Univerzita Hradec Králové

Přírodovědecká fakulta

Katedra matematiky

Speciální typy prvočísel

Bakalářská práce

Autor: Zdena Kratochvílová

Studijní program: B1101 Matematika

Studijní obor: Matematika se zaměřením na vzdělávání
Základy techniky se zaměřením na vzdělávání

Vedoucí práce: RNDr. Jitka Kühnová, Ph.D.

Hradec Králové duben 2015

Univerzita Hradec Králové

Přírodovědecká fakulta

Zadání bakalářské práce

Autor:	**Zdena Kratochvílová**
Studijní program:	B1101 Matematika
Studijní obor:	Matematika se zaměřením na vzdělávání Základy techniky se zaměřením na vzdělávání
Název závěrečné práce:	**Speciální typy prvočísel**
Název závěrečné práce AJ:	Some Special Types of Prime Numbers

Cíl, metody, literatura, předpoklady:

Cílem této práce je shrnout základní pojmy z teorie prvočísel, zaměřit se na některé speciální typy prvočísel a vše ilustrovat vhodně zvolenými příklady a aplikacemi.

Garantující pracoviště:	Katedra matematiky, Přírodovědecká fakulta UHK
Vedoucí práce:	RNDr. Jitka Kühnová, Ph.D.
Konzultant:	
Oponent:	RNDr. Ladislava Francová, Ph.D.
Datum zadání závěrečné práce:	24. 2. 2014
Datum odevzdání závěrečné práce:	30. 4. 2015

Prohlášení:

Prohlašuji, že jsem bakalářskou práci vypracovala samostatně a že jsem v seznamu použité literatury uvedla všechny prameny, z kterých jsem vycházela.

V Hradci Králové Jméno a příjmení

Anotace

KRATOCHVÍLOVÁ, Z. *Speciální typy prvočísel.* Hradec Králové, 2015. Bakalářská práce na Přírodovědecké fakultě Univerzity Hradec Králové. Vedoucí bakalářské práce Jitka Kühnová. 42 s.

Tato bakalářská práce se zabývá speciálními typy prvočísel. Její součástí je shrnutí základních pojmů týkajících se prvočísel. Hlavní část práce se věnuje třem speciálním typům prvočísel; Mersenovým, Fermatovým a Eukleidovým prvočíslům. Vše je ilustrováno vhodně zvolenými příklady a dalšími možnými aplikacemi.

Klíčová slova

prvočíslo, Mersennovo prvočíslo, dokonalé číslo, Fermatovo prvočíslo, pravidelný mnohoúhelník, Eukleidovo prvočíslo

Annotationes

KRATOCHVÍLOVÁ, Z. *Some Special Types of Prime Numbers.* Hradec Králové, 2015. Bachelor Thesis at Faculty of Science University of Hradec Králové. Thesis Supervisor Jitka Kühnová. 42 p.

The Bachelor Thesis examines some special types of prime numbers. A part of the work is a conclusion of the basic terminology regarding prime numbers. The main part of the thesis is dedicated to the three special types of prime numbers. The whole work is accompanied by moderately chosen examples and other possible applications.

Keywords

prime number, Mersenne prime, perfect number, Fermat prime, regular polygon, Euclidean prime

Úvod

Hlavním námětem této práce jsou speciální typy prvočísel. První část je věnována prvočíslům obecně, shrnuje základní pojmy a několik důležitých vět o prvočíslech. Zároveň představuje známé matematiky, kteří podali pro další studium prvočísel důležité základy. To vše je zasazeno do historického kontextu.

Druhá část je zaměřena na speciální typy prvočísel a má tři samostatné podkapitoly. První z nich přibližuje Mersennova prvočísla a jejich autora včetně domněnky, kterou vyslovil ohledně množiny těchto prvočísel. Zároveň je předložena spojitost Mersennových prvočísel jednak s dokonalými čísly, ale také s oborem kryptografie. Druhá podkapitola je zaměřena na Fermatova prvočísla a jejich autora a dále i na aplikaci Fermatových prvočísel v geometrii. Třetí část pak pojednává o Eukleidových prvočíslech.

Práce má hlavně informační charakter. Cílem je přehledně uspořádat důležitá a dosud poznaná fakta a dostatečně se seznámit s danou problematikou. Většina poznatků je doplněna konkrétními příklady, které pomohou lépe pochopit právě rozebíranou problematiku.

V celé práci se předpokládá znalost základních pojmů algebry.

Seznam symbolů

$\mathbb{N} = \{1, 2, 3, \dots\}$	množina přirozených čísel
$\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$	množina celých čísel
$\mathbb{R}$	množina reálných čísel
$\mathbb{Z}_n = \{\bar{0}, \bar{1}, \bar{2}, \dots, \overline{n-1}\}$	množina zbytkových tříd po dělení číslem n
$\bar{a} \in \mathbb{Z}_n$	$\bar{a} = \{x \in \mathbb{Z}; x = nq + a, 0 \leq a < r\}$
F_m	Fermatova čísla
M_p	Mersennova prvočísla
T_n	trojúhelníková čísla
$(n_1, n_2, \dots, n_k) = d$	největší společný dělitel d čísel $n_1, n_2, \dots, n_k$
$\{n_1, n_2, \dots, n_k\}$	množina k čísel $n_1, n_2, \dots, n_k$ (nezáleží na pořadí)
$\langle n_1, n_2, \dots, n_k \rangle$	uspořádaná k-tice čísel $n_1, n_2, \dots, n_k$ (záleží na pořadí)
(a_i)	posloupnost
$n \equiv k \ (mod\ m)$	n je kongruentní s k modulo m
$\approx$	přibližná rovnost
$m \mid n$	m dělí n
$m \nmid n$	m nedělí n
$\pi(x)$	počet prvočísel nepřevyšujících x
$\tau(n)$	počet všech kladných dělitelů čísla n
$\omega(n)$	počet všech prvočíselných dělitelů čísla n
$\sigma(n)$	součet všech kladných dělitelů čísla n
i, j, k	celočíselné jednotky
■	Halmosův symbol označující konec důkazu

1 Prvočísla napříč historií

1.1 První rozdělení čísel

Historie prvočísel začíná již několik století před naším letopočtem. Pythagoras ze Samu je středověký matematik žijící v letech 590–500 př. n. l. Ve svém mládí hodně cestuje, což mu pomáhá poznávat učení a různé filozofie jiných národů. Při svých cestách dokonce získává přístup i k utajovaným znalostem tehdejších kněží. Po návratu zpět na rodný Samos se rozhoduje právě pro dráhu filozofa, avšak pro nepřátelství s místním tyranem Polykratem, nemůže sehnat žáky. Kolem svých čtyřiceti let se tedy stěhuje do řecké osady v jihoitalském Krotonu a zakládá zde svou proslulou školu pythagorejců. Ačkoli je to filozofická škola, má neobvykle široký záběr: přes přírodní vědy, astronomii, lékařství, hudbu až k matematice, které je věnována největší pozornost. Pythagorejci jsou doslova fascinováni čísly, která považují za „stavební atomy" celého světa. Hledají mezi čísly různé vztahy, snaží se je rozkládat, nebo různě kombinovat a podávají tak dobrý základ pro teorii čísel. Ukazují například, že součet po sobě jdoucích lichých přirozených čísel je druhá mocnina nebo že součet dvou lichých po sobě jdoucích přirozených čísel je dělitelný čtyřmi. Při svém zkoumání dělitelnosti čísel, nacházejí taková, která mají právě dva různé dělitele. Poprvé v historii se začíná mluvit o prvočíslech. Od třetího století před naším letopočtem se začínají přirozená čísla dělit do následujících tří skupin:

1) Číslo 1 patří do samostatné skupiny, protože jako jediné není dělitelné žádným jiným číslem kromě sebe samotným.
2) Druhou skupinu tvoří čísla, které kromě sebe jsou dělitelné už jen číslem jedna a žádným jiným přirozeným číslem; ty se nazývají prvočísly.
3) Všechna ostatní čísla nepatřící ani do první a ani do druhé skupiny, jsou čísla složená.

Pro další zkoumání prvočísel je důležité dokázat následující věty:

Věta 1.1 (První Euklidova věta): Nechť p je prvočíslo a nechť $p|a_1a_2 \dots a_k$, kde $a_1, \dots, a_k, k$ jsou přirozená čísla. Potom buď $p|a_1$ nebo $p|a_2$ … nebo $p|a_k$.

Důkaz: Dokážeme matematickou indukcí podle k:

- $k = 2$, mohou nastat dva případy
  - pokud $p|a_1$ jsme hotovi
  - pokud $p \nmid a_1$ tak $(p, a_1) = 1$ a existují celá čísla x a y [1] tak, že $a_1x + py = 1$ a tedy $a_1xa_2 + pya_2 = a_2$
    protože $p|a_1a_2$ a $p|p$, vidíme, že $p|a_2$

[1] Pomocná věta: Nechť $k = (m, n)$ pro nějaká celá čísla m a n, která nejsou současně nulová. Pak existují celá čísla x a y tak, že $mx + ny = k$.

- nyní označme $A = a_1 \dots a_{k-1}$. Předpokládejme, že věta platí pro $k-1$ činitelů a dokažme, že platí i pro k činitelů. Podle předpokladu věty platí $p|Aa_k$. Rozlišujeme dva případy (podle předcházejících úvah): buď $p|A$ potom je naše tvrzení podle indukčního předpokladu pravdivé, nebo $p|a_k$.

■

([21], s. 55)

Věta 1.2 Každé složené číslo můžeme psát ve tvaru součinu prvočísel.

Důkaz: Dokážeme matematickou indukcí podle k

- $k = 4$ je nejmenší složené číslo a můžeme jej napsat jako $4 = 2 \cdot 2$, tedy tvrzení je pravdivé.
- Předpokládejme, že tvrzení je pravdivé pro všechna složená čísla menší než n.
  Pokud n je číslo složené, je možné jej zapsat ve tvaru $n = ab$, kde $1 < a < n$, $1 < b < n$. Buďto je a prvočíslo, nebo číslo složené a menší než n, a tak podle indukčního předpokladu je možné a ve tvaru součinu prvočísel. To samé platí i o b, a tak n je možné psát ve tvaru součinu prvočísel (nebo jen jako součin a a b, pokud to jsou prvočísla).

■

([21], s. 55, 56)

Věta 1.3 (Základní věta aritmetiky) Každé přirozené číslo $n > 1$ lze vyjádřit jediným způsobem ve tvaru

$$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$

kde $p_1 < p_2 < \cdots < p_k$ jsou prvočísla a $a_1, \dots, a_k$ jsou přirozená čísla.

Důkaz:

- Možnost takového vyjádření složených čísel jsme již ukázali v předchozí větě. Pokud n je prvočíslo, tak stačí, když $k = 1, p_1 = n, \alpha_1 = 1$.
- Musíme ještě dokázat, že pro každé přirozené číslo existuje jediné takové vyjádření. Předpokládejme, že pro nějaké n existují dvě vyjádření v kanonickém tvaru

  $$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k},$$
  $$n = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s},$$

  kde $p_1 < p_2 < \cdots < p_k$, $q_1 < q_2 < \cdots < q_s$ jsou prvočísla a $a_1, \dots, a_k$ a $\beta_1, \dots, \beta_s$ jsou přirozená čísla. Potom

  $$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}.$$
- Pro každé i tedy platí:

  $$p_i | q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}.$$

- Na základě Věty 1.1 z toho vyplývá, že $p_i | q_j^{\beta_j}$ pro nějaké j. Stačí ještě jednou aplikovat Větu 1.1, abychom dostali $p_i | q_j$; to je možné pouze tehdy, když $p_i = q_j$ (neboť obě čísla jsou prvočísla). Tedy v rovnosti
$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$
vystupuje na pravé straně alespoň tolik prvočísel jako na levé, tj. $k \leq s$. Podobnou úvahou můžeme dokázat, že $s \leq k$. Protože p_i a q_j jsou uspořádané podle velikosti, tak z uvedených úvah vyplývá, že
$$p_1 = q_1 \dots, p_k = q_k.$$
- Musíme ještě dokázat, že $\alpha_i = \beta_i$ pro $i = 1, 2, \dots, k$. To dokážeme nepřímo. Předpokládejme například, že $\alpha_i > \beta_i$. Potom z rovnosti
$$p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k} = q_1^{\beta_1} q_2^{\beta_2} \cdots q_s^{\beta_s}$$
(a z rovnosti $s = k$) po vydělení číslem $p_i^{\beta_i}$ dostaneme:
$$p_i^{\alpha_1} \cdots p_{i-1}^{\alpha_{i-1}} p_i^{\alpha_1 \beta_1} p_{i+1}^{\alpha_{i+1}} \cdots p_k^{\alpha_k} = p_1^{\beta_1} \cdots p_{i-1}^{\beta_{i-1}} p_{i+1}^{\beta_{i+1}} \cdots p_k^{\beta_k}.$$
Číslo $\alpha_i - \beta_i > 0$, a proto levá strana poslední rovnosti je dělitelná prvočíslem p_i, ale pravá ne, což je spor. Podobně bychom postupovali i v případě $\alpha_i < \beta_i$, takže pro všechna $i = 1, \dots, k$ platí $\alpha_i = \beta_i$.
To znamená, že každé dvě vyjádření čísla n v kanonickém tvaru jsou totožná, a tak libovolné n můžeme vyjádřit v kanonickém tvaru jediným způsobem.

■

([21], s. 56 – 58)

1.2 Kolik je prvočísel?

Už víme, co to prvočísla jsou, a dokázali jsme, že každé složené číslo lze rozložit na prvočísla. Naskýtá se tedy otázka, kolik prvočísel skutečně existuje? Mezi prvním tisícem přirozených čísel je 168 prvočísel. Dále mezi čísly 1 000 a 2 000 je právě 135 prvočísel, mezi 2 000 a 3 000 právě 127 prvočísel a mezi 3 000 a 4 000 je jich 120. Vidíme tedy, že prvočísel pomalu ubývá, vymizí však úplně? Mohlo by být ovšem nekonečně mnoho složených čísel, pokud by došly jejich „stavební kameny“ – prvočísla? Asi sto let po zavedení pojmu prvočíslo, předkládá Eukleides důkaz o jejich nekonečném počtu.

Celým jménem Eukleides z Alexandrie (325-265 př. n. l.) prožívá většinu svého života právě ve starověkém egyptském městě Alexandria, kam je povolán králem Ptolemaiem I. Přívlastek *z* u něj tedy výjimečně neoznačuje místo narození, ale místo, kde prožívá většinu svého života. Eukleides je králem dosazen do pozice vedoucího týmu matematiků v nově založené knihovně, známé také jako Múseion. Díky tomuto získává přístup k mnoha matematickým výsledkům, které utříbeně sepisuje a doplňuje vlastními poznatky. Takto vzniká

matematicko-literární poklad, jeho známé třináctisvazkové dílo Základy, podle kterého se matematika na školách vyučuje bezmála další dvě tisíciletí po jeho smrti. Poprvé se v tomto díle dokonce setkáváme s důkazy matematických vět.

Jedním z nejznámějších a zároveň vzorovým Eukleidovým důkazem, je důkaz o nekonečném počtu prvočísel:

Věta 1.4 (Druhá Euklidova věta) Prvočísel je více, než dané množství prvočísel.

Důkaz:

- Danými prvočísly buďtež $p_1, p_2, \dots, p_n$. Položme $d = p_1 p_2 \dots p_n$, $q = d + 1$. Je-li q prvočíslo, pak q je různé od každého z prvočísel $p_1, p_2, \dots, p_n$, neboť je větší, než kterékoli z nich.
- Nechť q není prvočíslo. Potom je $q = rp$, kde p je prvočíslo. Dokážeme, že p je různé od každého z prvočísel $p_1, p_2, \dots, p_n$. Nechť tomu tak není. Potom je $d = sp$, kde $s < r$;
$$1 = q - d = rp - sp = (r - s)p,$$
což je spor.

■

([4], s. 74)

1.2.1 Prvočíselná věta

S pomocí následující tabulky odvodíme vztah, kterým je možné určit přibližný počet prvočísel nepřevyšujících číslo n:

Tabulka 1

n	$\pi(n)$	$n/\pi(n)$	$\ln(n)$	chyba v %
1 000	168	5,9524	6,9077	16,0490
1 000 000	78 478	12,7592	13,8155	8,4487
1 000 000 000	50 847 534	19,6665	20,7232	5,3731
1 000 000 000 000	37 607 912 018	26,5901	27,6310	3,9146
1 000 000 000 000 000	29 844 570 422 669	33,6247	34,4465	2,7156

Druhý sloupec tabulky udává přesný počet prvočísel nepřevyšujících číslo n ze sloupce prvního. Stojí za povšimnutí, že čísla třetího sloupce, která jsou podílem čísel ze dvou prvních sloupců, vzrůstají pokaždé přibližně o číslo 7. Podobně se bude chovat i funkce přirozeného logaritmu $\ln(n)$ zapsána ve čtvrtém sloupci. Poslední sloupec uvádí procentuální rozdíl mezi sloupci tři a čtyři. S rostoucí přirozeným číslem n se tedy $ln(n)$ přibližuje hodnotě $n/\pi(n)$. Toho si jako první povšiml německý matematik Carl Friedrich Gauss (1777 – 1855) a vyslovil následující větu, která nám pomáhá určit přibližný počet prvočísel nepřevyšujících číslo n.

Věta 1.5 (Prvočíselná věta) Nechť funkce $\pi(n)$ označuje všechna prvočísla menší, než přirozené číslo n, pak platí následující vztah

$$\pi(n) \sim \frac{n}{\ln(n)}.$$

1.3 Hledání prvočísel

Nyní dokážeme rozlišit, zda dané číslo je či není prvočíslem. Vyvstává otázka: existuje nějaký algoritmus, pomocí kterého je možné prvočísla získat? Matematik Eratosthenes (276 – 194 př. n. l.), který mimo jiné ve své době s pozoruhodnou přesností (11,5%) dokázal spočítat obvod Země, poskytuje zajímavý algoritmus pro vyhledání prvočísel. Metoda se tak po něm jmenuje Eratosthenovo síto. Nejdříve vyslovíme větu, která použití Erastotenova síta velmi zjednoduší.

Věta 1.6 (Odmocninové kritérium) Každé složené číslo n má alespoň jednoho prvočíselného dělitele

$$p \leq \sqrt{n}.$$

Důkaz:

Je-li n číslo složené, pak $n = ab$, kde a, b jsou přirozená čísla, pro která platí $1 < a < n$, $1 < b < n$. Při vhodné volbě označení obou činitelů můžeme předpokládat $a \leq b$. Pak $n = ab \geq a^2$, a proto $a \leq \sqrt{n}$. Neboť číslo a má alespoň jednoho prvočíselného dělitele $p \leq a$ a tedy $p \leq \sqrt{n}$. Avšak číslo p jako dělitel čísla a, které je dělitelem čísla n, je dělitelem čísla n. Číslo n má tedy prvočíselného dělitele p, $p \leq \sqrt{n}$.

■

([15], s. 10)

Eratosthenovo síto:

- Budeme zjišťovat prvočísla menší než číslo a
- Vypíšeme všechna čísla od 1 do a
- Z posloupnosti budeme vyškrtávat všechna čísla, která nejsou prvočísly následujícím způsobem:
    - Nejprve škrtneme jedničku (nevyhovuje definici prvočísla).
    - Pro každé přirozené číslo $n > 1$ vyškrtneme všechna čísla větší než n, která jsou zároveň číslem n dělitelná.

Ilustrujme metodu na příkladu pro $a = 25$:

- 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25
- _, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14, 15, 16, 17, 18, 19, 20, 21, 22, 23, 24, 25
- _, **2**, 3, _, 5, _, 7, _, 9, _, 11, _, 13, _, 15, _, 17, _, 19, _, 21, _, 23, _, 25
- _, 2, **3**, _, 5, _, 7, _, _, _, 11, _, 13, _, _, _, 17, _, 19, _, _, _, 23, _, 25
- _, 2, 3, _, **5**, _, 7, _, _, _, 11, _, 13, _, _, _, 17, _, 19, _, _, _, 23, _, _
- Dál již nemusíme pokračovat, neboť $5 \geq \sqrt{25}$ a Věta 1.6 říká, že každé složené číslo b má alespoň jednoho prvočíselného dělitele menšího než $\sqrt{b}$. Z toho vyplývá, že složené číslo b již bylo vyškrtnuto jako násobek svého menšího dělitele.

Takový způsob hledání prvočísel je velmi jednoduchý a efektivní. Nedá se ovšem použít pokud je přirozené číslo a příliš velké. Například pro vypsání prvních 100 000 přirozených čísel je zapotřebí více než 150 normostran[2]. Hledání prvočísel v takovém množství by znamenalo dny možná i týdny monotónní mravenčí práce. Přesto se do takové práce pustil například profesor matematiky pražské univerzity Jakub Filip Kulik (1793 – 1863). Po dlouhém úsilí představil své dílo, které obsahuje tabulky prvočíselných dělitelů všech přirozených čísel do sta milionů, což je obdivuhodný výkon.

1.4 Rozložení prvočísel

Podívejme se na rozložení prvočísel mezi přirozenými čísly. Budou-li vyškrtnuta všechna čísla složená v množině přirozených čísel, vzniknou nám po nich různě dlouhé mezery ohraničené dvěma prvočísly. Pro ilustraci použijme řadu přirozených čísel od 1 do 200:

_, 2, 3, _, 5, _, 7, _, _, _, 11, _, 13, _, _, _, 17, _, 19, _, _, _, 23, _, _, _, _, _, 29, _, 31, _, _, _, _, _, 37, _, _, _, 41, _, 43, _, _, _, 47, _, _, _, _, _, 53, _, _, _, _, _, 59, _, 61, _, _, _, _, _, 67, _, _, _, 71, _, 73, _, _, _, _, _, 79, _, _, _, 83, _, _, _, _, _, 89, _, _, _, _, _, _, _, 97, _, _, _, 101, _, 103, _, _, _, 107, _, 109, _, _, _, 113, _, _, _, _, _, _, _, _, _, _, _, _, _, 127, _, _, _, 131, _, _, _, _, _, 137, _, 139, _, _, _, _, _, _, _, _, _, 149, _, 151, _, _, _, _, _, 157, _, _, _, _, _, 163, _, _, _, 167, _, _, _, _, _, 173, _, _, _, _, _, _, 179, _, 181, _, _, _, _, _, _, _, _, _, 191, _, 193, _, _, _, _, _, 199, _.

Vynechaná čísla jsou složená. Je tedy zřejmé, že výskyt prvočísel v uspořádané množině přirozených čísel je nepravidelný. Na druhou stranu je možné si povšimnout takových dvojic prvočísel $\langle p, q \rangle$, pro které platí, že $p < q$ a $q - p \leq 2$. Takové dvojice nazýváme prvočíselnými dvojčaty. Patří mezi ně například $\langle 2,3 \rangle$,

[2] Přibližně 3 650 znaků na stranu.

$\langle 3,5\rangle$, $\langle 5,7\rangle$, $\langle 11,13\rangle$, $\langle 191,193\rangle$, $\langle 10^9+7, 10^9+9\rangle$. Prvočíselná dvojčata se vyskytují velmi zřídka, avšak jestli úplně vymizí, zatím nevíme. Roku 1949 P. Clement dokázal následující větu o prvočíselných dvojčatech.

Věta 1.7 (Clementova) Číslo $p(p+2)$ dělí číslo $4\big((p-1)!+1\big)+p$ právě tehdy, když $\langle p, p+2\rangle$ jsou prvočíselná dvojčata.

S prvočíselnými dvojčaty úzce souvisí i další pojem, tj. prvočíselná čtyřčata. Čtveřici prvočísel $\langle p, q, r, s\rangle$ nazveme prvočíselná čtyřčata, jestliže $p < q < r < s$ a zároveň $s - p \leq 8$. Příkladem jsou $\langle 2, 3, 5, 7\rangle$, $\langle 11, 13, 17, 19\rangle$ nebo $\langle 10013951, 10013953, 10013957, 10013959\rangle$.

Vraťme se k rozložení prvočísel. Otázkou tedy je, jestli existuje jakkoli dlouhý úsek přirozených čísel, mezi nimiž není žádné prvočíslo. Odpověď dává důkaz následující věty:

Věta 1.8 V posloupnosti přirozených čísel existuje pro každé $k \in \mathbb{N}$ k členů této posloupnosti jdoucích za sebou, jež jsou všechna složená.

Důkaz:

Uvažujme přirozená čísla

$$(n+1)!+2, (n+1)!+3, \dots, (n+1)!+(k+1).$$

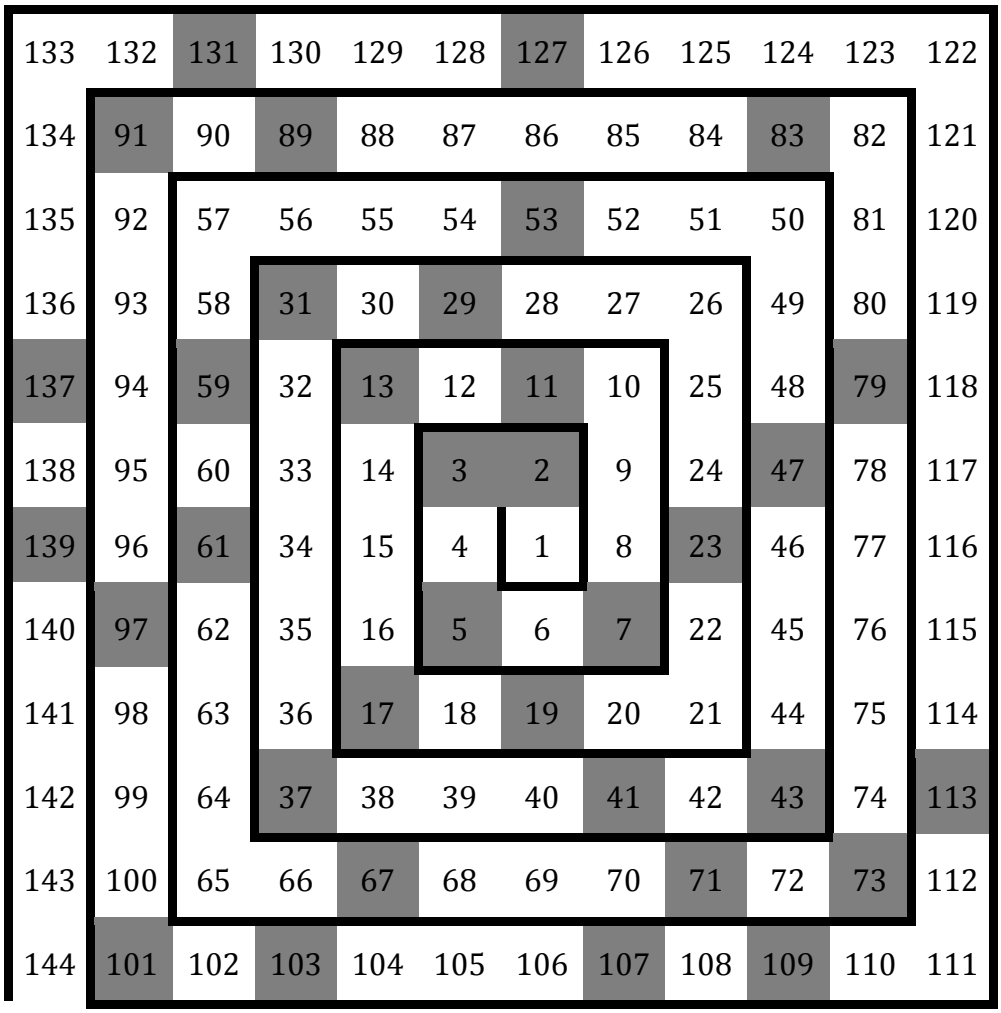
Pro $k < n$ je každé takové číslo složené, neboť

$$2|(n+1)!+2, 3|(n+1)!+3, \dots, (k+1)|(n+1)!+(k+1).$$

■

([6], s. 21, 22)

Vidíme tedy, že prvočísla jsou v posloupnosti přirozených čísel uspořádána nepravidelně. Nelze ovšem říci, že mezi prvočísly skutečně žádné uspořádání neexistuje. Věnujme pozornost následující spirále:



Obrázek 1 Ulmanova spirála

Roku 1965 tuto spirálu světu představuje polský matematik Stanislaw Marcin Ulman (1909 – 1984). Při řešení úloh na šachovnici zapisuje přirozená čísla od středu do spirály a zvýrazňuje mezi nimi prvočísla. Bude-li spirála pokračovat dále, začnou se v ní tvořit různě dlouhé úsečky se směrnicí ± 1. Takové úsečky odpovídají polynomům ve tvaru $u(x) = 4x^2 + bx + c$. Například pro $b = 10$ a $c = 4$ máme polynom

$$u(x) = 4x^2 + 10x + 5$$

a vidíme několik prvočísel ležící na úsečce o směrnici -1: $u(0) = 5,\ u(1) = 19,$ $u(2) = 41,\ u(3) = 71,\ u(4) = 109$ (viz obrázek Ulmanovy spirály).

1.5 Polynomy generující prvočísla

Podobné polynomy s celočíselnými argumenty x nabývající prvočíselných hodnot se matematici snažili najít již o mnoho let dříve.

Polynomy s celočíselnými argumenty x, které nabývají pro určitá x prvočíselných hodnot, se nazývají polynomy generující prvočísla.

Jmenujme například Leonharda Eulera (1707 – 1783), který se proslavil i mnoha dalšími významnými objevy v matematice. Euler se narodil ve Švýcarské Basileji do protestantské rodiny. Jeho rodiče měli o budoucnosti svého syna jasné představy. A tak mladý Leonhard ve svých šestnácti letech nastupuje ke studiím teologie na Basilejskou univerzitu, aby mohl jít ve stopách svého otce, který je pastorem reformované církve. Později se rozhodne studia teologie ukončit a věnovat se matematice. Pravděpodobně zásluhu na jeho rozhodnutí měla rodina Bernoulliů, která si byla s Eulerovými velmi blízká ještě před Leonhardovým narozením.

Není tedy divu, že právě J. Bernoullimu píše Euler roku 1772 o objevu kvadratického polynomu

$$p(x) = x^2 + x + 41,$$

který pro $x = 0, 1, \dots, 39$ dává tuto posloupnost prvočísel: 41, 43, 47, 53, 61, 71, 83, 97, 113, 131, 151, 173, 197, 223, 251, 281, 313, 347, 383, 421, 461, 503, 547, 593, 641, 691, 743, 797, 853, 911, 971, 1033, 1097, 1163, 1231, 1301, 1373, 1447, 1523, 1601. To je čtyřicet po sobě jdoucích argumentů x, pro která polynom $p(x)$ generuje prvočísla. Pokud přidáme i záporné argumenty, tak prvočísla dostaneme i pro $x = -40, -39, \dots, -1$. To znamená 80 po sobě jdoucích celočíselných argumentů x. Ještě zajímavější je, že pokud za x dosadíme čísla 0, 1, ..., 2377, polynom $p(x)$ bude nabývat prvočíselných hodnot v polovině případů. Dalšími zajímavými polynomy od Leonharda Eulera jsou $x^2 + x + 17$ pro $x = 1, \dots, 15$ a $x^2 + 79x + 1$ pro $x = 0, 1, \dots, 78$.

V matematické literatuře se objevují desítky dalších podobných polynomů od různých autorů. Uvedeme si některé z nich:

$$36x^2 - 810x + 2753$$

$$2x^2 + 29$$

$$103x^2 - 3945x + 34381$$

$$\begin{aligned}
&(k+2)\{1-[wz+h+j-q]^2-[(gk+2g+k+1)(h+j)+h-z]^2- \\
&-[16(k+1)^3(k+2)(n+1)^2+1-f^2]^2-[e^3(e+2)(a+1)^2+1-o^2]- \\
&-[2n+p+q+z-e]^2-[(a^2-1)y^2+1-x^2]^2-[16r^2y^4(a^2-1)+1-u^2]^2- \\
&-\left[\left(\left(a+u^2(u^2-a)\right)^2-1\right)(n+4dy^2)+1-(x+cu)^2\right]^2-[n+l+v-y]^2- \\
&-[(a^2-1)l^2+1-m^2]^2-[ai+k+1-l-i]^2- \\
&-[p+l(a-n-1)-b(2an+2a-n^2-2n-2)-m]^2- \\
&-[q+y(a-p-1)+s(2ap+2a-p^2-2p-2)-x]^2- \\
&-[z+pl(a-p)+t(2ap-p^2-1)-pm]^2\}
\end{aligned}$$

Poslední polynom publikovali roku 1976 společně čtyři matematici J. P. Jones, D. Sato, H. Wada a D. Wiens. Polynom je 25. stupně a má 26 různých argumentů $a, b, \dots, z$.

1.6 Malá Fermatova, Eulerova a Wilsonova věta

Na závěr kapitoly dokážeme tři důležité věty. První z nich zformuloval Francouz Pierre de Fermat v dopise svému příteli F. de Bessy roku 1640.

Pro důkaz Malé Fermatovy věty budeme potřebovat následující tvrzení, které vznikne přeformulováním Věty 1.1:

Je-li p prvočíslo a $ab \equiv 0\ (mod\ p)$, pak $a \equiv 0\ (mod\ p)$ nebo $b \equiv 0\ (mod\ p)$.

Věta 1.9 (Malá Fermatova věta) Jestliže $a \in \mathbb{N}$, a p je prvočíslo, pak $p|(a^p - a)$.

Důkaz:

- Případ pro $p = 2$ je zřejmý
- Nechť p je prvočíslo větší než 2.
    - Jestliže $p|a$, pak p také dělí číslo $a^p - a = a(a^{p-1} - 1)$.
    - Nechť čísla p a a jsou nesoudělná, tj. $(p, a) = 1$. Ukážeme, že $p|(a^{p-1} - 1)$:

      Uvažujme konečnou posloupnost

      $$a, 2a, 3a, \dots, (p-1)a.$$

      Vydělíme-li čísla ia a ja, $1 \leq j < i < p$, prvočíslem p, nemůžeme dostat stejný zbytek, protože pak by $p|(i-j)a$, což je podle výše zmíněné a přeformulované Věty 1.1 spor s tím, že $(a, p) = 1$. Posloupnost $a, 2a, 3a, \dots, (p-1)a$ proto dává $p-1$ různých nenulových zbytků při dělení prvočíslem p. Stejné zbytky (až na pořadí) dostaneme, když budeme dělit posloupnost $1, 2, 3, \dots, (p-1)$ prvočíslem p. Vynásobme mezi sebou tato čísla a pak také čísla v posloupnosti $a, 2a, 3a, \dots, (p-1)a$. Odtud pomocí vlastností kongruencí a následnou indukcí dospějeme ke kongruenci $(a^{p-1} - 1)(p-1)! \equiv 0\ (mod\ p)$.

      Tedy $(a^{p-1} - 1)(p-1)! \equiv 0\ (mod\ p)$ a první činitel na levé straně je dělitelný prvočíslem p podle výše odvozeného vztahu, jelikož platí $p \nmid (p-1)!$.

■

([9], s. 66, 67)

Zobecněním Malé Fermatovy věty je následující věta, kterou vyslovil asi o sto let později Leonhard Euler.

Definice 1.1 Funkce φ, definovaná na množině kladných čísel tak, že pro každé $n \in \mathbb{N}$ značí $\varphi(n)$ počet kladných celých čísel x takových, že $x \leq n$ a $(x, n) = 1$, se nazývá Eulerova funkce. Klademe $\varphi(1) = 1$.

Věta 1.10 (Eulerova) Jsou-li $a \in \mathbb{Z}, n \in \mathbb{N}, (a, n) = 1$, pak

$$a^{\varphi(n)} \equiv 1 (mod\ n)$$

Důkaz:

- Podmínka $(a, n) = 1$ znamená, že prvek $\bar{a}$ je nedělitel nuly v $\mathbb{Z}_n$.
- Nechť tedy $\bar{a}_1, \dots, \bar{a}_{\varphi(n)}$ jsou všichni nedělitelé nuly v $\mathbb{Z}_n$. Je tedy možné, že každý prvek $\bar{a} \cdot \bar{a}_i$ je také nedělitel nuly
- Pokud by platilo $\bar{a} \cdot \bar{a}_i = \bar{a} \cdot \bar{a}_j$ pro některé indexy i, j, bylo by také $\bar{a}_i = \bar{a}_j$. Z toho plyne, že $\bar{a} \cdot \bar{a}_i$ jsou všichni nedělitelé nuly v $\mathbb{Z}_n$.
- Poté platí
  $$\bar{a} \cdot \bar{a}_1 \cdots \bar{a} \cdot \bar{a}_{\varphi(n)} = \bar{a}_1 \cdots \bar{a}_{\varphi(n)},$$
  tj. $a^{\varphi(n)} \equiv 1 (mod\ n)$.

■

([6], s. 26)

Malá Fermatova a Eulerova věta jsou velmi užitečné například při hledání zbytku čísla a^k po dělení číslem m. Ukažme si obecně, jak algoritmus vypadá: Nalezněte zbytek po dělení čísla a^k číslem m.

- Pokud $(a, m) = 1$ a $k > \varphi(m)$, k můžeme zapsat jako
  $$k = \varphi(m)q + r,$$
  $0 \leq r < \varphi(m)$. Z tohoto zápisu vyplývá
  $$a^k = a^{\varphi(m)q+r} = a^{\varphi(m)q} a^r \equiv a^r (mod\ m).$$

Příklad: Nalezněte zbytek po dělení čísla 2^{52} číslem 45.

$\varphi(45) = (3^2 - 3)(5 - 1) = 24$ a $(2,45) = 1$ a $52 > 24$, jsou tedy splněny obě podmínky a můžeme psát $52 = 24 \cdot 2 + 4$, tedy

$$2^{52} = 2^{24 \cdot 2 + 4} = 2^{24 \cdot 2} \cdot 2^4 \equiv 2^4\ (mod\ 45).$$

Poznámka: Ve skutečnosti Euler svou větu zapsal bez použití kongruence. Zápis kongruence, tak jak je ve větě použit, zavedl až o několik let později německý matematik Carl Friedrich Gauss. Gaussova kongruence $a \equiv b (mod\ m)$ je ekvivalentní s výrazem $m|(b - a)$.

Poslední věta je pojmenována podle britského matematika Johna Wilsona (1741-1793). O její objev se ovšem zasloužil Edward Waring (1736 – 1798), který ji publikoval roku 1770 a Wilsonovi věnoval ve své knize.

Věta 1.11 (Wilsonova) Číslo $p > 1$ je prvočíslo právě tehdy, když

$$(p-1)! \equiv -1 \ (mod\ p)$$

Důkaz:

- Nejprve dokažme, že $\bar{a}^2 = \bar{1}$ v $\mathbb{Z}_p$ právě když $\bar{a} = \bar{1}$ nebo $\bar{a} = \overline{p-1}$
- Je-li $\bar{a}^2 = \bar{1}$, pak $(\bar{a} - \bar{1}) \cdot (\bar{a} + \bar{1}) = \bar{0}$
- $\mathbb{Z}_p$ je těleso, takže je buď $\bar{a} = \bar{1}$ nebo $\bar{a} = -1 = \overline{p-1}$
- To znamená, že pro $p > 2$ je každý z prvků $a \in \mathbb{Z}$, $2 \leq a \leq p-2$ různý od prvku k němu inverzního, tedy $\bar{2} \cdot \bar{3} \cdots \overline{p-2} = \bar{1}$
- Z předešlého vyplývá $\bar{1} \cdot \bar{2} \cdot \bar{3} \cdots \overline{p-2} \cdot \overline{p-1} = \overline{p-1} = -\bar{1}$,
$$(p-1)! \equiv -1 \ (mod\ p).$$

■

([6], s. 27)

Věta má praktický význam při testování prvočíselnosti. Z definice kongruence tedy vyplývá, že p je prvočíslo, právě když platí

$$p|(p-1)! + 1.$$

Ilustrujme si to na příkladu: číslo 7 je prvočíslo, protože

$$(7-1)! + 1 = 720 + 1 = 721$$

a platí že $7|721$.

2 Speciální typy prvočísel

Jak napovídá název kapitoly, budeme se zabývat speciálními typy prvočísel, což jsou prvočísla, která se získávají pomocí určitého vzorce. S něčím podobným jsme se již setkali v kapitole polynomy generující prvočísla. Díky tomu, že jsou prvočísla získávána ze vzorců, mají určité speciální vlastnosti a také mohou mít i další jedinečné využití. V této kapitole se tak představí tři nejznámější ze speciálních typů prvočísel – Mersennova, Fermatova a Eukleidova prvočísla.

2.1 Mersennova prvočísla

Právě jedny z takovýchto prvočísel, objevil nebo spíše blíže popsal[3] francouzský mnich Marin Mersenne. Možná je podivuhodné, že se o takový objev zasloužil právě mnich, ne však zcela neobvyklé.

Marin Mersenne se narodil 8. září 1588 v Bourg d´Oizé départementu Sarthe ve Francii. Ve svých šestnácti letech nastupuje ke studiím teologie na jezuitské koleji v nedalekém La Flèche (ačkoli zde zůstává několik let, do jezuitského řádu nikdy nevstoupí). A právě tady začíná jeho dlouholeté přátelství s René Descartem (1596 – 1650), který kolej také navštěvuje. Jejich přátelství pokračuje i dlouho po Mersennově odchodu. Po pěti letech u jezuitů se rozhodne ve svých studiích teologie pokračovat na pařížském Sorboně, kde zůstává až do roku 1611. Po ukončení studií vstupuje do řádu minimů, kde má možnost celých osm let vyučovat nejen filozofii, ale i matematiku v řádovém klášteře v Never. Nakonec se stěhuje i odtud. Jeho novým domovem je část Paříže poblíž Palace Royale, známého místa, kde se scházejí významní intelektuálové této doby. Setkání s nimi je však pro Mersenna zklamáním. Žádný z matematiků není ochoten se o své poznatky podělit s ostatními. Takovýto tajnůstkářský postoj se v Paříži objevil již o století dříve u takzvaných kosistů[4].

Je jasné, že takový nekolektivní způsob bádání rozvoji královny věd vůbec neprospívá. Je tedy načase podniknout radikální kroky. Mersenne se proto rozhodne u sebe doma pořádat pravidelná setkání nejen matematiků, ale i vědců ostatních oborů a společně diskutují o svých nápadech. Mezi nejznámější členy této komunity patří Blaise Pascal (matematik, fyzik, spisovatel a teolog; vytvořil první mechanický kalkulátor, podal základy teorie pravděpodobnosti), Pierre Gassendi (fyzik, astronom a profesor matematiky na Royal Colége), Gilles Personne de Roberval (filozof a matematik; zakladatel kinematické geometrie) a

[3] Dále v textu bude ukázáno, že o těchto číslech věděl již ve čtvrtém století př. n. l. Eukleides.

[4] Název povolání kosistů je odvozeno od italského cosa, neboli věc, což označovalo určitou neznámou ve výpočtu. Kosisté se nechali najímat tehdejšími obchodníky a podnikateli k různým druhům výpočtu. Znalost algoritmů výpočtů pro ně znamenala obživu, proto se snažili své poznatky všemožně před ostatními tajit.

Jean de Beaugrand. Je pravda, že ne všichni jsou příznivci těchto setkání a raději si své poznatky nechávají pro sebe nebo se o ně dělí pouze v soukromé korespondenci s některými ze svých přátel. Takto si i Mersenne dopisuje s více, než 78 významnými učenci své doby[5] Moc dobře tedy ví, jaké poklady pro další rozvoj nejen matematiky jejich autoři tají. Výzva je tedy jasná; kdo odmítne publikovat své práce, budou zveřejněny všechny jeho články i soukromé dopisy. Přestože veškeré Mersennovy úmysly jsou dobré (vzájemná spolupráce vědců znamená velké plus nejen pro matematiku, ale i pro lidstvo), není divu, že se Mersenne brzy setkává s velkým rozhořčením ze strany poškozených. Takovéto mnohdy nediskrétní jednání dokonce ukončuje i dlouholeté přátelství s Descartem. Poté, co se dozvídá, že Mersenne poskytl veřejnosti jeho filozofické spisy, s ním ukončuje veškerou komunikaci. Hromadné odtajňování korespondencí dalo vzniknout dokonce dobovému rčení, že informovat Mersenna o objevu znamená oznámit jej celé Evropě.

2.1.1 Hledání Mersennových prvočísel

Marin Mersenne se jako matematik ve svých objevech zdaleka nevyrovnal svým kolegům. I přesto jeden z jeho „objevů“ se stává neodmyslitelnou součástí teorie čísel. Jsou jím Mersennova prvočísla.

Mersenne se prvotně zabýval čísly, jejichž obecný předpis vypadá následovně;

$$k = 2^a - 1,$$

ne však pro každý exponent a vytvoří vzorec prvočíslo, podívejme se na následující větu.

Věta 2.1 Je-li $2^p - 1$ prvočíslo, pak p je také prvočíslo.

Důkaz: Tvrzení dokážeme sporem

Nechť $2^p - 1$ je prvočíslo a předpokládejme naopak, že p je číslo složené, tj. existují přirozená čísla i a j, pro která platí $p > i > 1$ a $p > j > 1$ tak, že $p = ij$. Pak oba činitelé na pravé straně rovnosti

$$2^{ij} - 1 = \left(2^i - 1\right)\left(2^{i(j-1)} + 2^{i(j-2)} + \cdots + 2^i + 1\right)$$

jsou větší než jedna, což znamená, že číslo $2^p - 1$ je složené, to je však spor s předpokladem.

■

([9], s. 111)

[5] Mersenne si vyměňoval korespondenci například s holandským fyzikem Christianem Huygensem, kterého přivedl na myšlenku využít kyvadla při přesnějším měření času, s významným italským fyzikem a matematikem Galileem Galileim, kterého se zastával při sporech s církví ohledně heliocentrismu. Mezi jeho dopisy najdeme i takové, jejichž autorem je český myslitel, spisovatel, filozof a hlavně učitel národů Jan Ámos Komenský.

Taková čísla budeme nazývat Mersennovými a značit $M_p = 2^p - 1$. Podmínka, že číslo M_p je prvočíslem pouze tehdy, je-li p prvočíslo je nutná, ne však postačující. Z toho plyne, že mezi Mersennovými čísly jsou jak prvočísla, tak čísla složená. Například pro $p = 11$ by bylo

$$M_{11} = 2^{11} - 1 = 2047 = 23 \cdot 89$$

číslo složené.

Mersenne ve své práci Cogitata Physica-Matematica určil prvních jedenáct prvočísel tvaru $2^n - 1$ pro $n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257$ a o ostatních číslech pro $n < 257$ tvrdil, že jsou složená. Dnes ovšem víme, že se v tomto tvrzení hned několikrát zmýlil. A do tohoto roku (2015) je známo již 48 Mersennových prvočísel, většina z nich hlavně díky moderní technice a projektu GIMPS[6] (Great Internet Mersenne Prime Search).

Abychom nepředbíhali, podívejme se na objevování Mersennových prvočísel postupně. Mersennovým výčtem všech možných prvočísel tvaru $2^p - 1$ ve skutečnosti nezačíná historie těchto speciálních typů prvočísel. Některá z nich jsou známá již dlouho před začátkem jeho života. Přesto jeho tvrzení ovlivňuje budoucí generace matematiků, protože se musí beze zbytku ověřit.

Je zřejmé, že prvních sedm Mersennových prvočísel[7] znali matematici ještě před Mersennem. Dokonce první čtyři z nich pro $p = 2, 3, 5, 7$ jsou známá již starověkým matematikům žijícím v období před naším letopočtem. Teprve roku 1536 Hudalricus Regius dokazuje, že číslo $2^p - 1$ pro $p = 11$ není prvočíslem ve svém díle Ultriusque Arithmetices. Zároveň v něm ukazuje, že M_{13} nemá žádné kromě triviálních dělitelů, tedy je skutečně v pořadí již pátým Mersennovým prvočíslem. V roce Mersennova narození (*1588) přichází na svět i další dvě Mersennova prvočísla. O jejich objevení se zasloužil profesor matematiky Pietro Cataldi, který sestavil tabulku prvočísel menších než číslo 750. Díky této tabulce a také se znalostí odmocninového kritéria dokazuje prvočíselnost M_{17} a M_{19}.

Po vyslovení Mersennovy domněnky roku 1644 o konečném počtu Mersennových prvočísel přebírá štafetu v dokazování Euler. S jasným výsledkem přichází roku 1750 a potvrzuje, že M_{31} je prvočíslo. S rostoucími exponenty roste i náročnost dokazování, a proto na potvrzení dalšího Mersennova prvočísla matematici čekají až do roku 1867. Édouard Lucas[8] potvrzuje prvočíselnost M_{127}. Se zajímavým tvrzením přichází v roce 1877 Ivan Mikheevich Pervushin. Mezi Mersennovými prvočísly nachází mezeru, kterou vyplňuje M_{61}. Netrvá dlouho a roku 1911 jsou objeveny další dvě mezery, které vyplňuje R. E. Powers

[6] Projekt stále probíhá na www.mersenne.org, tato stránka byla založena v lednu 1996 Georgem Woltmanem.

[7] Ačkoli pojmenování „Mersennova prvočísla“ pochází až ze 17. století, považuji za vhodné používat toto označení i v kontextu s dřívějším obdobím.

[8] Později ukážeme, že hlavně díky tomuto francouzskému matematikovi nabralo objevování dalších prvočísel nový rozměr, a to díky jeho zjednodušenému testu prvočíselnosti.

prvočísly M_{89} a M_{107}. Nejen, že v Mersennově výčtu některá prvočísla chybí, ale dokonce několik z nich i přebývá. Roku 1903 se daří americkému matematikovi Franku Nelsonu Colemu rozložit číslo M_{67} a tento výkon předvádí na půdě Americké matematické společnosti, jako svou přednášku. Ta je dodnes považována za legendární, neboť Cole při ní neřekl jediné slovo. Takto ji popsal jeden z účastníků Eric Temple Bell ([14], s. 18):

„Cole, beztak málomluvný člověk, přistoupil k tabuli, beze slov vzal křídu a spočítal 2^{67}*. Pak starostlivě odečetl 1 a jako výsledek získal číselné monstrum*

147 573 952 589 676 412 927

Poté pořád beze slov, vyhledal ještě volné místo na tabuli a ručně vynásobil krok za krokem

193 707 721 · 761 838 257 287

Když oba výsledky souhlasily, dostalo se mu bouřlivých ovací. Cole se vrátil na své místo, stále bez jediného slova. Mersennova domněnka tak zmizela ve hlubinách matematických hrdinných ság.“

Po Coleho úspěchu už zbývá objasnit poslední. Je číslo $2^p - 1$ pro $p = 257$ skutečně Mersennovým prvočíslem? Důkaz přichází roku 1922 z Belgie, kde matematik Maurice Kraitchika podává jednoznačný závěr: M_{257} je složené.

Věnujme chvíli pozornost porovnání Mersennových prvočísel, která sepsal Mersenne s těmi, ke kterým jsme nyní dospěli.

$$p = \mathbf{2}, \mathbf{3}, \mathbf{5}, \mathbf{7}, \mathbf{13}, \mathbf{17}, \mathbf{19}, \mathbf{31}, 67, \mathbf{127}, 257$$
$$p = 2, 3, 5, 7, 13, 17, 19, 31, \mathbf{61}, \mathbf{89}, \mathbf{107}, 127$$

V prvním řádku jsou tučně zvýrazněna čísla p, pro která jsou M_p skutečně prvočísla. Druhý řádek prozrazuje, na která Mersenne při svém pátrání zapomněl. Před nástupem moderní techniky, tedy do roku 1952, bylo známo pouhých 12 prvních Mersennových prvočísel (viz druhý řádek). Přesto je tento výkon pozoruhodný, neboť M_{127} má právě 39 cifer[9].

S příchodem moderní techniky se i hledání dalších prvočísel mnohem zjednodušuje, jejich počet tedy rychle stoupá. Již v roce 1952 představuje světu Raphael Robinson hned pět dalších prvočísel M_{521}, M_{607}, $M_{1\,279}$, $M_{2\,203}$, $M_{2\,281}$. V jeho stopách pokračují i další: Hans Riesel nalézá $M_{3\,217}$, Alexander Hurwitz $M_{4\,253}$ a $M_{4\,423}$. Donald Gallies[10] doplňuje řadu hned o tři další prvočísla $M_{9\,689}$, $M_{9\,941}$ a $M_{11\,213}$ a Bryant Tuckerman o $M_{319\,937}$. Společné úsilí při hledání vynakládají Landon Curt Noll spolu s Laurou Nickel a objevují $M_{21\,701}$, nakonec o pár měsíců

[9] V další podkapitole si ukážeme, co tento počet cifer znamená.

[10] Spierpiński (1966, s. 85) uvádí v poznámce pod čarou, že Gallies pracoval s počítačem Illiac II a potřebné časy k ověření prvočíselnosti byly po řadě 1h 23min, 1h 30min a 2h 15min.

později Noll, tentokrát sám, nachází ještě $M_{23\,209}$. Dalším matematikem, který si připisuje zásluhu na objevu hned několika prvočísel je David Slowinski, ten Mersennova prvočísla rozšiřuje hned o dalších sedm členů: $M_{44\,497}$, $M_{86\,243}$, $M_{132\,049}$, $M_{216\,091}$, $M_{756\,839}$, $M_{859\,443}$ *a* $M_{1\,257\,787}$. Nesmíme ovšem zapomenout, že při ověřování těchto čísel mu v mnoha případech pomáhají dva z jeho přátel; Harry Nelson a Paul Gage. Mezi Slowinskiho posloupností však chybí ještě jedno prvočíslo a to $M_{110\,503}$, jehož objeviteli jsou Watt Colquitt a Luke Welsh.

Posledním Slowinskiho objevem končí éra individuálního hledání Mersennových prvočísel. V lednu roku 1996 úsilí matematiků spojuje Georg Woltman založením celosvětového projektu GIMPS, do kterého se zapojují matematikové i laikové se zájmem o prvočísla z celého světa a poskytují své osobní počítače k hledání dalších Mersennových prvočísel. První ovoce projekt přináší již v listopadu téhož roku, kdy počítač Joela Armangauda zapojený do GIMPS hlásí nalezení již třicátého pátého prvočísla $M_{1\,398\,269}$. Jen do roku 2000 jsou objevena další tři prvočísla $M_{2\,976\,221}$, $M_{3\,021\,377}$, $M_{6\,972\,593}$. Poslední z nich je první známé prvočíslo, jehož počet cifer přesáhl milionovou hranici, konkrétně $M_{6\,772\,593}$ má 2 098 960 cifer. Samozřejmě i po začátku dalšího tisíciletí hledání Mersennových prvočísel nekončí a počítače z různých koutů světa hlásí objevení prvočísel $M_{13\,466\,919}$, $M_{20\,996\,011}$, $M_{24\,036\,583}$, $M_{25\,964\,951}$, $M_{30\,402\,457}$ a $M_{32\,582\,657}$. V září roku 2006 je známo, díky tomuto společnému úsilí, již 44 Mersennových prvočísel.

Netrvalo dlouho a přichází zprávy o nalezení dalších Mersennových prvočísel, u nich však nikdo s určitostí nedokáže říci, jestli je jejich pořadí správné, jinými slovy, zda se mezi nimi nevyskytují další ještě neobjevená Mersennova prvočísla. Patří k nim $M_{37\,156\,667}$, $M_{42\,643\,801}$, $M_{43\,112\,609}$ a $M_{57\,885\,161}$. Objev posledního Mersennova prvočísla přinesl počítač Curitse Coopera 25. ledna 2013 a chlubí se úctyhodnými 17 425 170 ciframi. Pro představu, zápis čísla by potřeboval více než 4 780 normostran. Nevíme sice, kolikátým Mersennovým prvočíslem ve skutečnosti je, co však víme bezpečně, že je to největší prvočíslo, které v současnosti známe.

2.1.2 Testování Mersennových prvočísel

To, že největší známé prvočíslo je právě jedno z Mersennových prvočísel není náhodné. Jak bylo poznamenáno výše, poslední ověřené prvočíslo bez použití moderní techniky, tj. M_{127} má 39 cifer. Co se ovšem pod touto informací skutečně skrývá? Znamená to, že kdybychom se rozhodli vyzkoušet dělitelnost tohoto čísla všemi menšími prvočísly než $\sqrt{M_{127}}$, kterých je podle prvočíselné věty přibližně $25 \cdot 10^{15}$, trvalo by to, při jedné operaci dělení za sekundu a

bez přestávek, zhruba 80 miliónů let[11]. Je zřejmé, že ověřovat takovým způsobem prvočísla je pro člověka s omezenou délkou života nemyslitelné. Mersennova prvočísla si pro svůj speciální zápis $2^p - 1$ zaslouží také speciální způsob ověřování. A právě ten zformuloval francouzský matematik Édouard Lucas. Nalezl kritérium, které velmi zjednodušilo zjišťování prvočíselnosti Mersennových prvočísel. Jeho ne moc jasnou formulaci upravil a zjednodušil Derrick H. Lehmer.

Věta 2.2 (Lucasova-Lehmerova): Číslo M_p, kde p je liché prvočíslo, je prvočíslem tehdy a jen tehdy, když číslo M_p je dělitelem $(p-1)$-ního členu posloupnosti $\{u_n\}$ definované podmínkami $u_1 = 4$, $u_{n+1} = u_n^2 - 2$ pro $n = 1, 2, 3, \ldots$, posloupnosti, jejímiž počátečními členy jsou čísla 4, 14, 194, 37 634.

Ukažme si, jak tento test bude fungovat v praxi a to pro M_7:

- Nechť $M_7 = 127$ a

$$u_{7-1} = (((((4^2 - 2)^2 - 2)^2 - 2)^2 - 2)^2 - 2) = 2\,005\,956\,546\,822\,746\,114$$

- $M_7 \mid u_6$ tedy číslo 127 musí beze zbytku dělit 2 005 956 546 822 746 114
- $2\,005\,956\,546\,822\,746\,114 : 127 = 15\,794\,933\,439\,549\,182$
- Výsledek nám vyšel beze zbytku, tedy podle Lucasova-Lehmerova kritéria se jedná o jedno z Mersennových prvočísel.

2.1.3 Dokonalá čísla

Mersennova prvočísla velmi úzce souvisí s dalším pojmem v teorii čísel. Mějme číslo n, jehož všechny dělitele (včetně triviálních) sečteme a vyjde číslo dvojnásobně velké než původní n.[12] Nejjednodušším příkladem je číslo 6, jeho dělitelé jsou 1, 2, 3 a 6 a jejich součet $1 + 2 + 3 + 6$ dává 12, tj. dvojnásobek šesti.

Taková vlastnost musela fascinovat hlavně Pythagorejce, kteří se především zabývali různými vztahy mezi čísly. Víme, že několik dokonalých čísel bylo známo dlouho před naším letopočtem a je pravděpodobné, že i velmi brzy se začala spojovat s prvočísly tvaru $2^p - 1$. Důkazem je následující věta ze třetího století před naším letopočtem. Začneme definicí funkce σ.

[11] Pro porovnání stáří vesmíru se odhaduje na 15 miliard let.
[12] Ve většině publikací, které mluví o dokonalých číslech, jsou nadefinována jako čísla, která po součtu svých dělitelů (kromě sebe samého) dávají původní číslo.

Definice 2.1 Nechť n je libovolné přirozené číslo. Označme $\sigma(n)$ součet všech jeho kladných dělitelů, tj.

$$\sigma(n) = \sum_{d|n} d.$$

Poznámka:

1) Pokud $n = p_1^{\alpha_1} \cdots p_k^{\alpha_k}$ tak funkce $\sigma(n) = \frac{p_1^{\alpha_1}-1}{p_1-1} \cdot \frac{p_1^{\alpha_2}-1}{p_2-1} \cdots \frac{p_k^{\alpha_k}-1}{p_k-1}$
2) Pomocí funkce σ můžeme vyslovit ekvivalentní definici: n je číslo dokonalé, právě když
$$\sigma(n) = 2n$$
3) Funkce σ je multiplikativní, tj. platí: jestliže $(m, n) = 1$ pak
$$\sigma(mn) = \sigma(m)\sigma(n),$$
jsou-li m a n nesoudělná přirozená čísla.

Věta 2.3.1 (Eukleidova) Když jest dáno po řadě od jednotky několik čísel v poměru jedné ke dvěma, až součet všech stane se číslem kmenným, a když se ten součet znásobí číslem posledním a vznikne jiné, vzniklé bude číslo dokonalé.

Takto větu publikoval Euklides ve svých Základech ([4], s. 182). Formulace přesně navádí k vytvoření dokonalého čísla, ale souvislost s Mersennovými prvočísly může na první pohled unikat. Přepišme tedy větu tak, jak jí prezentuje většina dnešních publikací:

Věta 2.3.2 Je-li $2^p - 1$ prvočíslo, pak je číslo $n = 2^{p-1}(2^p - 1)$ dokonalé.

Důkaz:

- Protože čísla 2^{p-1} a $2^p - 1$ jsou nesoudělná, platí
$$\sigma(n) = \sigma(2^{p-1})\sigma(2^p - 1) = \frac{2^p - 1}{2 - 1}(1 + 2^p - 1) = (2^p - 1)2^p = 2n,$$
a tedy n je dokonalé.

■

([9], s. 116)

Další zajímavý důkaz je uveden např. u Eukleida ([4], s. 182, 183).

Na příkladu ukažme, jak vzorec $n = 2^{p-1}(2^p - 1)$ funguje v praxi. Aplikujme jej pro p=5:

- $(2^5 - 1) = 31$ a číslo 31 je prvočíslo.
- Proto tedy $2^{5-1}(2^5 - 1) = 496$ by mělo být číslo dokonalé.
- Opravdu:
$$\sigma(496) = \sigma(2^4 \cdot 31) = \sigma(2^4) \cdot \sigma(31) = \frac{2^5 - 1}{2 - 1} \cdot 32 = 992 = 2 \cdot 496$$

Z příkladu vidíme, jak je Euklidova poučka v praxi jednoduchá, ke každému z Mersennových prvočísel můžeme vytvořit číslo dokonalé. Určitě tedy známe čtyřicet osm dokonalých čísel stejně jako Mersennových prvočísel. Otázka je, zda platí i obrácená implikace. Má každé dokonalé číslo své Mersennovo prvočíslo? Takové tvrzení dokázal v 18. stol. Leonhard Euler.

Věta 2.4 (Eulerova) Všechna sudá dokonalá čísla, mají tvar

$$n = 2^{p-1}(2^p - 1),$$

kde $p > 1$ a $2^p - 1$ je prvočíslo.

Důkaz:

- Jestliže n je sudé, můžeme psát $n = 2^{p-1}u$, kde $p > 1$ a u je liché. Protože 2^{p-1} a u jsou nesoudělná, součet dělitelů čísla n se rovná
$$\sigma(n) = \sigma(2^{p-1})\sigma(u) = (2^p - 1)\sigma(u).$$
- Je-li n dokonalé, máme
$$\sigma(n) = 2n = 2^p u,$$
a tedy
$$(2^p - 1)\sigma(u) = 2^p u.$$
- Jelikož $2^p - 1$ a 2^p jsou nesoudělná, vidíme, že
$$\sigma(u) = 2^p t \text{ a } u = (2^p - 1)t,$$
kde t je přirozené číslo. Protože však u má alespoň tyto dělitele: 1, t, $2^p - 1$ a $t(2^p - 1)$ pro $t > 1$, součet dělitelů u splňuje nerovnost
$$\sigma(u) \geq 1 + t + 2^p - 1 + t(2^p - 1) = 2^p(1 + t),$$
která odporuje rovnosti $\sigma(u) = 2^p t$. Tudíž $t = 1$. Pak ale
$$\sigma(u) \geq 1 + 2^p - 1 = 2^p$$
a požadovaná rovnost $n = 2^{p-1}(2^p - 1)$ platí jen, když $u = 2^p - 1$ je prvočíslo.

■

([9], 116)

Na další sudé dokonalé číslo tak musíme počkat, než společné úsilí členů projektu GIMPS přinese svůj další výsledek.

Dosud se všechny naše úvahy týkaly pouze sudých dokonalých čísel. Jak je to ale s těmi lichými. Existuje nějaké liché dokonalé číslo? Žádné takové neznáme, přesto matematici určili některé vlastnosti, které by muselo splňovat:

- Pokud by liché dokonalé číslo existovalo, mělo by více než 300 cifer.
- Bude mít nejméně 8 prvočíselných dělitelů, a pokud není dělitelné třemi, tak alespoň 11 prvočíselných dělitelů[13].
- Musela by mít strukturu; mocnina prvočísla krát druhá mocnina.

[13] Oproti tomu sudá dokonalá čísla mají pouze dva prvočíselné dělitele: 2 a sebe samo.

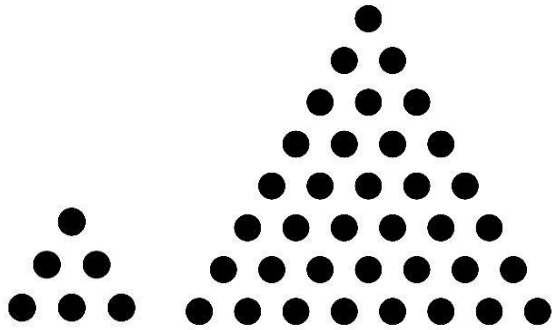
Jak dodává Ziegler [20], s. 104: *„O čísle, které nikdy nikdo neviděl a které možná (pravděpodobně?) neexistuje, toho tedy víme poměrně dost.“*

Z Věty 2.3.2 a Věty 2.4 vyplývá zajímavý vztah mezi dokonalými čísly a Mersennovými prvočísly:

$$n = 2^{p-1}(2^p - 1) = \frac{2^p}{2}(2^p - 1) = 1 + 2 + \cdots + (2^p - 1) = \sum_{i=1}^{M_p} i$$

Je zřejmé, že každé dokonalé číslo je rovno součtu M_p-členné aritmetické posloupnosti, jejíž první člen je jedna a diference také jedna. Součet právě takovéto posloupnosti tvoří trojúhelníková čísla. Pokud je číslo trojúhelníkové jeho velikost určuje počet puntíků, které tvoří pravidelný rovnostranný trojúhelník. Platí tedy následující věta:

Věta 2.5 Všechna sudá dokonalá čísla jsou trojúhelníková.



Obrázek 2 Gragické zobrazení trojúhelníkových čísel

Právě s faktem, že dokonalá čísla jsou zároveň trojúhelníková, úzce souvisí následující tvrzení, které vyslovil roku 1899 český matematik František Josef Studnička.

Věta 2.6 Pokud n je sudé dokonalé číslo ve tvaru $n = 2^{p-1}(2^p - 1)$, pak n lze binárně zapsat takto: 111 … 1000 … 0, kde je p jedniček a $p - 1$ nul.

Binární zápis několika prvních dokonalých čísel, by vypadal následovně:

Tabulka 2

n – dekadická soustava	n – binární soustava
6	110
28	11100
48**6**	111110000
8 1**28**	1111111000000
33 550 33**6**	1111111111111000000000000
8 589 869 05**6**	11111111111111111000000000000000000
137 438 691 3**28**	111 … 1000 … 0
2 305 843 008 139 952 1**28**	111 … 1000 … 0

Je možné ověřit, že i ostatní čísla, jiná než dokonalá, s binárním zápisem tvaru 111 … 1000 … 0, kde je p jedniček a $p-1$ nul jsou trojúhelníkovými čísly.

Ve třetím století našeho letopočtu řecký matematik Iamblichos z Chalkidy (asi 270 – 330) zkoumá zápis dokonalých čísel. Například si povšiml, že se poslední cifry u dokonalých čísel opakují. Tvrdí tedy, že končí buďto cifrou 6, nebo číslem 28 (v tabulce jsou konce zápisu zvýrazněny tučně). To, že je domněnka správná, přispělo k formulaci následující věty.

Věta 2.7 Přirozené číslo n takové, že $n = 2^{p-1}(2^p - 1)$ končí buď cifrou 6, nebo cifrou 8. Pokud navíc končí číslem 8, musí končit dvojčíslím 28.

Když Iamblichos domněnku vyslovil, měl k dispozici pouze první čtyři dokonalá čísla, takže také usoudil, že konce 6 a 28 se postupně střídají. Podle výše uvedené tabulky je zřejmé, že se mýlil. A mýlil se i v posledním ze svých závěrů. V něm předpokládal, že ke každému přirozenému číslu n existuje právě jedno dokonalé číslo o n cifrách[14].

2.1.4 Využití Mersennových prvočísel v kryptografii

Nakonec si řekněme několik slov o využití Mersennových prvočísel v kryptografii, neboť jsou s tímto oborem často spojovány[15]. Obecně mají prvočísla velké využití při bezpečnosti, v dnešní době hlavně při ochraně

[14] Takový předpoklad by upřednostňoval dekadický zápis čísel. Z matematického hlediska ovšem není žádný důvod, proč tento zápis vyvyšovat nad ostatními.

[15] Příklad dvou veřejností uznávaných webových stránek, které se o této problematice okrajově zmiňují: http://news.bbc.co.uk/2/hi/science/nature/1693364.stm, https://www.sciencenews.org/article/largest-known-prime-number-found

elektronických dat. Nejrozšířenějším šifrovacím systémem využívajícím velkých prvočísel (s více než stovkou cifer) je šifra RSA[16]. Systém funguje na jednoduchém asymetrickém[17] principu. Klíč potřebný k zašifrování je veřejně známý, je jím složené číslo n vzniklé vynásobením dvou velkých prvočísel, tj. $n = pq$. K rozšifrování zprávy je ovšem zapotřebí znát právě tato dvě prvočísla. Soukromý klíč, tedy prvočísla p, q, zná pouze příjemce zprávy[18]. Bezpečnost šifry je tak založena na nemožnosti rozložení (faktorizace) čísla n v reálném čase.

Použití Mersennových prvočísel by se pro takové šifry mohlo na první pohled zdát ideální, vždyť právě ta jsou jedna z největších známých. Ve skutečnosti pro jejich nízký počet, by bylo jednoduché zjistit, která dvě tvoří číslo složené. Vzhledem ke skutečnosti, jak často jsou s kryptografií Mersennova prvočísla spojována je závěr překvapivý: dodnes nenašla v tomto oboru praktické využití.

2.2 Fermatova prvočísla

Stejně jako předešlá kapitola i v této se budeme zabývat dalším typem speciálních prvočísel. Tentokrát se o jejich objevení zasloužil ctihodný soudní rada, pan Pierre de Fermat.

Ve zkratce se podíváme na Fermatův pozoruhodný život. Jeho příběh začíná 20. srpna 1601 ve městě Beaumont-de-Lomagne v jihozápadní Francii narozením do rodiny zámožného obchodníka s kůžemi. Díky finančnímu zaopatření své rodiny se mu dostává velmi dobrého vzdělání na půdě františkánského kláštera v Grandselve a poté i na univerzitě v Toulouse. Po studiích se ve svých třiceti letech stává toulouským parlamentním radou. Tento svůj úřad zastává s velkou pečlivostí a úměrným citem. Brzy je tak jeho práce náležitě oceněna, stává se příslušníkem honorace a tehdy je jeho jméno doplněno o slovíčko *de*. Tento výborný úředník má ještě svojí druhou tvář, kterou drží v skrytu i před mnoha ze svých blízkých přátel. Ale ti, kteří o ní vědí velmi dobře, jsou francouzští matematici. Mezi nimi si Fermate vysluhuje hned několik přezdívek, jako třeba „kníže amatérů“ od E. T. Bella. Ty méně uznalé jsou například „chvastoun“ od Reného Descarta, nebo „zpropadený Francouz“, jak jej nazval John Wallis.

Fermatovým předním koníčkem je matematika, které věnuje veškerý svůj volný čas. Se zálibou vyslovuje domněnky z různých matematických odvětví, které

[16] Název je odvozen od začátečních písmen jmen jeho autorů – Rivest, Shamin, Adleman.
[17] Jednosměrné šifrování s padacími vrátky. Funkce, kterou je informace zašifrována lze invertovat pouze na základě tajné informace.
[18] To, že zpráva před zašifrováním veřejným klíčem bude odpovídat odšifrované zprávě pomocí klíče soukromého, nám zajistí malá Fermatova a Eulerova věta – tj. Věta 1.9 a Věta 1.10.

formuluje do vět a posílá je jiným matematikům, ty zároveň nabádá k nalezení důkazu. Takové chování se žádnému z adresátů nelíbí a obratem vybízí Fermata k předložení jeho důkazu. Fermat si však důkazy a řešení svých vyřčených problémů nechává pro sebe, dokonce i po dlouhodobém naléhání jeho nejbližšího přítele Mersenna. Nejspíše se tak chce vyvarovat zdlouhavým procesům, které nastávají po zveřejnění důkazů – obhajoba metod, úprava nejasných částí i zdlouhavé diskuze s každým, kdo dané problematice jen trochu rozumí.

Spíše než nějaká sláva z objevů je pro Fermanta důležitý požitek z matematiky jako takové, radost z právě objeveného a možná i škodolibost, že dokáže objevit více než jeho kolegové. Rozhodně netouží po vyvyšování své práce. To dokazují jeho slova, které napsal Pascalovi ([17], s. 36): *„I kdyby cokoli z mé práce bylo hodno publikování, nechci, aby se v souvislosti s tím objevilo moje jméno.“* Naštěstí se jeho přání nevyplnilo a matematika je plná termínů, jako jsou: Malá Fermatova věta, Fermatova metoda rozkladu, Fermatova spirála, Fermatova funkce, Fermatovy koeficienty, Fermatova transformace, Fermatův bod, Fermatova čísla a další. Kromě toho společně s Pascalem představuje světu základy teorie pravděpodobnosti.

2.2.1 Hledání Fermatových prvočísel

Stejně jako Mersenne se i Fermatova pozornost zaměřuje na prvočísla. Hledá vzorec, který by vygeneroval pro každé přirozené číslo n prvočíslo. Podívejme se na vzorce, které každý z nich vytvořil:

- Mersennova prvočísla $2^n - 1$
- Fermatova prvočísla $2^n + 1$

Na první pohled si jsou vzorce velmi podobné a liší se pouze ve znaménku. To by znamenalo, že společně budou generovat prvočísla, která by zároveň byla prvočíselnými dvojčaty. Ve skutečnosti to tak není. Neboť Mersenne uvedl podmínku, že n mohou být pouze prvočísla. Naproti tomu, Fermate požaduje, aby číslo n bylo složené – konkrétně mocnina dvou. Vyslovme tedy následující větu.

Věta 2.8 Nechť n je přirozené číslo. Je-li $2^n + 1$ prvočíslo, pak $n = 2^m$ pro nějaké $m \in \{0, 1, 2, \dots\}$.

Důkaz:

- Jestliže k je přirozené číslo a $l \geq 3$ liché, pak
$$2^{kl} + 1 = (2^k + 1)\left(2^{k(l-1)} - 2^{k(l-2)} + \cdots - 2^k + 1\right).$$

Odtud plyne, že číslo $2^n + 1$ je složené, je-li exponent n dělitelný lichým přirozeným číslem $l \geq 3$. To, ale v posloupnosti $F_m = 2^{2^m} + 1$ pro $m = 0, 1, 2, \ldots$ nenastává. Proto n musí být mocninou čísla 2.

■

([9], s. 120)

Fermat vypočítal sedm prvních členů této posloupnosti, se kterými dále pracuje:

$$F_0 = 3$$
$$F_1 = 5$$
$$F_2 = 17$$
$$F_3 = 257$$
$$F_4 = 65\,537$$
$$F_5 = 4\,294\,967\,297$$
$$F_6 = 18\,446\,744\,073\,709\,551\,617$$

S domněnkou, že se jedná pouze o prvočísla, posílá Fermat tuto posloupnost v dopise svému příteli Bernardu Freniclovi de Bessymu a žádá ho, aby vše znovu prověřil. Ten dává Fermatovi v jeho tvrzení za pravdu. Je až zarážející, že ani jeden z nich nedokázal odhalit, že hned šesté číslo je složené. Přestože Frenicle je výborný počtář a Fermat, jak píše ve svých dopisech, věnuje zkoumání svých čísel velkou pozornost. Fermat navíc určuje metodu, která má pomoci odhalit potencionální dělitele jeho čísel.

Věta 2.9 Pokud je číslo $2^{2^m} + 1$ složené, jeho dělitel je tvaru $64n + 1$ pro nějaké přirozené číslo n.

A právě šesté Fermatovo číslo má dělitele 641. Je tedy pravděpodobné, že Fermat ve výpočtech udělal chybu a výsledek už nikdy nepřekontroloval. Do konce svého života (†1665) tak věří, že každé z jeho čísel je prvočíslo pro každé přirozené číslo m.

Postupem času Fermatovy závěry upadají v zapomnění. Změna přichází teprve roku 1732, kdy Leonhard Euler odhaluje číslo 641 jako dělitele šestého Fermatova čísla, tedy

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \cdot 6\,700\,417.$$

Od teď je jasné, že se Fermat ve svém tvrzení mýlil, ovšem jak velký jeho omyl ve skutečnosti byl, se ukazuje až o 120 let později. Dne 1. ledna 1855 píše německý astronom Thomas Clausen svému příteli Carlu Fridrichu Gaussovi, že nachází prvočíselný rozklad sedmého Fermatova čísla[19]

$$F_6 = 2^{64} + 1 = 274\,177 \cdot 67\,280\,421\,310\,721.$$

[19] V literatuře se často uvádí, že jako první rozložil číslo F. Landy ve svých 82 letech. Pravdou ale je, že Landy skutečně číslo rozložil a to nezávisle na Clausenovy, ovšem až o 25 let později.

2.2.2 Testování Fermatových prvočísel

Počet cifer dalších Fermatových čísel rychle narůstá a je čím dál obtížnější určit prvočíselnost hledáním dělitelů. Proto stejně jako pánové Lucas a Lehmer vymysleli způsob ověření prvočíselnosti Mersennových prvočísel, tak i J. F. Pépin nachází roku 1877 test prvočíselnosti pro Fermatova prvočísla.

Nejprve si dokážeme následující pomocnou větu k důkazu Pépinova testu.

Lemma 2.10 Je-li k celé nezáporné číslo a číslo $p = 2k + 5$, prvočíslo, pak číslo $3^{6k+2} + 1$ je dělitelné prvočíslem p.

Důkaz:

- Lemma je zřejmě pravdivé pro $k = 0$
- Dále tedy předpokládejme, že k je číslo přirozené
    - Nechť $p = 2k + 5$ a utvořme součin prvních $6k + 2$ přirozených čísel dělitelných třemi a rozdělme činitele do tří skupin – první skupina bude mít $2k$ členů, druhá a třetí pak $2k + 1$ členů
        - První skupina: $3 \cdot 6 \cdot 9 \cdots 6k$
        - Druhá skupina:
          $$(6k + 3)(6k + 6) \cdots (12k - 3) \cdot 12k \cdot (12k + 3),$$
          Protože je násobení komutativní, přepišme součin takto:
          $$(12k + 3) \cdot 12k \cdot (12k - 3) \ldots (6k + 6)(6k + 3).$$
          Protože $p = 2k + 5$ můžeme psát
          $$(p - 2)(p - 5)(p - 8) \cdots [p - (6k + 2)],$$
          Počet činitelů součinu je lichý (je jich $2k + 1$), kdy dostaneme po vynásobení a po sloučení sčítanců, které jsou násobky čísla p, číslo
          $$pu - 2 \cdot 5 \cdot 8 \cdot \ldots (6k + 2),$$
          kde u je jisté celé číslo
        - Třetí skupina: při vyjadřování součinu postupujeme analogicky jako u druhé skupiny:
          $$(12k + 6)(12k + 9)(12k + 12) \ldots (18k + 6) =$$
          $$= (p + 1)(p + 4)(p + 7) \ldots (p + 6k + 1) =$$
          $$= pv + 1 \cdot 4 \cdot 7 \cdot \ldots (6k + 1)$$
          kde v je přirozené číslo.
    - Sloučením těchto tří skupin dostáváme
      $$3 \cdot 6 \cdot 9 \cdots (18k + 6) =$$
      $$= [3 \cdot 6 \cdot 9 \cdots 6k] \cdot [pu - 2 \cdot 5 \cdot 8 \cdots (6k + 2)] \cdot$$
      $$\cdot [pv + 1 \cdot 4 \cdot 7 \cdots (6k + 1)] =$$
      $$= pw - 1 \cdot 2 \cdot 3 \cdot 4 \cdot 5 \cdot 6 \cdots (6k + 1)(6k + 2) =$$
      $$= pw - (6k + 2)!,$$
      kde w je číslo celé.
    - Zároveň platí rovnost

$$3 \cdot 6 \cdot 9 \cdots (18k+6) = (6k+2)!\, 3^{6k+2}.$$

- Oba výsledky porovnejme
$$pw - (6k+2)! = (6k+2)!\, 3^{6k+2}.$$
Z rovnice vyjádříme člen pw
$$pw = (6k+2)(3^{6k+2}+1).$$
- Z výše uvedené rovnosti plyne $p|(6k+2)(3^{6k+2}+1)$ poněvadž
$$6k+2 < 12k+5 = p,$$
nemůže být p dělitelem čísla $(6k+2)!$, a proto platí
$$p|(3^{6k+2}+1).$$

■

([15], s. 75,76)

Pro složitost důkazu Pépinova testu dokážeme pouze jednu z implikací:

Věta 2.11 Je-li F_n prvočíslo, pak číslo $3^{2^{2^n-1}}+1$ je dělitelné číslem F_n.

Důkaz:

- Nechť n je dané přirozené číslo. Platí tedy $2^n = 2m$, číslo m je přirozené. Můžeme psát
$$F_n - 1 = 2^{2m} = 4^m,$$
z toho plyne, že výraz $F_n - 5$ je dělitelné číslem 4. Zároveň platí
$$F_n - 1 = 4^m = (3+1)^m = 3t+1,$$
kde t je číslo přirozené. Odtud vypočteme
$$F_n - 5 = 3(t-1),$$
z toho vyplývá, že číslo $F_n - 5$ je dělitelné 3, a protože je zároveň dělitelné i 4, je tak dělitelné i číslem 12. Proto
$$F_n = 12k+5,$$
kde k je číslo celé.
- Avšak z lemmatu 2.10 vyplývá: Je-li F_n prvočíslo, pak číslo
$$3^{6k+2}+1 = 3^{(F_n-1)/2}+1 = 3^{2^{2^n-1}}+1$$
je dělitelné číslem F_n.

■

([15], s. 75,76)

Kompletní Pépinův test vypadá takto:

Věta 2.12 (Pépinův test) Pro $m \geq 1$ je Fermatovo číslo F_m prvočíslem právě tehdy, když $3^{(F_m-1)/2} \equiv -1\ (mod\ F_m)$.

Pomocí Pépinova testu tak například Felix Klein roku 1897 dokazuje, že i osmé Fermatovo číslo v pořadí je složené, jeho prvočíselný rozklad je ovšem nalezen až po více než 70 letech:

$$F_7 = (2^9 \cdot 116\,503\,103\,764\,643 + 1)(2^9 \cdot 11\,141\,971\,095\,088\,142\,685 + 1).$$

O čísle F_8 je rozhodnuto roku 1909, J. C. Moreheard a A. E. Western dokazují jeho možnou faktorizaci, ale rozklad neznají. Víme, že F_8 má právě 78 cifer, tedy prvočísel menších než $\sqrt{F_8}$je podle prvočíselné věty zhruba 10^{36}. Pokud by vyzkoušení jednoho dělitele trvalo jednu sekundu, pro rozložení devátého Fermatova čísla bychom tak potřebovali $3 \cdot 10^{28}$ let, což daleko přesahuje odhadované stáří celého vesmíru. Je tedy pozoruhodné, jak brzy se prvočinitel našel. Roku 1981 matematici Brent a Pollard dokazují, že číslo 1 238 926 361 552 897 dělí F_8.

Postupně se tak pravdivost Fermatovy domněnky rozplynula. Dodnes mnoho matematiků spekuluje, zda vůbec existuje nějaké další Fermatovo prvočíslo. Většina z nich se přiklání k tomu, že všechna ostatní čísla jsou složená, to se však zatím nikomu nepovedlo potvrdit a ani vyvrátit.

2.2.3 Rozložení Fermatových čísel na prvočinitele

Protože s rostoucím exponentem velmi rychle narůstá i počet cifer, které dané Fermatovo číslo má, je vítána každá pomoc, díky níž by se dal jednoduše najít rozklad Fermatových čísel. Jednou z metod, jak urychlit hledání rozkladu je použít Větu 2.9, která předkládá obecný tvar všech dělitelů Fermatových čísel. Další velkou pomocí při hledání prvočinitelů je následující věta:

Věta 2.13 (Lucasova) Jestliže prvočíslo p dělí F_m pro $m > 1$, pak existuje přirozené číslo k tak, že $p = k \cdot 2^{m+2} + 1$.

Abychom si dokázali představit, jak věta funguje v praxi, podívejme se na příklad, kterým se zabýval A. E. Western roku 1903. Pokoušel se s její pomocí dokázat, že číslo F_{18} je složené.

- Nalezněme přirozené číslo k, pro které je $p = k2^{20} + 1$ prvočíslo a zároveň p dělí F_{18}
- $p_1 = 7 \cdot 2^{20} + 1$ a $p_2 = 13 \cdot 2^{20} + 1$ jsou prvočísla (jak ukázal Western), dále se budeme zajímat o případ, kdy $k = 13$.
- Dokažme tedy, že číslo $p = 13 \cdot 2^{20} + 1 = 13\,631\,489$ dělí F_{18}:

$$2^{2^5} = 65\,536^2 \equiv 1\,048\,261 \ (mod\ 13\,631\,489)$$
$$2^{2^6} = 1\,048\,216^2 \equiv 3\,164\,342 \ (mod\ 13\,631\,489)$$
$$2^{2^7} = 3\,164\,342^2 \equiv 9\,153\,547 \ (mod\ 13\,631\,489)$$
$$\vdots$$
$$2^{2^{17}} = 1\,598\,622^2 \equiv 1\,635\,631 \ (mod\ 13\,631\,489)$$
$$2^{2^{18}} = 1\,635\,631^2 \equiv 13\,631\,488 \ (mod\ 13\,631\,489)$$

- Z poslední kongruence vyplývá

$$2^{2^{18}} + 1 \equiv 0 \ (mod\ 13\,631\,489)$$

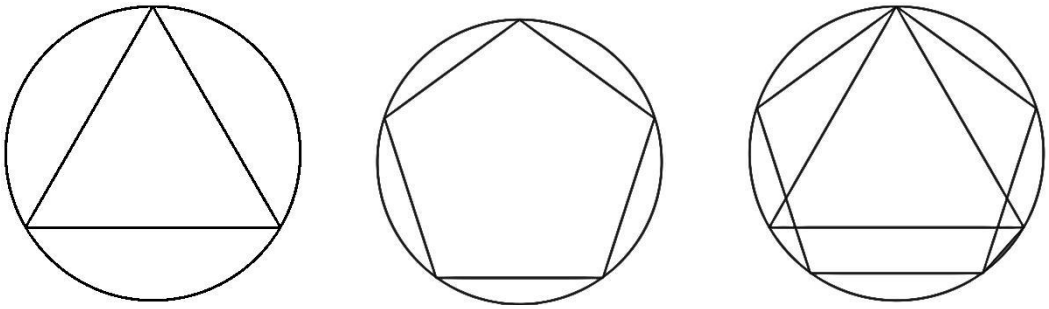
2.2.4 Konstrukce pravidelných mnohoúhelníků

Dodnes neznáme žádné jiné Fermatovo prvočíslo, kromě prvních pěti, která zkoumal již Fermat. A na rozdíl od Mersennových prvočísel je pravděpodobné, že pokusy při hledání dalších z nich nepovedou k úspěchu. Otázkou je; proč se na ně tedy upíná taková pozornost. Odpověď má kořeny již ve třetím století před naším letopočtem, kdy z poznatků čtvrté Eukleidovy knihy Základy plyne následující věta:

Věta 2.14 Pravidelný n-úhelník lze zkonstruovat pomocí pravítka a kružítka, jestliže $n = 2^i 3^j 5^k$, kde $n \geq 3$ a $i \geq 0$ jsou celá čísla a $j, k \in \{0, 1\}$.

Je jednoduché přímo ukázat konstrukci rovnostranného trojúhelníku a pravidelného pětiúhelníku. Eukleidovská konstrukce[20] pravidelného patnáctiúhelníku je méně známá a o něco těžší, i přesto ji lze zvládnout například zkombinováním konstrukce pravidelného trojúhelníku a pětiúhelníku.

Pravidelný trojúhelník	Pravidelný pětiúhelník	Pravidelný patnáctiúhelník - konstrukce[21]



Obrázek 3 Pravidelné mnohoúhelníky

Číslo 2^i hraje ve vzorci $n = 2^i 3^j 5^k$ jednoduchou roli, neboť počet vrcholů v mnohoúhelníku lze kdykoli zdvojnásobit například aplikováním operace dělení úhlu na dva stejné úhly.

Do konce 18. století není známa žádná eukleidovská konstrukce pravidelného mnohoúhelníku, která by neodpovídala Větě 2.13. Až roku 1796 přichází devatenáctiletý Carl Friedrich Gauss s překvapivou konstrukcí pravidelného sedmnáctiúhelníku. Nejprve uveďme několik slov o něm samotném.

[20] Pouze s pomocí pravítka a kružítka.

[21] Na obrázku je konstrukce pravidelného patnáctiúhelníku pouze naznačena. Pravidelný patnáctiúhelník je zde reprezentován pouze jednou stranou a to mezi nejbližším vrcholem pětiúhelníku a trojúhelníku. Pokud by se délka této strany postupně nanášela na opsanou kružnici, sestrojil by se pravidelný patnáctiúhelník.

Carl Friedrich Gauss (1777 – 1855) má v matematice velmi široký záběr. Jen v předchozích kapitolách jsme se s jeho jménem spojili prvočíselnou větu, nebo pojem kongruence. Navíc také jako první ve své disertační práci roku 1799 dokazuje Základní větu algebry. Gaussův život začíná v rodině zedníka a vodního mistra v Brunswidku v severním Německu. Již jako malý vyniká svou inteligencí. Ve třech letech například svého otce opravuje v jednoduchém výpočtu a velmi brzy se naučí i číst. Škola se tak pro něj stává nezajímavou. Na rozdíl od svých vrstevníků rychle nachází řešení různých problémů. Dokonce v devíti letech odvozuje vzorec pro součet aritmetické posloupnosti. Takto známou historku parafrázuje ve své knize Mareš [12], s. 128, 129:

„Když mu bylo devět, nechal učitel žáky sečíst čísla od 1 do 60. Nejspíš chtěl mít chvíli klid, ale moc si ho neužil. Malý Gauss se prakticky okamžitě dostavil ke katedře a znal správný výsledek – 1830. Uměl také vysvětlit, jak k němu přišel – spočítal prostě průměr posledního a prvního čísla (ten je 30,5) a vynásobil ho počtem všech čísel, tedy šedesáti.“

Gaussova neobvyklá bystrost na jeho učitele zapůsobila tak, že pro něj obstarává učebnici matematiky a chlapci ji předává se slovy, že už není nic, co by jej mohl naučit. V šestnácti letech získává Gauss pro další studia na místní univerzitě stipendium brunšvického vévody. Po třech letech přechází na slavnou univerzitu v Göttingenu, kde studuje dalších pět let. Právě tady vzniká jeho disertační práce se Základní větou algebry. Mimoto navazuje na některé z prací Leonharda Eulera a dává tak vzniknout například modulární algebře[22].

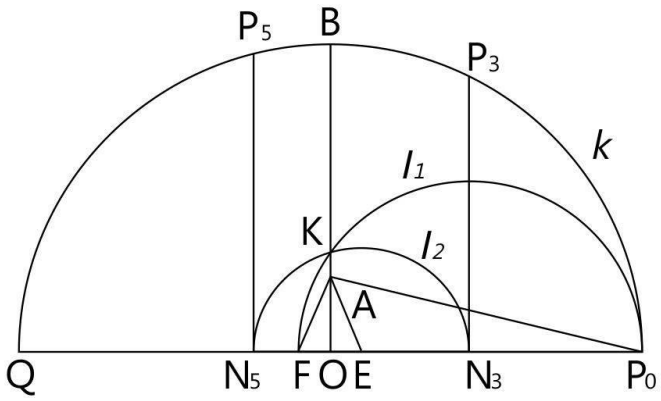
Kromě matematiky si Gauss také oblíbil astronomii a planetární mechaniku. A roku 1807 se stává profesorem astronomie a současně ředitelem univerzitní hvězdárny. V této funkci zůstává až do konce své profesní kariéry.

Přes všechny své úspěchy zůstává Gauss velmi skromným člověkem. Ačkoli mnoho svých závěrů představuje veřejnosti, ty nejdůležitější a nejpřevratnější výsledky si nechává pro sebe (například možnost neeukleidovské geometrie). Vraťme se ale k jeho konstrukci pravidelného sedmnáctiúhelníku.

[22] Je to algebra s konečně mnoha čísly, která se cyklicky opakují.

Tabulka 3

Konstrukce pravidelného sedmnáctiúhelníku	Popis konstrukce



1. $QP_0;\ QP_0$
2. $O; O = S_{QP_0}$
3. $k; k(O, \frac{1}{2}|QP_0|)$
4. $B; OB \perp QP_0 \wedge B \in k$
5. $A; A \in OB \wedge |OA| = \frac{1}{4}|OB|$
6. $E; E \in QP_0 \wedge |\sphericalangle OAE| = \frac{1}{4}|\sphericalangle OAP_0|$
7. $F; F \in QP_0 \wedge |\sphericalangle FAE| = \frac{\pi}{4}$
8. $l_1;\ l_1(S_{FP_0}, \frac{1}{2}\ |FP_0|)$
9. $K; K \in l_1 \cap OB$
10. $l_2;\ l_2(E, |EK|)$
11. $N_3, N_5;\ N_3, N_5 \in QN_0 \cap l_2$
12. $P_3;\ P_3 \in k \wedge P_3N_3 \perp QP_3$
13. $P_5;\ P_5 \in k \wedge P_5N_5 \perp QP_5$

V popisu konstrukce dále nebudeme pokračovat, neboť již máme sestrojené tři z vrcholů pravidelného sedmnáctiúhelníku P_0, P_3 a P_5. Nyní existuje hned několik možností jak najít i ostatní vrcholy sedmnáctiúhelníku. Nejjednodušším je například rozdělení úhlu P_3OP_5 na dvě stejné části – tak získáme bod P_4. A postupným nanášením vzdáleností $|P_3P_4|$ na kružnici k je možné zkonstruovat i všechny zbývající vrcholy pravidelného sedmnáctiúhelníku.

Na sestrojení sedmnáctiúhelníku je Gauss tak hrdý, že si jej přeje mít na svém náhrobku v Göttingenu. Toto přání mu sice splněno nebylo, zato podstavec jeho sochy v Braunschweigu zdobí pravidelná sedmnácticípá hvězda (tvar hvězdy byl vybrán záměrně, neboť pravidelný sedmnáctiúhelník by se dal na první pohled splést s kružnicí).

Zanedlouho po zkonstruování sedmnáctiúhelníku Gauss přichází s překvapivým tvrzením, které ukazuje až neuvěřitelnou souvislost eukleidovské konstrukce pravidelných mnohoúhelníků s Fermatovými prvočísly.

Věta 3.6 (Gaussova) Pravidelný n-úhelník lze eukleidovsky konstruovat právě tehdy, když počet jeho vrcholů je roven $n = 2^i p_1 p_2 \dots p_j$, kde $i \geq 0, j \geq 0, n \geq 3$ jsou celá čísla a $p_1, p_2, \dots, p_j$ jsou navzájem různá Fermatova prvočísla.

Původní Gaussův padesátistránkový důkaz je neúplný. Teprve roku 1837 větu dokazuje francouzský matematik Pierre Wantzel. Důkaz nebudeme uvádět, ale je možné jej najít ve Wantzelově knize ([19], s. 366-372).

A protože je dodnes známo pouze prvních pět Fermatových prvočísel, můžeme dokázat existenci eukleidovské konstrukce pouze pro $2^5 - 1 = 31$ pravidelných mnohoúhelníků právě s lichým počtem jejich vrcholů. I přestože byla popsána konstrukce pravidelného 257-úhelníku nebo dokonce pravidelného 65537-úhelníku jsou takové útvary v praktickém životě nepoužitelné, neboť jejich strany téměř splývají s kružnicí.

2.3 Eukleidova prvočísla

Poslední ze speciálních typů prvočísel, kterým v této práci budeme věnovat pozornost, jsou dílem řeckého matematika Eukleida z Alexandrie. Jeho jméno bylo již v první kapitole spojeno se známým důkazem o nekonečném počtu prvočísel. A právě tento důkaz dal vzniknout pravděpodobně prvnímu speciálnímu typu prvočísel.

Ve zkratce připomeňme myšlenku Věty 1.4 a jejího důkazu: Věta říká, že prvočísel je více než jakýkoliv počet prvočísel. Což znamená, že kdykoli můžeme vzít libovolné množství po sobě jdoucích prvočísel $p_1, p_2, \dots, p_n$ počínaje 2 a vytvořit jejich součin, který zvětšíme o jednotku. Takto vzniklé číslo $q = p_1 p_2 \dots p_n + 1$ je vždy dělitelné jiným a větším prvočíslem než $p_1, p_2, \dots, p_n$. Číslo q tedy budeme nazývat Eukleidovo číslo a v případě jeho prvočíselnosti Eukleidovo prvočíslo.

Je zjevné, že zastoupení prvočísel mezi ostatními Eukleidovými čísly pomalu řídne. Uveďme si několik z nich. Stejně jako v důkazu Věty 1.4 označme d za součin všech prvočísel menších nebo rovných p_n, tedy $d = p_1 p_2 \dots p_n$. Pak

$$q = p_1 p_2 \dots p_n + 1 = d + 1$$

je Eukleidovým prvočíslem, pokud je poslední člen součinu

$$p_n = 2, 3, 5, 7, 11, 31, 379, 1\,019\,1\,021, 2\,657, 3\,229, 4\,547, 4\,787, 11\,549, \dots$$

Podobně jako Mersennova a Fermatova prvočísla i ta Euklidova velmi brzy nabývají gigantických hodnot. Například již pro $p_n = 379$ dostáváme Eukleidovo číslo o téměř 200 cifrách. Na druhou stranu, na rozdíl od Mersennových a Fermatových prvočísel prozatím nenašla žádnou další možnou aplikaci.

Závěr

Jak poznamenal Leonhard Euler ([14], s. 29): *„Stěží se najde matematik, který by neztratil spoustu času na to, aby odhalil tajemství prvočísel.“* Jsem tedy ráda za možnost tuto oblast teorie čísel také blíže prozkoumat. Mým cílem nebylo pouze představit matematické definice, věty a jejich důkazy, ale snažila jsem se i seznámit s jejich autory a historickým pozadím, ve kterém vznikaly.

Nejprve jsem pro práci shromáždila základní informace o prvočíslech, které mi následně pomohly při hlubším zkoumání speciálních typů prvočísel. Díky tomu jsem si uvědomila, jak jsou věci v matematice provázané. A to nejen v určité oblasti této vědy. Jak například Gauss ukázal při nalezení souvislosti mezi teorií čísel a geometrií tam, kde by ji snad nikdo nehledal.

Práce pro mne byla v mnoha oblastech velkým přínosem. Naučila jsem se vyhledávat a orientovat se v matematických publikacích. A mimo jiné jsem získala určitý nadhled nad historií matematiky.

Seznam použité literatury

[1] CRILLY, A. *Velké otázky: matematika*. Vyd. 1. Překlad Jiří Jarník. Praha: Knižní klub, 2012, 208 s. Universum (Knižní klub). ISBN 9788024235967.

[2] DERBYSHIRE, John. *Posedlost prvočísly*. Vyd. 1. Praha: Academia, 2007, 407 s., [8] s. obr. příl. Galileo. ISBN 978-80-200-1479-5.

[3] EUKLEIDÉS,. *Základy*. Vyd. 2., oprav. Editor Petr Vopěnka. Překlad František Servít. Nymburk: OPS, 2008, 142 s. Prameny evropské vzdělanosti, 1. sv. ISBN 9788090377363.

[4] EUKLEIDÉS,. *Základy*. Překlad František Servít. Kanina: OPS, 2010, 189 s. Prameny evropské vzdělanosti, 4. sv. ISBN 9788070439630.

[5] FUSCH, Eduard. Co ještě nevíme o přirozených číslech: Od dokonalých čísel k Fermatovým prvočíslům. *Učitel matematiky*. 1999, roč. 7, č. 29-31, s. 1-8, 65-74, 130-136.

[6] HALAŠ, Radomír. *Teorie čísel*. 1. vyd. Olomouc: Vydavatelství Univerzity Palackého, 1997, 140 s. ISBN 80-7067-707-4.

[7] JACKSON, Tom a Richard BEATTY. *Matematika: 100 objevů, které změnily historii*. V Praze: Slovart, 2013, 144 s. ISBN 978-80-7391-770-8.

[8] KLÁN, Petr. *Čísla: vztahy, vhledy a věčné inspirace*. Vyd. 1. Praha: Academia, 2014, 246 s. ISBN 978-80-200-2137-3.

[9] KŘÍŽEK, Michal, Lawrence SOMER a Alena ŠOLCOVÁ. *Kouzlo čísel: od velkých objevů k aplikacím*. Vyd. 1. Praha: Academia, 2009, 365 s., [8] s. barev. obr. příl. ISBN 978-80-200-1610-2.

[10] KUŘINA, František. *Deset pohledů na geometrii*. Praha: Matematický ústav Akademie věd České republiky, 1996, 249 s. ISBN 80-85823-21-7.

[11] LEPKA, Karel. Malá Fermatova věta. *Učitel matematiky*. Praha: Jednota českých matematiků a fyziků, 1997, roč. 5, č. 23, s. 143-150.

[12] MAREŠ, Milan. *Příběhy matematiky: stručná historie královny věd*. 1. vyd. Příbram: Pistorius & Olšanská, 2008, 334 s. ISBN 978-80-87053-16-4.

[13] MLÝNEK, Jaroslav. *Zabezpečení obchodních informací*. Vyd. 1. Brno: Computer Press, c2007, vi, 154 s. ISBN 978-80-251-1511-4.

[14] PORUBSKÝ, Štefan. *Fermat a teorie čísel aneb Problematika dělitelů a dokonalá čísla*. Matematik Pierre de Fermat (eds A. Šolcová, M. Křížek, G. Mink), Cahiers du CEFRES, 2002, 31 s.

[15] SIERPIŃSKI, Waclaw. *Co víme a co nevíme o prvočíslech*. 1. vyd. Praha: Státní pedagogické nakladatelství, 1966, 105 s.

[16] SINGH, Simon. *Kniha kódů a šifer: tajná komunikace od starého Egypta po kvantovou kryptografii*. 2. vyd. v českém jazyce. Přeložil Petr Koubský. Praha: Dokořán, 2009, 382 s. ISBN 978-80-7363-268-7.

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

[18] ŠOLCOVÁ, Alena. *Fermatův odkaz*. Matematik Pierre de Fermat (eds M. Křížek, G. Mink), Cahiers du CEFRES, 2002, 25 s.

[19] WANTZEL, Pierre Laurent. *Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle et le compas.* J. Math. 2 (1837), s. 366-372.

[20] ZIEGLER, Günter M. *Matematika vám to spočítá: příběhy královny věd*. Vyd. 1. Přeložil Zdeněk Michňa. Praha: Knižní klub, 2011, 222 s. ISBN 978-80-242-3311-6.

[21] ZNÁM, Štefan. *Teória čísel*. 1. vyd. Bratislava: Alfa, 1977, 205 s.

[22] Cryptography. *Nathaniel Johnston* [online]. © 2007-2015 [cit. 2015-03-06]. Dostupné z: http://www.njohnston.ca/tag/cryptography/

[23] Great Internet Mersenne Prime Search: Finding World Record Primes Since 1996. *List of known Mersenne prime numbers* [online]. ©1996-2015 [cit. 2015-02-28]. Dostupné z: http://www.mersenne.org/primes/