STŘEDOŠKOLSKÁ ODBORNÁ ČINNOST

Obor SOČ: 1. Matematika a statistika

Důkaz Velké Fermatovy věty pro $n = 3$

Proof of Fermat's Last Theorem for $n = 3$

Autor: **Vojtěch Suchánek**

Škola: **Gymnázium, Brno,**
třída Kapitána Jaroše 14

Konzultanti: **Mgr. Aleš Kobza, Ph.D.**
Mgr. Michal Bulant, Ph.D.

Brno 2015

Prohlašuji, že jsem svou práci vypracoval samostatně, použil jsem pouze podklady (literaturu, SW atd.) citované v práci a uvedené v přiloženém seznamu a postup při zpracování práce je v souladu se zákonem č. 121/2000 Sb., o právu autorském, o právech souvisejících s právem autorským a o změně některých zákonů (autorský zákon) v platném znění.

V Brně dne 4. března 2015 .....

Rád bych na tomto místě poděkoval Michalu Bulantovi a mému trpělivému učiteli Aleši Kobzovi za jejich velkou ochotu a cenné nápady při vzniku této práce. Chtěl bych také poděkovat tvůrcům systému LaTeX, v němž je práce vysázena.

Anotace

Cílem je podat důkaz této věty za pomocí elementárních prostředků. K pochopení práce jsou potřebné znalosti, které jen částečně přesahují středoškolské poznatky. Jedná se především o úvod do teorie Eisensteinových čísel. Vlastnosti těchto čísel, o něž se předložený důkaz opírá, jsou proto v textu práce rovněž vyloženy.

Klíčová slova: Velká Fermatova věta; diofantická rovnice; Eisensteinova čísla; parametrizace.

Anotation

This work deals with the Fermat's Last Theorem for exponent 3. The aim of this paper is to provide a proof using only elementary tools. The necessity to understand this paper only partly exceeds high school knowledge. It is primarily a introduction to theory of Eisenstein numbers. Properties of these numbers are therefore also mentioned in the text.

Key words: Fermat's Last Theorem; Diophantine equation; Eisenstein numbers; parametrization.

Obsah

1. Úvod

1.1 Vymezení problému

Velká Fermatova věta je jedna z nejslavnějších vět v historii matematiky. Největší matematikové se v průběhu staletí snažili vyřešit tento problém. Všichni až na jednoho skončili nezdarem. Velká Fermatova věta mě fascinovala už od útlého věku, proto jsem se rozhodl, že se pokusím o vlastní důkaz pro její specifický exponent. Už od začátku jsem věděl, že to bude úkol nesnadný, nicméně jsem na něj zaměřil svoji práci. V druhé kapitole představuji čtenáři základy Eisensteinových čísel. Jsou hlavním pilířem, bez kterého by se důkaz neobešel. Eisensteinova čísla je velmi rozsáhlá problematika, která by samotná mohla být hlavním tématem práce. Přesto jsem se snažil uvést jen nezbytné minimum, aby byla práce srozumitelná pro středoškolského studenta.

V poslední kapitole seznamuji čtenáře s historií, kontextem a pozadím doby při řešení Velké Fermatovy věty.

1.2 Cíle práce

Cílem mé práce je vytvořit vlastní důkaz Velké Fermatovy věty pro $n = 3$. Mým úmyslem je přijít s důkazem pochopitelným pro středoškoleského studenta. Chci svůj důkaz porovnat s metodami využívajícími vysokoškolskou matematiku a s pracemi jiných matematiků.
Snažím se o srozumitelnou metodu, které by měl porozumět běžný člověk. Využívám postupy, které jsem se naučil na gymnáziu. Souběžně porovnávám svoje kroky s kroky jiných matematiků a snažím se o nejjednodušší řešení.
Daným problémem se zabývali největší géniové v dějinách, přesto si myslím, že elementární důkaz od středoškolského studenta by mohl přinést nový pohled na věc.

1.3 Úvod do problematiky

Velká Fermatova věta pojednává o diofantické rovnici, což je typ rovnice, který obecně představuje jeden z poměrně obtížných matematických problémů. Tyto rovnice připouštějí řešení pouze v oboru celých čísel. Zní takto:

Neexistují celá čísla x, y, z *a* n*, pro která* $x^n + y^n = z^n$*, kde* $n > 2$ *a* $x, y, z \neq 0$.

Moje závěrečná maturitní práce se zabývá konkrétním případem $n = 3$.
Tedy:
Neexistují celá čísla x, y, z*, pro která* $x^3 + y^3 = z^3$*, kde* $x, y, z \neq 0$.

Chceme-li se vyhnout formulaci pomocí rovnice, můžeme větu formulovat následujícím způsobem.
Nelze přerovnat kostičky tvořící dvě menší krychle tak, aby vznikla třetí, větší krychle.
Říká se, že matematická věta je tím krásnější, čím je její důkaz delší a obtížnější a čím je její formulace kratší a jednodušší.
Velká Fermatova věta toto hledisko splňuje vrchovatě. Přestože lze její formulaci zapsat na jediném řádku a pochopí ji i žáci základní školy, na důkaz se čekalo dlouhých 350 let, během kterých se o něj marně pokoušela řada velkých matematiků.

2. Eisensteinova čísla

2.1 Základní definice

Než si nadefinujeme Eisensteinova čisla, tak si označme ω jako jednu ze třetích odmocnin z jedné, a to:

$$\omega = \frac{-1+\sqrt{3}i}{2}.$$

Podotkněme, že ω je řešením rovnice $\omega^3 - 1 = 0$. Často budeme také potřebovat vztah $\omega^2 + \omega + 1 = 0$, který vyplývá z rozkladu $\omega^3 - 1 = (\omega - 1)(\omega^2 + \omega + 1) = 0$.

Definice 2.1.1 (Eisensteinova čísla)**.** *Každé číslo tvaru $a + b\omega$, kde $a, b \in \mathbb{Z}$, nazveme Eisensteinovým číslem.*

Množinu všech Eisensteinových čísel budeme značit $\mathbb{Z}[\omega]$.

Pro čtenáře, který není zasvěcený do pokročilejší algebraické teorie čísel, se můžou zdát Eisensteinova čísla nepraktická a důvod, proč jsme si zrovna vybrali tato čísla, nemusí být jasný. Nicméně ukážu, že tento okruh má velmi mnoho výhodných vlastností.
Eisensteinova čísla tvoří okruh. Okruh má netriviální definicí. My se spokojíme s tvrzením, že jde o matematickou strukturu, ve které můžeme sčítat a násobit. Dalším známým okruhem jsou celá čísla $\mathbb{Z}$.
Podobně jako v okruhu celých čísel bychom rádi používali pojmy jako prvočíslo, dělitelnost, nesoudělnost a podobně. Dalším stěžejním termínem je jednoznačný rozklad na prvočinitele. Ten samozřejmě nemusí platit v každém okruhu. V této kapitole se k tomuto tvrzení postupně propracuji, abych ho pak mohl použít v důkazu.

V učivu komplexních čísel jsme se na střední škole setkali s komplexně sdruženým číslem. V teorii Eisensteinových čísel budeme pracovat s podobným pojmem.

Definice 2.1.2. *Nechť $\alpha \in \mathbb{Z}[\omega]$, kde $\alpha = a + b\omega$, pro $a, b \in \mathbb{R}$. Pak číslo konjugované k číslu α budeme nazývat číslo ve tvaru $a + b\omega^2$. Budeme ho značit $\overline{\alpha}$.*

Neméně důležitým pojmem je norma.

Definice 2.1.3. *Normou prvku $\alpha = a + b\omega$ rozumíme součin $\alpha\overline{\alpha}$. Značíme ji $N(\alpha)$.*

Mnohdy budeme používat vztah $N(\alpha) = a^2 - ab + b^2$.
Snadno se o tom přesvědčíme: $\alpha\overline{\alpha} = (a + b\omega)(a + b\omega^2) = a^2 + ab(\omega^2 + \omega) + b\omega^3 = a^2 - ab + b^2$. Jelikož jsou navíc čísla a, b celá, pak je i libovolná norma celé číslo. Dokonce je to číslo nezáporné, neboť $a^2 - ab + b^2 = (\frac{a}{2} - b)^2 + \frac{3a^2}{4} \geq 0$.
Pro normu platí také, že je takzvaně multiplikativní. Platí totiž následující věta.

Věta 2.1.1. *Nechť $\alpha, \beta \in \mathbb{Z}[\omega]$. Potom $N(\alpha\beta) = N(\alpha)N(\beta)$.*

Její důkaz vyplývá z definice normy.

$$N(\alpha\beta) = (\alpha\beta)\overline{(\alpha\beta)} = \alpha\beta\overline{\alpha}\overline{\beta} = \alpha\overline{\alpha}\beta\overline{\beta} = N(\alpha)N(\beta).$$

Nyní k velmi známe dělitelnosti v $Z[\omega]$.

Definice 2.1.4. *Nechť $\alpha, \beta \in Z[\omega]$. Řekněme, že β dělí α, pokud existuje $\gamma \in \mathbb{Z}[\omega]$ takové, že $\alpha = \beta\gamma$.*

Tady si ukážeme, proč jsme závaděli normu. Platí totiž velmi silný vztah.

Věta 2.1.2. *Nechť $\alpha, \beta \in \mathbb{Z}[\omega]$ a $\alpha \mid \beta$. Pak $N(\alpha) \mid N(\beta)$.*

Definice 2.1.5. *Čísla, která dělí číslo 1, nazýváme jednotkami.*

Budeme rozlišovat teda dva pojmy: pojem „jednotky“ a pojem „jedničky“, t.j. čísla 1. Celá čísla nám nabízejí jednotky dvě 1 a -1. V okruhu Eisensteinových čísel jich máme více.

Věta 2.1.3. *Okruh Eisensteinových čísel má právě šest jednotek: ± 1, $\pm\omega$, $\pm\omega^2$.*

Díky větě 2.2.1. to snadno dokážeme. Z definice jednotky tedy nechť existuje $\epsilon = a + b\omega$, že $\epsilon \mid 1$. Pak i $N(\epsilon) \mid N(1) = 1$. $N(\epsilon)$ je ale číslo nezáporné, celé. Proto nutně $N(\epsilon) = a^2 - ab + b^2 = 1$. To vede ke kvadratické rovnici, která má řešení jen když $D = -3b^2 + 4 \geq 0$, tedy $b = 0$ nebo ± 1. Dopočítáme pro každý případ a a dostáváme řešení $(\pm 1, 0), (\pm 1, \pm 1), (0, \pm 1)$. Těm odpovídají čísla $\pm 1, \pm 1 \pm \omega = \pm\omega^2$ a $\pm\omega$, což jsme chtěli ukázat.
Z provedeného důkazu vyplývá platnost následující věty.

Věta 2.1.4. *Nechť $\epsilon \in \mathbb{Z}[\omega]$, pak ϵ je jednotka právě tehdy, když $N(\epsilon) = \pm 1$.*

Tím jsme se seznámili s pojmem jednotka a jeho vlastnostmi.

2.2 Aritmetika Eisensteinových čísel

Začneme s větou o dělení se zbytkem.

Věta 2.2.1. *Mějme dvě Eisensteinova čísla α, β, $\beta \neq 0$, pak existují Eisensteinova čísla ν a μ takové, že platí*

$$\alpha = \beta\mu + \nu, kde\ N(\nu) < N(\beta).$$

Důkaz. Nechť $\frac{\alpha}{\beta} = A + B\omega$, kde $A, B \in \mathbb{Q}$, a x, y jsou celá čísla taková, že platí

$$|A - x| \leq \frac{1}{2},$$
$$|B - y| \leq \frac{1}{2}.$$

Mějme nyní Eisensteinova čísla $\mu = x + \omega y$ a $\nu = \alpha - \mu\beta$. Tyto čísla splňují požadované vlastnosti:

$$\nu = \alpha - \mu\beta = \beta\left(\frac{\alpha}{\beta} - \mu\right) = \beta(A + B\omega - x - \omega y) = \beta[(A - x) + \omega(B - y)],$$

dále podle věty 2.1.1. přejdeme k normám a dostáváme

$$N(\nu) = N(\beta)[(A - x)^2 - (A - x)(B - y) + (B - y)^2] \leq$$
$$\leq N(\beta)\left(\frac{1}{4} + \frac{1}{4} + \frac{1}{4}\right) = \frac{3}{4}N(\beta) < N(\beta)$$

Definice 2.2.1. *Největším společným dělitelem dvou Eisensteinových čísel α, β nazveme takové číslo, které*

1. *dělí α i β,*
2. *má tu vlastnost, že je dělitelné každým společným dělitelem čísel α, β.*

Stěžejním nástrojem v teorii čísel je Euklidův algoritmus. I mi si ho zde zavedeme

Věta 2.2.2 (Euklidův algoritmus)**.** *Pro každé dvě Eisensteinova čísla α, β, z nichž alespoň jedno z nich je různé od nuly, existuje největší společný dělitel δ. Ten je až na asociovanost určen jednoznačně a lze vyjádřit ve tvaru*

$$\delta = \alpha\xi + \beta\eta,$$

kde ξ a η jsou Eisensteinova čísla.

Důkaz. Předpokládejme $\beta \neq 0$. Podle věty 2.2.1. můžeme sestavit systém rovnic

$$\alpha = \mu_0\beta + \nu_0, \quad N(\nu_0) < N(\beta),$$
$$\beta = \mu_1\nu_0 + \nu_1, \quad N(\nu_1) < N(\nu_0),$$
$$\nu_0 = \mu_2\nu_1 + \nu_2, \quad N(\nu_2) < N(\nu_1),$$
$$\vdots$$

$$\nu_{k-2} = \mu_k \nu_{k-1} + \nu_k, \quad N(\nu_k) < N(\nu_{k-1}),$$

$$\nu_{k-1} = \mu_{k+1} \nu_k,$$

kde $k \in \mathbb{N}, \nu_0, ..., \nu_{k+1}, \mu_0, ..., \mu_{k+1}$ jsou Eisensteinova čísla. Dostáváme klesající posloupnost

$$N(\beta) > N(\nu_0) > N(\nu_1) > \cdots > N(v_k) > N(v_{k+1}) = 0,$$

tedy pro určité k musí platit $N(\nu_{k+1}) = 0$. Eisensteinovo číslo $\nu_k = \delta$ potom je největší společný dělitel čísel α a β. Rovnice Euklidova algoritmu pak můžeme upravit do tzv. *Bezoutovy rovnosti.*

$$\delta = \alpha\xi + \beta\eta.$$

Definice 2.2.2. *Dvě Eisensteinova čísla nazveme nesoudělnými, pokud je jejich největším společným dělitelem jednotka.*

Věta 2.2.3. *Nechť α, β, γ jsou Eisensteinova čísla, α a β jsou nesoudělná a $\alpha \mid \beta\gamma$. Pak $\alpha \mid \gamma$.*

Důkaz. Čísla α a β jsou nesoudělná, existují tedy $\xi, \eta \in \mathbb{Z}[\omega]$ tak, že platí $\alpha\xi + \beta\eta = 1$. Celou rovnici vynásobíme číslem γ, dostáváme $\alpha\xi\gamma + \beta\eta\gamma = \gamma$. Zjevně $\alpha \mid \alpha\gamma$ a také $\alpha \mid \beta\gamma$, tedy $\alpha \mid \alpha\xi\gamma + \beta\eta\gamma$, neboli $\alpha \mid \gamma$.

Definice 2.2.3. *Eisensteinovo číslo π nazveme prvočíslo, pokud je dělitelné pouze jednotkami a čísly s π asociovanými.*

Věta 2.2.4. *Mějme Eisensteinovo prvočíslo π a Eisensteinova čísla α, β. Když $\pi \mid \alpha\beta$ a $\pi \nmid \beta$, platí $\pi \mid \alpha$.*

Důkaz. Protože $\pi \nmid \beta$, pak jsou nesoudělná a tedy $\pi \mid \alpha$.

Věta 2.2.5. *Nechť je α Eisensteinovo číslo a $N(\alpha) = p$, kde p je prvočíslo. Potom α je Eisensteinovým prvočíslem.*

Důkaz. Důkaz povedeme sporem. Předpokládejme, že α není Eisensteinovým prvočíslem a můžeme ho psát ve tvaru $\alpha = \eta\xi$, kde $\eta, \xi \in \mathbb{Z}[\omega]$, $N(\eta) > 1$ a $N(\xi) > 1$. Tedy $p = N(\alpha) = N(\eta)N(\xi)$, prvočíslo p ale nemůžeme rozložit na součin dvou přirozených čísel větší než jedna. Dostáváme spor.

Základní věta aritmetiky nám udává důležitou vlastnost přirozených čísel (tedy i celých, až na znaménka) a to jednoznačnost rozkladu na součin prvočísel. Každé přirozené číslo totiž můžeme zapsat jako součin několika prvočísel – například $15 = 3 \cdot 5$, $37 = 37$, a tento rozklad je vždy jediný možný (až na pořadí činitelů). Podobně to ale platí i pro Eisensteinova čísla.

Věta 2.2.6. *Nechť je α Eisensteinovo číslo. Pak leze toto číslo rozložit na součin konečného počtu Eisensteinových prvočísel. Až na pořadí a asociativitu dělitelů je tento rozklad jednoznačný.*

Důkaz. Nejprve si ukažme, že rozklad Eisensteinova čísla na prvočísla vždy existuje indukcí. Každé Eisensteinovo číslo α takové, že $N(\alpha) = 2$, je podle věty 2.2.5. Eisensteinovým prvočíslem. Tedy pro tento případ jsem hotovi.
Předpokládejme nyní Eisensteinovo číslo α, $N(\alpha) > 2$ a platnost věty pro každé

číslo β, pro které $N(\beta) < N(\alpha)$. Když α je Eisensteinovo prvočíslo, tak je důkaz hotový. V opačném případě je možné číslo α rozložit na $\alpha = \beta\gamma$, kde $\beta, \gamma \in \mathbb{Z}[\omega]$ a platí $1 < N(\beta) < N(\alpha)$ a $1 < N(\gamma) < N(\alpha)$. Podle indukčního předpokladu však lze čísla β a γ rozložit na součin Eisensteinových prvočísel. Tím je indukce hotová. Nyní musíme dokázat jednoznačnost tohoto rozkladu.
Nechť $\alpha = \pi_1\pi_2...\pi_n$ a $\alpha = \pi_1^*\pi_2^*...\pi_m^*$ jsou dva rozklady čísla α $(n, m \in \mathbb{N})$. Platí $\pi_1 \mid \alpha$ tedy $\pi_1 \mid \pi_1^*\pi_2^*...\pi_m^*$ což vede k $\pi_1 \mid \pi_i^*$ pro nějaké i. Čísla π_1 a π_i^* jsou Eisensteinova prvočísla a platí $\pi_i^* = \epsilon_1\pi_2$, kde ϵ_1 je jednotka. Můžeme tedy vydělit oba rozklady číslem π_i^* a zároveň si přeznačíme druhý rozklad tak, aby $\pi_i^* = \pi_1^{**}$. Dostáváme tedy

$$\pi_2\pi_3...\pi_n = \epsilon_2\pi_2^{**}\pi_3^{**}...\pi_m^{**}.$$

Tento postup opakujeme, dokud na jedné straně nezbude žádné Eisensteinovo prvočíslo. Pokud by bylo $n < m$, dostali bychom po n krocích

$$1 = \epsilon^*\check{\pi}_{n+1}...\check{\pi}_m,$$

to ovšem není možné. Stejně by dopadl i případ $n > m$. Musí tedy platit, že $n = m$ a oba rozklady jsou až na pořadí a asociativitu dělitelů shodné.

Tím jsme završili náš krátký úvod do Eisensteinových čísel. Nyní se můžeme pustit do samotného důkazu.

3. Důkaz Velké Fermatovy věty pro $n = 3$

3.1 Parametrizace rovnice

Parametrizace řešení rovnice nebo jen krátce parametrizace rovnice je nalezení předpisu řešení této rovnice. Používáme ho velmi často v případech, kdy je počet řešení nekonečně mnoho. Snad nejznámějším příkladem je parametrizace rovnice $a^2 + b^2 = c^2$. To je jak víme Pythagorova věta a čísla splňující tuto rovnici se nazývají Pythagorejská trojice. Těch je nekonečně mnoho včetně všech násobků tří, čtyř a pěti. Relativně snadným postupem zjistíme, že všechna jsou tvaru $((m^2 - n^2)k, 2mnk, (m^2 + n^2)k)$ nebo $(2mnk, (m^2 - n^2)k, (m^2 + n^2)k)$ pro všechna $m, n, k \in \mathbb{Z}$. Můžeme tedy tímto způsobem generovat všechny Pythagorejské trojice.
Méně známé jsou například Pythagorejské čtveřice, tedy ty čísla, která splňují rovnici $a^2 + b^2 + c^2 = d^2$. Řešení této rovnice lze také parametrizovat $(m^2 + n^2 - p^2 - q^2, 2mq + 2np, 2nq - 2mp, m^2 + n^2 + p^2 + q^2)$ pro libovolná celá m, n, p, q.
Právě vzorce pro Pythagorejské trojice se využívá v důkazu Velké Fermatovy věty pro $n = 4$. Vidíme tedy, že parametrizace řešení rovnice je velmi silná zbraň.
V důkazu ke kterému směřujeme tuto metodu také použijeme. V následujících odstavcích budeme rozebírat rovnici, která na první pohled nemusí souviset s Velkou Fermatovou větou, nicméně se nám bude skutečně hodit.

Hledejme v $\mathbb{Z}[\omega]$ parametrizaci řešení rovnice

$$x^2 - 3xy + 3y^2 = z^3, \tag{3.1}$$

kde navíc $3 \mid y$ a x, y, z jsou po dvou nesoudělná.
V oboru celých čísel se levá strana těžko rozkládá, ale v $\mathbb{Z}[\omega]$ to lze snadno, neboť

$$x^2 - 3xy + 3y^2 = (x - y)^2 - y(x - y) + y^2.$$

Po této úpravě si můžeme všimnout normy čísla $(x - y) + \omega y$, kterou rozložíme z obecné definice normy

$$N(x - y + \omega y) = (x - y + \omega)(\overline{x - y + \omega y}) = (x - y + \omega y)(x - y + \omega^2 y).$$

Dále dosadíme do (1)

$$(x - (1 - \omega)y)(x - (1 - \omega^2)y) = z^3.$$

Pro další přehlednost si navíc označme $\alpha = x - (1 - \omega)y$, $\overline{\alpha} = x - (1 - \omega^2)y$.
Nyní zkoujmeme soudělnost čísel α a $\overline{\alpha}$. Nechť $\pi \in \mathbb{Z}[\omega]$ je prvočíslo takové, že

$$\pi \mid \alpha, \quad \pi \mid \overline{\alpha}.$$

Pak dělí i jejich libovolnou lineární kombinaci

$$\pi \mid (\alpha - \overline{\alpha}) = (x - (1-\omega)y - x + (1-\omega^2)y) = \omega y(1-\omega).$$

A také

$$\pi \mid ((1+\omega)\alpha - \overline{\alpha}) = (1+\omega)(x-(1-\omega)y) - x + (1-\omega^2)y =$$

$$= x(1+\omega) - (1-\omega^2)y - x + (1-\omega^2)y = x\omega.$$

ω je jednotka, proto $\pi \mid (1-\omega)y$ a $\pi \mid x$, což vede k $\pi \mid (1-\omega)y$. Jelikož jsou ale x, y nesoudělná, pak mohu tvrdit, že

$$\pi \mid (1-\omega).$$

Opět využijme vlastnosti normy:

$$N(\pi) \mid N(1-\omega) = 1 - 1 \cdot (-1) + (-1)^2 = 3,$$

kde π není jednotka, proto $N(\pi) \neq 1$. Nutně tedy $N(\pi) = 3$.
Nyní se vraťme k (1).

$$\pi \mid z^3 \Rightarrow N(\pi) \mid N(z^3) \Rightarrow 3 \mid z^6 \Rightarrow 3 \mid z$$

A tady dostáváme konečně spor, protože $3 \mid y$ a $(y, z) = 1$.

Proto neexistuje takové π. Čísla α, $\overline{\alpha}$ jsou tedy nutně nesoudělná. Díky tomu, že jejich součin je třetí mocnina, pak i α a $\overline{\alpha}$ jsou třetí mocniny (případně vynásobené jednotkou). Neboli:

$$\exists \beta \in \mathbb{Z}[\omega] : \quad \alpha = \omega^k \beta^3, \quad \overline{\alpha} = \overline{\omega^k \beta^3} = \overline{\omega}^k \overline{\beta}^3.$$

Kde $k \in \{0, 1, 2\}$ nám výhodně obstarává ony jednotky. Ty jak víme jsou ± 1, $\pm\omega$, $\pm\omega^2$ s tím, že případné znaménko mínus si můžeme 'skrýt' do činitele β^3.
Pokračujme dále, má platit

$$z^3 = \alpha\overline{\alpha} = \omega^k \beta^3 \overline{\omega}^k \overline{\beta}^3 = (\beta\overline{\beta})^3 = N(\beta)^3.$$

Vyjádřeme si nyní β v algebraickém tvaru: $\beta = s + t\omega$ a dosaďme:

$$z^3 = N(\beta)^3 = (s^2 - st + t^2)^3 \Rightarrow z = s^2 - st + t^2.$$

Vyjádřit si x, y už je rutinní záležitost. Musíme ale rozebrat tři případy pro $k \in \{0, 1, 2\}$.
1) $k = 0$, tedy

$$\beta^3 = \alpha, \quad \overline{\beta}^3 = \overline{\alpha}.$$

Po dosazení pak

$$(s + \omega t)^3 = x - (1-\omega)y = \alpha, \quad (s + \omega^2 t)^3 = x - (1-\omega^2)y = \overline{\alpha}.$$

Odečtením α a $\overline{\alpha}$ získáme y:

$$y(\omega - \omega^2) = (s + t\omega)^3 - (s + t\omega^2)^3 = 3s^2 t\omega + 3st^2\omega^2 - 3s^2 t\omega^2 - 3st^2\omega$$

$$= 3s^2t(\omega - \omega^2) - 3st^2(\omega - \omega^2)$$
$$\Rightarrow y = 3st(s - t).$$

Následnou vhodnou linární kombinací si vyjádříme x:

$$(1+\omega)\alpha - \overline{\alpha} = x(1+\omega) - (1-\omega^2)y - x + (1-\omega^2)y =$$
$$= (s+t\omega)^3(1+\omega) - (s+t\omega^2)^3 =$$
$$= 3st^2\omega^2 + s^3\omega^3 + 3s^2t\omega^4 + 3st^2\omega^5 + t^3\omega^4 - 3st^2\omega =$$
$$= 3st^2(\omega^2 - \omega + 1) + \omega(s^3 + t^3) + 3s^2t\omega = \omega(s^3 + t^3 + 3s^2t - 6st^2)$$
$$\Rightarrow x = s^3 + t^3 + 3s^2t - 6st^2.$$

Pro tento případ jsme hotovi.
2) $k = 1$, tedy

$$\omega\beta^3 = \alpha, \quad \overline{\omega\beta^3} = \overline{\alpha}.$$

Opět dosadíme:

$$\omega(s+\omega t)^3 = x + (1-\omega)y, \quad \omega^2(s+\omega^2 t)^3 = x + (1-\omega^2)y.$$

A podobným odečtením získáme y

$$y(\omega - \omega^2) = \omega(s+t\omega)^3 - \omega^2(s+t\omega^2)^3 = \omega s^3 + 3st^2\omega^3 + 3s^2t\omega^2 + t^3\omega^4 -$$
$$-s^3\omega^2 - t^3\omega^8 - 3s^2t\omega^4 - 3st^2\omega^6 = s^3(\omega - \omega^2) - 3s^2t(\omega - \omega^2) + t^3(\omega - \omega^2).$$

Což vede k

$$y = s^3 - 3st^2 + t^3.$$

Tady si uvědomíme, že $3 \mid y$, proto

$$3 \mid s^3 + t^3 = (s+t)(s^2 - st + t^2) = (s+t)z.$$

Zřejmě pak $3 \mid (s+t)$. Úpravou $z = s^2 - st + t^2 = (s+t)^2 - 3st$ ale vidíme, že $3 \nmid (s+t)$, protože $3 \nmid z$. A to je tedy spor, pro tento případ žádné řešení neexistuje.
3) $k = 2$

$$\omega^2\beta^3 = \alpha, \quad \overline{\omega^2\beta^3} = \overline{\alpha}.$$

Dosaďme:

$$\omega^2(s+\omega t)^3 = x - (1-\omega)y, \quad \omega(s+\omega^2 t)^3 = x - (1-\omega^2)y.$$

A odečtením čísel α a $\overline{\alpha}$ získáme y

$$y(\omega - \omega^2) = \omega(s+t\omega^2)^3 - \omega^2(s+t\omega)^3 = \omega s^3 + 3^2st\omega^3 + 3st^2\omega^5 + t^3\omega^7 -$$
$$-s^3\omega^2 - t^3\omega^5 - 3s^2t\omega^3 - 3st^2\omega^4 = s^3(\omega - \omega^2) - 3st^2(\omega - \omega^2) + t^3(\omega - \omega^2).$$

Upravíme a máme opět jako v případě 2): $y = s^3 - 3st^2 + t^3$. Což jak víme vede ke sporu.
Jediným vhodným kandidátem je tedy případ 1)$k = 0$.

Teď už zbývá jenom tuto parametrizaci ověřit dosazením

$$(s^3+t^3+3s^2t-6st^2)^2-3(s^3+t^3+3s^2t-6st^2)(3st(s-t))+3s^2t^2(s-t)^2 = (s^2-st+t^2)^3.$$

Rutinním výpočtem lze zjistit, že tato rovnost skutečně platí.
Máme tedy parametrizaci řešení:

$$(x, y, z) = (s^3 + 3s^2t - 6st^2 + t^3, 3st(s - t), s^2 - st + t^2),$$

která splňuje rovnici (3.1) pro libovolná celá s, t.

3.2 Vlastní důkaz

Připomeňme, že chceme dokázat, že neexistuje trojice nenulových celých čísel x, y, z vyhovující rovnici

$$x^3 + y^3 + z^3 = 0. \tag{3.2}$$

Předpokládejme, že tato rovnice nějaké řešení skutečně má. Navíc hledejme „nejmenší“ řešení, minimalizujme tedy například hodnotu $|xyz|$. Můžeme uvažovat jen po dvou nesoudělná x, y, z, pokud by totiž existovalo prvočíslo, které by dělilo dvě z nich, pak by dělilo i třetí. Rovnici bychom pak mohli tímto prvočíslem vykrátit.

Uvědomíme-li si, že třetí mocnina má vždy zbytek $0, 1$ nebo -1 po dělení devíti, pak snadno prohlédneme, že alespoň jedna z nich musí být dělitelná devíti. Ať už si navolíme znaménka v rovnici $\pm 1 \pm 1 = \pm 1$ jakkoliv, nikdy nebude platit. Proto je dokonce právě jedno z čísel x, y, z dělitelné třemi. Předpokládejme bez újmy na obecnosti , že $3|z$:
Pak určitě $3|x^3 + y^3$, po rozložení $x^3 + y^3 = (x + y)(x^2 - xy + y^2)$ dále můžeme tvrdit, že $3|x + y$ nebo $3|x^2 - xy + y^2$.
Šikovnou úpravou zjistíme následující ekvivalenci

$$3 \mid (x^2 - xy + y^2) = (x + y)^2 - 3xy \Leftrightarrow 3 \mid (x + y).$$

Nyní si označme $z_1 = \frac{-z}{3}$, $y_1 = \frac{x+y}{3}$ a dosaďme do 3.2

$$\begin{aligned} x^3 + y^3 = (x + y)(x^2 - xy + y^2) &= -z^3 \\ 3y_1(x^2 - x(3y_1 - x) + (3y_1 - x)^2) &= 27z_1^3 \\ 3y_1(3x^2 - 9xy_1 + 9y_1^2) &= -27z_1^3 \\ y_1(x^2 - 3xy_1 + 3y_1^2) &= -3z_1^3. \end{aligned}$$

Díky úvodnímu předpokladu $(x, y) = 1$ i (x, y_1). Zejména pak $(y_1, x^2 - 3xy_1 + 3y_1^2) = 1$. Na základě toho a poslední rovnice platí $3 \mid y_1$. Následně využijeme substituci:

$$\exists u, v \in \mathbb{Z}, (u, v) = 1 : y_1 = 3u^3, \quad x^2 - 3xy_1 + 3y_1^2 = v^3.$$

Tady dostáváme rovnici u níž jsme v minulé podkapitole zjistili parametrizaci jejích řešení. Vzpomene si na počáteční podmínku, že všechny neznámé musí být po dvou nesoudělné a má platit $3 \mid y_1$. Všechny tyto požadavky naše rovnice splňuje, proto můžeme nasadit předpis řešení.

$$x = s^3 + 3s^2t - 6st^2 + t^3 \quad y_1 = 3st(s - t) \quad v = s^2 - st + t^2 \quad (s, t) = 1.$$

Hlavně nás zajímá $y_1 = 3st(s - t)$, neboť s, t a $(s - t)$ jsou po dvou nesoudělné. Proto použijeme znovu substituci:

$$-s = a^3, t = b^3, s - t = c^3 \quad a, b, c \in \mathbb{Z}.$$

Sečtením těchto tří členů ale dostáváme

$$a^3 + b^3 + c^3 = 0.$$

A tady máme konečný spor s minimalitou $|xyz|$, protože jsme našli čísla a, b, c splňující rovnici 3.2, kde $|abc| < |y_1| < |x + y| < |xyz|$.
Tím jsme dokončili důkaz Velké Fermatovy věty pro $n = 3$.

3.3 Nevyřešená rovnice

Dříve než jsem se pustil do studia Eisensteinových čísel, pokoušel jsem se o důkaz, který by používal čistě jen základy teorie čísel (dělitelnost, největší společný dělitel,...). Přestože jsem v důkazu hodně pokročil, dokončit se mi jej tímto způsobem nepodařilo. Domnívám se však, že může být zajímavé, když v této části čtenáři nabídnu několik úvah a zjištění, které jsem při tomto postupu provedl.

$$x^3 + y^3 = z^3 \tag{3.3}$$

Stejně jako ostatní jsem dokazoval sporem. Předpokládal jsem, že rovnice 3.3 má řešení a snažil se dojít ke sporu.
První co mě napadlo při pohledu na onu rovnici, byly její rozklady:

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

$$x^3 = z^3 - y^3 = (z-y)(z^2 + zy + y^2),$$

$$y^3 = z^3 - x^3 = (z-x)(z^2 + zx + x^2).$$

Jelikož jsem předpokládal nesoudělnost daných čísel x, y, z (přesněji řečeno: jsou po dvou nesoudělná), tak jsem rozebíral společné dělitele závorek v takto vzniklých rozkladech.

$$d = (z - y, z^2 + zy + y^2),$$

$$f = (x + y, x^2 - xy + y^2),$$

$$g = (z - x, z^2 + zx + y^2).$$

Ukázalo se, že $d, f, g \in \{1, 3\}$ a nejvýše jeden z d, f, g je roven třem. Bez újmy na obecnosti jsem tedy stanovil $f = g = 1$, díky tomu jsem dostal rovnice

$$p^3 = x + y, \quad q^3 = x^2 - xy + y^2, \tag{3.4}$$

$$u^3 = z - x, \quad v^3 = z^2 + zx + x^2. \tag{3.5}$$

Dále jsem rozlišil případy $d = 1$ a $d = 3$. Pro $d = 1$ se snadno přesvědčíme o rovnosti

$$(x + y - z)^3 = 3(pub)^3,$$

ve které je zřejmý spor, neboť levá strana rovnice je třetí mocnina, zatímco pravá není.
Případ $d = 3$ se ukázal nejsložitější. Podobně jako pro f, g 3.4, 3.5 jsem odvodil vztahy

$$3^5 b^3 = z - y, \quad 3a^3 = z^2 + zy + y^2. \tag{3.6}$$

Z rovnic (3.4), (3.5), (3.6) jsem si vyjádřil neznámé x, y, z

$$x = \frac{p^3 - u^3 + 3^5 b^3}{2} \quad y = \frac{p^3 + u^3 - 3^5 b}{2} \quad z = \frac{p^3 + u^3 + 3^5 b^3}{2},$$

a dosadil do vztahu

$$(x + y - z)^3 = 3^6 (pub)^3.$$

Což tedy vedlo k rovnici

$$p^3 - u^3 - 3^5 b^3 = 18pub.$$

Stačí tedy dokázat, že neexistují p, u, b, která by byla řešením této rovnice. Nicméně zde narážíme na problém, neboť žádný takový důkaz jsem nenašel. Nikdo koho jsem požádal o pomoc nebyl schopen tuto rovnici vyřešit s využitím elementárních prostředků. Dokonce není jisté, jestli takový důkaz existuje. Prozkoumal jsem četné způsoby, vyzkoušel různé metody, vždy se ziskem jistých informací, přesto bez úspěchu.Za zmínku stojí, že pokud se vyznáte v eliptických křivkách podaří se vám to. Stačí dokázat neřešitelnost rovnice pomocí její transformace na eliptickou křivku, o níž se poté dokáže, že nemá žádné (netriviální) racionální body.

Po nesčetně neúspěšných pokusů jsem opustil teorii čísel a rozebíral jsem hodnotu poměru k:

$$\frac{p-u}{b} = \frac{18up + 3^5 b^2}{p^2 + pu + u^2} = k, \quad k \in \mathbb{R}^+$$

Kde pro různá k jsem důkaz po částech dokončoval. Jediný interval který odolal, byl $k \in (6, \sqrt[3]{3^5})$ (Pro představu $\sqrt[3]{3^5}$ je přibližně 6,24.).
Pro tento interval zůstává důkaz nedokončen. Často mě napadla myšlenka, zda vůbec tato cesta někam vede. Nevím to dodnes, rád bych se však tímto dosud otevřeným problémem v budoucnu ještě chtěl zabývat.

4. Historie Velké Fermatovy věty

4.1 Historie

Při studiu jednoho antického spisu, Diofantovy Aritmetiky, si Pierre de Fermat napsal na prázdný okraj vedle textu rovnici. Na této větě nebylo samo o sobě nic špatného. Byla to prostě jen jedna z mnoha hypotéz v teorii čísel. Jenže Fermat vedle ještě připsal: „Našel jsem úžasný důkaz tohoto tvrzení, ale nevejde se mi na tento okraj."
Když zemřel, v jeho pozůstalosti nebyl zmíněny důkaz nikde nalezen. Od té doby jeho poznámka mučila nesčetné generace matematiků. Všechny ostatní Fermatovy hypotézy byly mezitím dokázány nebo vyvráceny, ale jeho velká věta vzdorovala všem pokusům. Stala se z ní jedna z největších matematických záhad a milovníky čísel přivedla k sebevraždám a soubojům. V roce 1908 slavná göttingeská univerzita v Německu vypsala odměnu 100 tisíc marek pro toho, kdo důkaz velké Fermatovy věty nalezne.
V červnu roku 1993 se konala v nedávno otevřeném Newtonově ústavu v Cambridgi matematická konference, na niž se sjela řada expertů v teorii čísel, což je jedna z mnoha specializovaných matematických disciplin. Jedním z přednášejících byl čtyřicetiletý Andrew Wiles, profesor matematiky z univerzity v Princetonu. Wiles měl sérii tří přednášek s názvem Modulární formy, eliptické křivky a Galoisovy reprezentace. Přestože málokteří přítomní poznali, k čemu Wiles směřuje, několik zasvěcenců tušilo, o co jde. Na třetí přednášku, ve středu 23. června, se dostavilo více než 60 posluchačů. Ti se pak stali svědky snad největší matematické senzace tohoto století: Důkaz, který Wiles ve svých přednáškách nastínil, je důkazem Fermatovy věty. Už v prosinci téhož roku oponenti odhalili v jeho důkaze chybu. Wiles poté spolu s dalším matematikem Taylorem provedl opravy a předložil novou verzi důkazu. Tato konečná verze se ukázala, že je v pořádku. Zabírá víc než 200 stránek složité matematiky. Nyní už je jasné, že Fermat opravdu tehdy důkaz nenašel, neboť tehdy nebyly dostupné metody jako jsou dnes.

4.2 Pierre de Fermat

I když Fermat nikdy nesepsal důkaz své Velké věty, zapsal v jakési zakódované formě náznak takového důkazu pro speciální případ $n = 4$ a ve svém výtisku *Aritmetiky* jej včlenil do poznámek týkajících se naprosto odlišného problému. I když jde svým způsobem o nejucelenější výpočet, jaký kdy Fermat svěřil papíru, je postup důkazu stále pouze naznačený a neúplný, zakončený slovy, že nedostatek času a místa brání tomu, aby bylo podáno úplné vysvětlení. Bez ohledu na chybějící podrobnosti tato Fermatova poznámka jasně ukazuje na jistou formu důkazu sporem známou jako metoda nekonečného sestupu.
Aby dokázal, že neexistuje žádně řešení rovnice $a^4+b^4 = c^4$, předpokládal Fermat, že takové hypotetické řešní existuje:

$$a = A_1, \quad b = B_1, \quad c = C_1$$

Na základě podrobnějšího studia vlastností této troji čísel dále ukázal, že pokud tato hypotetická trojice skutečně existuje, musí existovat i trojice menších čísel, která rovněž řeší rovnici. Zkoumáním vlastností tohoto nového řešení pak ukázal, že musí existovat ještě menší řešení a tak dále.
Fermat tak z řešení rovnice $a^4 + b^4 = c^4$ sestavil klesající schodiště, které by teoreticky sestupoval do nekonečna a obsahovalo stále menší a menší kladná čísla. Protože však a, b, c musí být přirozená čísla, není nikdy nekončící posloupnost stále menších řešení možná. Mezi kladnými celými čísly totiž musí existovat nejmenší řešení. Počáteční předpoklady byl nesprávný. Metodou nekonečného sestupu tak Fermat dokázal, že rovnice nemůže mít pro $n = 4$ žádné kladné celočíselné řešení.

4.3 Leonhard Euler

Případ $n = 3$ byl dokázán Leonhardem Eulerem v roce 1770. Jedná se o nejstarší dochovaný důkaz. Odlišné důkazy byly publikovány mnoha dalšími matematiky jako je Kausler, Legendre, Calzolari, Gambioli, Krey, Rychlik a mnoho dalších

Euler se snažil vyjít z metody Fermata a chtěl zkonstruovat pomocí ní obecný důkaz platný pro všechny ostatní rovnice. Vedle postupného zvyšování hodnoty n až do nekonečna zajímala Eulera rovněž hodnota n o jedničku nižší, $n = 3$, a právě pro tuto hodnotu se pokusil rovnici dokázat nejdříve. Aby Fermatem navržený důkaz pro $n = 4$ přizpůsobil případu $n = 3$, musel Euler použít takzvaná imaginární čísla. Imaginární čísla, nebo taky komplexní čísla, poskytla matematice doslova novou dimenzi. Euler dokázal, že použitím imaginárního čísla i může dosáhnout toho, aby důkaz metodou nekonečného sestupu fungoval i pro případ $n = 3$.

Závěr

Příběh Fermatovy věty se prolíná celými dějinami matematiky jako červená nít a dotýká se všech oblastí teorie čísel. Dává nám jedinečnou možnost nahlédnout, co je hnací silou matematiky, a to je snad ještě důležitější, čím jsou matematikové inspirováni. Na chvíli jsem pocítil, jaké to je řešit problém, aniž bych věděl, jestli má řešení.
Současný důkaz Velké Fermatovy věty je natolik složitý, že jej zcela chápe jen hrstka lidí. Podobně jsou na tom důkazy ostatních důležitých vět. Cílem této práce bylo přijít s důkazem pro specifický exponent, který by pochopil téměř každý.

Tato práce je i kvalitním základem po případný výzkum důkazů pro jiné exponenty.

Seznam použité literatury

[1] SINGH, Simon. *Velká Fermatova věta*. 1. vydání. Praha: Academia, 2000, 198s. ISBN 80-200-0394-0.

[2] SCHWARZ, Štefan. *Algebraické čísla*. 1.vydání. Praha:Přírodovědecké nakladatelství, 1950, 290 s.

[3] CRILLY, A. *Matematika: 50 myšlenek, které musíte znát*. 1. vydání. Překlad Josef Koval. Praha: Slovart, 2010, 208 s. ISBN 978-807-3914-097.

[4] RIBENBOIM, P. *13 Lectures on Fermat's Last Theorem*. 1. Title. Springer-Verlag New York ISBN 0-387-90432-8.

[5] IVIČ, V. *Základy kvadratických těles*. Brno: Vysoké učení technické, 2011.

[6] COHEN, H. *Number Theory: Volume I: Tools and Diophantine Equations*. Springer; 2007 edition ISBN 978-0387499222.