DŮKAZ VELKÉ FERMATOVY VĚTY PRO EXPONENT 3

PETR GOLAN

Tuto práci bych rád věnoval památce bývalého děkana Elektrotechnické fakulty ČVUT profesora Ing. Jana Hlavičky, DrSc., který byl mým školitelem a přítelem v době našeho společného působení ve Výzkumném ústavu matematických strojů. Od jeho předčasné smrti uplynulo letos v září 19 let.

Abstrakt. V článku je prezentován nový netradiční důkaz Fermatova tvrzení, že neexistují přirozená čísla, jež by vyhovovala diofantické rovnici $x^3+y^3=z^3$. Důkaz je založen na tom, že tuto rovnici lze převést do ekvivalentního součinového tvaru $(3k)^3=(x+y-z)^3=3(x+y)(z-x)(z-y)$, kde $x+y$, $z-x$, $z-y$ jsou po dvou nesoudělná čísla. Pokud $3 \mid z$, tak $z-y=x-3k=X^3$, $z-x=y-3k=Y^3$ a $x+y=z+3k=9Z^3$. Odtud lze odvodit podmínku $Y^3(Y^2+3ZX)^3=(z-x)(z^2+zx+x^2)$ a $(Y^2+3ZX)^3=x^2+xz+z^2$. Použitím substituce $Y^2+3ZX=a^2+ab+b^2=(a-b)^2+3ab$, $x=a^3+3a^2b-b^3$, $z=b^3+3ab-a^3$ pak obdržíme identitu. Porovnáním podmínek pro x a z dostaneme $X^3+3XYZ=a^3+3a^2b-b^3$ a $3Z(3Z^2-XY)=b^3+3ab^2-a^3$, odkud plyne, že $3 \mid (b^3-a^3)$ a $3 \mid X$. To je ale ve sporu s výchozím předpokladem $3 \mid z$ a s nesoudělností čísel x a z. K obdobnému sporu dojdeme i v případě $3 \mid x$ nebo $3 \mid y$. To, že ani další možné substituce nevedou k řešení, je dokázáno pomocí rozkladu x^2+xz+z^2 v oboru Eisensteinových čísel. Článek je doplněn některými důsledky, jako jsou např. různé typy iracionálních identit nebo řada neřešitelných diofantických rovnic, jejichž neřešitelnost plyne z Velké Fermatovy věty pro $p=3$.

1. Úvod

Velká Fermatova věta (Fermat's Last Theorem, dále jen FLT) byla po více než tři a půl století výzvou pro matematiky celého světa. Fermat sám dokázal svou domněnku pro $n=4$ v roce 1637 a, jak známo, v Diofantově knize Arithmetica zanechal na okraji jedné stránky ručně psanou poznámku, která naznačovala, že znal i obecný důkaz. Ten však nikdy nepublikoval, zůstává proto otevřenou otázkou, zda takový důkaz skutečně objevil nebo se mýlil. Kompletní důkaz se podařil teprve prof. A. Wilesovi, který jej publikoval v roce 1995 na více než 100 stránkách [5, 4]. Před ním byla publikována řada dílčích důkazů pro různé hodnoty exponentů n včetně exponentu 3. Jejich přehled je uveden např. v Ribenboimově knize [3]. Pokusy o jednodušší a elegantnější důkaz FLT pokračují i v dnešní době – viz např. [1].

2010 *MSC.* Primární 11D25; Sekundární 11D61, 11J72, 97F50.
Klíčová slova. Velká Fermatova věta, diofantická rovnice, Eisensteinova čísla, iracionální čísla.

Shrňme nejprve několik známých základních faktů. Velká Fermatova věta tvrdí, že pro přirozený exponent $n > 2$ žádná trojice čísel $x, y, z \in \mathbb{N}$, kde $\mathbb{N}$ značí množinu přirozených (kladných celých) čísel, nevyhovuje diofantické rovnici

$$x^n + y^n = z^n. \tag{1.1}$$

Lze ukázat, že stačí uvažovat vzájemně nesoudělná čísla x, y, z. Kdyby totiž např. platilo, že $gcd(A, B) = D$, tj. D je největší společný dělitel A a B, pak lze D^n z čísla $A^n + B^n = C^n$ vytknout a platí

$$A^n + B^n = D^n x^n + D^n y^n = D^n(x^n + y^n) = C^n = D^n z^n,$$

čili D by muselo být faktorem i C, takže místo $A^n + B^n = C^n$ stačí vyšetřovat $x^n + y^n = z^n$. FLT stačí dokazovat pro exponenty $n = p$, kde p je liché prvočíslo, a samostatně ještě pro první složené sudé číslo 4. Pro všechna ostatní složená čísla totiž platí, že jsou buď násobkem nějakého lichého prvočísla nebo mocninou dvojky. A pokud neexistuje řešení $x^q + y^q - z^q = 0$ pro q, které je rovno prvočíslu nebo číslu 4, neexistuje řešení ani pro složené exponenty, neboť $A^{tq} + B^{tq} - C^{tq} = (A^t)^q + (B^t)^q - (C^t)^q$. Případ $q = 2$ nevede vždy k neexistenci řešení (1.1), jelikož existují trojice celých čísel x, y, z (tzv. pythagorejské triplety), jež vyhovují rovnici (1.1) s $n = 2$. Proto pro exponenty, jež jsou mocninami čísla 2, je potřeba vycházet v důkazu FLT z nejmenší hodnoty exponentu $q = 2^2$ a nikoli $q = 2$.

Z Fermatovy rovnice (1.1) je zřejmé, že pro každé liché prvočíslo p platí nerovnosti $x^p < z^p = x^p + y^p < (x + y)^p$ a $y^p < z^p = x^p + y^p < (x + y)^p$. Bez újmy na obecnosti proto můžeme vzhledem k symetrii (1.1) vůči x a y předpokládat, že pro čísla, jež mají splňovat Fermatovu rovnici (1.1), platí ostré nerovnosti $0 < y < x < z < x + y$. Případ $x = y$ nemůže být řešením (1.1), neboť $2x^p = z^p$ nemá v oboru přirozených čísel řešení.

2. FERMATOVA VĚTA PRO EXPONENT 3

K důkazu budeme potřebovat čtyři pomocná tvrzení. Nutno ještě poznamenat, že symboly x, y, z značíme pro jednoduchost jak čísla, tak neznámé v rovnicích. Z kontextu je zřejmé, jakou roli v daném případě konkrétní symbol zastává.

Lemma 2.1. *Fermatova rovnice v součtovém tvaru $x^3 + y^3 = z^3$ je ekvivalentní rovnici v součinovém tvaru*

$$(x + y - z)^3 = 3(x + y)(z - x)(z - y). \tag{2.1}$$

Důkaz. Přímým ověřením. □

Číslo $x + y - z$ je tedy násobkem čísla 3, můžeme proto místo (2.1) psát také

$$(3k)^3 = 3(z + 3k)(y - 3k)(x - 3k), \tag{2.2}$$

kde k je přirozené číslo takové, že $3k = x + y - z$, a tedy

$$x + y = z + 3k. \tag{2.3}$$

Lemma 2.2. *Jsou-li x, y, z přirozená čísla z Fermatovy rovnice $x^3 + y^3 = z^3$, pak čísla $x + y = z + 3k$, $z - x = y - 3k$, $z - y = x - 3k$, kde $3k = x + y - z$ jsou po dvou nesoudělná.*

Důkaz. Předpokládejme naopak, že $q \mid z+3k$ i $q \mid y-3k$ pro nějaké prvočíslo q. Jelikož platí (2.2), tak $q \mid (3k)^3$ a $q \mid 3k$. Pak ale $q \mid z$ a $q \mid y$, což je spor s předpokladem nesoudělnosti z a y. Stejným zůsobem dospějeme ke sporu pro dvojici čísel $z+3k$, $x-3k$ a dvojici čísel $x-3k$, $y-3k$. Čísla $x+y$, $z-x$, $z-y$ tedy nemají žádného společného dělitele a jsou po dvou nesoudělná. □

Lemma 2.3. *Pro všechna reálná čísla a, b platí identita*

$$(a-b)(2a+b)(a+2b)(a^2+ab+b^2)^3 = \left(a^3+3a^2b-b^3\right)^3 - \left(-a^3+3ab^2+b^3\right)^3. \quad (2.4)$$

Důkaz. Přímým ověřením. □

Pro $b \neq a$, $b \neq -2a$ a $a \neq -2b$ můžeme vydělit celou rovnici (2.4) číslem $(a-b)(2a+b)(a+2b) = 2a^3+3a^2b-3ab^2-2b^3 = (a^3+3a^2b-b^3)-(-a^3+3ab^2+b^3)$, a tak z (2.4) pomocí vzorce pro rozdíl třetích mocnin $(R^3-S^3)/(R-S) = R^2+RS+S^2, R \neq S$, dostaneme

$$\begin{aligned}\left(a^2+ab+b^2\right)^3 &= \frac{(a^3+3a^2b-b^3)^3-(-a^3+3ab^2+b^3)^3}{(a^3+3a^2b-b^3)-(-a^3+3ab^2+b^3)} \\ &= (a^3+3a^2b-b^3)^2+(a^3+3a^2b-b^3)(-a^3+3ab^2+b^3) \\ &\quad +(-a^3+3ab^2+b^3)^2.\end{aligned} \quad (2.5)$$

Lemma 2.4. *Pro všechna reálná čísla a, b platí identity*

$$\begin{aligned}&(3a^2b+3ab^2)^2+(3a^2b+3ab^2)(a^3-3ab^2-b^3) \\ &\qquad = (a^3+3a^2b-b^3)^2-(a^3+3a^2b-b^3)(a^3-3ab^2-b^3),\end{aligned} \quad (2.6)$$

a

$$\begin{aligned}&(3a^2b+3ab^2)^2+(3a^2b+3ab^2)(a^3-3ab^2-b^3)+(a^3-3ab^2-b^3)^2 \\ &\qquad = (a^3+3a^2b-b^3)^2+(a^3+3a^2b-b^3)(-a^3+3ab^2+b^3) \\ &\qquad\quad +(-a^3+3ab^2+b^3)^2.\end{aligned} \quad (2.7)$$

Důkaz. Přímým ověřením. □

Věta 2.5 (Velká Fermatova věta pro $p=3$)**.** *Diofantická rovnice*

$$x^3+y^3=z^3 \quad (2.8)$$

nemá řešení v oboru přirozených čísel.

Důkaz. Jak bylo ukázáno v úvodu, stačí uvažovat jen vzájemně nesoudělná přirozená čísla x, y, z. Z (2.2) plyne, že buď x nebo y nebo z musí mít faktor 3, takže $3 \mid xyz$. Předpokládejme nejprve, že $3 \mid z$, neboli $z = 3z_1$. Číslo $x+y$, které lze z x^3+y^3 vytknout, musí mít proto faktor 3. Zapíšeme-li levou stranu (2.8) ve formě součinu dvou nesoudělných čísel

$$3(x+y)\left[(x+y)\frac{(x+y)}{3}-xy\right] = (3z_1)^3$$

je ihned patrné, že $x+y$ má faktor dokonce 3^2, neboť $3 \nmid xy$. Potom z rovnic (2.1), (2.2) a Lemmatu 2.2 plyne, že čísla $3(z+3k) = 3(x+y)$, $y-3k = z-x$ a $x-3k = z-y$ musí být třetí mocniny, takže můžeme zavést takovéto značení:

$$x - 3k = z - y = X^3, \tag{2.9}$$

$$y - 3k = z - x = Y^3, \tag{2.10}$$

$$z + 3k = x + y = 9Z^3 = X^3 + Y^3 + 6k, \tag{2.11}$$

$$3k = x + y - z = 3XYZ. \tag{2.12}$$

Z (2.9) až (2.12) můžeme vyjádřit x, y, z pomocí čísel X, Y, Z:

$$x = X^3 + 3XYZ = X(X^2 + 3YZ), \tag{2.13}$$

$$y = Y^3 + 3XYZ = Y(Y^2 + 3XZ), \tag{2.14}$$

$$z = 9Z^3 - 3XYZ = 3Z(3Z^2 - XY) = X^3 + Y^3 + 3XYZ. \tag{2.15}$$

Z (2.13), (2.14) a (2.15) je patrné, že čísla X, Y, $3Z$ jsou po dvou nesoudělná, neboť $X \mid x$, $Y \mid y$ a $3Z \mid z$ a x, y, z jsou po dvou nesoudělná čísla. Ze součinu těchto rovnic je také vidět, že $3k$ musí dělit číslo xyz. Dále je z (2.15) zřejmé, že X^3+Y^3 musí mít faktor 3. A protože platí $X^3+Y^3 = (X+Y)[(X+Y)^2-3XY]$ a $3 \nmid XY$, tak $3 \mid (X+Y)$, $3 \mid [(X+Y)^2-3XY]$, $9 \mid (X^3+Y^3)$, $3 \mid Z$ a $9 \mid z$.

Fermatovu rovnici (2.8) můžeme přepsat do tvaru

$$y^3 = z^3 - x^3 = (z-x)(x^2+xz+z^2). \tag{2.16}$$

S využitím (2.14) dostaneme

$$y^3 = Y^3(Y^2+3ZX)^3 = Y^3(x^2+xz+z^2), \tag{2.17}$$

odkud pak plyne

$$(Y^2+3ZX)^3 = x^2+xz+z^2. \tag{2.18}$$

Položme $A = Y^2+3ZX$. Ukážeme nejprve, že diofantická rovnice tvaru

$$A^3 = x^2+xz+z^2 \tag{2.19}$$

má nekonečně mnoho řešení, jako např. $(A,x,z) = (3,3,3), (12,24,24), (19,17,73)$ atd. Jedna množina řešení se nabízí hned, a to (A, aA, bA), jako např.$(7,7,14)$, $(13,13,39)$, $(19,38,57)$, …, neboť substituce

$$A = a^2+ab+b^2, \quad a,b \in \mathbb{Z}, \tag{2.20}$$

$$x = aA = a^3+a^2b+ab^2, \tag{2.21}$$

$$z = bA = a^2b+ab^2+b^3 \tag{2.22}$$

mění (2.19) na identitu $A^3 = (aA)^2 + abA^2 + (bA)^2 = A^2(a^2+ab+b^2)$. Takováto řešení rovnice (2.19) však můžeme předem vyloučit, protože vyžadujeme nesoudělnost x, z. Díky Lemmatu 2.3 lze (2.19) parametrizovat pomocí substitucí

$$A = a^2+ab+b^2,$$

$$x = -a^3+3ab^2+b^3, \tag{2.23}$$

$$z = a^3+3a^2b-b^3, \tag{2.24}$$

protože po dosazení do (2.19) dostaneme

$$(a^2+ab+b^2)^3 = (a^3+3a^2b-b^3)^2+(a^3+3a^2b-b^3)(-a^3+3ab^2+b^3)+(-a^3+3ab^2+b^3)^2,$$

což je identita (2.5). Za povšimnutí stojí, že parametrizací (2.23), (2.24) dostáváme některá řešení, jako např. $(3,3,3)$, $(12,24,24)$, shodná s řešeními, jež lze získat parametrizací (2.21), (2.22). To nastává v případech, když $x = z$, a tedy $a = b$.

Libovolný výběr celých čísel a, b tedy vede k řešení rovnice (2.19), podobně jako Euklidova parametrizace $x = a^2 - b^2$, $y = 2ab$, $z = a^2 + b^2$, $(a^2 - b^2)^2 + (2ab)^2 = (a^2 + b^2)^2$ řeší problém pythagorejských tripletů, jež jsou celočíselným řešením Pythagorovy diofantické rovnice $z^2 = x^2 + y^2$.

V případě parametrizace vzorce (2.18) musí být ovšem splněny ještě podmínky (2.13) až (2.15), jež ukazují požadovanou vnitřní strukturu hledaného řešení. Porovnáním (2.13) s (2.23) a (2.15) s (2.24) tak dostáváme

$$X^3 + 3XYZ = -a^3 + 3ab^2 + b^3, \tag{2.25}$$

$$3Z(3Z^2 - XY) = a^3 + 3a^2b - b^3. \tag{2.26}$$

Z (2.26) je vidět, že $3 \mid (a^3 - b^3)$. Z (2.25) pak plyne, že 3 musí dělit X^3, což je ale ve sporu s nesoudělností X a Z, resp. x a z.

Díky identitě (2.6) lze k řešení rovnice (2.18) použít také substituce

$$A = a^2 + ab + b^2,$$

$$x = a^3 - 3ab^2 - b^3, \tag{2.27}$$

$$z = 3a^2b + 3ab^2 = 3ab(a + b), \tag{2.28}$$

protože z (2.7) a (2.5) je vidět, že platí také identita

$$(a^2 + ab + b^2)^3 = (a^3 - 3ab^2 - b^3)^2 + 3ab(a + b)(a^3 - 3ab^2 - b^3) + (3ab)^2(a + b)^2,$$

jež je rovněž parametrizací rovnice (2.19). Takováto substituce též vyhovuje podmínce $3 \mid z$, $3 \nmid x$. Navíc musí čísla a, b v (2.28) splňovat podmínku $3 \mid ab(a + b)$, neboť $9 \mid z$. Tato substituce poskytuje řešení rovnice (2.19) např. $(A, x, z) = (7, 1, 18), (13, 17, 36), (21, 51, 60), \ldots$. Existence této další parametrizace znamená, že je potřeba rozšířit důkaz neřešitelnosti diofantické rovnice (2.18) i na substituce (2.20), (2.27), (2.28), případně i jiné substituce, pokud existují.

Substituci (2.20) můžeme zapsat ekvivalentním způsobem

$$A = a^2 + ab + b^2 = (a - b)^2 + 3ab,$$

takže pro všechny substituce, jež řeší diofantickou rovnici (2.18), resp. (2.19), musí být číslo $(a - b)^2 + 3ab$ vyjádřitelné ve tvaru

$$Y^2 + 3XZ = A = (a - b)^2 + 3ab.$$

Ze všech dvojic a, b jsou proto v substitucích (2.20), (2.27), (2.28) využitelné jen takové, pro něž platí

$$a - b = Y, ab = XZ, \tag{2.29}$$

$$3ab(a - b) = 3XZY. \tag{2.30}$$

Sečtením (2.28) a (2.30) dostaneme $6a^2b = 6aXZ = z + 3XYZ$, což je ale spor, protože díky nesoudělnosti x, z platí, že $X \nmid z$. Takže ani substituce (2.20), (2.27), (2.28) neřeší rovnici (2.18).

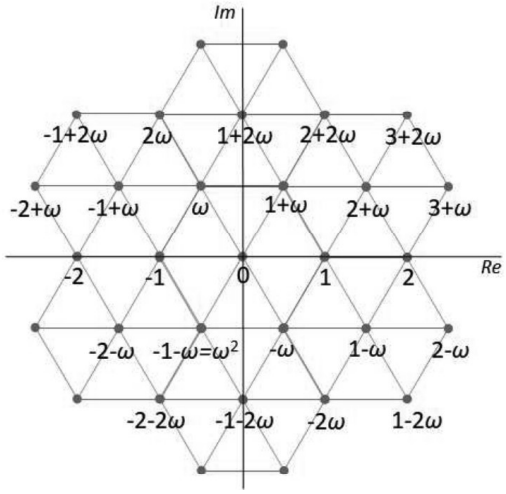
Aby byl důkaz neřešitelnosti Fermatovy rovnice (2.8) úplný, je potřeba zjistit, zda náhodou neexistují ještě jiné substituce pro řešení rovnice $A^3 = x^2 + xz + z^2$, a pokud ano, dokázat spor s podmínkami řešitelnosti Fermatovy rovnice (2.15), (2.16), (2.17) pro každou z nich. K tomu již s elementární matematikou nevystačíme.

K nalezení úplné množiny substitucí pro nesoudělná čísla x, z použijeme vlastností Eisensteinových čísel [3]. Profesionálním matematikům jsou Eisensteinova čísla a jejich vlastnosti dobře známy z teorie čísel. Pro čtenáře např. z řad studentů, kteří se ještě s Eisensteinovými čísly nesetkali, uvedeme stručně přehled základních vlastností těchto čísel.

Množina $a + b\omega, a, b \in \mathbb{Z}$, kde $\omega = -\frac{1}{2} + \frac{\sqrt{3}}{2}i$ je komplexní třetí odmocnina z jedné, tvoří podobor oboru komplexních čísel $\mathbb{C}$. Tento obor se nazývá Eisensteinova celá čísla.

Obor Eisensteinových čísel má šest jednotkových prvků ± 1, $\pm\omega$, $\pm\omega^2$ a pro ω platí, že $\omega = e^{(2\pi/3)i}$. A díky tomu také musí platit $\omega\omega^2 = \omega^3 = (e^{(2\pi/3)i})^3 = e^{2\pi i} = 1$ a $\omega + \omega^2 = e^{(2\pi/3)i} + e^{(4\pi/3)i} = e^{(2\pi/3)i} + e^{-(2\pi/3)i} = -1$, čili $\omega^2 + \omega + 1 = 0$.

Rozložení Eisensteinových čísel v komplexní rovině ukazuje obrázek 1.



Obrázek 1. Eisensteinova čísla v komplexní rovině.

Čísla ve vzorci (2.19) tvaru x^2+xz+z^2 jsou tzv. Löschova čísla [2], jež mají řadu praktických aplikací, včetně např. využití při různých optimalizacích využívajících hexagonálních sítí.

Pokud na výraz $x^2 + xz + z^2$ budeme na chvíli pohlížet jako na trojčlen s neurčitou x, jenž je sestrojen nad nějakým oborem integrity, pak jej pomocí

Viètových vzorců můžeme rozložit na součin kořenových dvojčlenů

$$x^2 + xz + z^2 = (x - z\omega_1)(x - z\omega_2) = x^2 + x(-z\omega_1 - z\omega_2) + z^2\omega_1\omega_2,$$

kde $z\omega_1$, $z\omega_2$ jsou kořeny tohoto trojčlenu a musí pro ně platit $z\omega_1 + z\omega_2 = -z$, $z\omega_1 z\omega_2 = z^2$, čili (při $z \neq 0$) $\omega_1 + \omega_2 = -1$ a $\omega_1\omega_2 = 1$. Když tedy položíme $\omega_1 = \omega$ a $\omega_2 = \omega^2$, kde ω je jednotkový prvek v oboru Eisensteinových čísel, je vidět, že v tomto oboru platí rozklad $x^2 + xz + z^2 = (x - z\omega)(x - z\omega^2)$.

Díky tomu, že $1 + \omega + \omega^2 = 0$, můžeme při násobení nebo umocňování Eisensteinových čísel vyjádřit vyšší mocniny ω^j prostřednictvím nulté a první mocniny ω, protože pomocí vzorce $\omega^2 = -1 - \omega$ můžeme podle potřeby opakovaně snižovat vyšší hodnoty exponentu o jedničku.

V oboru Eisensteinových čísel je stejně jako v $\mathbb{C}$ definována norma vzorcem

$$N(\alpha) = |\alpha|^2 = \alpha\alpha^* = (a + b\omega)(a + b\omega^2),$$

kde $\alpha^* = (a + b\omega^2)$ je tzv. konjugované číslo, což je obdoba komplexně sdruženého čísla v $\mathbb{C}$. Platí $N(\alpha) = (a + b\omega)[a - b(1 + \omega)] = (a + b\omega)(a - b - b\omega)$. Eisensteinovo číslo $(x - z\omega)$ má tedy normu

$$N(x - z\omega) = (x - z\omega)(x - z\omega^2) = x^2 + xz + z^2,$$

což je výše zmíněné Löschovo číslo, jež se vyskytuje ve zkoumané diofantické rovnici (2.19). Norma je také Eisensteinovo číslo, neboť do oboru Eisensteinových čísel patří rovněž všechna celá čísla. Z definice normy je patrné, že Eisensteinova čísla a čísla k nim konjugovaná mají stejnou normu. Jelikož norma je vzhledem k x, z symetrická, musí také platit $N(x - z\omega) = N(z - x\omega) = x^2 + xz + z^2$. Platí také, že norma součinu se rovná součinu norem. Norma všech šesti jednotkových prvků Eisensteinova oboru má hodnotu 1, tudíž také všech šest jednotkových násobků Eisensteinova čísla $x - z\omega$ a šest k nim konjugovaných Eisensteinových čísel má stejnou normu $x^2 + xz + z^2$. A vzhledem k symetrii této normy vůči x, z bude mít stejnou normu ještě dalších dvanáct Eisensteinových čísel s prohozenými čísly x, z u souřadnic v komplexní rovině a žádné jiné.

Eisensteinova čísla tvoří dokonce Euklidovský obor (funguje tam Euklidův algoritmus), takže rozklad každého Eisensteinova čísla na prvočinitele je až na volbu jednotkového prvku jednoznačný. Tyto prvočinitele nazýváme Eisensteinova prvočísla. Vyznačují se tím, že mají prvočíselnou normu. Platí také, že když Eisensteinovo číslo α dělí Eisensteinovo číslo β, tak $N(\alpha)|N(\beta)$. Lze ukázat, že $(x - z\omega)$ a $(x - z\omega^2)$ jsou nesoudělná Eisensteinova čísla. Označme největší společný dělitel čísel $(x - z\omega)$ a $(x - z\omega^2)$ jako δ. Součet a rozdíl těchto dvou Eisensteinových čísel musí být dělitelný číslem δ. Platí $(x - z\omega) + (x - z\omega^2) = (x - z\omega) + x + z + z\omega = 2x + z$ a $(x - z\omega) - (x - z\omega^2) = (x - z\omega) - (x + z + z\omega) = -z - 2z\omega = -z(1 + 2\omega)$. Číslo $2x + z$ leží na reálné číselné ose Re, číslo $-z(1 + 2\omega)$ leží na imaginární ose Im (viz obr. 1). Čísla x, z jsou podle předpokladu nesoudělná, takže $\delta = gcd(1 + 2\omega, 2x + z)$. Číslo $1 + 2\omega$ má prvočíselnou normu $N(1 + 2\omega) = 3$, je to tedy Eisensteinovo prvočíslo, a má-li být soudělné s přirozeným číslem $2x + z$, musí platit $(1 + 2\omega) \mid (2x + z)$ a norma čísla $2x + z$ musí být násobkem čísla 3. Ale podle předpokladu platí $3 \nmid x$,

$3 \mid z$, takže $3 \nmid (2x+z)$ a $gcd(1+2\omega, 2x+z) = 1$. δ proto musí být jednotkový prvek Eisensteinova oboru. Čísla $(x-z\omega)$ a $(x-z\omega^2)$ jsou tudíž nesoudělná.

Má-li platit $(x-z\omega)(x-z\omega^2) = A^3$, musí existovat celá čísla a, b taková, že činitelé $(x-z\omega)$ a $(x-z\omega^2)$ jsou v oboru Eisensteinových čísel třetími mocninami, tj. $A^3 = (a-b\omega)^3(a-b\omega^2)^3$. Pro $x - z\omega = (a-b\omega)^3$ obdržíme po umocnění $a^3-3a^2b\omega+3ab^2\omega^2-b^3 = (a^3-3ab^2-b^3)-(3a^2b+3ab^2)\omega$, odkud $x = a^3-3ab^2-b^3$ a $z = 3a^2b+3ab^2$. To odpovídá substitucím (2.27), (2.28). Dosazením různých hodnot a, b se můžeme přesvědčit, že tyto substituce generují jiná řešení rovnice (2.19) než substituce (2.23), (2.24). Ukážeme výčtem všech možností, že další substituce, vyplývající z rozkladu trojčlenu x^2+xz+z^2 v oboru Eisensteinových čísel, poskytují (až na případná opačná znaménka) stejné hodnoty x a z jako vzorce (2.23), (2.24) a (2.28).

Pokud vypíšeme do tabulky 1 všech 24 možných tvarů Eisensteinových čísel

	Parametrizovaná Eisensteinova čísla $x-z\omega$ s normou x^2+xz+z^2:	
1	$(a-b\omega)^3 = (a^3-3ab^2-b^3)-(3a^2b+3ab^2)\omega = -(b-a\omega^2)^3$	20
2	$-(a-b\omega)^3 = -(a^3-3ab^2-b^3)+(3a^2b+3ab^2)\omega = (b-a\omega^2)^3$	19
3	$\omega(a-b\omega)^3 = (3a^2b+3ab^2)+(a^3+3a^2b-b^3)\omega = -\omega(b-a\omega^2)^3$	22
4	$-\omega(a-b\omega)^3 = -(3a^2b+3ab^2)-(a^3+3a^2b-b^3)\omega = \omega(b-a\omega^2)^3$	21
5	$\omega^2(a-b\omega)^3 = -(a^3+3a^2b-b^3)-(a^3-3ab^2-b^3)\omega = -\omega^2(b-a\omega^2)^3$	24
6	$-\omega^2(a-b\omega)^3 = (a^3+3a^2b-b^3)+(a^3-3ab^2-b^3)\omega = \omega^2(b-a\omega^2)^3$	23
7	$(a-b\omega^2)^3 = (a^3+3a^2b-b^3)+(3a^2b+3ab^2)\omega = -(b-a\omega)^3$	14
8	$-(a-b\omega^2)^3 = -(a^3+3a^2b-b^3)-(3a^2b+3ab^2)\omega = (b-a\omega)^3$	13
9	$\omega(a-b\omega^2)^3 = -(3a^2b+3ab^2)+(a^3-3ab^2-b^3)\omega = -\omega(b-a\omega)^3$	16
10	$-\omega(a-b\omega^2)^3 = (3a^2b+3ab^2)-(a^3-3ab^2-b^3)\omega = \omega(b-a\omega)^3$	15
11	$\omega^2(a-b\omega^2)^3 = -(a^3-3ab^2-b^3)-(a^3+3a^2b-b^3)\omega = -\omega^2(b-a\omega)^3$	18
12	$-\omega^2(a-b\omega^2)^3 = (a^3-3ab^2-b^3)+(a^3+3a^2b-b^3)\omega = \omega^2(b-a\omega)^3$	17
	Parametrizovaná Eisensteinova čísla $z-x\omega$ s normou x^2+xz+z^2:	
13	$(b-a\omega)^3 = (b^3-3ba^2-a^3)-(3b^2a+3ba^2)\omega = -(a-b\omega^2)^3$	8
14	$-(b-a\omega)^3 = -(b^3-3ba^2-a^3)+(3b^2a+3ba^2)\omega = (a-b\omega^2)^3$	7
15	$\omega(b-a\omega)^3 = (3b^2a+3ba^2)+(b^3+3b^2a-a^3)\omega = -\omega(a-b\omega^2)^3$	10
16	$-\omega(b-a\omega)^3 = -(3b^2a+3ba^2)-(b^3+3b^2a-a^3)\omega = \omega(a-b\omega^2)^3$	9
17	$\omega^2(b-a\omega)^3 = -(b^3+3b^2a-a^3)-(b^3-3ba^2-a^3)\omega = -\omega^2(a-b\omega^2)^3$	12
18	$-\omega^2(b-a\omega)^3 = (b^3+3b^2a-a^3)+(b^3-3ba^2-a^3)\omega = \omega^2(a-b\omega^2)^3$	11
19	$(b-a\omega^2)^3 = (b^3+3b^2a-a^3)+(3b^2a+3ba^2)\omega = -(a-b\omega)^3$	2
20	$-(b-a\omega^2)^3 = -(b^3+3b^2a-a^3)-(3b^2a+3ba^2)\omega = (a-b\omega)^3$	1
21	$\omega(b-a\omega^2)^3 = -(3b^2a+3ba^2)+(b^3-3ba^2-a^3)\omega = -\omega(a-b\omega)^3$	4
22	$-\omega(b-a\omega^2)^3 = (3b^2a+3ba^2)-(b^3-3ba^2-a^3)\omega = \omega(a-b\omega)^3$	3
23	$\omega^2(b-a\omega^2)^3 = -(b^3-3ba^2-a^3)-(b^3+3b^2a-a^3)\omega = -\omega^2(a-b\omega)^3$	6
24	$-\omega^2(b-a\omega^2)^3 = (b^3-3ba^2-a^3)+(b^3+3b^2a-a^3)\omega = \omega^2(a-b\omega)^3$	5

Tabulka 1. Seznam Eisensteinových čísel s normou x^2+xz+z^2. Nejsou zahrnuta čísla $(a^3+a^2b+ab^2)-(a^2b+ab^2+b^3)\omega$ a jejich jednotkové násobky z vyloučených substitucí (2.21), ((2.22).

s normou x^2+xz+z^2 s výjimkou takových, jež vzniknou pomocí (2.21), (2.22),

obdržíme dvanáct různých substitucí (čísla řádků 1 až 12), které v oboru Eisensteinových čísel řeší rovnici $A^3 = x^2 + xz + z^2$ (čísla v pravém krajním sloupci tabulky ukazují, s kterým jiným pořadovým číslem řádku nastává shoda).

Jak je vidět z tabulky, čtyři substituce, konkrétně č. 3, 4, 9 a 10, kde $x = \pm(3b^2a + 3ba^2)$, jsou ve sporu s předpokladem $3 \nmid x$. Zbylých osm substitucí je založeno (až na případné znaménko) na vzorcích (2.23), (2.24) a (2.28), u nichž jsme došli ke sporu s podmínkami řešitelnosti Fermatovy rovnice (2.8). Rovnice (2.18) je proto v oboru přirozených čísel při podmínkách (2.13), (2.14), (2.15) neřešitelná, jelikož jiné parametrizace rovnice (2.18) neexistují. Z toho pak vyplývá neřešitelnost rovnice (2.8).

Zbývá případ $3 \mid x$ a $3 \mid y$. Vzhledem k symetrii (2.8) vůči x a y stačí uvažovat např. jen případ $3 \mid y$. Budou platit obdobné rovnice jako v případě $3 \mid z$, jen faktor 3 bude nyní obsažen v čísle y a faktor 9 bude svázán s Y^3. Rovnice (2.9) až (2.15) se změní na

$$\begin{aligned} x - 3k &= z - y = X^3, \\ y - 3k &= z - x = 9Y^3, \\ z + 3k &= x + y = Z^3 = X^3 + 9Y^3 + 6k, \\ 3k &= x + y - z = 3XYZ. \end{aligned}$$

Odtud vyjádříme x, y, z pomocí X, Y, Z a z toho pak plyne obdoba rovnice (2.18), tj.

$$(3Y^2 + ZX)^3 = x^2 + xz + z^2. \tag{2.31}$$

K řešení diofantické rovnice (2.31) použijeme zase substituce (2.23), (2.24) a z jejich rozdílu obdržíme

$$\begin{aligned} z - x &= 2a^3 + 3a^2b - 3ab^2 - 2b^3, \\ 9Y^3 &= 2(a^3 - b^3) + 3ab(a - b). \end{aligned} \tag{2.32}$$

Ale ze substitucí (2.23), (2.24) a podmínek $3 \nmid x$, $3 \nmid z$ plyne, že $3 \nmid (a^3 - b^3)$, takže levá strana (2.32) nemůže mít faktor 3. Dospěli jsme tedy opět ke sporu. Jiné substituce k řešení (2.31) nelze použít, protože použitím substituční rovnice (2.28) by číslo x nebo z obsahovalo faktor 3, což se neslučuje s podmínkou $3 \mid y$. Diofantická rovnice (2.31) proto nemá řešení.

Tím je Fermatova věta pro exponent p=3 dokázána. □

3. Několik dalších důsledků fermatovy věty

Rovnici (2.3) lze pomocí (2.1) a (2.2) přepsat také do tvaru identity

$$x + y = \sqrt[3]{x^3 + y^3} + \sqrt[3]{3(x + y)(\sqrt[3]{x^3 + y^3} - x)(\sqrt[3]{x^3 + y^3} - y)}. \tag{3.1}$$

Z této identity je vidět, že každé přirozené číslo větší než 1 lze zapsat jako součet odmocnin tvaru (3.1). A jelikož platí Fermatova věta, tak dílčí odmocniny ve vzorci (3.1) jsou vždy iracionálními čísly. Použijeme-li např. k vyjádření čísla 9

dvou různých součtů 5+4 a 8+1, pak při využití (3.1) dostaneme

$$9 = \sqrt[3]{5^3+4^3} + \sqrt[3]{3(5+4)(\sqrt[3]{5^3+4^3}-5)(\sqrt[3]{5^3+4^3}-4)},$$
$$9 = \sqrt[3]{8^3+1^3} + \sqrt[3]{3(8+1)(\sqrt[3]{8^3+1^3}-8)(\sqrt[3]{8^3+1^3}-1)},$$

odkud porovnáním a po další úpravě obdržíme rovnost

$$\sqrt[3]{7} + \sqrt[3]{(\sqrt[3]{189}-5)(\sqrt[3]{189}-4)} = \sqrt[3]{19} + \sqrt[3]{(\sqrt[3]{513}-8)(\sqrt[3]{513}-1)}.$$

To otvírá možnost generovat takovéto rovnosti třeba pro důkazové úlohy matematických olympiád. Zmiňme ještě, že díky identitám (2.1) a (2.2) platí

$$3(x+y)(z-x)(z-y) = 3(x+y)[xy+z^2-z(x+y)] = 3(x+y)(xy-3kz),$$

odkud

$$xy = 3kz + (z-x)(z-y). \tag{3.2}$$

Díky tomu lze součin celých čísel xy, $x \neq -y$, vyjádřit pomocí součtu součinů iracionálních čísel zase takovouto identitou:

$$xy = \sqrt[3]{3(x+y)\big(\sqrt[3]{x^3+y^3}-x\big)\big(\sqrt[3]{x^3+y^3}-y\big)} \cdot \sqrt[3]{x^3+y^3} + \big(\sqrt[3]{x^3+y^3}-x\big)\big(\sqrt[3]{x^3+y^3}-y\big).$$

Tak můžeme třeba pro číslo -20 obdržet rovnosti

$$\begin{aligned}
-1\cdot 20 &= \sqrt[3]{57\big(\sqrt[3]{7999}-20\big)\big(\sqrt[3]{7999}+1\big)} \cdot \sqrt[3]{7999} + \big(\sqrt[3]{7999}-20\big)\big(\sqrt[3]{7999}+1\big) \\
&= 5\cdot(-4) = \sqrt[3]{3\big(\sqrt[3]{61}-5\big)\big(\sqrt[3]{61}+4\big)} \cdot \sqrt[3]{61} + \big(\sqrt[3]{61}-5\big)\big(\sqrt[3]{61}+4\big) \\
&= 4\cdot(-5) = 4\cdot\Big[\sqrt[3]{-12\big(\sqrt[3]{-124}+5\big)\big(\sqrt[3]{-124}-1\big)} \cdot \sqrt[3]{-124} \\
&\qquad + (\sqrt[3]{-124}+5)(\sqrt[3]{-124}-1)\Big] \\
&= -4\cdot 5 = -4\cdot\Big[\sqrt[3]{18\big(\sqrt[3]{126}-5\big)\big(\sqrt[3]{126}-1\big)} \cdot \sqrt[3]{126} \\
&\qquad + \big(\sqrt[3]{126}-5\big)\big(\sqrt[3]{126}-1\big)\Big],
\end{aligned}$$

odkud vidíme, jak odlišné může být vyjádření téhož celého čísla pomocí iracionálních čísel.

Rovnici (3.2) lze díky (2.9) a (2.10) také zapsat ve tvaru $xy - 3kz = X^3Y^3$. Za povšimnutí rovněž stojí, že součin xy musí být vyjádřitelný ve formě rozdílu třetích mocnin

$$xy = (3Z^2)^3 - (3Z^2 - XY)^3, \tag{3.3}$$

což lze odvodit např. z identity $3xy(x+y) = (x+y)^3 - (x^3+y^3)$ dosazením $9Z^3$ za $x+y$ a z^3 za x^3+y^3. Proto x a y musí být podle Viètových vzorců kořeny kvadratické rovnice

$$t^2 - 9Z^3 t + [(3Z^2)^3 - (3Z^2 - XY)^3] = 0, \tag{3.4}$$

neboť $(t-x)(t-y) = t^2 - (x+y)t + xy = 0$.

Z (3.2) a (3.3) také plyne, že $3kz = (3Z^2)^3 - (3Z^2 - XY)^3 - (XY)^3$, což odpovídá tomu, že $3(3Z^2)(3Z^2 - XY)(XY) = (3Z^2)^3 - (3Z^2 - XY)^3 - (XY)^3$ je identita. A protože má podle (2.11) platit $3k + z = 9Z^3$, musí být $3k$ a z kořeny kvadratické rovnice

$$t^2 - 9Z^3 t + [(3Z^2)^3 - (3Z^2 - XY)^3 - (XY)^3] = 0, \tag{3.5}$$

neboť $(t-3k)(t-z) = t^2 - (3k+z)t + 3kz = 0$.

Paraboly (3.4) a (3.5) se tedy liší jen vertikálním posunem o $(XY)^3$. Pokud bychom znali správné hodnoty X a Y, mohli bychom díky tomuto poznatku určit správnou hodnotu Z graficky. Na vodorovné souřadnicové ose t vyneseme úsečku délky $X^3 + Y^3$, v koncových bodech vztyčíme kolmice délky X^3Y^3 a sestrojíme obdélník - v obrázku 2 naznačený čárkovaně. Vrcholem $[3k, X^3Y^3]$ a vrcholem $[z, X^3Y^3]$ tohoto obdélníka vedeme přímky r a s osově souměrné podle společné vertikální osy čárkovaného obdélníka a paraboly (3.4). Otáčení přímek r a s kolem vrcholů $[3k, X^3Y^3]$, $[z, X^3Y^3]$ umožňuje najít na vertikální ose bod $[(9Z^3)/2, 3(XYZ)^2/2]$ a na horizontální ose t body $[0,0]$ a $[9Z^3, 0] = [X^3 + Y^3 + 6XYZ, 0]$. Pro směrnici přímek pak bude platit $\tan\alpha = \pm(X^3Y^3)/3XYZ = \pm(3(XYZ)^2)/(9Z^3) = \pm(X^2Y^2)/(3Z)$. Existuje jen jedna poloha přímek r a s, kde to platí, protože při otáčení se zmenšováním úhlu α úsek vyťatý přímkami r a s na vodorovné ose t prodlužuje, jinými slovy k hodnotě $3XYZ$ se při otáčení přímky s blížíme zdola, zatímco vertikální souřadnice průsečíku s osou obdélníka se zmenšuje, čili k hodnotě $3(XYZ)^2/2$ se blížíme shora. Tím je možné graficky určit hodnoty $3XYZ$, $9Z^3$, a tudíž i Z. Bohužel tím, ale není nikterak garantováno, že Z je celé číslo. Obr. 2 nám ale může posloužit k lepší představě o tom, s jak velkými čísly máme při řešení FLT do činění.

Jak již bylo ukázáno, když $3 \mid z$, tak z (2.15) plyne, že $3 \mid Z$. Proto $x + y = 3k + z = 9Z^3$ je násobkem čísla $3^5 = 243$. Z tabulek goniometrických funkcí lze zase vyčíst, že $\tan(89°50') \doteq 343{,}7731$. Stačí tedy, aby poměr $(X^2Y^2)/3Z$ byl větší než tato hodnota a sklon přímek r a s se bude velmi blížit k $90°$.

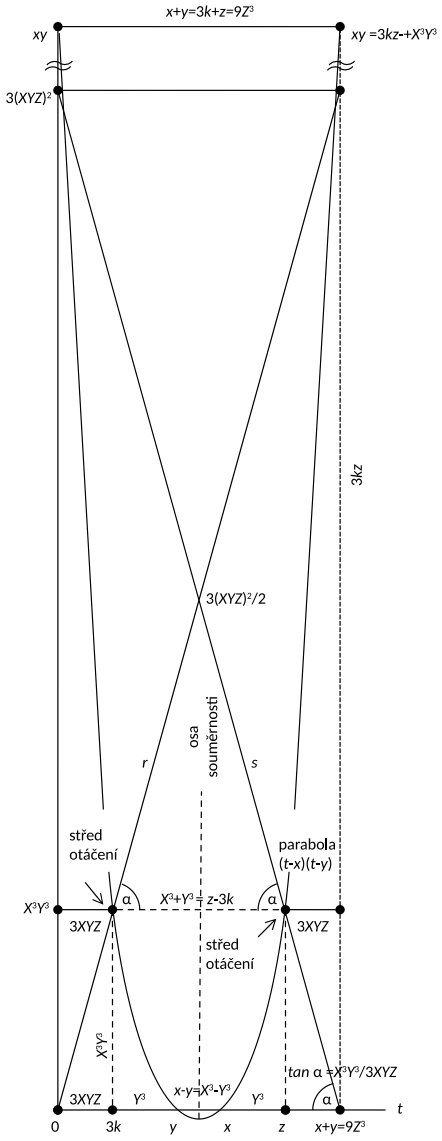
Dalším důsledkem platnosti Fermatovy věty je např. to, že diofantické rovnice

$$\begin{aligned}(3XYZ + X^3)^3 + (3XYZ + Y^3)^3 &= (3XYZ + X^3 + Y^3)^3 \\ &= (9Z^3 - 3XYZ)^3,\end{aligned} \tag{3.6}$$

$$(z - X^3)^3 + (z - Y^3)^3 = z^3 \tag{3.7}$$

nemají v oboru přirozených čísel řešení. Rovnice (3.6) vyplývá z (2.13), (2.14) a (2.15), rovnice (3.7) vznikne dosazením ze vztahů (2.9) a (2.10) do (2.8).

Důsledkem platnosti Fermatovy věty je také to, že k sečně s_1 křivky $f(t) = t^3$, jež prochází body s celočíselnými souřadnicemi $[z, z^3]$, $[x, x^3]$, nemůže existovat rovnoběžná sečna s_2, procházející body $[y, y^3]$, $[3k, 0]$. Plyne to z (2.10) a (2.14), protože směrnice takové sečny je $\tan\beta = (z^3 - x^3)/(z - x) = z^2 + zx + x^2 = y^3/(y - 3k) = y^3/Y^3 = (Y^2 + 3XZ)^3$. A o rovnici (2.18) jsme dokázali, že v oboru přirozených čísel nemá řešení. Rovnici (2.18) lze zapsat s využitím (2.10) také ve tvaru $3xz = (Y^2 + 3XZ)^3 - (Y^2)^3$ nebo po dosazení z (2.13) a (2.15) ve tvaru $9XZ(X^2 + 3YZ)(3Z^2 - XY) = (Y^2 + 3XZ)^3 - (Y^2)^3$. Součin xz lze též



Obrázek 2. Grafické určení hodnoty Z.

nahradit výrazy $xz = ((z+x)/2)^2 - ((z-x)/2)^2 = ((9Z^3+X^3)/2)^2 - (Y^3/2)^2$ nebo $xz = ((3XZ+(X^2+3YZ)(3Z^2-XY))/2)^2 - ((3XZ-(X^2+3YZ)(3Z^2-XY))/2)^2$, odkud bychom dostali další neřešitelné diofantické rovnice.

Existuje celá řada jiných diofantických rovnic, jež jsou ekvivalentní s Fermatovou rovnicí (2.8), a nemají tudíž řešení. Např. rovnice $(z^3)^3 - (x^3)^3 - (y^3)^3 =$

$3(xyz)^3$, která by v případě platnosti $z^3 = x^3 + y^3$ byla identitou. S Fermatovou rovnicí $z^3 = x^3 + y^3$ jsou ekvivalentní také např. rovnice

$$\begin{gathered}(x+y)^3 - (z-x)^3 - (z-y)^3 - (x+y-z)^3 = 6xyz,\\ (x+y)^3 - (z-x)^3 - (z-y)^3 = 6xyz + 3(x+y)(z-x)(z-y),\\ (z-x)[(z-x)^2 + 3(z+x)^2] = 4y^3,\end{gathered}$$

jak lze ověřit výpočtem. Podobně není řešitelná žádná diofantická rovnice ekvivalentní s rovnicí

$$9Z^3 - 6XYZ = X^3 + Y^3, \tag{3.8}$$

kterou dostaneme z (2.15). Kdybychom pomocí vzorce pro kubické rovnice separovali v (3.8) např. proměnnou Z, obdržíme

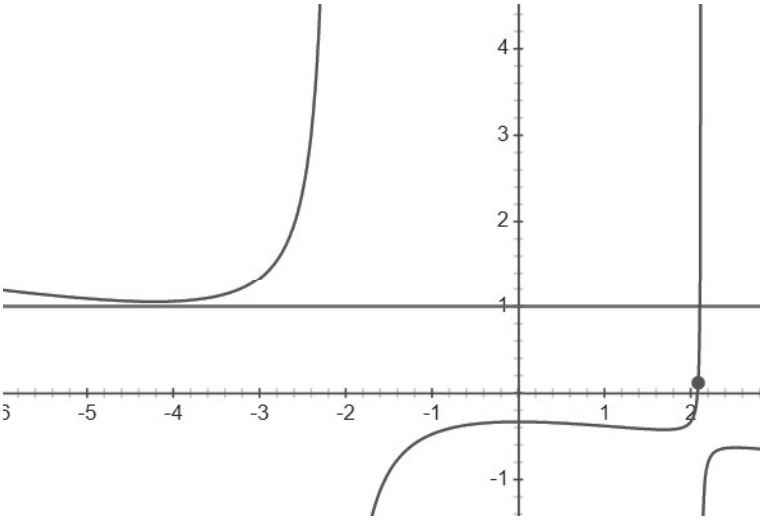
$$Z = \frac{4\sqrt[3]{2XY + \sqrt[3]{4\sqrt[3]{((3X^3 + \sqrt{(9X^6 - 14X^3Y^3 + 9Y^6)} + 3Y^3)^2)}}}}{6\sqrt[3]{(3X^3 + \sqrt{(9X^6 - 14X^3Y^3 + 9Y^6)} + 3Y^3)}}, \tag{3.9}$$

jak lze pohodlně ověřit pomocí webu http://www.wolframalpha.com.

Substitucí $Z = (X+Y)/r$, $r \in \mathbb{R}^+$, lze rovnici (3.9) zapsat ve tvaru

$$\begin{gathered}9((X+Y)/r)^3 - [(X+Y)^3 - 3XY(X+Y)] - 6XY((X+Y)/r) = 0,\\ 9(X+Y)^2(1/r)^3 - [(X+Y)^2 - 3XY] - 6XY(1/r) = 0,\\ 9(X+Y)^2 - [(X+Y)^2 - 3XY]r^3 - 6XYr^2 = 0,\\ (r^3 - 6r^2 + 18)XY - (r^3 - 9)(X^2 + Y^2) = 0,\\ -(6r^2 - 27)XY - (r^3 - 9)(X^2 + Y^2 - XY) = 0,\\ (9 - r^3)/(6r^2 - 27) = XY/(X^2 + Y^2 - XY).\end{gathered} \tag{3.10}$$

Díky nerovnosti $(X-Y)^2 > 0$ platí vždy $X^2+Y^2-XY > XY$. Zlomek $XY/(X^2+Y^2-XY)$ na pravé straně (3.10) bude proto vždy menší než 1. Zajímá nás, pro jaké hodnoty r je zlomek $(9-r^3)/(6r^2-27)$ na levé straně (3.10) kladný, ale menší než 1, aby se obě strany (3.10) mohly rovnat. To snadno zjistíme vyšetřením průběhu funkce $f(r) = (9-r^3)/(6r^2-27)$. Předně je vidět, že $f(r)$ má dva body nespojitosti, kde funkce není definována. Jsou to body odpovídající kořenům kvadratické rovnice $6r^2 - 27 = 0$, čili $r = \pm 3/\sqrt{2} \doteq \pm 2{,}121320$. Pro všechna $r > 3/\sqrt{2}$ je jmenovatel zlomku $(9-r^3)/(6r^2-27)$ kladné číslo, zatímco čitatel je záporný. Funkce $f(r)$ tudíž v této oblasti nesplňuje požadovanou podmínku $0 < f(r) < 1$, protože je pro $r > 3/\sqrt{2}$ záporná. Funkce $f(r) = (9-r^3)/(6r^2-27)$ je nulová, když $9 - r^3 = 0$, neboli pro $r = \sqrt[3]{9} \doteq 2{,}080083$. Pro $r \in (0, \sqrt[3]{9})$ je jmenovatel zlomku $(9-r^3)/(6r^2-27)$ kladný a čitatel záporný, jak lze ověřit dosazením. Funkce $f(r)$ je tudíž na tomto intervalu záporná. Podmínce $0 < f(r) < 1$ lze proto při $r \in \mathbb{R}^+$ vyhovět jen pro r z intervalu $(\sqrt[3]{9}, 3/\sqrt{2}) \doteq (2{,}08, 2{,}12)$. Dostáváme tak podmínku řešitelnosti rovnice (3.9) ve tvaru $\sqrt[3]{9} < (X+Y)/Z < 3/\sqrt{2}$. Graf průběhu funkce $f(r)$ je pro ilustraci zachycen na obrázku 3, kde je vyznačen také přípustný interval funkčních hodnot mezi nulou a jedničkou.



Obrázek 3. Graf funkce $f(r) = (9 - r^3)/(6r^2 - 27)$.

Uveďme na závěr bez odvozování řadu ekvivalentních diofantických rovnic, jež na množině kladných čísel mají stejné řešení (3.9):

$$3((3Z^3)/2)^2 + ((X^3 - Y^3)/2)^2 = (3Z^2 - XY)^3,$$

$$(9Z^3)^3 - (X^3)^3 - (Y^3)^3 = 3XYZ\Big[6(3Z^2 - XY)(X^2 + 3YZ)(Y^2 + 3XZ) + (3XYZ)^2\Big],$$

$$(9Z^3)^2 + (X^3)^2 + (Y^3)^2 = 3(3Z^2 - XY)(X^2 + 3YZ)(Y^2 + 3XZ) + X^3Y^3 - 9Z^3(X^3 + Y^3),$$

$$(9Z^3)^2 + (X^3)^2 + (Y^3)^2 = 9XYZ(9Z^3 - X^3 - Y^3 - 2XYZ) - 2X^3Y^3 + 18Z^3(X^3 + Y^3),$$

$$(Y^2 + 3XZ)^3 = (9Z^3 - 3XYZ)^2 + (9Z^3 - 3XYZ)(X^3 + 3XYZ) + (X^3 + 3XYZ)^2,$$

$$(3Z^3)^2 + 3Z^3\frac{X^3 - Y^3 - 3Z^3}{2} + \left(\frac{X^3 - Y^3 - 3Z^3}{2}\right)^2 = \frac{(X^3 + 3XYZ)^3 + (Y^3 + 3XYZ)^3}{(3Z)^3},$$

$$[(X + Y)^3 - (2Z)^3 - Z^3][3Z(X + Y - Z) - XY] = XY(3Z - X - Y)^3,$$

$$(9Z^3 - X^3 + Y^3)(9Z^3 + X^3 - Y^3) = 4XY(X^2 + 3YZ)(Y^2 + 3XZ),$$

$$3XY(X + Y - 2Z) = (X + Y)^3 - (2Z)^3 - Z^3,$$

$$3(X+Y-2Z)[3Z(X+Y-Z)-XY]=(3Z-X-Y)^3,$$
$$[X+Y-2Z][(X+Y)^2+(X+Y)2Z+(2Z)^2-3XY]=Z^3,$$
$$[X+Y-2Z][(X-Y)^2-(X-Y)(2Z+X)+(2Z+X)^2]=Z^3,$$
$$[X+Y-2Z][(X-Y)^3+(2Z+X)^3]=(2X-Y+2Z)Z^3,$$
$$3(X+Y-2Z)(X-Z)(Y-Z)=(X+Y-2Z)^3+(X+Y)^3 - (X+Y-Z)^3-(2Z)^3,$$
$$(X+Y-Z)^3-3(X+Y)(Z-X)(Z-Y)=(2Z)^3-6XYZ,$$
$$16Z^3-6XYZ=(X+Y)^3-(Z-X)^3 - (Z-Y)^3-3(X+Y)(Z-X)(Z-Y),$$
$$3(X+Y)(Z-X)(Z-Y)=(X+Y)^3-(Z-X)^3 - (Z-Y)^3-7Z^3-X^3-Y^3,$$
$$[(Y^3)^2+3(9Z^3+X^3)^2]=4(Y^2+3XZ)^3,$$
$$[X+Y-2Z][(Y-2Z-2X)^2+3(Y+2Z)^2]=4Z^3,$$
$$Z[3((2X+2Y-Z)/2)^2+(Z/2)^2]=(2Z)^3+(Z-X)^3+(Z-Y)^3,$$
$$Z\Big[(2X+2Y-Z)^2-(2X+2Y-Z)(X+Y-Z)+(X+Y-Z)^2\Big] = (2Z)^3+(Z-X)^3+(Z-Y)^3,$$
$$(3Z^2-XY)(X^2+3YZ)-Y(Y^3+3XYZ)=3X^2Z^2,$$
$$(X^2+3YZ)(Y^2+3XZ)=3Z(9Z^3-3XYZ)+X^2Y^2,$$
$$XY(X^2+3YZ)(Y^2+3XZ)=(3Z^2)^3-(3Z^2-XY)^3,$$
$$9XZ(X^2+3YZ)(3Z^2-XY)=(Y^2+3ZX)^3-(Y^2)^3,$$
$$(9Z^3+X^3-Y^3)(9Z^3-X^3+Y^3)=4[(3Z^2)^3-(3Z^2-XY)^3],$$
$$(9Z^3+X^3-Y^3)^3+(9Z^3-X^3+Y^3)^3=(9Z^3+X^3+Y^3)^3,$$
$$(3Z)^3[(3Z^2-XY)^2]^3=X^3[Y(Y^3+3XYZ)+3Z^2X^2]^3 + Y^3[X(X^3+3XYZ)+3Z^2Y^2]^3,$$
$$(X+Y)^3-(2Z)^3=(X+Y-Z)^3+(Z-X)^3+(Z-Y)^3,$$
$$(9Z^3+X^3+Y^3)^3+(6XYZ)^3=(9Z^3+X^3-Y^3)^3 + (9Z^3-X^3+Y^3)^3+(9Z^3-X^3-Y^3)^3,$$
$$(9Z^3-6XYZ)^3=(X^3)^3+3(X^2Y)^3+3(XY^2)^3+(Y^3)^3,$$
$$3([(3Z^2)^3-(3Z^2-XY)^3])(X^3-Y^3)=(X^3+3XYZ)^3 - (Y^3+3XYZ)^3-(X^3-Y^3)^3.$$

Přímý důkaz neřešitelnosti kterékoli z těchto rovnic bude proto znamenat další nový důkaz FLT pro $p=3$. Speciálně první rovnice $3(\frac{3Z^3}{2})^2+(\frac{X^3-Y^3}{2})^2=$

$(3Z^2 - XY)^3$, která se ve tvaru $3v^2 + u^2 = s^3$ vyskytuje v klasických důkazech neřešitelnosti Fermatovy rovnice (2.8), nabízí díky dodatečným podmínkám, jež vyplývají ze znalosti potřebné vnitřní struktury v, u, s, snazší a kratší důkaz bez nutnosti použití důkazové metody nekonečného sestupu.

4. Závěr

Fermatovu rovnici v součtovém tvaru (1.1) lze převést do součinového tvaru i pro libovolný jiný prvočíselný exponent $p > 3$. Na rozdíl od případu $p = 3$ však bude součinový tvar kromě $p(x + y)(z - x)(z - y)$ ještě obsahovat dalšího činitele $W = (x+y-z)^p/[p(x+y)(z-x)(z-y)]$, takže $(pk)^p = p(x+y)(z-x)(z-y)W$, a rovnice (3.8) změní svůj tvar na $p^{(p-1)}Z^p - 2pXYZW = X^p + Y^p$. Důkaz neřešitelnosti této rovnice by znamenal nalezení důkazu Fermatovy věty pro libovolný exponent.

Poděkování

Děkuji touto cestou profesoru RNDr. Michalu Křížkovi, DrSc. z Matematického ústavu AV ČR a profesoru RNDr. Aleši Drápalovi, CSc., DSc. z Matematicko-fyzikální fakulty Univerzity Karlovy za podnětné připomínky. Velký dík patří také profesoru Ing. Miroslavu Valachovi, CSc. ze San José State Univertity, California, díky němuž jsem se problematice důkazu Velké Fermatovy věty začal před časem věnovat. Oba posledně jmenovaní jsou stejně jako já bývalými pracovníky již zaniklého Výzkumného ústavu matematických strojů (VÚMS) založeného světoznámým počítačovým odborníkem profesorem Dr. Ing. Antonínem Svobodou. Můj dík patří také mému synovi RNDr. Martinu Golanovi, Ph.D. za pomoc při převodu textu z formátu LyX do formátu LaTeX.

Reference

[1] N. F. Benschop: *Additive structure of the group of units mod pk with core and carry concepts for extension to integers*, Acta Math. Univ. Comenian. **74** (2005), No. 2, 169–184.
[2] A. Lósch: *The Economics of Location*, Yale University Press, 1954.
[3] P. Ribenboim: *Fermat's Last Theorem for Amateurs*, Springer-Verlag, New York, 1999.
[4] R. Taylor, A. Wiles: *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math. **141** (1995), 553–572.
[5] A. Wiles: *Modular elliptic curves and Fermat's Last Theorem*, Ann. of Math. **141** (1995), 443-551.

Petr Golan, Praha; autor je bývalý vědecký pracovník Výzkumného ústavu matematických strojů v Praze, následně byl jednatelem společností VUMS Computers, APOGEE.CZ a Apogee Software, nyní je v důchodu,
e-mail: petrgolan@volny.cz