# Velká Fermatova věta

*Radek Erban*

Velká Fermatova věta je jeden z nejslavnějších matematických problémů, jehož řešení odolávalo matematikům celá staletí. Začalo to celkem nevinně, to si Pierre Fermat při četbě Diofantovy Aritmetiky poznamenal na okraj knížky, že pro přirozené číslo $n \geq 3$ neexistují netriviální celočíselná řešení rovnice

$$x^n + y^n = z^n.$$

Napsal také, že objevil jednoduchý důkaz tohoto tvrzení, nicméně se mu na ten kraj už nevejde, proto ho nebude psát. Po Fermatově smrti tato úloha zaměstnávala mnoho matematiků. Jednoduchost jejího zadání vedla k tomu, že jí zasvětilo život i mnoho matematických laiků. Velká Fermatova věta se stala inspirací k rozvoji mnoha matematických disciplín, na počátku století byla rovněž vypsána peněžitá odměna za její důkaz, její sláva ji přivedla i jako téma do beletrie pro nematematickou veřejnost. Až teprve před pěti lety tento nejslavnější matematický oříšek rozlousknul Andrew Wiles.

V tomto sborníčku nalezne čtenář seznam nejdůležitějších pojmů a tvrzení, kterými se na přednášce budeme zabývat, aby se mu lépe přednáška chápala. Některé z uvedených vět jsou zřejmé, jiné pak vyžadují sofistikovanější zdůvodnění. K jejich dobrému pochopení je dobré si rozmyslet různé analogie se známými věcmi, ale o tom až na přednášce.

## Seznam definic

**Definice.** *Definujme komplexní číslo $\varrho$ předpisem*

$$\varrho = \frac{1}{2}\left(-1 + i\sqrt{3}\right),$$

*tj. $\varrho$ je řešením kvadratické rovnice*

$$\varrho^2 + \varrho + 1 = 0.$$

**Definice.** *Množinu čísel $k(\varrho)$ tvoří čísla tvaru $a + b\varrho$, kde $a$, $b$ jsou celá čísla.*

**Definice.** *Řekneme, že číslo $\xi \in k(\varrho)$ je dělitelné číslem $\eta \in k(\varrho)$, pokud existuje číslo $\zeta \in k(\varrho)$ takové, že $\xi = \eta\zeta$. Tuto skutečnost zapisujeme $\eta|\xi$.*

**Definice.** *Řekneme, že číslo $\varepsilon \in k(\varrho)$ je jednotka (unit) v $k(\varrho)$, pokud pro každé $\xi \in k(\varrho)$ platí $\varepsilon|\xi$.*

**Definice.** *Pokud $\varepsilon \in k(\varrho)$ je jednotka, pak číslo $\varepsilon\xi$ je asociováno (associated) s číslem $\xi \in k(\varrho)$.*

**Definice.** *Prvočíslo je číslo různé od nuly a jednotky, které je dělitelné jen čísly asociovanými s ním nebo s jedničkou.*

**Definice.** *Norma čísla $\xi = a + b\varrho$ je*

$$N\xi = (a + b\varrho)(a + b\varrho^2) = a^2 - ab + b^2.$$

## Seznam vět

**Věta.** *Obecné řešení rovnice*

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

*splňující podmínky*

$$x > 0,\ y > 0,\ z > 0,\ (x, y) = 1,\ 2|x$$

*je tvaru*

$$x = 2ab,\ y = a^2 - b^2,\ z = a^2 + b^2,$$

*kde $a$, $b$ jsou čísla opačné parity a $(a, b) = 1$, $a > b > 0$.*

**Věta.** *Neexistují kladná celá čísla $x$, $y$, $z$ vyhovující diofantické rovnici*

$$x^4 + y^4 = z^2.$$

**Věta.** (Vlastnosti normy)
*(a)* *Norma je vždy nezáporná.*
*(b)* $|a + b\varrho|^2 = N(a + b\varrho)$.
*(c)* $N\alpha N\beta = N(\alpha\beta)$.
*(d)* *Norma jednotky je 1 a každé číslo jehož norma je 1 je jednotka.*
*(e)* *Číslo z $k(\varrho)$, jehož norma je (racionální) prvočíslo, je prvočíslo.*

**Věta.** (O prvočíslech)
*(a)* *Každé číslo z $k(\varrho)$ různé od jednotky je dělitelné prvočíslem z $k(\varrho)$.*
*(b)* *Každé číslo z $k(\varrho)$ různé od nuly a jednotky je součinem prvočísel z $k(\varrho)$.*

**Věta.** (Jednotky v $k(\varrho)$) *Jednotky v $k(\varrho)$ jsou čísla $\pm 1$, $\pm\varrho$ a $\pm(1 + \varrho)$.*

**Věta.** *Máme-li dvě čísla $\gamma$, $\gamma_1$ taková, že $\gamma_1 \neq 0$, pak existují čísla $\kappa$, $\gamma_2$ taková, že platí*

$$\gamma = \kappa\gamma_1 + \gamma_2, \quad N\gamma_2 < N\gamma_1.$$

**Věta.** (Základní věta aritmetiky v $k(\varrho)$) *Vyjádření čísla z $k(\varrho)$ jako součin prvočísel je jednoznačné až na pořadí čísel, přítomnost jednotek a možných záměn mezi asociovanými čísly.*

**Věta.** (O čísle $\lambda$)
*(a)* $\lambda = 1 - \varrho$ *je prvočíslo.*
*(b)* *Při dělení číslem $\lambda$ dávají čísla $k(\varrho)$ tyto možné zbytky: 0, 1 a -1.*
*(c)* *3 je asociováno s $\lambda^2$.*
*(d)* *čísla $\pm(1-\varrho)$, $\pm(1-\varrho^2)$ a $\pm\varrho(1-\varrho)$ jsou všechny asociované s $\lambda$.*

**Věta.** *Neexistují řešení rovnice*

$$\xi^3 + \eta^3 + \zeta^3 = 0 \qquad (\xi \neq 0,\, \eta \neq 0, \zeta \neq 0)$$

*mezi čísly z $k(\varrho)$. Odtud plyne Velká Fermatova věta pro $n = 3$.*

**Věta.** (Pomocná)
*(a)* *Pokud $\omega \in k(\varrho)$ není dělitelná $\lambda = 1 - \varrho$, pak $\omega^3 \equiv \pm 1 \pmod{\lambda^4}$.*
*(b)* *Pokud $\xi^3 + \eta^3 + \zeta^3 = 0$, pak jedno z čísel $\xi$, $\eta$, $\zeta$ je dělitelné $\lambda$.*