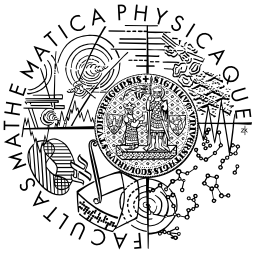


MATEMATICKO-FYZIKÁLNÍ FAKULTA
Univerzita Karlova

BAKALÁŘSKÁ PRÁCE

Adam Zemánek

Fermatova prvočísla v geometrii

Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D.
Studijní program: Obecná matematika

Praha 2024

Prohlašuji, že jsem tuto bakalářskou práci vypracoval(a) samostatně a výhradně s použitím citovaných pramenů, literatury a dalších odborných zdrojů. Beru na vědomí, že se na moji práci vztahují práva a povinnosti vyplývající ze zákona č. 121/2000 Sb., autorského zákona v platném znění, zejména skutečnost, že Univerzita Karlova má právo na uzavření licenční smlouvy o užití této práce jako školního díla podle §60 odst. 1 autorského zákona.

V ..... dne ....

Podpis autora

Tímto bych chtěl z celého srdce poděkovat vedoucímu mé práce docentovi Janu Žemličkovi, za jeho trpělivost a nápomocné rady.

Název práce: Fermatova prvočísla v geometrii

Autor: Adam Zemánek

Katedra algebry: Katedra algebry

Vedoucí bakalářské práce: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Katedra algebry

Abstrakt: V této práci se budeme ze začátku zabývat obecnými vlastnostmi Fermatových čísel, ukážeme libovolné dvě různé Fermatova čísla jsou nesoudělná. Také se budeme věnovat Fermatovým prvočíslům u kterých zmíníme kdy je již nutně prvočíslo Fermatovo a později zajimavou vlastnost spojenou s Eulerovou funkcí φ. Dále se věnujeme tématu konstruovatelnosti a ukážeme postupy konstrukcí. Posledními tématy bude konstruovatelnost pravidelných n-úhelníků a Heronovy trojúhelníky.

Klíčová slova: Fermatova čísla, Konstruovatelnost pravidelných mnohoúhelníků, Heronovy trojúhelníky

Title: Fermat primes in geometry

Author: Adam Zemánek

Department of algebra: Department of algebra

Supervisor: doc. Mgr. et Mgr. Jan Žemlička, Ph.D., Department of algebra

Abstract: In this thesis we firstly show some elementary properties of Fermat numbers, we will show that any two distinct Fermat numbers are coprime. Also we will dedicate some time for Fermat primes, for which we prove when prime is necessarily Fermats and later we state interesting property of Fermat primes and Eulers totient function. After all that we will talk about constructability and methods of constructions. Last topics will be constructibility of regular polygons and Heronian triangles.

Keywords: Fermat numbers, Constructible polygons, Heronian triangles

Obsah

Úvod

Dvě na dvě na m-tou to celé plus jedna, posloupnost, o které francouzský matematik Pierre de Fermat někdy v 17. století předpokládal, že pro libovolné přirozené číslo m i s nulou, generuje jen a pouze prvočísla. Čísla generovaná totou posloupností nesou jeho jméno a nazývají se Fermatova čísla a značí se $F_m = 2^{2^m} + 1$. Jenže Fermatova hypotéza byla mylná a vyvrátil ji o necelých sto let později věhlasný švýcarský matematik Leonhard Euler, který ukázal, že F_5 je dělitelné číslem 641. Tímto sice Euler ukončil příběh Fermatovy hypotézy, ale odstartoval lov na další dělitele čísel tohoto tvaru.

Počátkem 19. století německý matematick Carl Friedrich Gauss dokázal větu, o které se Fermatovi během zkoumání svých čísel snad ani nezdálo. A to větu, která spojuje Fermatova čísla s geometrií, přesněji hovoří o tom, pro jaká přirozená n je pravidelný n-úhelník konstruovatelný pomocí kružítka a pravítka. Tato věta zajímavým způsobem propujuje dvě odvětví matematiky, geometrii s teorií čísel.

Další spojitost mezi Fermatovými čísly a geometrií objevil rumunský matematik Florian Luca v 21. století , jeho věta se vztahuje k Heronovým trojúhelníkům. Jedná se vcelku o nový objev pro tak staré téma, kterým jsou tato čísla. Ještě do dnešní doby se pomocí počítačů hledají další a další dělitelé Fermatových čísel, na internetových stránkách se může kdokoliv zapojit do hledání. Jak vidíme zájem o Fermatova čísla neupadl.

První sekce bakalářské práce se věnuje obecným vlastnostem Fermatových čísel a prvočísel. Ukážeme si zajímavé vlastnosti, mezi které například patří, nesoudělnost dvou různých Fermatových čísel, podmínku kdy obecné prvočíslo je nutně Fermatovo prvočíslo a také rekurentní vzorec pro tyto čísla.

Druhá sekce bude opakování pojmů, které by čtenář měl znát. Pokud nejsou pro čtenáře pojmy zmíněné v této bakalářské práci známy, tak je může dohledat ve skriptech zmíněných v této sekci.

Třetí sekcí bude konstruovatelnost, ve které se budeme věnovat pojmu konstruovatelnosti pomocí kružítka a pravítka a ukážeme si pohled z perspektivy komplexních čísel. Budou se zde vysvětlovat pomocí obrázků postupy, jak zkonstruovat daná čísla a také si ukážeme v řeči tělesových rozšířeních, kdy je komplexní číslo konstruovatelné pomocí kružítka a pravítka.

Čtvrtou sekcí je první hlavní kapitola této práce a tou je Gaussova-Wantzelova věta, tato věta nám říká, kdy lze pravidelný n-úhelník zkonstruovat pomocí pravítka a kružítka. Ukážeme si další zajímavý vztah Fermatových prvočísel a tím bude jejich spojitost s Eulerovou funkcí φ. Dále dokážeme kdy je Galoisova grupa cyklická a tohle tvrzení nám pomůže v důkazu Gaussovy-Wantzelovy věty.

Poslední sekcí je druhá hlavní kapitola, která se zabývá Heronovými trojúhelníky. Vysvětlíme si, co musí trojúhelník splňovat, abychom ho nazvali Heronovým trojúhelníkem. Dokážeme si lemmata, kdy naopak trojúhelník nemůže být Heronův a poslední větou celé práce bude Lucova věta, která nám dává do spojitosti Fermatova prvočísla a Heronovy trojúhelníky.

1 Fermatova čísla

Začneme sekcí, ve které zmíníme jednoduché vlastnosti Fermatových čísel. Vycházím z knížek [1] a [2], ale důkazy byly jednoduché, tak jsem je udělal více méně sám.

Definice. *Přirozené číslo tvaru $n = 2^{2^m} + 1$, pro $m \in \mathbb{N}_0$ nazveme Fermatovým číslem, značíme F_m. Je-li navíc n prvočíslo nazveme jej Fermatovým prvočíslem.*

Podívejme se na pár prvních čísel tohoto tvaru

$$\begin{aligned} m = 0: &\quad F_0 = 3, \\ m = 1: &\quad F_1 = 5, \\ m = 2: &\quad F_2 = 17, \\ m = 3: &\quad F_3 = 257, \\ m = 4: &\quad F_4 = 65\,537, \\ m = 5: &\quad F_5 = 4\,294\,967\,297, \\ \cdots &\quad \cdots \end{aligned}$$

Pro $m = 0{,}1, \cdots 4$ jsou F_m prvočísla, F_5 již prvočíslo není a doposud nebylo nalezeno jiné Fermatovo prvočíslo než těchto prvních pět.

Co je ihned zřejmé z předpisu Fermatových čísel je velmi rychlý růst této posloupnosti, ale i přesto jednu číslici pro libovolně velká (až na první dvě) Fermatova čísla známe a to poslední číslici, kterou je pokaždé 7. Stačí se podívat na rovnost $F_m = 2^{2^m} + 1$ modulo 10, přesněji modulo 2 i modulo 5 abychom mohli použít Eulerovo zobecnění Malé Fermatovy věty a následným použitím Čínské zbytkové věty zjistit, že $F_m \equiv 7 \pmod{10}$, pro $m > 1$.

Nyní se budeme věnovat jednoduchých, ale i přesto zajímavých tvzením o Fermatových číslech.

Lemma 1.1. *Pro každé Fermatovo číslo platí*

1. $F_{m+1} = {F_m}^2 - 2F_m + 2$,
2. $F_{m+1} = F_0 F_1 \cdots F_m + 2$.

Důkaz. K důkazu prvního si stačí uvědomit, že

$$F_{m+1} = 2^{2^{m+1}} + 1 = (2^{2^m})^2 + 1 = (F_m - 1)^2 + 1 = {F_m}^2 - 2F_m + 2,$$

čímž máme hotovo.

Druhý vztah dokážeme indukcí, zřejmě

$$5 = F_1 = F_0 + 2 = 3 + 2 = 5.$$

Tímto jsme nastartovali indukci, nyní náším indukčním předpokladem jest,

$$F_k = F_0 F_1 \cdots F_{k-1} + 2$$

a chceme onu rovnost dokázat pro $k + 1$. Využitím první rovnosti a indukčního předpokladu dostáváme,

$$F_{k+1} = F_k F_k - 2F_k + 2 = (F_0 F_1 \cdots F_k + 2)F_k - 2F_k + 2 = F_0 F_1 \cdots F_k + 2.$$

□

Tvrzení 1.2. *Nechť F_m a F_n jsou dvě různá Fermatova čísla, pak*

$$\mathrm{NSD}(F_m, F_n) = 1$$

Důkaz. Stačí nám dokázat následující

$$\forall p \in \mathbb{N},\ p \neq 1 :\ p \mid F_m \Rightarrow p \nmid F_n.$$

Mějme tedy takové p a nechť $n < m$, pak podle Lemmatu 1.1

$$F_m = F_0 F_1 \cdots F_n \cdots F_{m-1} + 2.$$

Tedy p dělí levou stranu rovnice, takže musí dělit i pravou stranu rovnice, jenže pokud by $p \mid F_n$, pak $p \mid 2$ a tedy $p = 2$. Jenže F_m není dělitelné dvěmi $\forall m \in \mathbb{N}$.

Nyní pokud $n > m$, pak opět podle Lemmatu 1.1

$$F_n = F_0 F_1 \cdots F_m \cdots F_{n-1} + 2,$$

odtud

$$F_0 F_1 \cdots F_m \cdots F_{n-1} = F_n - 2.$$

Opět máme, že p dělí levou stranu rovnice neboť $p \mid F_m$ a tedy musí dělit i pravou stranu. Pokud by $p \mid F_n$, pak by nutně $p \mid 2$ a tedy $p = 2$, ale opět F_m není dělitelné dvěmi.

Takže dohromady máme že pro libovolné n nutně $p \nmid F_n$ a odtud již plyne, že $\mathrm{NSD}(F_m, F_n) = 1$. □

Tvrzení 1.2 dává, že pro libovolné prvočíslo které dělí Fermatovo číslo F_m neexistuje žádné jiné Fermatovo číslo F_n takové, aby bylo dělitelné oním provočíslem.

Tedy i přesto, že hypotéza ohledně posloupnosti $F_m = 2^{2^m} + 1$,která podle Fermata generuje pouze prvočísla byla lichá, tak přece jen nějakým způsobem generuje různá prvočísla. A to v prvočíselném rozkladu oněch členů posloupnosti. Jenže ani s touto informací nejsme schopni zodpovědět na otázku zdali existuje nekonečně mnoho složených Fermatových čísel. Takže nejenže nevíme, zdali existuje nekonečně mnoho Fermatových prvočísel, ale ani nevíme, zdali nekonečně mnoho složených.

Lemma 1.3. *Pokud $p = 2^j + 1$ je prvočíslo, pak p je nutně Fermatovo prvočíslo.*

Důkaz. Nechť $p = 2^j + 1$ je prvočíslo a pro spor ať $j = 2^m k$ pro $k > 1$ liché, pak použitím rovnosti

$$a^k + b^k = (a + b)(a^{k-1} - a^{k-2}b + \cdots + b^{k-1}),$$

pro $a = 2^{2^m}$ a $b = 1$ máme

$$p = 2^{2^m k} + 1 = (2^{2^m})^k + 1^k = (2^{2^m} + 1)(2^{2^m(k-1)} - 2^{2^m(k-2)} + \cdots + 1).$$

Tedy p je součinem dvou přirozených čísel větších než jedna, což je spor s prvočíselností p. Odtud $k = 1$ z čehož plyne $p = 2^{2^m} + 1$. □

2 Opakování

V této sekci zmíníme bez důkazu věty a definice, kterým se více věnují snad každá skripta algebry či komutativní algebry, proto čtenáře odkážu například na skripta Davida Stanovského [3] a Vítězslava Kaly [4], [5].

Definice. *Pro $n \in \mathbb{N}$ definujeme Eulerovu funkci $\varphi(n)$ jakožto počet přirozených čísel $k \leq n$, nesoudělných s číslem n, neboli*

$$\varphi(n) = |\{k \in \mathbb{N} \mid 1 \leq k \leq n, \text{NSD}(k,n) = 1\}|.$$

Poznámka. Mějme $n \in \mathbb{N}$ a jeho prvočíselný rozklad $n = {p_1}^{k_1} \cdots {p_m}^{k_m}$, pak pro Eulerovu funkci platí,

$$\varphi(n) = {p_1}^{k_1-1}(p_1 - 1) \cdots {p_m}^{k_m-1}(p_m - 1).$$

Definice. *Pro $n \in \mathbb{N}$, řekneme že koplexní číslo ζ_n je primitivní n-tá odmocnina z jedné, pokud je kořenemem polynomu $x^n - 1$ a není kořenem polynomu $x^k - 1$ pro $k < n$.*

Definice. *Pro $n \in \mathbb{N}$ a ζ_n primitivní odmocninu z jedné, definujeme cyklotomický polynom jako*

$$\Phi_n = \prod_{\substack{1 \leq k \leq n \\ \text{NSD}(k,n)=1}} (x - {\zeta_n}^k).$$

Pozorování 2.1. *Je-li Φ_n cyklotomický polynom, pak* $\deg(\Phi_\text{n}) = \varphi(\text{n})$, *kde $\varphi(n)$ je Eulerova funkce.*

Věta 2.2. *Cyklotomický polynom $\Phi_n \in \mathbb{Z}[x]$ je ireducibilní nad $\mathbb{Q}[x]$.*

Větu výše využijeme v jednodušší verzi a to, že cyklotomický polynom Φ_p pro p prvočíslo je ireducibilní. Tato věta bude potřeba v důkazu hlavní věty čtvrté sekce, kterou jsem dokázal tímto jednodušším tvrzením, zatímco zdroje z kterých jsem vycházel používaly onu těžší verzi věty.

Tvrzení 2.3. *Buď $T \leq S$ tělesové rozšíření a $s \in S$ alegebraický prvek, pak*

$$[T(s) : T] = \deg(\text{m}_{\text{s,T}}),$$

kde $m_{s,T}$ je minimální polynom prvku s nad tělesem T.

Tvrzení 2.4. *Mějme tělesová rozšíření $U \leq V \leq T$, pak*

$$[T : U] = [T : V][V : U]$$

Definice. *Mějme rozšíření těles $T \leq U$ množinu T-automorfismů $U \longrightarrow U$, to jest izomorfismů z $U \longrightarrow U$ zachovávající prvky tělesa T, s operacemi skládání a invertování nazveme Galoisovou grupou a značíme* Gal(U/T)

Definice. *Mějme U těleso a* Aut(U) *grupu automorfismů na U, dále ať G je podgrupa této grupy, pak definujeme* $\text{Fix(U,G)} = \{\text{u} \in \text{U} \mid \text{g(u)} = \text{u}, \forall \text{g} \in \text{G}\}$.

Lemma 2.5. *Ať T je těleso a $f \in T[x]$ ireducibilní polynom a U jeho rozkladové nadtěleso pak pro každé dva prvky tělesa u,$v \in U$ existuje prvek grupy $\varphi \in \mathrm{Gal(U/T)}$ takový, že $\varphi(u) = v$.*

Definice. *Mějme T těleso charakteristiky 0. Pak rozkladové nadtěleso ireducibilního polynomu f nad T nazveme Galoisovo.*

Lemma 2.6. *Je-li $U \supset T$ Galoisovo rozšíření, pak $|\mathrm{Gal(U/T)}| = [\mathrm{U : T}]$.*

Věta 2.7 (Základní věta Galoisovy teorie)**.** *Ať $U \supset T$ je Galoisovo rozšíření, pak máme antiizomorfismus uspořádaných množin.*

$$\begin{aligned} \{\textit{těleso } V \mid T \leq V \leq U\} &\longleftrightarrow \{\textit{podgrupy } H \leq \mathrm{Gal(U/T)}\} \\ V &\longmapsto \mathrm{Gal(U/V)} \\ \mathrm{Fix(U,H)} &\longleftarrow\!\shortmid H \end{aligned}$$

Definice. *Ať p je prvočíslo a $a \in \mathbb{Z}$, řekneme že a je kvadratický zbytek modolu p, pokud existuje $b \in \mathbb{Z}$ takové, že $a \equiv b^2\,(mod p)$.*
Dále definujme Legenderův symbol jako

$$\left(\frac{a}{p}\right) = \begin{cases} 1 & \textit{pokud } p \nmid a, a \textit{ je kvadratický zbytek modulo } p, \\ -1 & \textit{pokud } p \nmid a, a \textit{ není kvadratický zbytek modulo } p, \\ 0 & \textit{pokud } p \mid a. \end{cases}$$

Lemma 2.8. *Ať p je liché prvočíslo, pak*

$$\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}.$$

3 Konstruovatelnost

V této sekci se věnujeme konstruovatelnosti, budu vycházet ze zdrojů [6], [7] a také inspirací byly skripta [3]. Jenže tyto zdroje se nevěnují následujícím tvrzením dopodrobna, tak jsem doplnil důkazy v některých případech i s obrázky. Poslední dva důkazy jsem poupravil ze zdroje [7].

Co přesně je konstrukce pomocí pravítka a kružítka? Představme si, že máme body A, B a C v rovině, označme množinu těchto bodů M_0, a chceme sestrojit bod D. Tento bod nemusí jít sestrojit přímo použitím bodů z výchozí množiny M_0, ale můžeme sestrojit pomocné body, které následnou kostrukci cílového bodu D umožní. Tedy máme posloupnost bodů $D_1, D_2, \cdots, D_{n-1}$, které postupně přidáváme do množiny M_0.

$$M_0,\ M_1 = M_0 \cup \{D_1\},\ M_2 = M_1 \cup \{D_2\}, \cdots,\ M_{n-1} = M_{n-2} \cup \{D_{n-1}\}.$$

Až nakonec jsme schopni zkonstruovat bod D z množiny M_{n-1} a přidáme jej do množiny $M_n = M_{n-1} \cup \{D\}$.
Chceme-li sestrojit více bodů, tak budeme postupovat obdobným způsobem a konstuovat jeden bod po druhém.

Mluvíme-li o konstrukci pomocí kružítka a pravítka představíme si body v $\mathbb{R}^2$, jenže $\mathbb{R}^2$ můžeme ztotožnit s komplexní rovinou $\mathbb{C}$. Tedy dále budeme hovořit o konstrukci komplexních čísel nikoliv bodů z $\mathbb{R}^2$, tento pohled na věc má své výhody, jak bude vidět ve Větě 3.3.

Značení. *Kružnici se středem $a \in \mathbb{C}$ a poloměrem $r \in \mathbb{R}$, značíme $k(a,r)$.*
Přímku vedenou čísly $a,b \in \mathbb{C}$, značíme $\overleftrightarrow{ab}$.

K hledání konstrukcí daných čísel se nám budou hodit způsoby jak vyjádřit přímky a kružnice v komplexní rovině, tyto rovnice jsou snadným důsledkem známých rovnic přímek a kružnic v $\mathbb{R}^2$.
Přímku $p = \overleftrightarrow{ab}$, pro $a, b \in \mathbb{C}$ můžeme vyjádřit následující způsoby

$$p = \{z \in \mathbb{C} \mid z = a + t(b-a),\ t \in \mathbb{R}\},$$
$$p = \{z \in \mathbb{C} \mid (\overline{a} - \overline{b})(z-a) + (b-a)(\overline{z} - \overline{a}) = 0\}.$$

Chceme-li vyjádřit přímku q pomocí směrnice a čísla $c \in \mathbb{C}$ ležícím na přímce, využijeme následující rovnice. Ať má q směrnici shodnou s přímkou p, neboli $q \| p$ a $c \in q$, pak

$$q = \{z \in \mathbb{C} \mid z = c + t(b-a),\ t \in \mathbb{R}\},$$
$$q = \{z \in \mathbb{C} \mid (\overline{a} - \overline{b})(z-c) + (b-a)(\overline{z} - \overline{c}) = 0\}.$$

Kružnici $k = k(a,r)$, kde $a \in \mathbb{C}$ a r je reálné, vyjádříme jako

$$k = \{z \in \mathbb{C} \mid |z-a| = |r|\},$$
$$k = \{z \in \mathbb{C} \mid (z-a)\overline{z-a} = r\overline{r}\}.$$

Definice. *Číslo $z \in \mathbb{C}$ je konstruovatelné pomocí pravítka a kružítka, pokud existuje posloupnost konečných podmnožin komplexních čísel $\{0,1\} = M_0 \subseteq M_1 \subseteq \cdots \subseteq M_n$ takových, že $z \in M_n$ a $M_{j+1} = M_j \cup \{x\}$, kde číslo x vzniklo jako*

1. *průsečík dvou přímek,* $x = \overleftrightarrow{ab} \cap \overleftrightarrow{cd}$,

2. *prusečík kružnice a přímky,* $x = k(a, |b|) \cap \overleftrightarrow{cd}$,

3. *průsečík dvou kružnic,* $x = k(a, |b|) \cap k(c, |d|)$,

kde $a,b,c,d \in M_j$.
Množinu konstruovatených čísel budeme značit K.

Volbu výchozí množiny $M_0 = \{0,1\}$, jsme si mohli dovolit, neboť k zahájení kostrukce potřebujeme minimálně dva body v rovině, jeden z nich označíme jako 0 a druhý jako 1 a tím získáme jednotkovou délku. Povedeme přímku skrz tyto dva body a dostaneme reálnou osu, nyní můžeme nanášet pomocí kružítka jednotkouvou délku na tuto přímku a tím rozšířit naši množinu konstruovatelných čísel o libovolné celé číslo. Nyní sestrojme kolmici k reálné ose vztyčenou z bodu 0, kterou nazveme imaginární osou. Tedy máme souřadné osy.

Jenže dopustili jsme se konstrukce, která není zahrnutá v definici výše a to jest konstrukce kolmice. Následující tvrzení ukáže, že všechno je v souladu s definicí.

Tvrzení 3.1. *Mějme* $a, b, c \in K$ *a označme* $p = \overleftrightarrow{ab}$, *pak*

1. *jsme schopni zkostruovat přímku* q, *takovou že* $q \perp p$ *a* $c \in q$,

2. *jsme schopni zkonstruovat přímku* q, *takovou že* $q \| p$ *a* $c \in q$.

Důkaz. 1) Bez újmy na obecnosti předpokládejme, že $|c-a| \geq |c-b|$, pak vezměme kružnici $k = k(c, |c-a|)$ a označme $d \in k \cap p$, $d \neq a$. Dále ať $l = k(d, |a-d|)$ a $m = k(a, |a-d|)$ jsou kružnice jejich průsečíky označme $e,f \in l \cap m$. Pak $q = \overleftrightarrow{ef}$ je hledaná kolmice.

2) Pokud c leží na přímce p tak máme hotovo, ať tedy $c \notin p$, pak použitím prvního bodu zkostruujme kolmici $r \perp p$ a $c \in r$, dále zkostruujme kolmici $q \perp r$ takovou, že $c \in q$, pak $q \| p$. □

Tvrzení výše nám neříká nic jiného, než zcela známou věc a to, že kolmice a rovnoběžky lze sestrojit pomocí kružítka a pravítka.

Tímto jsme tedy odůvodnili správnost konstrukce imaginární osy a budeme pokračovat v našem povídání. Pomocí kružítka zaznačíme v jednotkové vzdálenosti od bodu 0 na imaginární ose bod, kterému budeme říkat imaginární jednotka, tedy i. Opět postupným nanášením jednotkové vzdálenosti pomocí kružítka na tuto osu dostaneme libovolný celočíselný násobek námi právě zkonstruovaného čísla i. Rozšířili jsme tedy konstruovatelná čísla o $i\mathbb{Z}$, celkově máme $\mathbb{Z} \cup i\mathbb{Z} \subset K$, použitím Tvrzení 3.1 dokonce $\mathbb{Z}[i] \subset K$.

Důsledek 3.2. *Mějme* $z \in K$, *pak* $Re(z), Im(z) \in K$.

Důkaz. Ke konstrukci stačí uvažovat kolmice spuštěné z komplexního čísla z k reálné ose a k imaginární ose. □

Dále pro libovolné $z \in K$ jsme schopni zkonstruovat i $|z|$, neboť se jedná o průsečík kružnice $k(0, |z|)$ a reálné osy Re. To nejsou zdaleka všechna čísla, která jsme schopni zkonstruovat, jak nám následující věta ukáže.

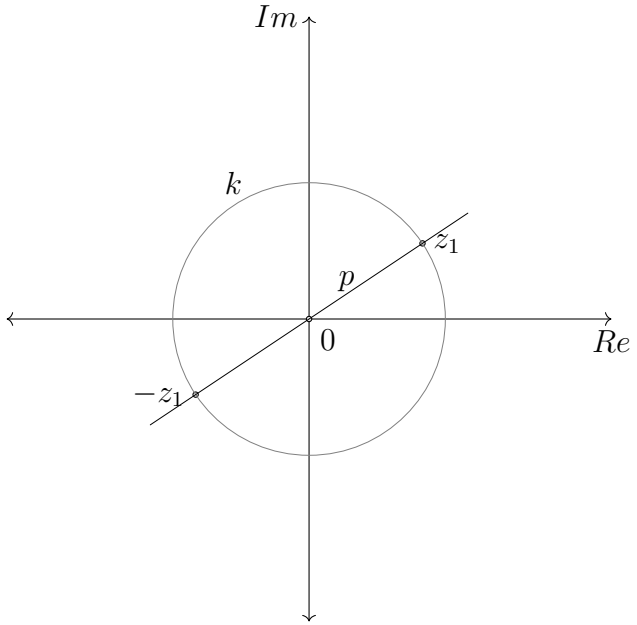
Věta 3.3. *Označme* $\{0,1\} \subset K \subset \mathbb{C}$ *množinu kostruovatelných čísel, pak*

1. $\forall z_1 \in K \Rightarrow -z_1 \in K$,
2. $\forall z_1, z_2 \in K \Rightarrow z_1 + z_2 \in K$,
3. $\forall z_1, z_2 \in K \Rightarrow z_1 - z_2 \in K$,
4. $\forall z_1, z_2 \in K,\ z_2 \neq 0 \Rightarrow |z_1 z_2|, \frac{1}{|z_2|} \in K$
5. $\forall z_1, z_2 \in K \Rightarrow z_1 z_2 \in K$,
6. $\forall z_1 \in K \Rightarrow \overline{z_1} \in K$
7. $\forall z_1 \in K,\ z_1 \neq 0 \Rightarrow z_1^{-1} \in K$,
8. $\forall z_1, z_2 \in K,\ z_2 \neq 0 \Rightarrow \frac{z_1}{z_2} \in K$. .

Důkaz. 1) Mějme z_1 nenulové, pro nulové z_1 je $-z_1 = z_1$, tedy již konstruovatelné, pak mějme kružnici k a přímku p

$$p = \{z \in \mathbb{C} \mid z = tz_1,\ t \in \mathbb{R}\},$$
$$k = \{z \in \mathbb{C} \mid |z| = |z_1|\},$$

Máme $-z_1 \in p$ a také $-z_1 \in k$, tedy $-z_1 \in p \cap k$, tudíž opačné číslo je konstruovatelné.



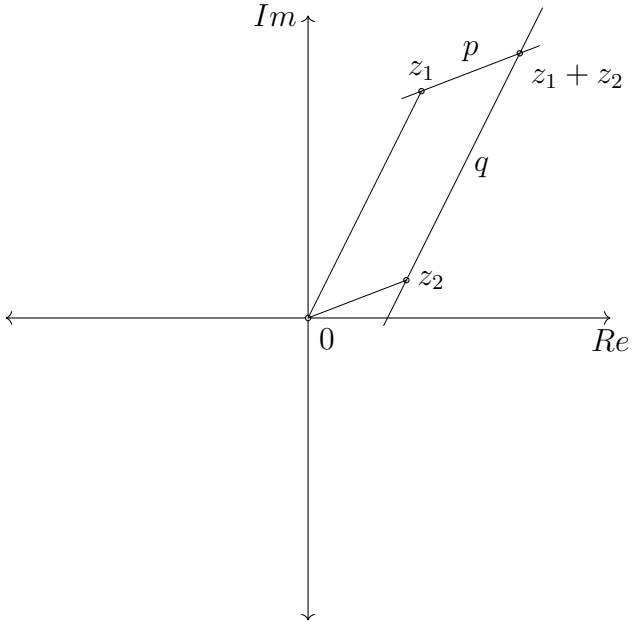
2) Pokud aspoň jedno z čísel z_1, z_2 je nulové tak zřejmě z_1+z_2 je konstruovatelné. Ať jsou tedy obě čísla nenulová a $z_1 \neq tz_2$ pro $t \in \mathbb{R}$, dále zkonstruujme přímky p,q, kde p je rovnoběžná s přímkou $\overleftrightarrow{z_2 0}$ a $z_1 \in p$. Přímka q je naopak rovnoběžná s $\overleftrightarrow{z_1 0}$ a $z_2 \in q$,

$$p = \{z \in \mathbb{C} \mid z = z_1 + tz_2,\ t \in \mathbb{R}\},$$
$$q = \{z \in \mathbb{C} \mid z = z_2 + sz_1,\ s \in \mathbb{R}\}.$$

Volbou $t = s = 1$ máme $z_1 + z_2 \in p$ a $z_1 + z_2 \in q$, tudíž číslo $z = z_1 + z_2 \in p \cap q$ je konstruovatelné.
Pokud z_1, z_2 jsou nenulové a $z_1 = tz_2$ pro nějaké $t \in \mathbb{R}$, pak $z_1 + z_2$ zkonstruujeme pomocí přímky r a kružnice k.

$$r = \{z \in \mathbb{C} \mid z = z_1 + tz_2,\, t \in \mathbb{R}\},$$
$$k = \{z \in \mathbb{C} \mid |z - z_1| = |z_2|\}.$$

Zřejmě $z_1 + z_2 \in r$ a také $z_1 + z_2 \in k$, tedy $z_1 + z_2 \in r \cap k$ je konstruovatelné.



3) K důkazu využijeme již známé, tedy $z_1 - z_2 = z_1 + (-z_2)$ z 1) máme, že $-z_2 \in K$ a z 2) máme, že i $z_1 + (-z_2) \in K$, tedy i $z_1 - z_2 \in K$.

4) Ať $z_1, z_2 \neq 0$, jinak zřejmě $0 \in K$. Vezměme přímku $p \ni 0$, která je různá od souřadných os a takovou, že $z_1, z_2 \notin p$.

$$p = \{z \in \mathbb{C} \mid z = tz_3,\, t \in \mathbb{R}\},$$

kde $z_3 \in K$ (takové z_3 bude rozhodně existovat, protože už víme, že $\mathbb{Z}[i] \subset K$). Nyní mějmě kružnice $k = k(0, 1)$ a $l = k(0, |z_2|)$, tedy

$$k = \{z \in \mathbb{C} \mid |z| = 1\},$$
$$l = \{z \in \mathbb{C} \mid |z| = |z_2|\}.$$

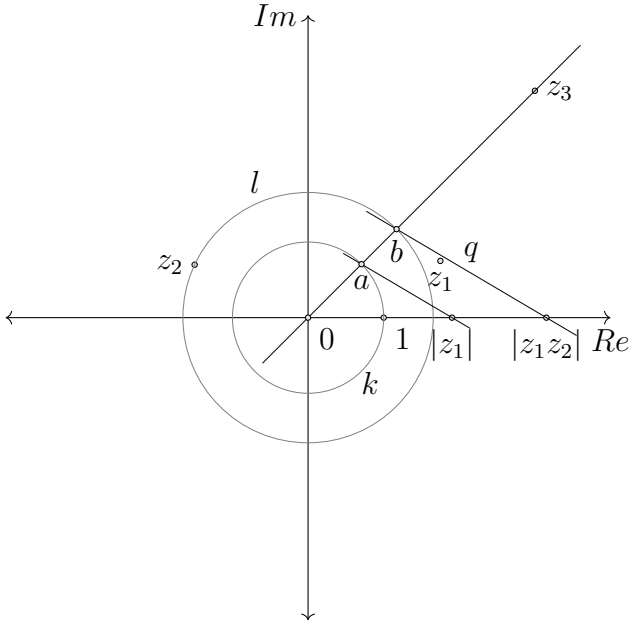
A označme $a \in p \cap k$, $b \in p \cap l$,

$$a = \frac{z_3}{|z_3|}, \quad b = \frac{|z_2|}{|z_3|} z_3.$$

Dále zkostruujme přímku $q \| \overleftrightarrow{|z_1|a}$, tak aby $b \in q$, a označme Re reálnou osu tedy

$$q = \left\{ z \in \mathbb{C} \;\middle|\; \frac{|z_2|}{|z_3|} z_3 + t \left(\frac{z_3}{|z_3|} - |z_1| \right),\, t \in \mathbb{R} \right\}$$

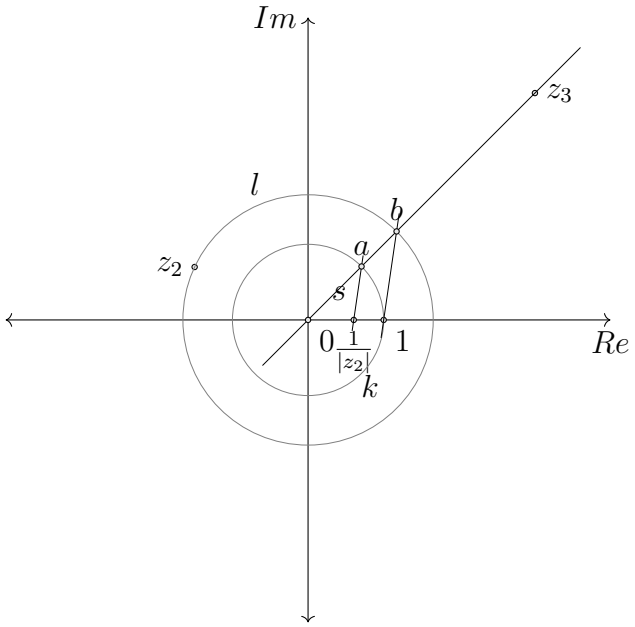
Volbou $t = -|z_2|$ dostaneme, $|z_1 z_2| \in q$ a to je zřejmě reálné číslo tedy $|z_1 z_2| \in q \cap Re$. Odtud $|z_1 z_2| \in K$.



Zbyvá ukázat, že $\frac{1}{|z_2|} \in K$, k tomu využijeme značení uvedené výše. Označme s přímku takovou, že $s \| \overleftrightarrow{b1}$ a $a \in s$

$$s = \left\{ z \in \mathbb{C} \;\middle|\; z = \frac{z_3}{|z_3|} + t\left(1 - \frac{|z_2|}{|z_3|} z_3\right), t \in \mathbb{R} \right\}.$$

Pro $t = \frac{1}{|z_2|}$, máme $\frac{1}{|z_2|} \in s \cap Re$, tedy je konstruovatelné.



5) Ať z_1, z_2 jsou nenulová, jinak zřejmě $z_1 z_2 = 0 \in K$. Díky 4) můžeme předpokládat, že aspoň jedno z čísel z_1, z_2 má nenulovou imaginární složku, jelikož

$|z_1 z_2| \in K$. Ať tedy z_2 je takové číslo, zkonstruujme kružnici $k = k(0,1)$ a přímky

$$p = \{z \in \mathbb{C} \mid z = tz_1,\, t \in \mathbb{R}\},$$
$$q = \{z \in \mathbb{C} \mid z = tz_2,\, t \in \mathbb{R}\}.$$

Průsečíky kružnice s těmito přímkami označíme $a = p \cap k$, $b = q \cap k$. Vyjádřeno algebraicky $a = \frac{z_1}{|z_1|}$, $b = \frac{z_2}{|z_2|}$. Dále zkonstruujme kružnici $l = k(b, |a-1|)$

$$l = \left\{ z \in \mathbb{C} \;\middle|\; \left| z - \frac{z_2}{|z_2|} \right| = \left| \frac{z_1}{|z_1|} - 1 \right| \right\},$$

zajímá nás průsečík $k \cap l$, jelikož $\frac{z_1 z_2}{|z_1 z_2|} \in l$, neboť

$$\left| \frac{z_1 z_2}{|z_1 z_2|} - \frac{z_2}{|z_2|} \right| = \left| \frac{z_1}{|z_1|} - 1 \right|$$
$$\left| \frac{z_2}{|z_2|} \right| \left| \frac{z_1}{|z_1|} - 1 \right| = \left| \frac{z_1}{|z_1|} - 1 \right|$$
$$\left| \frac{z_1}{|z_1|} - 1 \right| = \left| \frac{z_1}{|z_1|} - 1 \right|.$$

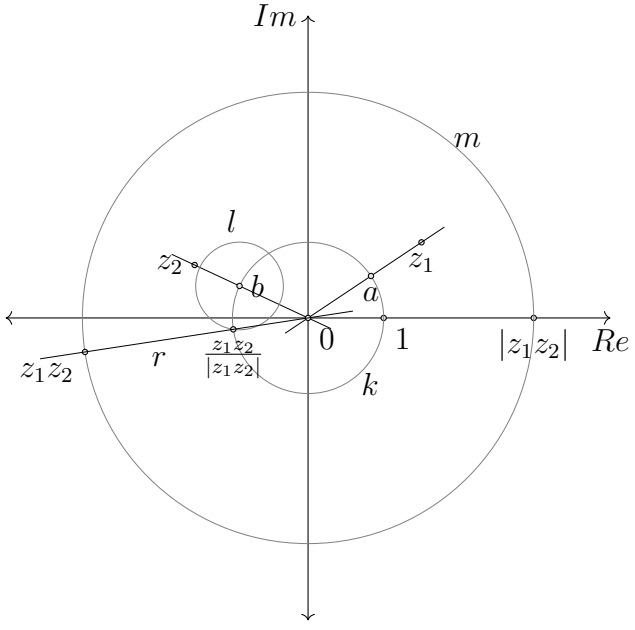
A také $\frac{z_1 z_2}{|z_1 z_2|} \in k$, neboť

$$\left| \frac{z_1 z_2}{|z_1 z_2|} \right| = 1,$$

tak máme $\frac{z_1 z_2}{|z_1 z_2|} \in k \cap l$. Nyní už snadno z 4) víme, že $|z_1 z_2| \in K$, tedy můžeme zkonstruovat kružnici $m = k(0, |z_1 z_2|)$. Zřejmě $z_1 z_2 \in m$, dále zkonstrujme přímku

$$r = \left\{ z \in \mathbb{C} \;\middle|\; z = t\frac{z_1 z_2}{|z_1 z_2|},\, t \in \mathbb{R} \right\},$$

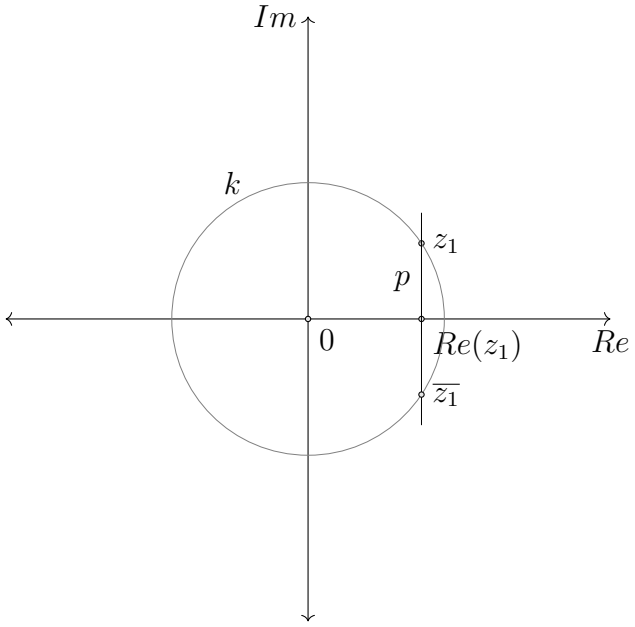
pak $z_1 z_2 \in m \cap r$, tedy je konstruovatelné.



6) Mějme $z_1 \in K$ číslo s nenulovou imaginární částí, jinak zřejmě $\overline{z_1} = z_1 \in K$. Zkonstruujme kružnici $k = k(0, |z_1|)$, zřemě $\overline{z_1} \in k$, a přímku $p = \overleftrightarrow{z_1 Re(z_1)}$,

$$p = \left\{ z \in \mathbb{C} \;\middle|\; z = z_1 + t\left(z_1 - \frac{z_1 + \overline{z_1}}{2}\right),\, t \in \mathbb{R} \right\}.$$

Volbou $t = -2$ dostáváme, že $\overline{z_1} \in p$, tedy $\overline{z_1} \in p \cap k$.



7) Nejprve upravíme $z^{-1} = \frac{\overline{z_1}}{|z_1|^2}$ a využijeme již dokázaného. Použitím 4) máme, že $\frac{1}{|z_1|} \in K$, použitím 5) $\frac{1}{|z_1|^2} \in K$ dále pomocí 6) a znovu 5) máme $\frac{\overline{z_1}}{|z_1|^2} \in K$.

8) Snadno pomocí 7) a 5) neboť $\frac{z_1}{z_2} = z_1 z_2^{-1} \in K$.

□

Důsledek 3.4. *Množina konstruovatelných čísel K tvoří podtěleso komplexních čísel.*

Důkaz. Plyne ihned z Věty 3.3, máme že $\{0, 1\} \subset K$ je uzavřená na sčítání a součin, ke každému prvku existuje opačný a ke každému nenulovému existuje inverz. □

Touto větou jsme razantně rozšířili naši množinu konstruovatelných čísel nyní víme, že $\mathbb{Q}(i) \subset K$ a dokonce jelikož K je těleso, tak $\mathbb{Q}(i) < K$.

Jak jsem již zmínil na začátku sekce o konstruovatelnosti, tak volba komplexních čísel namísto $\mathbb{R}^2$ má výhodu například v tom, že nemusíme speciálně definovat operace s body v $\mathbb{R}^2$ (například součin), ale můžeme pracovat se známými operacemi komplexních čísel.

Tvrzení 3.5. *Je-li z_1 konstruovatelné, pak také $\sqrt{z_1}$ je konstruovatelné.*

Důkaz. Ať je z_1 nenulové, jinak je zřejmě $\sqrt{z_1}$ konstruovatelná. Zkonstruujme kružnici $k = k(\frac{|z_1|-1}{2}, \frac{|z_1|+1}{2})$, kde obě čísla $\frac{|z_1|-1}{2}, \frac{|z_1|+1}{2} \in K$ díky Větě 3.3 a protněme ji s imaginární osou Im.

$$k = \left\{ z \in \mathbb{C} \;\middle|\; \left| z - \frac{|z_1| - 1}{2} \right| = \left| \frac{|z_1| + 1}{2} \right| \right\}.$$

Ukážeme, že $i\sqrt{|z_1|} \in k \cap Im$. Zřejmě máme, že ono číslo leží na imaginární ose, dosaďme nyní číslo do předpisu kružnice

$$\left|i\sqrt{|z_1|} - \frac{|z_1|-1}{2}\right| = \left|\frac{|z_1|+1}{2}\right|,$$
$$\sqrt{\frac{|z_1|^2 - 2|z_1|+1}{4} + |z_1|} = \frac{|z_1|+1}{2}.$$

Nastane rovnost, tedy opravdu $i\sqrt{|z_1|} \in k \cap Im$ a odtud zřejmě $\sqrt{|z_1|} \in K$. Pokud $z_1 \in \mathbb{R}$, tak již máme $\sqrt{z_1} \in K$, zbývá pro čísla s nenulovou imaginární složkou. Zkostruujme bisekci argumentu komplexního čísla z_1. Mějme přímku p a kružnici $l = k(0,\sqrt{|z_1|})$

$$p = \{z \in \mathbb{C} \mid z = (z_1 + |z_1|)t,\, t \in \mathbb{R}\},$$
$$l = \left\{z \in \mathbb{C} \mid |z| = \left|\sqrt{|z_1|}\right|\right\}.$$

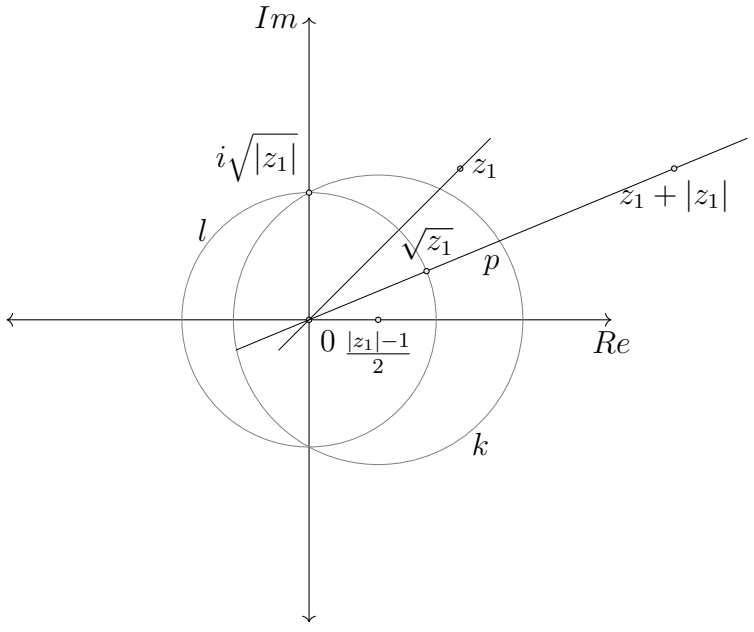
Ověříme,že $z_2 := \frac{\sqrt{z_1}}{z_1+|z_1|} \in \mathbb{R}$, k tomu použijeme goniometrický tvar komplexního čísla $z_1 = |z_1|(\cos(\varphi) + \mathrm{i}\sin(\varphi))$.

$$\frac{\sqrt{z_1}}{z_1 + |z_1|} = \frac{\left|\sqrt{z_1}\right|(\cos(\frac{\varphi}{2}) + \mathrm{i}\sin(\frac{\varphi}{2}))}{|z_1|(\cos(\varphi) + \mathrm{i}\sin(\varphi) + 1)},$$

Stačí se podívat pouze na imaginární část tohoto výrazu,

$$\sin(\frac{\varphi}{2})\cos(\varphi) - \sin(\varphi)\cos(\frac{\varphi}{2}) + \sin(\varphi) = \sin(-\frac{\varphi}{2}) + \sin(\frac{\varphi}{2}) = 0.$$

Použili jsme známe rovnosti goniometrických funkcí a dostali, že imaginární část čísla z_2 je nulová, tedy jedná se o reálné číslo. Proto můžeme volbou $t = z_2$ zjistit, že $\sqrt{z_1} \in p$, tedy $\sqrt{z_1} \in p \cap l$ a tím máme konstruovatelnost odmocniny.



□

Tohle tvrzení nám jako navíc dává konstrukci bisekce úhlu. Protože pro jednotkové komplexní číslo $z = e^{i\varphi} \in K$, kde φ je argument komplexního čísla, nám tvrzení výše říká, že jsme schopni zkonstruovat $\sqrt{z} = e^{i\frac{\varphi}{2}}$, neboli bisekci úhlu φ. Induktivně můžeme s půlením úhlu pokračovat a tím zkonstruovat $e^{i\frac{\varphi}{2^j}}$, pro libovolné $j \in \mathbb{N}$.

Věta 3.6. *Nechť komplexní číslo x vzniklo konstrukcí v jednom kroku pomocí kružítka a pravítka z prvků tělesa $L < \mathbb{C}$, pak $[L(x) : L] \leq 2$.*

Důkaz. Číslo x mohlo vzniknou třemi způsoby, jako

1. průsečík dvou různoběžných přímek,
2. průsečík kružnice a přímky,
3. průsečík dvou kružnic.

1) Máme dvě různoběžné přímky p, q

$$p = \{z \in \mathbb{C} \mid z = a + t(b-a),\, t \in \mathbb{R}\},$$
$$q = \{z \in \mathbb{C} \mid (\overline{c} - \overline{d})(z - c) + (d - c)(\overline{z} - \overline{c}) = 0\},$$

kde $a, b, c, d \in L$. Průsečík teda bude

$$(\overline{c} - \overline{d})(a + t(b-a) - c) + (d-c)(\overline{a} + t(\overline{b} - \overline{a}) - \overline{c}) = 0,$$
$$((b-a)(\overline{c} - \overline{d}) + (\overline{b} - \overline{a})(d-c))t + (\overline{c} - \overline{d})(a-c) + (d-c)(\overline{a} - \overline{c}) = 0.$$

Což je pro $t = \frac{x-a}{b-a}$ lineární polynom v $L(x)$, jehož je x kořenem, tedy podle Tvrzení 2.3 $[L(x) : L] = 1$.

2) Máme přímku p a kružnici $k = k(c, |d|)$

$$p = \{z \in \mathbb{C} \mid z = a + t(b-a),\, t \in \mathbb{R}\},$$
$$k = \{z \in \mathbb{C} \mid |z - c| = |d|\},$$

kde $a, b, c, d \in L$, průsečík bude

$$|a + t(b-a) - c| = |d|,$$
$$(a + t(b-a) - c)(\overline{a} + t(\overline{b} - \overline{a}) - \overline{c}) = d\overline{d},$$
$$(b-a)(\overline{b} - \overline{a})t^2 + ((\overline{b} - \overline{a})(a-c) + (b-a)(\overline{a} - \overline{c}))t + (\overline{a} - \overline{c})(a-c) - d\overline{d} = 0.$$

Opět pro $t = \frac{x-a}{b-a}$ máme kvadratický polynom v $L(x)$, pro který je x kořenem, tedy opět díky Tvrzení 2.3 $[L(x) : L] \leq 2$.

3) Máme dvě kružnice $k = k(a, |b|)$ a $l = k(c, |d|)$

$$k = \{z \in \mathbb{C} \mid |z - a| = |b|\},$$
$$l = \{z \in \mathbb{C} \mid |z - c| = |d|\},$$

kde $a, b, c, d \in L$, upravme první rovnici

$$\begin{aligned}(z-a)(\overline{z}-\overline{a}) &= b\overline{b},\\ (z-a)\overline{z} &= b\overline{b}+\overline{a}(z-a),\\ \overline{z} &= \frac{b\overline{b}}{z-a}+\overline{a}.\end{aligned}$$

Nyní konečně průsečík bude

$$\begin{aligned}|z-c| &= |d|,\\ (z-c)\left(\frac{b\overline{b}}{z-a}+\overline{a}-\overline{c}\right) &= d\overline{d},\\ (\overline{a}-\overline{c})z^2+(b\overline{b}-d\overline{d}-(a+c)(\overline{a}-\overline{c}))z+ac(\overline{a}-\overline{c})+ad\overline{d} &= 0.\end{aligned}$$

Pro $z = x$ máme kvadratický polynom v $L(x)$, který má x za kořen, použijeme Tvrzení 2.3 a dostaneme $[L(x) : L] \leq 2$. □

Věta 3.7. *Ať $z \in \mathbb{C}$ je konstruovatelné. Pak existuje posloupnost těles*

$$\mathbb{Q} = T_0 \leq T_1 \leq \cdots \leq T_{k-1} \leq T_k,$$

taková, že $z \in T_k$ a $[T_i : T_{i-1}] \leq 2$ pro $1 \leq i \leq k$. A navíc $[\mathbb{Q}(z) : \mathbb{Q}]$ je mocnina dvojky.

Důkaz. Jelikož je z konstruovatelné tak podle definice existuje posloupnost množin

$$\{0, 1\} = M_0 \subset M_1 \subset \cdots \subset M_{k-1} \subset M_k,$$

kde $z \in M_k$, $|M_i \backslash M_{i-1}| = 1$ a každé $x_i \in M_i \backslash M_{i-1}$ pro $1 \leq i \leq k$ vzniklo konstrukcí pomocí kružítka a pravítka z čísel množiny M_{i-1}. Mějmě posloupnost těles

$$\mathbb{Q} = T_0 \leq T_1 \leq \cdots \leq T_{k-1} \leq T_k,$$

kde $T_i = T_{i-1}(x_i)$ pro $1 \leq i \leq k$, potom $z \in T_k$ a podle Věty 3.6 platí $[T_i : T_{i-1}] \leq 2$, tedy jsme našli onu posloupnost těles.

Druhá část věty je důsledkem již dokázaného, protože $\mathbb{Q}(z)$ je nejmenší nadtěleso tělesa $\mathbb{Q}$ obsahující prvek z a T_k je nějaké nadtěleso tělesa $\mathbb{Q}$ obsahující z, tedy $\mathbb{Q} \leq \mathbb{Q}(z) \leq T_k$, pak $[T_k : \mathbb{Q}] = [T_k : \mathbb{Q}(z)][\mathbb{Q}(z) : \mathbb{Q}]$. Neboli

$$[\mathbb{Q}(z) : \mathbb{Q}] \mid [T_k : T_{k-1}][T_{k-1} : T_{k-2}] \cdots [T_1 : T_0],$$

a každý stupeň rozšíření je menší roven dvěmi, tedy $[\mathbb{Q}(z) : \mathbb{Q}] = 2^l$ pro nějaké $l \in \mathbb{N}_0$, $l \leq k$. □

Lemma 3.8. *Buď $T \leq \mathbb{C}$ těleso takové, že existuje posloupnost těles*

$$\mathbb{Q} = T_0 \leq T_1 \leq \cdots \leq T_{n-1} \leq T_n = T,$$

splňující $[T_i : T_{i-1}] = 2$, pro $1 \leq i \leq n$, pak $T \leq K$, kde K jsou konstruovatelná čísla.

Důkaz. Z Věty 3.3 plyne zřejmě, že $T_0 = \mathbb{Q} \leq K$. Jelikož $[T_1 : \mathbb{Q}] = 2$, tak podle Tvrzení 2.3 existuje $t_0 \in \mathbb{Q}$ takové, že $T_1 = \mathbb{Q}(\sqrt{t_0})$ a díky Tvrzení 3.5 $T_1 \leq K$. Dále budeme postupovat indukcí, jestliže $[T_i : T_{i-1}] = 2$ a $T_{i-1} \leq K$, tak podle Tvrzení 2.3 existuje $t_{i-1} \in T_{i-1}$ splňující $T_i = T_{i-1}(\sqrt{t_{i-1}})$, jenže konstruovatelná čísla jsou uzavřená na odmocniny Tvrzení 3.5, tedy $T_i \leq K$ a celkově nám indukce dává, že $T \leq K$. □

4 Gaussova-Wantzelova věta

V této sekci se podíváme na konstruovatelnost pravidelných n-úhelníků pomocí kružítka a pravítka, budeme zde pracovat pouze s n-úhelníky pro $n \geq 3$, žádné degenerované 0, 1, 2-úhelníky nebudeme brát v potaz. Také budeme hovořit pouze o n-úhelnících s jednotkovým poloměrem a středem v počátku souřadnic, pokud bychom chtěli hovořit o konstrukci n-úhelníku se středem v $s \in \mathbb{C}$ a poloměrem $r \in \mathbb{R}$, pak abychom se vůbec mohli bavit o konstruovatelnosti, musí zřejmě $s, r \in K$.

Budu vycházet ze zdrojů [2] a [7], ale důkaz hlavní věty jsem poupravil a obohatil o vynechané tvzení o cykličnosti Galoisovy grupy $\mathrm{Gal}(\mathbb{Q}(\zeta_p/\mathbb{Q})$ pro p prvočíslo.

Ale ještě než se vrhneme na hlavní větu této sekce, podívejme se nejprve na tvrzení, která k tomu budeme potřebovat. Následující lemma nám předkládá další pěknou vlastnost Fermatových čísel a dává je do spojitosti s Eulerovou funkcí φ.

Lemma 4.1. *Mějme přirozené číslo $n \geq 2$, pak $\varphi(n)$ je mocnina dvojky právě tehdy, když $\exists j, k \in \mathbb{N}_0\ \exists F_{m_1}, \cdots, F_{m_k}$, k po dvou různých Fermatových prvočísel, tak že*

$$n = 2^j F_{m_1} \cdots F_{m_k}.$$

Důkaz. ($\Leftarrow$) Jestliže $n = 2^j F_{m_1} \cdots F_{m_k}$, pak podle vlastnosti Eulerovy funkce zmíněné v Poznámce 2 máme

$$\begin{aligned}\varphi(n) &= 2^{j-1}(F_{m_1} - 1) \cdots (F_{m_k} - 1)\\ &= 2^{j-1}(2^{2^{m_1}} + 1 - 1) \cdots (2^{2^{m_k}} + 1 - 1)\\ &= 2^{j-1+2^{m_1}+\cdots+2^{m_k}} = 2^i,\end{aligned}$$

pro $i := j - 1 + 2^{m_1} + \cdots + 2^{m_k}$.

($\Rightarrow$) Nechť $n \geq 2$ a $\varphi(n) = 2^i$ pro nějaké $i \in \mathbb{N}_0$. Případ kdy $i = 0$, zřejmě implikuje, že $n = 2$, tedy n je požadovaného tvaru. Pro případ kdy $i \geq 1$, mějme prvočíselný rozklad čísla n

$$n = {p_1}^{k_1} \cdots {p_l}^{k_l},$$

kde $p_1, \cdots, p_j$ jsou po dvou různá prvočísla. Pak opět podle Poznámky 2

$$2^i = \varphi(n) = {p_1}^{k_1-1}(p_1 - 1) \cdots {p_l}^{k_l-1}(p_l - 1),$$

tedy

$$2^i = {p_1}^{k_1-1}(p_1 - 1) \cdots {p_l}^{k_l-1}(p_l - 1).$$

Nyní, levá strana rovnice je mocnina dvojky tedy i pravá strana musí být. Jenže pokud naše číslo n obsahuje ve svém prvočíselném rozkladu liché prvočíslo ve vyšší než-li první mocnině pak pravá strana rovnice obsahuje mocninu lichého čísla, takže

$$n = 2^{k_1} p_2 \cdots p_l,$$

kde $p_2, \cdots, p_l$ jsou po dvou různá lichá prvočísla.

$$2^i = 2^{k_1-1}(p_2 - 1) \cdots (p_l - 1) \quad \Rightarrow \quad p_2 = 2^{s_2} + 1, \cdots, p_l = 2^{s_l} + 1,$$

jenže pomocí Lemma 1.3 jsou $p_1, \cdots, p_l$ po dvou různá Fermatova prvočísla, tedy

$$n = 2^j F_{m_1} \cdots F_{m_k}.$$

□

Tvrzení 4.2. *Pravidelný n-úhelník je konstruovatelný pravě tehdy, když primitivní n-tá odmocnina z* 1 *je konstruovatelná.*

Důkaz. Označme primitivní n-tou odmocninu z 1 jako ζ_n. Pak vrcholy pravidelného n-úhelníku budou ζ_n^k, pro $k \in \{1, \cdots, n\}$.
Jelikož jsme schopni zkonstruovat náš n-úhelník, tak jsme zřejmě schopni zkonstruovat jeden z jeho vrcholů, což je komplexní číslo ζ_n
Nyní opačná implikace, jestliže jsme schopni zkonstruovat číslo ζ_n, pak podle Věty 3.3 jsme schopni zkostruovat ζ_n^k, pro $k \in \{1, \cdots, n\}$, tedy celý n-úhelník. □

Lemma 4.3. *Mějme p prvočíslo a ζ_p primitivní p-tou odmocninu z jedné, pak* $\mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q})$ *je cyklická grupa řádu* $p - 1$.

Důkaz. Číslo ζ_p je kořenem polynomu Φ_p, který má podle definice za kořeny čísla ζ_p^a, pro $1 \leq a \leq p$, a nesoudělná s p. Jelikož p je prvočíslo tak množina kořenů polynomu Φ_p je zřejmě

$$M = \{\zeta_p, \zeta_p^2, \cdots, \zeta_p^{p-1}\},$$

a $\mathbb{Q}(\zeta_p)$ je rozkladové nadtěleso tohoto polynomu. Jedná se tedy o Galoisovo rozšíření a podle Lemmatu 2.6 platí

$$|\mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q})| = [\mathbb{Q}(\zeta_\mathrm{p}) : \mathbb{Q}] = \mathrm{p} - 1,$$

kde poslední rovnosti plynou z Tvrzení 2.3 a Pozorování 2.1. Nyní se podíváme na grupu $\mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q})$, libovolný prvek φ této grupy je permutací na množině kořenů M a pro každé dva kořeny existuje právě jeden prvek $\varphi_a \in \mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q})$ takový, že $\varphi_a(\zeta_p) = \zeta_p^a$. Existence plyne z Lemmatu 2.5 a jednoznačnost plyne z následujícího. Kdyby existovali dva takové T-automorfismy $\varphi, \vartheta \in \mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q})$, a mějme $q \in \mathbb{Q}(\zeta_p)$, pak $q = q_0 + q_1\zeta_p + \cdots + q_{p-1}\zeta_p^{p-1}$ a pro ony automorfismy platí

$$\varphi(q) = q_0 + q_1\zeta_p^a + \cdots + q_{p-1}\zeta_p^{a(p-1)} = \vartheta(q).$$

Tedy φ, ϑ se rovnají na libovolném prvku $q \in \mathbb{Q}(\zeta_p)$, tedy jsou rovny. Zadefinujme zobrazení σ, jako

$$\sigma : \mathbb{Z}_p^* \to \mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q}),$$
$$a \mapsto \varphi_a,$$

ukážeme, že tohle zobrazení je grupový izomorfismus. Mějme libovolné $a, b \in \mathbb{Z}_p^*$, pak

$$\sigma(ab) = \varphi_{ab} = \varphi_a \circ \varphi_b = \sigma(a) \circ \sigma(b),$$

kde druhá rovnost platí, neboť $\varphi_{ab}(\zeta_p) = \zeta_p^{ab} = \varphi_a(\zeta_p^b) = \varphi_a(\varphi_b(\zeta_p))$. Tedy σ je homomorfismus, zřejmě $\mathrm{Ker}(\sigma) = 1$, tedy je to prostý homomorfismus a $|Z_p^*| = |\mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q})| = \mathrm{p} - 1$, čímž dostáváme izomorfismus dvou grup, kde $\mathbb{Z}_p^*$ je cyklická, tedy i $\mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q})$ je cyklická. □

Věta 4.4 (Gauss-Wantzel)**.** *Pravidelný n-úhelník je konstruovatelný pomocí kružítka a pravítka právě tehdy, když*

$$n = 2^i F_{m_1} \cdots F_{m_k},$$

kde $n, i, k \in \mathbb{N}_0$*,* $n \geq 3$ *a* $F_{m_1}, \cdots, F_{m_k}$ *jsou po dvou různá Fermatova prvočísla.*

Důkaz. ($\Rightarrow$) Z Tvrzení 4.2 víme, že nám stačí konstruovatelnost ζ_n. Toto komplexní číslo je kořenem cyklotomického polynomu Φ_n, podle Věty 2.2 je tento polynom ireducibilní a tedy i minimální polynom. Takže máme

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \deg(\Phi_\mathrm{n}) = \varphi(\mathrm{n}),$$

kde poslední rovnost platí díky Pozorování 2.1. Nyní protože je ζ_n konstruovatelné, tak podle Věty 3.7 musí platit

$$[\mathbb{Q}(\zeta_n) : \mathbb{Q}] = \varphi(n) = 2^l$$

pro nějaké $l \in \mathbb{N}_0$, jenže tato rovnost nastane, jak jsme ukázali v Lemmatu 4.1, jen a pouze pro n tvaru

$$n = 2^i F_{m_1} \cdots F_{m_k},$$

pro nějaké $i, k \in \mathbb{N}_0$ a $F_{m_1}, \cdots, F_{m_k}$ po dvou různá Fermatova prvočísla.

($\Leftarrow$) Nechť $n = 2^i F_{m_1} \cdots F_{m_k}$ je jako ve znění věty a $\zeta_{2^i}, \zeta_{F_{m_1}}, \cdots, \zeta_{F_{m_k}}$ jsou primitivní odmociny z jedné. Budeme chtít dokázat konstruovatelnost primitivní n-té odmocnincy z 1, pak totiž díky Tvrzení 4.2 máme konstruovatelnost celého n-úhelníku. Jelikož součin $\zeta_{2^i}\zeta_{F_{m_1}} \cdots \zeta_{F_{m_k}} = \zeta_n$ je primitivní n-tá odmocina, tak díky Větě 3.3 nám bude stačit dokázat konstruovatelnost jednotlivých čísel v daném součinu.

Nejprve se podíváme na konstruovatelnost ζ_{2^i}, pro $i \in \mathbb{N}_0$, konstrukce tohoto čísla ihned plyne z povídání pod Tvrzením 3.5, které nám říká, že jsme schopni půlit úhly.

Nyní se podíváme na konstruovatelnost ζ_p, pro $p = 2^{2^m} + 1$ Fermatovo prvočíslo. Pro primitivní p-tou odmocninu z jedničky podle Lemmatu 4.3 platí, že $\mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q})$ je cyklická grupa izomorfní $\mathbb{Z}_p^*$. Vezměme generátor grupy $g \in \mathbb{Z}_p^*$ a označme $G_s = \langle g_s \rangle$, kde $g_s = g^{2^s}$, pro $s \in \{0, 1, \cdots, 2^m\}$, $|G_s| = 2^{2^m - s}$. Pak platí

$$1 = G_{2^m} \leq G_{2^m - 1} \leq \cdots \leq G_1 \leq G_0 = \mathbb{Z}_p^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q}),$$

a také $[G_s : G_{s+1}] = 2$. Nyní použitím Základní věty Galoisovy teorie máme posloupnost těles

$$\mathbb{Q} = T_0 \leq T_1 \leq \cdots \leq T_{2^m - 1} \leq T_{2^m} = \mathbb{Q}(\zeta_p),$$

takových že $T_s = \mathrm{Fix}(\mathbb{Q}(\zeta_\mathrm{p}),\, \mathrm{G_s})$ a $[T_s : T_{s-1}] = 2$. Odtud již použitím Lemmatu 3.8 máme $\mathbb{Q}(\zeta_p) \leq K$, kde K jsou konstruovatelná čísla, tedy ζ_p je konstruovatelné pro libovolné $p = 2^{2^m} + 1$ Fermatovo prvočíslo.

□

Nezapomeňme, že otázka zda-li existuje více Fermatových prvočísel než-li F_0, F_1, F_2, F_3, F_4, je stále otevřená. Tedy nevíme jestli existuje konstrukce pravidelného n-úhelníku pro jiná n, než n tvaru,

$$n = 2^a \cdot 3^b \cdot 5^c \cdot 17^d \cdot 257^e \cdot 65\,537^f \quad a \in \mathbb{N}_0, \quad b, c, d, e, f \in \{0,\, 1\}.$$

Jak jsem již zmínil, tak jsem důkaz poupravil a dokazoval kostruovatelnost ζ_n přes prvočíselný rozklad čísla n. Navíc bych také zmínil, že jsem se pokoušel dokázat větu bez použití Galoisovy teorie a to hledáním vhodných tělesových rozšíření. Mějme posloupnost grup jako v důkazu věty

$$1 = G_{2^m} \leq G_{2^m-1} \leq \cdots \leq G_1 \leq G_0 = \mathbb{Z}_p^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_\mathrm{p})/\mathbb{Q}).$$

Definujme $\theta_s = \sum_{g \in G_s} \zeta_p^g$, pro $s \in \{0, 1, \cdots, 2^m\}$, pak vhodným kandidátem na takovou posloupnost těles by mohla být

$$\mathbb{Q} = T_0 \leq T_1 \leq \cdots \leq T_{2^m-1} \leq T_{2^m} = \mathbb{Q}(\zeta_p).$$

Taková, že $T_j = T_{j-1}(\theta_j)$, pro $j \in \{1, \cdots, 2^m\}$ a $T_0 = \mathbb{Q}(\theta_0)$. Pro prvek θ_0 platí

$$\theta_0 = \sum_{g \in G_0} \zeta_p^g = \zeta_p^{p-1} + \zeta_p^{p-2} + \cdots + \zeta_p = -1,$$

protože sčítáme přes všechny prvky grupy $G_0 = \mathbb{Z}_p^*$ a ζ_p je kořenem cyklotomického polynomu $x^{p-1} + x^{p-2} + \cdots + x + 1$. Tedy celkově máme $T_0 = \mathbb{Q}$ a $T_{2^m} = \mathbb{Q}(\zeta_p)$, jelikož $\theta_{2^m} = \zeta_p$. Kdyby se nám podařilo dokázat, že platí $[T_k : T_{k-1}] = 2$, pro $k \in \{1, \cdots, 2^m\}$, pak bychom měli onu hledanou posloupnost těles a použitím Lemmatu 3.8, bychom dostali, že $\zeta_p \in K$.
Jenže stačí nám dokázat, že $[T_k : T_{k-1}] \leq 2$ nebo $[T_k : T_{k-1}] \geq 2$, protože ζ_p je kořenem ireducibilního polynomu Φ_p, podle Věty 2.2, jehož stupeň je $\varphi(p) = p - 1 = 2^{2^m}$, tedy celkově použitím Tvrzení 2.3 máme

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}] = \varphi(p) = 2^{2^m}.$$

Odtud již plyne

$$2^{2^m} = [\mathbb{Q}(\zeta_p : \mathbb{Q}] = \prod_{k=1}^{2^m} [T_k : T_{k-1}],$$

kde na pravé straně máme 2^m součinů, tedy pokud platí $[T_k : T_{k-1}] \leq 2$ nebo $[T_k : T_{k-1}] \geq 2$, pak už nutně $[T_k : T_{k-1}] = 2$.

Příklad. Ukážeme, že ζ_5 je konstruovatelná bez použití Galoisovy teorie. Máme tedy posloupnost grup

$$1 = G_2 \leq G_1 \leq G_0 = \mathbb{Z}_5^* \cong \mathrm{Gal}(\mathbb{Q}(\zeta_5)/\mathbb{Q}).$$

Spočtěme příslušná θ_i pro $i \in \{0, 1, 2\}$. Víme, že $\theta_0 = -1$ a $\theta_2 = \zeta_5$, tedy zbývá θ_1. Protože $G_0 = Z_5^* = \langle 3 \rangle$, tak $G_1 = \langle 3^2 \rangle = \langle 4 \rangle$, tedy

$$\theta_1 = \sum_{g \in \{1, 4\}} \zeta_5^g = \zeta_5^4 + \zeta_5.$$

Nyní potřebujeme ukázat, že $[\mathbb{Q}(\zeta_5^4 + \zeta_5) : \mathbb{Q}] \leq 2$ a $[\mathbb{Q}(\zeta_5) : \mathbb{Q}(\zeta_5^4 + \zeta_5)] \leq 2$. Jelikož

$$(\zeta_5^4 + \zeta_5)^2 + (\zeta_5^4 + \zeta_5) - 1 = \zeta_5^3 + 2 + \zeta_5^2 + \zeta_5^4 + \zeta_5 - 1 = 0,$$

tak $\zeta_5^4 + \zeta_5$ je kořenem polynomu $x^2 + x - 1$, tedy první nerovnost platí. Dále

$$\zeta_5^2 - (\zeta_5^4 + \zeta_5)\zeta_5 + 1 = \zeta_5^2 - 1 - \zeta_5^2 + 1 = 0,$$

takže ζ_5 je kořenem polynomu $x^2 - (\zeta_5^4 + \zeta_5)x + 1$, což je polynom nad $\mathbb{Q}(\zeta_5^4 + \zeta_5)$, čímž máme i druhou nerovnost. Celkově dostáváme $\zeta_5 \in K$, díky povídání nad příkladem.

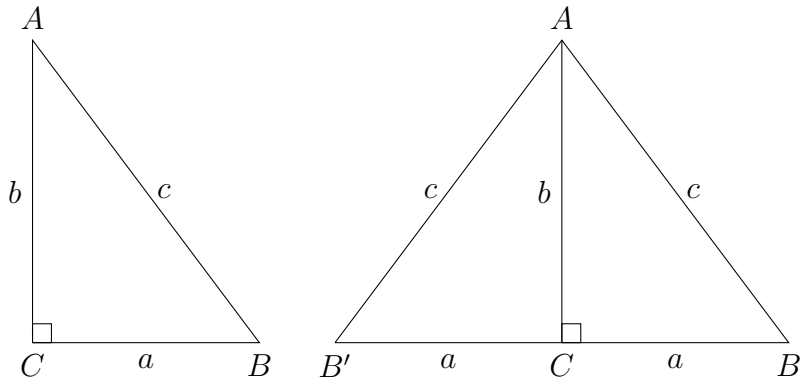
5 Heronův trojúhelník

Tato sekce vychází ze zdroje [8], jenže ten se nevěnuje následujícím jednoduchým tvrzením do podrobna, tak jsem navíc doplnil i důkazy. Dalším zdrojem této sekce je [1].

Definice. *Trojúhelník, jehož strany a obsah jsou přirozené čísla, nazveme Heronovým trojúhelníkem.*

Zřejmě všechny pravoúhlé trojúhelníky s celočíselnými stranami tvoří Heronův trojúhelník, neboť aspoň jedna z odvěsen musí být sudé délky. Kdyby byly obě odvěsny liché tak z rovnosti $a^2 + b^2 = c^2$, plyne že $c^2 \equiv 2 \pmod 4$, což nelze, neboť dvojka není kvadratický zbytek modulo čtyři (viz skripta Vítězslava Kaly [5]). Tedy $S = \frac{1}{2}ab$, je přirozené číslo, kde a, b jsou délky odvěsen. Máme tedy nekonečně mnoho Heronových trojúhelníků, stačí například vzít pravoúhelné trojúhelníky tvaru $(3k, 4k, 5k)$, pro $k \in \mathbb{N}$.

Dalším příkladem Heronových trojúhelníků může být rovnoramenný trojúhelník vzniklý z předchozího příkladu osovou souměrou podle jedné z odvěsen. Vizuálně vysvětleno na obrázku níže pro a, b, c přirozená čísla.



Následující větu uvádíme s důkazem, i přestože se jedná o velmi známé a snadné tvrzení, tak se důkaz často opomíjí.

Věta 5.1 (Heron)**.** *Mějme trojúhelník se stranami a, b, c a označme $s = \frac{a+b+c}{2}$, pak obsah onoho trojúhelníku bude*

$$S = \sqrt{s(s-a)(s-b)(s-c)}.$$

Důkaz. Mějme trojúhelník s délkami stran a, b, c. Použijeme cosinovou větu pro stranu c, tedy $c^2 = a^2 + b^2 - 2ab\cos(\gamma)$ a vzorec pro obsah $S = \frac{1}{2}ab\sin(\gamma)$, kde γ je protější úhel ke straně c. Upravíme rovnice a umocníme

$$4a^2b^2\cos^2(\gamma) = (a^2 + b^2 - c^2)^2,$$
$$4a^2b^2\sin^2(\gamma) = 16S^2,$$

nyní sečteme tyto rovnice a použijeme známou rovnost pro sinus a cosinus

$$4a^2b^2 = (a^2 + b^2 - c^2)^2 + 16S^2.$$

Odtud upravami dostaneme

$$\begin{aligned} 16S^2 &= (2ab + a^2 + b^2 - c^2)(2ab - a^2 - b^2 + c^2), \\ &= ((a+b)^2 - c^2)(c^2 - (a-b)^2), \\ &= (a+b+c)(a+b-c)(c+a-b)(c-a+b), \end{aligned}$$

což je pro $2s = a + b + c$ a drobných úpravách přesně co jsme chtěli dokázat. □

Heronův vzorec můžeme upravit na následující tvary

$$\begin{aligned} 16S^2 &= (a+b+c)(a+b-c)(a+c-b)(b+c-a), \\ 16S^2 &= ((a+b)^2 - c^2)(c^2 - (a-b)^2). \end{aligned}$$

Řešení těchto rovností v přirozených číslech jsou Heronovy trojúhelníky. Jedná se tedy o nutnou i postačující podmínku k tomu aby byl trojúhelník Heronův.

Na začátku jsme si ukázali, jak Heronův trojúhelník může vypadat, nyní si ale ukážeme opak. Tedy vrhneme se na podmínky, které žádný Heronův trojúhelník nesplňuje.

Lemma 5.2. *Neexistuje rovnostranný Heronův trojúhelník.*

Důkaz. Ať náš trojúhelník má stranu délky $a \in \mathbb{N}$, využitím vzorce Věta 5.1 máme $s = \frac{3}{2}a$ a obsah bude

$$S = \frac{\sqrt{3}}{4}a^2,$$

což zřejmě nemůže být přirozené číslo. □

Tímto jednoduchým lemmatem jsme si ukázali, že existuje nekonečně mnoho trojúhelníků s celočíselnými délkami stran, které nejsou Heronovy. Stačí trojúhelníky tvaru (k, k, k) pro $k \in \mathbb{N}$. Tedy víme, že všechny Heronovy trojúhelníky tvoří ostrou podmnožinu všech trojúhelníků s celočíselnými délkami stran.

Lemma 5.3. *Trojúhelník, jehož všechny strany jsou liché delky, nemůže být Heronův. Trojúhelník s jednou lichou a dvěma sudými délkami stran nemůže být Heronův.*

Důkaz. K tomu, aby byl trojúhelník Heronův, musí splňovat

$$16S^2 = (a+b+c)(a+b-c)(a+c-b)(b+c-a),$$

jenže pro dané restrikce délek stran je pravá strana rovnice lichá, kdežto levá je sudá. Tedy trojúhelník se zadanými restrikcemi nemůže být Heronův. □

Lemma 5.4. *Trojúhelník s délkou strany* 1 *nemůže být Heronův.*

Důkaz. Mějmě trojúhelník se stranami $a, b, 1$, kde $a, b \in \mathbb{N}$. Trojúhelníková nerovnost $|a - b| < 1$, nám dá pouze jednu možnost pro tvar strany b a to $b = a$. Tedy máme trojúhelník se stranami $a, a, 1$, pokud je a liché, tak všechny délky stran jsou liché. Pokud je a sudé tak máme jednu lichou a dvě sudé délky stran. Podle Lemmatu 5.3 ani jedna možnost nedává Heronův trojúhelník. □

Lemma 5.5. *Trojúhelník s délkou strany* 2 *nemůže být Heronův.*

Důkaz. Mějme trojúhelník se stranami $a, b, 2$, pro $a, b \in \mathbb{N}$. Opět podle trojúhelníkové nerovnosti máme $b = a - 1$ nebo $b = a$ nebo $b = a + 1$.
Pro $b = a$, máme po dosazení do Heronova vzorce

$$16S^2 = 4(4a^2 - 4).$$

Neboli $S^2 = a^2 - 1$, což nelze pro kladné S, tedy tato kombinace nedává Heronův trojúhelník.
Zbývající možnosti nám pro b liché dají a sudé a pro b sudé dají a liché. Ve všech případech máme trojúhelník s jednou lichou a dvěmi sudými délkami stran, což podle Lemmatu 5.3 nemůže být Heronův trojúhelník. □

Na chvíli odbočíme k tématu pythagorejských trojic. Pythagorejská trojice je taková trojice (a, b, c) přirozených čísel splňujících $c^2 = a^2 + b^2$. Jak jsme si již zmínili, tak taková trojice tvoří Heronův trojúhelník.

Definice. *Uspořádanou trojici (a, b, c) přirozených čísel nazveme primitivní pythagorejskou trojicí, pokud*

$$a^2 + b^2 = c^2 \quad a \quad \mathrm{NSD}(a, b, c) = 1.$$

Důvod odbočky k tématu pythagorejských trojic je následující tvrzení, které poté využijeme k důkazu hlavní věty této sekce. Tvrzení nám říká, že primitivní pythagorejskou trojici lze parametrizovat. Tato věta je poupravenou verzí věty z knihy [1].

Tvrzení 5.6. *Uspořádaná trojice (a, b, c) je primitivní pythagorejskou trojicí právě tehdy, když existují nesoudělná přirozená čísla $m > n$ různé parity taková, že*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2$$

nebo

$$a = 2mn, \quad b = m^2 - n^2, \quad c = m^2 + n^2.$$

Čísla m, n jsou jednoznačně určená.

Důkaz. ($\Rightarrow$) Ať (a, b, c) je primitivní pythagorejská trojice, kdyby a, b byly obě sudá čísla, tak i c je sudé číslo, jelikož $a^2 + b^2 = c^2$, což je spor s nesoudělností čísel a, b, c. Kdyby a, b byly lichá čísla, pak $a^2 \equiv 1 \pmod 4$ a také $b^2 \equiv 1 \pmod 4$, tedy $c^2 = a^2 + b^2 \equiv 2 \pmod 4$, jenže dvojka není kvadratický zbytek modulo 4. Tedy nutně a, b mají různou paritu.

Ať a je liché a b je sudé, tedy $b = 2k$, pro nějaké k přirozené číslo. Z rovnosti $c^2 = a^2 + b^2$ plyne, že c je liché, dále

$$k^2 = \frac{c^2 - a^2}{4} = \frac{(c + a)(c - a)}{4}.$$

Položme $e := \frac{c+a}{2}$ a $f := \frac{c-a}{2}$, pak zřejmě $e > f$ a jsou to přirozená čísla, jelikož a, c jsou lichá. Dále e, f jsou nesoudělná, neboť kdyby existoval dělitel $d \geq 1$, pak by dělil i jejich součet, což je c, a jejich rozdíl, což je a, z rovnosti $c^2 = a^2 + b^2$ by dělil i b. Měli bychom spor s nesoudělností a, b, c, tedy e, f jsou nesoudělná. Dále z rovnosti $k^2 = ef$ a $\mathrm{NSD}(e, f) = 1$ plyne, že e i f jsou druhé mocniny, označme $m^2 := e$ a $n^2 := f$, pro nějaké $m, n \in \mathbb{N}$, nesoudělná a $m > n$, protože $e > f$.

Jenže tím máme hotovo, neboť $e + f = c$ a $e - f = a$, odtud $c = m^2 + n^2$ a $a = m^2 - n^2$, dosazením do $c^2 = a^2 + b^2$, máme $b = 2mn$. A m, n mají různou paritu, neboť e, f mají také různou, díky rovnosti $c = e + f$, pro c liché.

Případ pro a sudé a b liché je naprosto analogický. Stačí nahradit v důkazu všechny výskyty a za b a vice versa.

($\Leftarrow$) Mějme $m > n$ nesoudělná přirozená čísla různé parity a

$$(a, b, c) = (m^2 - n^2, 2mn, m^2 + n^2) \quad \text{nebo} \quad (a, b, c) = (2mn, m^2 - n^2, m^2 + n^2).$$

Zřejmě obě trojice jsou trojicemi přirozených čísel, pro které platí

$$a^2 + b^2 = m^4 + 2m^2n^2 + n^4 = (m^2 + n^2)^2 = c^2.$$

Dále obě trojice obsahují nesoudělná čísla, neboť kdyby existoval společný prvočíselný dělitel $d > 1$ čísel $m^2 - n^2, 2mn, m^2 + n^2$, pak by $d \mid 2mn$, tedy $d = 2$ nebo $d \mid m$ nebo $d \mid n$
Případ $d = 2$. Díky rozdílné paritě m a n jsou obě čísla $m^2 - n^2, m^2 + n^2$ lichá. Tedy $d = 2$ nemůže být jejich společný dělitel.
Případ $d \mid m$. Jenže d je také dělitel $m^2 + n^2$, tedy z $d \mid m$ plyne, že d dělí také n, což je spor s nesoudělností čísel m, n.
Případ $d \mid n$. Nám stejným argumentem jako výše dá spor s nesoudělností čísel m, n.

Celkově máme trojice nesoudělných přirozených čísel, splňujících rovnost $c^2 = a^2 + b^2$, tedy jedná se o primitivní pythagorejské trojice.

□

Nyní se vrhneme zpět k Heronovým trojúhelníkům a k hlavní větě této sekce. Vycházím z onoho již zmíněného zdroje [8], který obsahoval následující lemma, které jsem poupravil a důkaz upřesnil.

Lemma 5.7. *Ať S je obsah a p^i, b, c jsou délky stran Heronova trojúhelníku, pro $i, b, c \in \mathbb{N}$ a p prvočíslo takové, že $p = 2$ nebo $p \equiv 2\,(mod\,3)$. Pak*

$$p^{i+1} \mid (b^2 - c^2) \quad a \quad p^{i+1} \mid 4S, \quad pro\ p = 2$$

nebo

$$p^i \mid (b^2 - c^2) \quad a \quad p^i \mid S, \quad pro\ p \equiv 3\,(mod\,4).$$

Důkaz. Pro $b = c$ zřejmě platí, tedy ať $b \neq c$, upravme Heronův vzorec 5.1

$$16S^2 = ((b + c)^2 - p^{2i})(p^{2i} - (b - c)^2)$$
$$(4S)^2 = 2p^{2i}(b^2 + c^2) - p^{4i} - (b^2 - c^2)^2.$$

Nejprve dokážeme lemma pro $p \equiv 3 \pmod 4$. Podívejme se na naši rovnost modulo p^{2i}

$$(4S)^2 \equiv -(b^2 - c^2)^2 \pmod{p^{2i}}.$$

Pro spor ať $p^i \nmid (b^2 - c^2)$, tedy bude existovat přirozené číslo $j < i$ takové, že $p^j \mid (b^2 - c^2)$ a ať je největší s takovou vlastností. Tedy $(b^2 - c^2) = p^j k$, kde

$k \in \mathbb{N}$ je nesoudělné s p. Pak díky kongurenci výše bude i $4S$ dělitelné p^j, tak tedy vydělme onu kongurenci číslem p^{2j},

$$\left(\frac{4S}{p^j}\right)^2 \equiv -k^2 \,(\mathrm{mod}\, p^{2(i-j)}).$$

Jelikož k je nesoudělné s p tedy i s $p^{2(i-j)}$, tak bude existovat inverz ke k, tedy $l \in \mathbb{N}$ splňující $kl \equiv 1(\mathrm{mod}\, p^{2(i-j)})$, pak ale

$$\left(\frac{4S}{p^j}l\right)^2 \equiv -1 \,(\mathrm{mod}\, p^{2(i-j)}).$$

Podíváme-li se na rovnost pouze modulo p dostaneme, že -1 je kvadratický zbytek modulo p, což není podle Lemmatu 2.8, máme tedy spor a proto $j = i$, tedy $p^i \mid 4S$ a $p^i \mid (b^2 - c^2)$.

Nyní pro $p = 2$. Dosadíme-li za p dvojku do rovnosti na začátku důkazu dostaneme

$$(4S)^2 + (b^2 - c^2)^2 = 2^{2i+1}(b^2 + c^2) - 2^{4i}.$$

Vidíme, že levá strana rovnice je dělitelná 2^{2i+1}, ale ne jen to z Lemmatu 5.3 plyne, že b,c jsou nutně lichá čísla, tedy $b^2 + c^2$ je sudé. Celkově, zde ještě nutno ověřit, že $4i \geq 2i + 2$, což pro $i \in \mathbb{N}$ platí, je tedy levá strana dělitelná číslem 2^{2i+2}. Máme

$$(4S)^2 \equiv -(b^2 - c^2)^2 \,(\mathrm{mod}\, 2^{2i+2}),$$

a obdobně jako u prvního případu, ať $2^{i+1} \nmid (b^2 - c^2)$ a $j < i + 1$ je maximální přirozené číslo takové, že $2^j \mid (b^2 - c^2)$. Pak existuje liché číslo m spňující $b^2 - c^2 = 2^j m$, vydělme kongurenci uvedenou výše číslem 2^{2j},

$$\left(\frac{4S}{2^j}\right)^2 \equiv -m^2 \,(\mathrm{mod}\, 2^{2(i+1-j)}).$$

Opět jelikož m je nesoudělné s $2^{2(i+1-j)}$, tak je inveribilní, s inverzem označeným n, a dostaneme

$$\left(\frac{4S}{2^j}n\right)^2 \equiv -1 \,(\mathrm{mod}\, 2^{2(i+1-j)}).$$

Podíváme-li se na kongurenci pouze modulo 4, což si můžeme dovolit neboť $i + 1 > j$, dostaneme, že -1 je kvadratický zbytek modulo 4, ale to není. Máme tedy spor a nutně $j = i + 1$ a platí $2^{i+1} \mid (b^2 - c^2)$ a $2^{i+1} \mid 4S$. □

Následující lemma v mém zdroji nebylo a důkaz byl odbyt použitím jednodušší verze Catalanovy věty.

Lemma 5.8. *Mějme $x, i, k \in \mathbb{N}$ splňující $x^i - 2^{2k} = 1$, pak nutně $i = 1$.*

Důkaz. Z rovnosti $x^i - 2^{2k} = 1$ ihned vidíme, že x je liché. Rozdělíme důkaz podle parit čísla i.

Předokládejme, že i je sudé, tedy $i = 2j$ pro nějaké $j \in \mathbb{N}$. Pak onu rovnost můžeme upravit do tvaru

$$(x^j - 2^k)(x^j + 2^k) = 1.$$

Jelikož všechna čísla jsou přirozená, tak se oba výrazy v závorkách rovnají buď jedné nebo mínus jedné. Druhý případ zřejmě nemůže nastat jelikož $x^j + 2^k > 0$. Nyní případ kdy $x^j - 2^k = 1$ a $x^j + 2^k = 1$. Sečteme-li tyto rovnice dostaneme

$$2x^j = 2,$$

pro $j \in \mathbb{N}$ má tato rovnost řešení pouze pro $x = 1$, jenže pak by $2^{2k} = 0$, což nelze.

Nyný předpokládejme, že i je liché. Upravíme rovnost ze zadání do tvaru

$$(x-1)(x^{i-1} + x^{i-2} + \cdots + x + 1) = 2^{2k},$$

odtud dostáváme, že oba výrazy v závorkách musí být mocninou dvojky. Jenže výraz $x^{i-1} + \cdots + 1$ je lichý, neboť x a i jsou liché a tedy sčítáme lichý počet lichých čísel, tedy je nutně roven jedné. Což nastane pro $i = 1$ čímž máme hotovo. □

Věta 5.9 (Luca)**.** *Mějme Heronův trojúhelník, jehož strany jsou mocninami prvočísel. Pak se nutně jedná o trojúhelník* $(3, 4, 5)$ *nebo* $(F_m, F_m, 4(F_{m-1} - 1))$*, pro nějaké* $m \geq 1$ *a* F_m *Fermatovo prvočíslo.*

Důkaz. Ať ${p_1}^i, {p_2}^j, {p_3}^k$, jsou strany Heronova trojúhelníku, pro p_1, p_2, p_3 prvočísla a $i, j, k \geq 0$ jsou přirozená čísla. Díky Lemmatu 5.4 jsou i, j, k nutně kladná. Rozdělme naši větu na případy podle parit délek stran.

Všechna prvočísla jsou lichá nebo dvě jsou sudá a jedno liché. Ihned z Lemmatu 5.3 plyne spor.

Všechna prvočísla jsou sudá. Tedy $p_1 = p_2 = p_3 = 2$, dále můžeme bez újmy na obecnosti předpokládt, že $i \geq j \geq k$, z rovnosti

$$\begin{aligned} 16S^2 &= ((2^i + 2^j)^2 - 2^{2k})(2^{2k} - (2^i - 2^j)^2), \\ &= 2^{4k}((2^{i-k} + 2^{j-k})^2 - 1)(1 - (2^{i-k} - 2^{j-k})^2), \end{aligned}$$

vidíme, že výraz $((2^{i-k} + 2^{j-k})^2 + 1)(1 - (2^{i-k} - 2^{j-k})^2)$ musí být druhou mocninou. Jenže tyto dva výrazy v závorkách jsou nesoudělné, neboť pokud by existoval prvočíselný dělitel $d > 1$ těchto dvou čísel, tak by dělil i jejich součet. Tedy $d \mid 2^2 2^{i-k} 2^{j-k}$, takže $d = 2$, což vede ke sporu, protože $2 \nmid ((2^{i-k} + 2^{j-k})^2 + 1)$. Tedy výrazy jsou nesoudělné, ale aby součin dvou nesoudělných čísel byl druhou mocninou tak obě musí být druhou mocninou, tedy $(2^{i-k} + 2^{j-k})^2 + 1$ musí být nutně čtverec, což není pro $i, j, k \geq 1$.

Dvě prvočísla jsou lichá a jedno je sudé. Tedy ať p_1, p_2 jsou liché a $p_3 = 2$. Tuto poslední možnost rozdělíme dále na dvě.

Předpokládejme, že je trojúhelník rovnoramenný, neboli $p_1 = p_2$ a $i = j$, potom díky Pythagorově větě máme

$${p_1}^{2i} = v^2 + 2^{2(k-1)},$$

kde v je výška trojúhelníku. Díky rovnosti výše máme zřejmě, že $v^2 \in \mathbb{N}$, ale zároveň platí $S = \frac{1}{2} 2^k v$, kde S je obsah trojúhelníku, který je Heronův, takže S je přirozené a odtud dostáváme, že $v \in \mathbb{Q}$. Dohromady v je racionální číslo jehož druhá mocnina je přirozená, odtud $v \in \mathbb{N}$. Tedy $({p_1}^i, v, 2^{k-1})$ je primitivní

pythagorejská trojice, takže podle Tvrzení 5.6 existují nesoudělná $t, s \in \mathbb{N}$, různé parity taková, že

$$\begin{aligned} {p_1}^i &= t^2 + s^2, \\ v &= t^2 - s^2, \\ 2^{k-1} &= 2ts. \end{aligned}$$

Ať t je sudé, pak s je liché a z poslední rovnosti plyne, že $t = 2^{k-2}$ a $s = 1$. Podle Lemmatu 5.5 $k \geq 2$, takže $t \in \mathbb{N}$. Dosazením do první rovnice dostáváme

$${p_1}^i = 2^{2(k-2)} + 1.$$

Jenže Lemma 5.8 říká, že pro totu rovnost neexistuje řešení pro $i > 1$. Tedy nutně $i = 1$

$$p_1 = 2^{2(k-2)} + 1.$$

Jenže podle Lemmatu 1.3 je p_1 nutně Fermatovo prvočíslo, tedy $p_1 = F_m$, pro nějaké $m \geq 0$. Jelikož $p_1 = t^2 + s^2$, pro t, s různé parity, tak $p_1 > 3$, tedy $m \geq 1$. Dále rovnost $2^{2^m} + 1 = 2^{2(k-2)} + 1$ nám dává $k = 2^{m-1} + 2$, tedy ${p_3}^k = 4(2^{2^{m-1}} + 1 - 1) = 4(F_{m-1} - 1)$. Takže celkově máme Heronův trojúhelník $(F_m, F_m, 4(F_{m-1} - 1))$.

Nyní ať trojúhelník není rovnoramenný, máme tedy délky stran ${p_1}^i, {p_2}^j, 2^k$, kde $p_1 \neq p_2$. Z Lemmatu 5.7 pro 2^k máme, že $2^{k+1} \mid ({p_1}^{2i} - {p_2}^{2j})$ a $2^{k+1} \mid 4S$. Z druhé vlastnosti plyne, že nutně $2^k \mid 2S$ a z první $2^{k+1} \mid ({p_1}^i + {p_2}^j)({p_1}^i - {p_2}^j)$, jelikož p_1, p_2 jsou liché tak

$$2^k \mid ({p_1}^i + {p_2}^j) \quad \text{nebo} \quad 2^k \mid ({p_1}^i - {p_2}^j).$$

Ale 2^k je délka strany trojúhelníku a z trojúhelníkové nerovnosti $|{p_1}^i - {p_2}^j| < 2^k$, může nastat pouze první možnost, takže $2^k \mid ({p_1}^i + {p_2}^j)$. Jelikož podle Lemmatu 5.5 je $k \geq 2$, tak musí jedna ze stran kongruentní 1 modulo 4 a druhá 3 modulo 4. Bez újmy na obecnosti ať ${p_1}^i \equiv 1 \,(\mathrm{mod}\, 4)$ a ${p_2}^j \equiv 3 \,(\mathrm{mod}\, 4)$. Z druhé kongruence máme nutně, že $p_2 \equiv 3 \,(\mathrm{mod}\, 4)$ a j je liché.
Použijeme Lemma 5.7 pro stranu ${p_2}^j$ a dostaneme, že ${p_2}^j \mid S$, jelikož je p_2 liché tak ${p_2}^j \mid 2S$. Výše jsme ukázali, že $2^k \mid 2S$, dohromady protože $2^k, {p_2}^j$ jsou nesoudělná, máme $2^k {p_2}^j \mid 2S$, odtud $2S \geq 2^k {p_2}^j$ neboli $S \geq \frac{1}{2} 2^k {p_2}^j$. Jenže obsah obecného trojúhelníku můžeme vyjádřit jako $S = \frac{1}{2} 2^k {p_2}^j \sin(\alpha)$, kde α je protější úhel ke straně ${p_1}^i$. Máme

$$S \geq \frac{1}{2} 2^k {p_2}^j \quad \text{a} \quad S = \frac{1}{2} 2^k {p_2}^j \sin(\alpha),$$

z čehož plyne, že $\sin(\alpha) \geq 1$, nutně musí nastat rovnost. tedy α je pravý úhel. Podle Pythagorovy věty

$${p_1}^{2i} = {p_2}^{2j} + 2^{2k},$$

$p_1, p_2, 2$ jsou nesoudělná, tedy $(2^k, {p_2}^j, {p_1}^i)$ tvoří primitivní pythagorejskou trojici, takže podle Tvrzení 5.6 existují nesoudělná $t, s \in \mathbb{N}$ rozdílné parity, taková že

$$\begin{aligned} {p_1}^i &= t^2 + s^2, \\ {p_2}^j &= t^2 - s^2, \\ 2^k &= 2ts. \end{aligned}$$

Ať t je sudé a s liché, pak z poslední rovnosti máme, že $t = 2^{k-1}$ a $s = 1$. Dosadíme do druhé rovnosti a dostaneme ${p_2}^j = (t-1)(t+1)$, jelikož $t-1$, $t+1$ jsou nesoudělná lichá čísla a jejich součin je roven mocnině lichého prvočísla, tak nutně $t - 1 = 1$, tedy $t = 2$. Jednoduchým dopočítáním zjistíme, že $k = 2$, $p_2 = 3$, $j = 1$, $p_1 = 5$ a $i = 1$. Tedy máme trojúhelník $(3, 4, 5)$.

□

Závěr

Tímto ukončuji práci na téma Fermatova prvočísla v geometrii. Zabývali jsme se nejprve vlastnostmi Fermatových čísel, kde jsme si ukázali důležitou podmínku, kdy prvočíslo určitého tvaru je již nutně Fermatovo prvočíslo. Další kapitolou byla konstruovatelnost, kde jsme se věnovali podrobněji otázce, jak zkonstruovat různá čísla a také kdy je dané číslo nutně konstruovatelné. Poslední dvě kapitoly se již věnovali hlavním větám této práce a těmi jsou Gaussova-Wantzelova věta a Lucova věta.

Na rozdíl od zdrojů ze, kterých jsem vycházel jsem detailněji rozpracoval důkazy, dokázal co bylo ponecháno čtenáři nebo důkazy poupravil. Dále jsem se věnoval přesným postupům konstrukce určitých čísel, které jsem doplnil o obrázky. Knížka, která mě inspirovala k této baklářce byla Kouzlo čísel [1]. Ještě bych vzpomněl zdroj, ze kterého jsem čerpal historické poznatky v úvodu [9].

Na závěr bych zmínil, že existuje ještě jedna věta, která se vztahuje k Fermatovým prvočíslům a geometrii a tou je věta Abelova.

Abelova věta nám říká, že lemniskáta lze rozdělit pomocí kružítka a pravítka na n stejných částí právě tehdy, když $n = 2^i F_{m_1} \cdots F_{m_k}$, kde $n, i, k \in \mathbb{N}_0$, a $F_{m_1}, \cdots, F_{m_k}$ jsou po dvou různá Fermatova prvočísla.

Literatura

1. Křížek, Michal; Somer, Lawrence; Šolcová, Alena. *Kouzlo čísel: od velkých objevů k aplikacím*. Academia, 2018.
2. Křížek, Michal; Luca, Florian; Somer, Lawrence. *17 lectures on Fermat numbers: from number theory to geometry*. Sv. 9. Springer, 2001.
3. Stanovský, David. *Algebra 2021/22* [online]. [cit. 2024-02-07]. Dostupné z: `https://www.karlin.mff.cuni.cz/~stanovsk/vyuka/2122/algebra22.pdf`.
4. Kala, Vítězslav. *Úvod do komutativní algebry* [online]. [cit. 2024-02-07]. Dostupné z: `https://karlin.mff.cuni.cz/~kala/files/UKA22.pdf`.
5. Kala, Vítězslav. *Teorie čísel* [online]. [cit. 2024-02-07]. Dostupné z: `https://www.karlin.mff.cuni.cz/~kala/files/TC22.pdf`.
6. Isaacs, I Martin. *Algebra: a graduate course*. Sv. 100. American Mathematical Soc., 2009.
7. Pérez Zarraonandia, Josu. The Galois theory of the lemniscate. 2022. Dostupné také z: `https://addi.ehu.es/bitstream/handle/10810/58925/TFG_Josu_Perez_Zarraonandia.pdf?sequence=3&isAllowed=y`.
8. Luca, Florian. Fermat Primes and Heron Triangles with Prime Power Sides. *The American Mathematical Monthly* [online]. 2003, roč. 110, č. 1, s. 46–49 [cit. 2024-07-02]. ISSN 00029890, ISSN 19300972. Dostupné z: `http://www.jstor.org/stable/3072343`.
9. Morelli, Luigi. *Distributed Search for Fermat Number Divisors* [online]. [cit. 2024-02-07]. Dostupné z: `http://www.fermatsearch.org/history.html`.