Pavel Bartoš

Poznámka k istému Fermatovmu problému

Matematický časopis, Vol. 18 (1968), No. 1, 21--24

Persistent URL: http://dml.cz/dmlcz/126761

Matematický časopis 18 (1968), No. 1

POZNÁMKA K ISTÉMU FERMATOVMU PROBLÉMU

PAVEL BARTOŠ, Bratislava

Jeden známy Fermatov problém žiada určiť také pytagorejské trojuholníky, ktorých obsah je štvorcom celého čísla. Algebraicky ide o riešenie rovnice

$$xy(x^2 - y^2) = z^2 \tag{1}$$

v prirodzených číslach. Je dokázané (pozri napr. [1], str. 206), že rovnica (1) takéto riešenie nemá, a teda neexistuje ani trojuholník žiadanej vlastnosti.

V tejto poznámke dokážeme dve vety, ktoré s týmto problémom v istom zmysle súvisia.

Veta 1. *Nech n je ľubovoľné prirodzené číslo, $k, m = 1, 2$. Všetky riešenia rovnice*

$$xy\,[x^{2kn} + (-1)^m y^{2kn}] = kz^2 \tag{2}$$

v celých číslach x, y, z sú tieto:

1. *v prípade $k = 1$, $m = 2$:*

$$x = 0, y = a, z = 0; \quad x = a, y = 0, z = 0, \tag{3}$$

kde a je ľubovoľné celé číslo;

2. *v prípade $k = 1$, $m = 1$ a $k = 2$, $m = 1$ riešenia* (3) *a ešte*

$$x = y = a, \ z = 0, \tag{4}$$

kde a je ľubovoľné celé číslo;

3. *v prípade $k = m = 2$ riešenia* (3) *a ešte*

$$x = y = a, z = a^{2n+1}; \quad x = y = a, z = -a^{2n+1} \tag{5}$$

kde a je ľubovoľné celé číslo.

Poznámka. Rovnica (1) je špeciálny prípad rovnice (2) pre $k = m = n = 1$.

Dôkaz. Predpokladajme, že rovnica (2) má riešenie v celých číslach x, y, z. Hľadajme najprv riešenia, v ktorých aspoň jedno z čísel x, y, z je nula. Ak je $x = 0$, alebo $y = 0$, je aj $z = 0$. Stačí teda uvažovať o rovnici

$$xy\,[x^{2kn} + (-1)^m y^{2kn}] = 0$$

a k jej riešeniam pripojiť $z = 0$. V prípade $m = 2$ má len korene $x = a$, $y = 0$ a $x = 0$, $y = a$, kde a je ľubovoľné celé číslo, čo dáva riešenia (3). V prípade $m = 1$ dostávame korene $x = a$, $y = 0$; $x = 0$, $y = a$; $x = y = a$, z ktorých dostávame riešenia (3) a (4).

Teraz uvažujme o riešeniach, v ktorých aspoň jedno z čísel x, y, z je záporné a $xyz \neq 0$. Ak je riešením x, y, z, je riešením aj $x, y, -z$. Stačí teda uvažovať o záporných hodnotách x a y. Keďže $kz^2 > 0$, musí byť v prípade $m = 2$ $x < 0$, $y < 0$ a v prípade $m = 1$ buď $x < 0$, $y > 0$, $|x| < y$, buď $x > 0$, $y < 0$, $x < |y|$, buď $x < 0$, $y < 0$, $|x| > |y|$. V prvom a poslednom prípade vykonajme v rovnici (2) substitúciu $x = -\xi$, $y = -\eta$, v druhom prípade substitúciu $x = -\eta$, $y = \xi$ a v treťom prípade $x = \eta$, $y = -\xi$. Tu ξ, η sú prirodzené čísla a v prípade $m = 1$ platí $\xi > \eta$. Vo všetkých prípadoch dostaneme rovnicu

$$\xi\eta\,[\xi^{2kn} + (-1)^m \eta^{2kn}] = kz^2$$

Z toho vidno, že ak rovnica (2) má riešenie (x, y, z), má aj riešenie $(|x|, |y|, |z|)$ alebo $(|y|, |x|, |z|)$. Stačí teda hľadať jej riešenia v prirodzených číslach, k ich riešeniu sa teraz obrátime.

Predpokladajme, že $(x, y) = 1$ (čo nie je na ujmu všeobecnosti) potom aj $(x, x^{2kn} + (-1)^m y^{2kn}) = (y, x^{2kn} + (-1)^m y^{2kn}) = 1$.

Ak je $k = 1$, môžeme písať $x = u^2$, $y = v^2$, $x^{2n} + (-1)^m y^{2n} = w^2$. Z toho vyplýva $u^{4n} + (-1)^m v^{4n} = w^2$ a táto rovnica nemá riešenia v prirodzených číslach u, v, w (pozri [2] veta 3, dôsledok 1, str. 54 a veta 4, str. 88).

Ak je $k = 2$, rozlíšme dva prípady:

1. x je párne, y nepárne číslo. Vtedy možno písať $x = 2u^2$, $y = v^2$, $x^{4n} + (-1)^m y^{4n} = w^2$. Posledná rovnica však — ako už vieme — nemá riešenia v prirodzených číslach x, y, w. Ak je x nepárne a y párne číslo, dostaneme rovnakým postupom ten istý výsledok.

2. Ak sú obe čísla x, y nepárne, možno písať $x = u^2$, $y = v^2$, $u^{8n} + (-1)^m v^{8n} = 2w^2$.

Ak je $m = 1$, máme rovnicu $(u^{4n} + v^{4n})(u^{4n} - v^{4n}) = 2w^2$. Keďže $(u, v) = (x, y) = 1$ a u, v sú nepárne čísla, $2 \mid u^{4n} + v^{4n}$, ale $2^2 \nmid u^{4n} + v^{4n}$, a teda $(u^{4n} + v^{4n}, u^{4n} - v^{4n}) = 2$, a tak možno písať $u^{4n} + v^{4n} = 2w_1^2$, $u^{4n} - v^{4n} = w_2^2$. Posledná rovnica však nemá riešenia v prirodzených číslach u, v, w_2.

Ak je $m = 2$, má rovnica $u^{8n} + v^{8n} = 2w^2$ len riešenie $u = v$ (pozri [2] str. 60) a keďže $(u, v) = 1$, je $u = v = w = 1$, $x = y = z = 1$. Všetky riešenia tejto rovnice v prirodzených číslach x, y, z potom sú $x = y = a$, $z = a^{2n+1}$, kde a je ľubovoľné prirodzené číslo. Z nich vyplývajú riešenia (5) rovnice (2) v celých číslach x, y, z.

Tým je veta dokázaná.

Veta 2. *Nech n, m sú ľubovoľné prirodzené čísla. Existuje také prirodzené číslo $k_0 = k_0(m)$, že rovnica*

$$xy(x^{2^k n} - y^{2^k n}) = m, \tag{6}$$

kde $k \geq k_0$ je tiež prirodzené číslo, nemá riešenia v celých číslach x, y.

Dôkaz. Z dôkazu 1. vety vyplýva, že aj tu stačí hľadať riešenia v prirodzených číslach, lebo ostatné riešenia v celých číslach x, y, pre ktoré tu platí $xy \neq 0$, sa z nich dajú odvodiť. Predpokladajme preto, že existuje riešenie rovnice (6), v ktorom x, y sú prirodzené čísla a $(x, y) = 1$,[1] a teda aj $(x, x^{2^k n} - y^{2^k n}) = (y, x^{2^k n} - y^{2^k n}) = 1$. Každé prirodzené číslo m môžeme písať buď v tvare $m = m_1^2$, buď v tvare $m = p_1 p_2 \ldots p_l m_1^2$, kde $l \geqq 1$ a $p_1, p_2, \ldots, p_l$ sú navzájom rôzne prvočísla. Zvolme $k \geqq k_0 = l + 3$ (v prípade $m = m_1^2$ položme $l = 0$). Potom

$$x^{2^k n} - y^{2^k n} = (x^{2^2 n} - y^{2^2 n})(x^{2^2 n} + y^{2^2 n})(x^{2^3 n} + y^{2^3 n}) \ldots (x^{2^{k-1} n} + y^{2^{k-1} n}) \tag{7}$$

Rozklad (7) má $k - 1$ činiteľov a — keďže $k \geqq k_0 = l + 3$ — aspoň $l + 2$ činiteľov, ktorí sú väčší než 1, lebo rovnice $x^{4i} + y^{4i} = 1$ (i ľubovoľné prirodzené číslo) nemajú riešenia v prirodzených číslach. Všetky sú navzájom buď nesúdeliteľné (keď x, y sú rôznej parity), buď majú každé dva z nich najväčšieho spoločného deliteľa 2. To nahliadneme takto:

Zrejme $(x^{4n} - y^{4n}, x^{4n} + y^{4n}) \leqq 2$, teda aj každý činiteľ tvaru $x^{2^\lambda n} + y^{2^\lambda n} (2 < \lambda \leqq k - 1)$ je so súčinom $x^{2^\lambda n} - y^{2^\lambda n}$ všetkých jemu v rozklade (7) predchádzajúcich činiteľov buď nesúdeliteľný, buď je ich najväčší spoločný deliteľ 2. Avšak najväčší spoločný deliteľ d činiteľa $x^{2^\lambda n} + y^{2^\lambda n}$ a ľubovoľného činiteľa, ktorý ho v rozklade (7) predchádza, nemôže byť väčší. Teda $d \leqq 2$, a to zrejme $d = 1$, keď x, y sú rôznej parity aináč $d = 2$. Keďže počet týchto činiteľov je aspoň $l + 2$ a počet navzájom rôznych prvočísel p_i je l, vyplýva z toho, že v rozklade (7) existuje aspoň jeden činiteľ tvaru $x^{2^{2+j} n} + y^{2^{2+j} n}$ ($j = 0, 1, \ldots, k - 3$), pre ktorý musí platiť

$$x^{2^{2+j} n} + y^{2^{2+j} n} = z_1^2 \quad \text{alebo} \quad x^{2^{2+j} n} + y^{2^{2+j} n} = 2z_1^2.$$

Ako už vieme, prvá z týchto rovníc nemá riešenia v prirodzených číslach x, y, z_1 a druhá má len riešenie, v ktorom $x = y$, čo je však pre rovnicu (6) vylúčené, lebo $m \neq 0$.

Neexistuje teda riešenie rovnice (6) v prirodzených číslach x, y a tak ani v celých číslach. Tým je veta dokázaná. Treba ešte poznamenať, že podľa vety 1 stačí v prípade $m = m_1^2$ už aj voľba $k_0 = 1$ a v prípade $m = 2m_1^2$ $k_0 = 2$.

---

[1] Ani tu nie je tento predpoklad na ujmu všeobecnosti, pretože v opačnom prípade v ďalšom určené číslo l sa nezmení, keď prejdeme k rovnici s nesúdeliteľnými neznámymi.

Poznámka. Z rozkladu (7) na základe tejže úvahy ako v dôkaze vety 2, vyplýva, že ani rovnica

$$x^{2^k n} - y^{2^k n} = m$$

kde n, m sú ľubovoľné prirodzené čísla v tom prípade, že prirodzené číslo $k \geqq k_0 = l + 3$, nemá riešenia v celých číslach x, y.

LITERATÚRA

[1] Schwarz Š., *Algebraické čísla*, Přírodovědecké vydavatelství, Praha 1950.
[2] Sierpiński W., *Elementary theory of numbers*, Warszawa 1964.

Došlo 29. 6. 1966.

NOTE ON A PROBLEM OF FERMAT

Pavel Bartoš

Summary

The article deals with the solution of the equation (2) in integers (n is an arbitrary natural, $k, m = 1, 2$).

It is shown that the equation (2) has only trivial solutions (i. e. at least one of x, y, z is 0) in the cases of $k = m = 1$; $k = 1, m = 2$; $k = 2, m = 1$. In the case of $k = m = 2$ there is a solution $x = y = a, z = \pm a^{2n+1}$, where a is an arbitrary integer.

It is shown further that for an arbitrary natural m there exists a natural number $k(m)$ such that equation (6) is not solvable for any $k \geq k(m)$.