničelnih celoštevilskih rešitev.

Dokaz. Če bi enačba imela rešitev x_0, y_0, z_0, potem zapišemo $t_0 = z_0^2$. Sledi, da je x_0, y_0, z_0^2 rešitev enačbe $x^4 + y^4 = z^2$, ki pa nima rešitve torej smo prišli v protislovje. □

Izrek smo dokazali tudi v splošnem, vendar dokaza zaradi omejitve dolžine članka žal ne moremo zapisati.

Literatura

[1] D. M. Burton, *Elementary number theory*, Revisited printing, Allyn and Bacon, Boston, 1976.

[2] I. Majcen, *Smelo na Olimp: 303 naloge iz teorije števil*, DMFA, Ljubljana, 2011.

[3] K. H. Rosen, *Elementary number theory and its applications*, 2nd ed., Addison-Wesley, Reading, 1987.

[4] *Fermat's Last Theorem*, v: Wikipedia: The Free Encyclopedia, [ogled 18. 8. 2016], dostopno na `https://en.wikipedia.org/wiki/Fermat%27s_Last_Theorem`.