VI. Pytagorovy trojúhelníky, velká věta Fermatova pro $n = 4$, racionální trojúhelníky

In: Karel Rychlík (author): Úvod do elementární teorie číselné. (Czech). Praha: Jednota čs. matematiků a fysiků, 1931. pp. 93–99.

Persistent URL: http://dml.cz/dmlcz/402942

VI. Pytagorovy trojúhelníky, velká věta Fermatova pro $n=4$, racionální trojúhelníky.

§ 50. Nazveme problémem Fermatovým úlohu, řešiti rovnici

$$x^n + y^n = z^n \tag{1}$$

čísly racionálními x, y, z; n je dané číslo celé kladné.

Jsou řešení samozřejmá, při nichž jedna z neznámých má hodnotu 0, totiž

$$x = 0,\ y = \pm z \text{ a } y = 0,\ x = \pm z \text{ pro } n \text{ sudé},$$
$$x = 0,\ y = z;\ y = 0,\ x = z;\ z = 0,\ x = -y \text{ pro } n \text{ liché}.$$

To jsou tak zvaná řešení triviální. Jest však otázka, zda vedle řešení triviálních existují jiná. Fermat vyslovil domněnku, že pro $n > 2$ jiných řešení není. Toto tvrzení se nazývá velkou větou Fermatovou*).

Je-li $n = n_1 n_2$, kdež n_1 a n_2 jsou čísla celá > 1, lze psáti (1) ve tvaru $(x^{n_2})^{n_1} + (y^{n_2})^{n_1} = (z^{n_2})^{n_1}$.

Platí-li tedy věta Fermatova pro mocnitele n_1, platí i pro mocnitele n, který je násobkem n_1. Aby věta Fermatova byla dokázána v plném rozsahu, stačí ji dokázati pro případ, kdy n je buď 4 neb n rovno libovolnému lichému prvočíslu.

Omezíme se na uvažování případů $n = 2$ a $n = 4$.

Nazveme řešením primitivním případ, kdy čísla x, y, z jsou čísla nesoudělná (a tudíž celá, viz § 4 str. 14). Mají-li x, y, z největšího společného dělitele $\neq \pm 1$, nazveme řešení takové neprimitivním. Je patrno, že stačí uvažovati řešení primitivní, ježto, mají-li x, y, z n. s. d. d, je $x/d, y/d, z/d$ řešení primitivní.

*) Fermat vyslovil tuto větu v rukopisné poznámce na okraji exempláře spisů Diofantových vydaných Bachetem.

Má-li řešení býti primitivní, stačí, aby dvě z čísel x, y, z byla spolu nesoudělná. Kdyby na př. x, y měla společného dělitele d, plynulo by z (1), že též z je d dělitelno.*)

§ 51. Případ $n = 2$.

Jedná se o řešení rovnice

$$x^2 + y^2 = z^2 \tag{1}$$

čísly racionálními x, y, z. Bez újmy všeobecnosti lze předpokládati, že x, y, z jsou čísla kladná. Pak x, y jsou odvěsny a z přepona pravoúhlého trojúhelníku. Úloze můžeme dáti tvar geometrický: Nalézti pravoúhlé trojúhelníky, jejichž strany jsou čísla racionální.

Takové trojúhelníky pravoúhlé nazývají se trojúhelníky Pytagorovy.

Konečně stačí se omeziti na řešení primitivní. Příslušný trojúhelník pravoúhlý nazveme také primitivní.

Uvažujeme-li pak rovnici (1) jako kongruenci (mod 2), vidíme, že z čísel x, y, z jsou dvě lichá, jedno sudé. Čísla x, y však nemohou býti lichá, tedy z sudé. Kdybychom totiž rovnici (1) uvažovali jako kongruenci (mod 4), dostali bychom $2 \equiv 0 \pmod 4$, což je nemožné. Je tedy jedna z hodnot x, y sudá, druhá lichá. Jelikož můžeme spolu x a y v (1) zaměniti, budeme předpokládati, že x je sudé, y liché; z pak bude liché.

Rovnici (1) lze psáti ve tvaru $y^2 = z^2 - x^2$ neb

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

Čísla $z - x$ a $z + x$ jsou spolu nesoudělná. Jejich společný dělitel musil by býti dělitelem jejich součtu $2z$ a jejich rozdílu $2x$. Ježto podle předpokladu x a z jsou nesoudělná, je 2 n. s. d. čísel

*) Z literatury, zabývající se větou Fermatovou hlavně na základě elementární číselné teorie, uvádím:

Lind: Über das letzte Fermatsche Theorem, Leipzig 1910.

Dickson, II, Chapter 21, 22, 26.

Teorii čísel algebraických předpokládají:

Hilbert: Theorie d. alg. Zahlkörper, Berlin 1897 (Jahresbericht d. d. Math.-Verein. 4).

Bachmann: Das Fermatproblem in seiner bisherigen Entwicklung, Leipzig-Berlin, 1919.

Landau, III.

Hasse: Bericht über neuere Untersuchungen aus der Theorie der algebraischer Zahlkörpen, T. II., Leipzig-Berlin 1930 (Jahresbericht d. d. Math.-Verein., Erg.-bd. 6).

Z posledně uvedeného spisu uvádím, že věta Fermatova je dokázána pro prvočísla $n < 307$ a pro prvočísla $n < 14.000$ v případě, že žádné z čísel x, y, z není dělitelné n.

$2z$ a $2x$. Avšak $z - x$ a $z + x$ jsou čísla lichá, jsou tedy skutečně nesoudělná.

Ježto součin čísel nesoudělných je čtverec čísla celého, platí

$$z + x = \varepsilon u^2, \quad z - x = \varepsilon v^2,$$

kdež $\varepsilon = \pm 1$ a u, v jsou čísla celá. Jsou to čísla lichá spolu nesoudělná. Ježto však, jak jsme již řekli, stačí uvažovati případ, kdy x, y, z jsou čísla kladná, bude $\varepsilon = 1$, tedy $z + x = u^2$, $z - x = v^2$.

Odtud plyne $x = \frac{1}{2}(u^2 - v^2)$, $z = \frac{1}{2}(u^2 + v^2)$, z (2) pak $y = uv$.

Aby bylo skutečně $x > 0$, dlužno voliti $u > v$.

Naopak, zvolíme-li u, v tak, aby splňovala uvedené podmínky, ale jinak libovolně, dostaneme dosazením za x, y, z do (1), že příslušná čísla x, y, z jsou primitivním řešením rovnice (1).

Dostáváme tedy primitivní řešení rovnice (1) *pomocí vzorců*

$$x = \tfrac{1}{2}(u^2 - v^2), \quad y = uv, \quad z = \tfrac{1}{2}(u^2 + v^2),$$

kdež u, v jsou čísla celá kladná lichá, spolu nesoudělná, $u > v$, jinak libovolná.

Vzorcům těm lze dáti trochu jiný tvar. Položme $\frac{1}{2}(u+v) = u'$, $\frac{1}{2}(u - v) = v'$. Lze snadno nahlédnouti, že u, v budou tehdy a jen tehdy vyhovovati podmínkám na ně kladeným, budou-li u', v' čísla celá spolu nesoudělná, kladná, jedno sudé, druhé liché a $u' > v'$. Lze tedy říci, že *primitivní kladná řešení rovnice* (1) *jsou dána vzorci* (*píšeme-li u, v místo u', v'*)

$$x = 2uv, \quad y = u^2 - v^2, \quad z = u^2 + v^2,$$

kdež u, v jsou čísla celá kladná, jedno sudé, druhé liché, spolu nesoudělná, $u > v$, jinak libovolná.

Obecné řešení rovnice (1) *čísly racionálními* (*kladnými i zápornými*) *dostaneme pak buď ve tvaru*

$$x = \tfrac{1}{2}\, d(u^2 - v^2), \quad y = duv, \quad z = \tfrac{1}{2}\, d(u^2 + v^2),$$

kdež u, v splňují právě uvedené podmínky a jinak jsou libovolné, neb ve tvaru

$$x = 2duv, \quad y = d\,(u^2 - v^2), \quad z = d\,(u^2 + v^2),$$

kdež u, v jsou čísla celá kladná lichá, spolu nesoudělná, $u > v$, jinak libovolná, d je libovolné číslo racionální.

Označíme-li v trojúhelníku Pytagorově o stranách x, y, z α úhel ležící proti x, β úhel proti y, je

$$\sin\alpha = \cos\beta = \frac{x}{z} = \frac{2uv}{u^2 + v^2} = \frac{2\lambda}{1 + \lambda^2},$$

$$\cos\alpha = \sin\beta = \frac{y}{z} = \frac{u^2 - v^2}{u^2 + v^2} = \frac{1 - \lambda^2}{1 + \lambda^2},$$

klademe-li $\lambda = v/u$.

λ má jednoduchý geometrický význam:

$$\lambda = \operatorname{tg} \tfrac{1}{2}\alpha.$$

Úhel α, jehož sin a cos jsou racionální, nazveme úhlem racionálním. Je-li $\operatorname{tg} \frac{1}{2}\alpha$ racionální, je úhel α racionální. Je totiž

$$\sin\alpha = \frac{2 \operatorname{tg} \frac{1}{2}\alpha}{1 + \operatorname{tg}^2 \frac{1}{2}\alpha}, \quad \cos\alpha = \frac{1 - \operatorname{tg}^2 \frac{1}{2}\alpha}{1 + \operatorname{tg}^2 \frac{1}{2}\alpha}.$$

A naopak u racionálních úhlů je $\operatorname{tg} \frac{1}{2}\alpha$ racionální neb ∞. Je totiž

$$\operatorname{tg} \tfrac{1}{2}\alpha = \frac{\sin\alpha}{1 + \cos\alpha}.$$

§ 52. Věta Fermatova pro $n = 4$.

Dokážeme, že *rovnice obecnější*

$$x^4 + y^4 = z^2 \tag{1}$$

nemá jiných řešení čísly racionálními vyjma ta, kde buď x neb y je rovno 0.

Můžeme předpokládati, že x, y, z jsou čísla celá nesoudělná. Dejme tomu, že by n. s. d. čísel x, y, z byl d, $d \mid \neq 1$. Položme $x = dx'$, $y = dy'$, $z = dz'$. Pak x', y', z' jsou čísla celá nesoudělná. I dostali bychom z rovnice (1)

$$d^2 (x'^4 + y'^4) = z'^2.$$

Pak $(z'/d)^2$ by bylo číslo celé, tedy i z'/d. Položme $z' = dz''$. x', y', z'' by splňovala rovnici $x'^4 + y'^4 = z''^2$, téhož tvaru jako (1). Ježto x', y', z' jsou čísla spolu nesoudělná, jsou spolu také nesoudělná čísla $x', y', z'' = z'/d$.

Z předpokladu, že x, y, z jsou čísla spolu nesoudělná, plyne, že nejsou všechna sudá; není také možno, aby byla dvě sudá a jedno liché, ani aby byla všechna tři lichá. Je tedy jedno sudé, dvě lichá. Uvažujeme-li pak (1) jako kongruenci (mod 4), shledáváme, že není možno, aby x, y byla lichá, z sudé. Je tedy z liché a jedno z čísel x, y sudé, druhé liché.

Předpokládejme, že je x sudé, y liché, $x = 2^n x'$, kdež je n číslo celé $\geqq 1$, x' číslo liché. Z dané rovnice dostaneme

$$2^{4n} x'^4 = z^2 - y^4,$$

kdež x', y, z jsou čísla lichá spolu nesoudělná.

Provedeme důkaz, že rovnice obecnější

$$\varepsilon \cdot 2^{2n}x^4 = z^2 - y^4, \tag{2}$$

kdež $\varepsilon = \pm 1$ a n je číslo celé kladné, není řešitelná čísly lichými nesoudělnými x, y, z. Důkaz provedeme úplnou indukcí.

Pro $n = 1$ dostaneme rovnici

$$4\varepsilon x^4 = z^2 - y^4. \tag{3}$$

Uvažujme ji jako kongruenci(mod 8). Pro lichá čísla x, y, z platí

$$x \equiv \pm 1,\ y \equiv \pm 1,\ z \equiv \pm 1 \pmod 4,$$

tedy

$$x^4 \equiv 1,\ y^4 \equiv 1,\ z^2 \equiv 1 \pmod 8.$$

Tak bychom dostali z (3) nemožnou kongruenci $4\varepsilon \equiv 0 \pmod 8$. Není tedy rovnice (3) řešitelná čísly lichými.

Budiž nyní v (2) $n > 1$. Pišme (2) ve tvaru

$$\varepsilon \cdot 2^{2n}x^4 = (z - y^2)(z + y^2). \tag{4}$$

Snadno lze nahlédnouti, že $z - y^2$ a $z + y^2$ mají n. s. d. 2. Bude tedy

$$z - y^2 = \varepsilon' \cdot 2u^4,\ z + y^2 = \varepsilon'' \cdot 2^{2n-1}v^4 \tag{5}$$

$$\text{neb}\quad z - y^2 = \varepsilon' \cdot 2^{2n-1}u^4,\ z + y^2 = \varepsilon'' \cdot 2v^4 \tag{6}$$

($\varepsilon', \varepsilon'' = \pm 1$, $\varepsilon'\varepsilon'' = \varepsilon$, u, v čísla lichá nesoudělná).

Ale soustavu (6) dostaneme ze soustavy (5), zaměníme-li z v $-z$, ε' v $-\varepsilon''$, ε'' v $-\varepsilon'$, u ve v, v v u. Stačí tedy uvažovati (5). Odtud plyne

$$y^2 = \varepsilon'' \cdot 2^{2n-2}v^4 - \varepsilon' u^4. \tag{7}$$

Je-li $n > 1$, bude, uvažujeme-li tuto rovnici jako kongruenci (mod 4), $y^2 \equiv -\varepsilon' u^4 \pmod 4$, tedy $\varepsilon' = -1$. I dostaneme z rovnice (7) rovnici

$$\varepsilon'' \cdot 2^{2(n-1)}v^4 = y^2 - u^4$$

téhož tvaru jako (2), jenže místo n je $n - 1$. Tím důkaz proveden.

Zároveň je též patrno, že *věta Fermatova platí pro každý exponent dělitelný čtyřmi.*

Rovnice (2) se vyskytuje při důkaze věty:

Plocha pravoúhlého trojúhelníku s celými stranami není nikdy čtvercem, ani dvojnásobným čtvercem čísla racionálního.

Jinak řečeno: Není možno najíti čísla racionální x, y, z, t tak, aby platilo

$$x^2 + y^2 = z^2,$$

$$xy = 2^k t^2,\ k = 0 \text{ neb } 1.$$

Stačí se omeziti na primitivní řešení první rovnice. Čísla x, y jsou pak nesoudělná, jedno z nich, na př. x, sudé, druhé, y, liché. Z rovnice $xy = 2^k t^2$, $k = 0$ neb 1 plyne, že t^2 je číslo celé, takže i t je celé. Pišme rovnici tu ve tvaru $xy = 2^n s^2$, kdež s je číslo celé liché, n číslo celé > 0. I dostaneme, protože x a y jsou nesoudělná,

$$x = 2^n u^2, \quad y = v^2.$$

První pak přejde v rovnici

$$2^{2n} u^4 + v^4 = z^2$$

a ta je skutečně neřešitelná čísly celými $u, v, z \neq 0$.

§ 53. Trojúhelník, jehož strany a, b, c a plocha Δ jsou čísla racionální, nazveme trojúhelníkem racionálním (Heronovým). Trojúhelník Pytagorův je racionální.

V racionálním trojúhelníku jsou výšky v_1, v_2, v_3, poloměr kružnice opsané R, poloměr kružnice vepsané ϱ, poloměry kružnic vně vepsaných $\varrho_1, \varrho_2, \varrho_3$ čísla racionální. Úhly takového trojúhelníku α, β, γ jsou racionální.

Je totiž

$$2\Delta = av_1 = bv_2 = cv_3,$$
$$4\Delta R = abc,$$

$\Delta = s\varrho = (s-a)\varrho_1 = (s-b)\varrho_2 = (s-c)\varrho_3$, kdež $2s = a+b+c$, $\varrho = (s-a)\operatorname{tg}\frac{1}{2}\alpha = (s-b)\operatorname{tg}\frac{1}{2}\beta = (s-c)\operatorname{tg}\frac{1}{2}\gamma$.

Klademe-li

$$\operatorname{tg}\tfrac{1}{2}\alpha = \lambda, \quad \operatorname{tg}\tfrac{1}{2}\beta = \mu,$$

bude

$$\operatorname{tg}\tfrac{1}{2}\gamma = \frac{1}{\operatorname{tg}\frac{1}{2}(\alpha+\beta)} = \frac{1-\lambda\mu}{\lambda+\mu},$$

$$\sin\alpha = \frac{2\lambda}{1+\lambda^2}, \quad \sin\beta = \frac{2\mu}{1+\mu^2}, \quad \sin\gamma = \frac{2(\lambda+\mu)(1-\lambda\mu)}{(1+\lambda^2)(1+\mu^2)}.$$

Ježto

$$\frac{a}{\sin\alpha} = \frac{b}{\sin\beta} = \frac{c}{\sin\gamma} = 2R,$$

bude

$$a = \frac{4\lambda R}{1+\lambda^2}, \quad b = \frac{4\mu R}{1+\mu^2}, \quad c = \frac{4(\lambda+\mu)(1-\lambda\mu)R}{(1+\lambda^2)(1+\mu^2)},$$

$$\Delta = \frac{16\lambda\mu(\lambda+\mu)(1-\lambda\mu)R^2}{(1+\lambda^2)^2(1+\mu^2)^2},$$

$$s = \frac{4(\lambda+\mu)R}{(1+\lambda^2)(1+\mu^2)}, \quad \varrho = \frac{4\lambda\mu(1-\lambda\mu)R}{(1+\lambda^2)(1+\mu^2)},$$

$$s-a = \frac{4\mu(1-\lambda\mu)R}{(1+\lambda^2)(1+\mu^2)}, \quad s-b = \frac{4\lambda(1-\lambda\mu)R}{(1+\lambda^2)(1+\mu^2)},$$

$$s-c = \frac{4\lambda\mu(\lambda+\mu)R}{(1+\lambda^2)(1+\mu^2)}.$$

Zvolíme-li za λ, μ, R racionální čísla >0, $\lambda\mu<1$ (aby $\operatorname{tg}\frac{1}{2}\gamma>0$), budou a, b, c, Δ, ježto jsou racionální funkce λ, μ, R, též čísla racionální a trojúhelník bude pak racionální.

LITERATURA:

Bachmann: *1.* Zahlentheorie I. Die Elemente der elementaren Zahlentheorie, Lipsko 1925.
2. Grundlehren der neueren Zahlentheorie, 2. vyd. Berlín, Lipsko 1921.
3. Niedere Zahlentheorie, Lipsko I. 1901, II. 1910.

Cahen: *1.* Eléments de la théorie des nombres, Paříž 1900.
2. Théorie des nombres, Paříž I. 1914, II. 1924.

Dickson: History of the theory of numbers, Washington I. 1919, II. 1920, III. 1923.

Encyklopädie der mathematischen Wissenschaften: I C 1, *Bachmann:* Niedere Zahlentheorie.

Hensel: Zahlentheorie, Berlín, Lipsko 1913.

Kraïtchik: 1. Théorie des nombres, Paříž I. 1922, II. 1926.
2. Recherches sur la théorie des nombres, Paříž I. 1924, II. 1929.

Landau: Vorlesungen über Zahlentheorie, I.—III., Lipsko 1927.

Lucas: Théorie des nombres, Paříž 1891.

Lejeune-Dirichlet, Dedekind: Vorlesungen über Zahlentheorie, 4. vyd. Brunšvig 1894.

Studnička: Základové nauky o číslech, Praha 1875.

Weber-Wellstein: Encyklopädie der Elementarmathematik, I. Arithmetik, Algebra u. Analysis, 4. vyd. zpr. Epstein, Lipsko, Berlín 1922.

Wertheim: 1. Elemente der Zahlentheorie, Lipsko 1887.
2. Anfangsgründe der Zahlenlehre, Brunšvig 1902.
