JAK MOHL FERMAT UVAŽOVAT

LADISLAV KOCANDA

ABSTRAKT. Článek je rozdělen na dvě části. Vprvní části dokážeme, že pro žádná přirozená čísla x, y, z a n, kde $n \geq 3$, neplatí rovnost $xn + yn = zn$. Kdůkazu nepoužijeme přímo čísla x, y, z ale jejich rozklad na čísla v, d a p, pro která platí: $x = p + d, y = p + v$a $z = p + d + v$. Vdruhé části dokážeme dvě nejzávažnější věty, na které je vprvní části odkazováno.

1. ÚVOD

Pierre de Fermat (1601–1665) zanechal před třista čtyřiceti osmi léty ve své pozůstalosti jistou Diofantovu knihu, v níž poznamenává, že pro žádná přirozená čísla x, y, z a n, kde $n \geq 3$, neplatí rovnost $x^n + y^n = z^n$. Pro více informací je možné nahlédnout do literatury [1, 2, 3, 4].

Vztah $x^n + y^n = z^n$ funguje bez problémů v oboru přirozených čísel pro $n = 1$ a s použitím vzorců i pro $n = 2$. Uvažujme o tom, co se změnilo, když za n zvolíme číslo liché větší nebo rovno 3.

2. DŮKAZ VELKÉ FERMATOVY VĚTY

Ze vztahu $x^n + y^n = z^n$ je patrné, že $x < z$ a $y < z$, a proto musí existovat přirozené číslo v takové, že $z = x + v$, a přirozené číslo d takové, že $z = y + d$.

Lze dokázat, že existuje přirozené číslo p takové, že $x+y = z+p$. Nahradíme-li ve vztahu $x + y = z + p$ číslo z, pak

$$x + y = z + p = x + v + p,$$

tedy $y = p + v$ a $x + y = y + d + p$, z toho $x = p + d$.

Při nahrazení čísel x a y platí $(p + d) + (p + v) = z + p$, a tedy $z = p + d + v$. Platí-li pro přirozená čísla x, y, z a n vztah $x^n + y^n = z^n$, pak platí i $y^n = z^n - x^n$, tedy $y^n = (zx) \cdot G$, kde G je číslo přirozené. Položíme-li $z - x = v$, lze dokázat, že ze vztahu $y^n = v \cdot G$ bude $v_1 = \gcd(y, v)$. Dále, platí-li pro přirozená čísla x, y, z a n, vztah $x^n + y^n = z^n$, pak platí i $x^n = z^n y^n$, a tedy $x^n = (zy) \cdot W$, kde W je číslo přirozené. Položíme-li $z - y = d$, pak ze vztahu $x^n = d \cdot W$, dostáváme $d_1 = \gcd(x, d)$. Ze vztahu $v_1 = \gcd(y, v)$ je

$$y = v_1 \cdot g1 \text{ a } v = v_1 \cdot g_2,$$

2010 *MSC.* Primární 11D41.

Klíčová slova. Velká Fermatova věta, Pierre de Fermat.

Práce byla podporována projektem A-Math-Net – Síť pro transfer znalostí v aplikované matematice (CZ.1.07/2.4.00/17.0100).

kde $\gcd(g_1, g_2) = 1$, a ze vztahu $d_1 = \gcd(x, d)$ vyplývá, že

$$x = d_1 \cdot w_1 \text{ a } d = d_1 \cdot w_2,$$

kde $\gcd(w_1, w_2) = 1$. Protože $p = yv$, je $p = v_1 \cdot (g_1 - g_2)$ a $p = x - d$ je $p = d_1 \cdot (w_1 - w)$ a platí, že

$$v_1 \cdot (g_1 - g_2) = d_1 \cdot (w_1 - w_2).$$

Protože v_1 a d_1 jsou čísla nesoudělná (v opačném případě by byla soudělná i čísla x, y, z), platí, že $v_1 = (w_1 - w_2)$ a $d_1 = (g_1 - g_2)$, tedy $p = v_1 \cdot d_1$.

Nyní se vraťme k otázce, co by se změnilo, pokud by číslo n bylo větší nebo rovno 3, a hlavně, když n bude liché. Mějme tedy n číslo liché větší nebo rovno třem. Jestliže pro přirozená nesoudělná čísla x, y, z platí $z^n = x^n + y^n$, pak platí, že $z^n = (x + y) \cdot U$, kde U je číslo přirozené, tedy $z_1 = \gcd((x + y), z)$. Pak $z = z_1 \cdot u_1$ a $(x + y) = z_1 \cdot u_2$. Protože $x + y = z + p$, musí platit $z + p = z_1 \cdot u_2$. Z předchozího plyne, že $z_1 \cdot u_1 + v_1 \cdot d_1 = z_1 \cdot u_2$ a následně $v_1 \cdot d_1 = z_1 \cdot u_2 - z_1 \cdot u_1$ a $v_1 \cdot d_1 = z_1 \cdot (u_2 - u_1)$. Z tohoto zápisu ale vyplývá, že buď v_1 nebo d_1 musí být soudělné s číslem z_1. Tedy pro $n > 2$ liché budou čísla v_1, d_1, z_1 soudělná a tím budou soudělná i čísla x, y, z. Z toho plyne závěr, že neexistují přirozená nesoudělná čísla x, y, z a liché číslo $n > 2$, pro něž platí $x^n + y^n = z^n$.

Zde dokážeme dvě věty, na které je v textu odkazováno.

Věta 2.1. *Platí-li pro přirozená nesoudělná čísla vztah $x^n + y^n = z^n$, pak existuje přirozené číslo p takové, že platí $x + y = z + p$.*

Důkaz. Podívejme se, v jakém vztahu jsou přirozená čísla $x+y$ a číslo z. Pokud by $x+y < z$, pak pro $n > 1$ platí $(x+y)^n < z^n$. Tedy $x^n + nx^{n-1}y + \ldots + y^n < z^n$ a $x^n + nx^{n-1}y + \ldots + y^n - z^n < 0$. Protože $x^n + y^n z^n = 0$ a $nx^{n-1}y + \ldots nxy^{n-1}$ je kladné, dojdeme ke sporu. Když tedy $x + y > z$, pak existuje přirozené číslo p takové, že $x + y = z + p$. □

Poznámka 2.2. Pokud ve vztahu $x^n + y^n = z^n$ je $n = 1$, pak $x + y = z$, a tedy $p = 0$.

Věta 2.3. *Platí-li pro přirozená nesoudělná čísla x, y, z a $n > 1$ vztah $x^n + y^n = z^n$, pak ze vztahu $x+y = z+p$ je číslo $p = v_1 \cdot d_1$, kde $v_1 = \gcd(y, v)$ a $d_1 = \gcd(x, d)$ při $zx = v$ a $z - y = d$.*

Důkaz rozdělíme na dvě části.

Věta 2.4. *Platí-li* $\gcd((g_1 - g_2), (w_1 - w_2)) = 1$ *a* $\gcd(x, y, z) = 1$*, pak* $p = v_1 \cdot d_1$.

Důkaz. K důkazu použijeme známou větu: Jestliže $b | a_1 \cdot b_1$ a je-li $\gcd(b, a_1) = 1$, pak $b | b_1$.

Nechť $\gcd((g_1 - g_2), (w_1 - w_2)) = 1$ ve vztahu $v_1 \cdot (g_1 - g_2) = d1 \cdot (w_1 - w_2)$, kdy $(g_1 - g_2) | d_1 \cdot (w_1 - w_2)$, při $\gcd((g_1 - g_2), (w_1 - w_2)) = 1$ je $(g_1 - g_2) | d_1$, tedy $d_1 = k \cdot (g_1 - g_2)$. Po dosazení $v_1 \cdot (g_1 - g_2) = k \cdot (g_1 - g_2) \cdot (w_1 - w_2)$ je $v_1 = k \cdot (w_1 - w_2)$, pak dostáváme

$$\begin{aligned}
x &= d_1 \cdot w_1 = k \cdot (g_1 - g_2) \cdot w_1, \\
y &= v_1 \cdot g_1 = k \cdot (w_1 - w_2) \cdot g_1, \\
z &= x + v = k \cdot (g_1 - g_2) \cdot w_1 + k \cdot (w_1 - w_2) \cdot g_2 = \\
&= k \cdot ((g_1 - g_2) \cdot w_1 + (w_1 - w_2) \cdot g_2).
\end{aligned}$$

Závěr: Bude-li $k > 1$, pak čísla x, y, z jsou soudělná. Při $k = 1$ jsou čísla x, y, z nesoudělná, jak bylo požadováno. Tedy platí, že je-li $d_1 = g_1 - g_2$ a $v_1 = w_1 - w_2$, pak dostáváme $p = v_1 \cdot d_1$. □

Věta 2.5. *Přirozená čísla x, y, z jsou nesoudělná právě tehdy, když $p = v_1 \cdot d_1$.*

Důkaz. Pro násobky trojice přirozených čísel x, y, z, pro která platí

$$\gcd(x, y, z) = 1$$

zaveďme: $X = k \cdot x$, $Y = k \cdot y$, $Z = k \cdot z$, kdy $\gcd(X, Y, Z) = k$.

1. Důkaz první části věty „jestliže $\gcd(x, y, z) = 1$, pak $p = v_1 \cdot d_1$“ provedeme nepřímo. Předpokládejme, že $p = v_1 \cdot d_1 \cdot k$. Pak

$$p = v_1 \cdot d_1 \cdot k = v_1 \cdot (g_1 - g_2),$$

   z toho

$$d_1 \cdot k = (g_1 - g_2) \text{ a } d_1 = \frac{1}{k} \cdot (g_1 - g_2).$$

   Dále $v_1 \cdot d_1 \cdot k = d_1 \cdot (w_1 - w_2)$, pak

$$v_1 \cdot k = (w_1 - w_2) \text{ a } v_1 = \frac{1}{k} \cdot (w_1 - w_2).$$

   Dostáváme

$$\begin{aligned} x = d_1 \cdot w_1 &= \frac{1}{k} \cdot (g_1 - g_2) \cdot w_1, & X &= x \cdot k = (g_1 - g_2) \cdot w_1, \\ y = v_1 \cdot g_1 &= \frac{1}{k}(w_1 - w_2) \cdot g_1, & Y &= y \cdot k = (w_1 - w_2) \cdot g_1, \end{aligned}$$

   a tedy

$$\begin{aligned} z &= x + v = \frac{1}{k}((g_1 - g_2) \cdot w_1 + (w_1 - w_2) \cdot g_2), \\ Z &= z \cdot k = g_1 \cdot w_1 + w_2 \cdot g_2. \end{aligned}$$

   Závěr: Bude-li $k > 1$, pak jsou X, Y, Z čísla soudělná. Aby byla čísla X, Y, Z nesoudělná, musí být $k = 1$ a platí naše tvrzení: Jestliže $\gcd(x, y, z) = 1$, pak $p = v_1 \cdot d_1$.
2. Důkaz druhé části věty „jestliže $p = v_1 \cdot d_1$, pak $\gcd(x, y, z) = 1$“, provedeme opět nepřímo. Jestliže $k = \gcd(X, Y, Z)$, pak dostáváme $P = v_1 \cdot d_1 \cdot k$. Protože platí:

$$\begin{aligned} X + Y &= Z + P, \\ k \cdot x + k \cdot yk \cdot z &= P, \end{aligned}$$

   Pak $P = k \cdot (x + y - z) = k \cdot p = k \cdot v_1 \cdot d_1$. Tedy platí: Jestliže $p = v_1 \cdot d_1$, pak $\gcd(x, y, z) = 1$.

Závěr: Přirozená čísla x, y, z jsou nesoudělná právě tehdy, jestliže $p = v_1 \cdot d_1$. □

3. Závěr

Důkaz známé věty, posléze nazvané Velká Fermatova věta, nebyl v pozůstalosti Pierre de Fermata objeven, ale víme, že Fermat našel důkaz pro n rovno čtyřem. Pro jiná čísla důkaz údajně nehledal. Dovoluji si vyslovit myšlenku, že Pierre de Fermat objevil podobný jednoduchý důkaz, který předkládám. Z tohoto důkazu je patrné, že platí pro všechna lichá čísla větší nebo rovná číslu 3. Proto vidím jako logické, že Fermat musel najít důkaz pro n rovno čtyřem, aby jeho důkaz byl úplný.

Reference

[1] F. Veselý: *O dělitelnosti čísel celých*, Praha, 1966.
[2] J. Polák: *Přehled středoškolské matematiky*, SPN Praha, 1972.
[3] W. Sierpinski: *Co víme a co nevíme o prvočíslech*, SPN Praha, 1966.
[4] J. Sedláček: *Co víme o přirozených číslech*, Praha, 1961.

Ladislav Kocanda, Na Pískách 69/II, 391 81 Veselí nad Lužnicí, Česká republika,
e-mail: `ladislav.kocanda@gmail.com`