HYPOTÉZA FRANCISZKA JAKÓBCZYKA O MERSENNOVÝCH ČÍSLECH

JIŘÍ KLAŠKA

Abstrakt. Před 70-ti lety formuloval polský kněz a matematik Franciszek Jakóbczyk zajímavý a obtížný problém týkající se Mersennových čísel. Do dnešní doby zůstává problém nevyřešen. Následující článek poskytne čtenáři základní přehled o problematice Mersennových čísel, Jakóbczykově hypotéze a její souvislosti s Wieferichovými prvočísly.

1. Marine Mersenne a jeho prvočísla

Přirozené číslo m nazýváme dokonalé, je-li rovno součtu všech svých dělitelů menších než m. Například čísla $6, 28, 496, 8128$ jsou dokonalá, protože platí:

$$6 = 1 + 2 + 3,$$
$$28 = 1 + 2 + 4 + 7 + 14,$$
$$496 = 1 + 2 + 4 + 8 + 16 + 31 + 62 + 124 + 248,$$
$$8128 = 1 + 2 + 4 + 8 + 16 + 32 + 64 + 127 + 254 + 508 + 1016 + 2032 + 4064.$$

Kolem roku 300 př. n. l. dokázal řecký matematik Euklides (Základy, Kniha IX, Tvrzení 36) následující implikaci:

$$\textit{Je-li } 2^n - 1 \textit{ prvočíslo, pak číslo } 2^{n-1}(2^n - 1) \textit{ je dokonalé.} \tag{1}$$

Původní formulaci Euklidova tvrzení (1) a jeho důkaz může čtenář nalézt v českém překladu Základů z roku 1907 od Františka Servíta (1848–1923). Viz [46, str. 154–155]. Téměř o dva tisíce let později, v roce 1640, dokázal francouzský matematik Pierre de Fermat (1601–1665) následující tři tvrzení [10, str. 12], která považoval za základní objevy týkající se dokonalých čísel.

Věta 1.1 (Fermat, 1640)**.** *Platí:*

(i) *Je-li* $n \in \mathbb{N}$ *složené číslo, pak je složené také číslo* $2^n - 1$.
(ii) *Je-li* $n \in \mathbb{N}$ *prvočíslo, pak* $2n$ *dělí* $2^n - 2$.
(iii) *Je-li* $n \in \mathbb{N}$ *prvočíslo, pak* $2^n - 1$ *je dělitelné pouze prvočísly tvaru* $2kn + 1$, $k \in \mathbb{N}$.

Tvrzení (i) Věty 1.1 bývá častěji formulováno v ekvivalentním tvaru (iv), který je obměnou implikace (i):

2010 *MSC.* Primární 11A41, 11A07, 11-02.
Klíčová slova. Mersennova čísla, Franciszek Jakóbczyk, Wieferichova prvočísla.

(iv) *Je-li číslo* $2^n - 1$ *prvočíslo, pak* n *je prvočíslo.*

Více informací o dokonalých číslech a jejich historii je možno nalézt v prvním dílu knihy *History of the Theory of Numbers* [10] od Leonarda Eugena Dicksona (1874–1954) a také v článcích [41] a [51]. Přibližně v polovině roku 1640 zaslal Fermat dopis Marinu Mersennovi (1588–1648), ve kterém ho seznámil se svými výsledky uvedenými ve Větě 1.1. V roce 1644 pak Mersenne vyslovil v úvodu knihy *Cogitata Physica - Mathematica* [37] tvrzení, že jedinými prvočísly mezi čísly $2^n - 1$, kde $n \leq 257$, jsou čísla mající exponenty

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 67, 127, 257. \tag{2}$$

Pro zajímavost uveďme, že již v roce 1591 Petrus Bungus v knize *Numerorum Mysteria* [7], sestavil seznam 28 čísel, která považoval za dokonalá. Mersenne však prohlásil, že pouze 8 čísel z Bungusova seznamu je uvedeno správně a navíc k těmto osmi číslům přidal další tři hodnoty. Tak vznikl seznam (2), obsahující celkem jedenáct čísel [10, str. 12–13]. Čísla $M_n = 2^n - 1$, kde $n \in \mathbb{N}$, dnes nazýváme Mersennova čísla. Mersennovým prvočíslem pak rozumíme číslo M_n, které je prvočíslo. V průběhu let se začalo ukazovat, že také Mersennův seznam není správný. Ve skutečnosti v (2) chybí čísla $n = 61$, 89, 107, pro která je M_n prvočíslo. Naopak, čísla $n = 67$ a 257 do seznamu (2) nepatří, protože jsou složená. Opravený Mersennův seznam má tedy tvar

$$n = 2, 3, 5, 7, 13, 17, 19, 31, 61, 89, 107, 127. \tag{3}$$

Čtenáře možná překvapí, že vytvořit správný seznam (3), se všemi detaily, trvalo dalších 303 let, tedy až do roku 1947. Důvod, proč ověření správnosti trvalo tak dlouhou dobu, souvisí s nesmírně obtížným problémem faktorizace přirozených čísel. Je vhodné zde připomenout, že problém zjistit zda dané přirozené číslo je prvočíslo, je mnohem lehčí než nalézt jeho prvočíselný rozklad.

Vlastnosti dělitelů Mersennových čísel byly zkoumány řadou autorů. Jedno z důležitých tvrzení o tvarech prvočíselných dělitelů Mersennových čísel objevil v roce 1750 Leonhard Euler (1707–1783) a v roce 1775 dokázal Joseph Louis Lagrange (1736–1813).

Věta 1.2 (Euler, 1750)**.** *Je-li* p *prvočíslo,* $p \equiv 3 \pmod 4$*, pak* $2p + 1$ *dělí* M_p *právě tehdy, když* $2p + 1$ *je prvočíslo. V důsledku, jsou-li* $p \equiv 3 \pmod 4$ *a* $2p + 1$ *prvočísla, pak* $p = 3$ *nebo* M_p *je složené číslo.*

Euler rovněž dokázal opačnou implikaci k tvrzení (1). Jeho objev byl však publikován až v roce 1849, tedy 66 let po Eulerově smrti:

$$\begin{gathered} \textit{Každé sudé dokonalé číslo má tvar } 2^{n-1}(2^n - 1), \\ \textit{kde } n > 1 \textit{ a } 2^n - 1 \textit{ je prvočíslo.} \end{gathered} \tag{4}$$

Tvrzení (1) spolu s tvrzením (4) dokazují platnost Euklidovy–Eulerovy věty.

Věta 1.3 (Euklides, Euler)**.** *Sudé přirozené číslo je dokonalé právě tehdy, když je tvaru* $2^{n-1}(2^n - 1)$*, kde* $2^n - 1$ *je prvočíslo.*

Z Euklidovy–Eulerovy věty plyne existence vzájemně jednoznačné korespondence mezi sudými dokonalými čísly a Mersennovými prvočísly. Existuje domněnka, že existuje nekonečně mnoho Mersennových prvočísel. Tato domněnka však nebyla do dnešní doby dokázána. Rovněž není známo, zda existují lichá dokonalá čísla.

V roce 1876 objevil François Édouard Anatole Lucas (1842–1891) test prvočíselnosti Mersennových čísel [35, str. 316], který později zjednodušil a dokázal Derric Henry Lehmer (1905–1991). Lehmerovy výsledky byly publikovány v článcích [28] a [29]. Lucasův–Lehmerův test prvočíselnosti Mesennových čísel lze formulovat následovně.

Věta 1.4 (Lucas, Lehmer)**.** *Nechť* $S_1 = 4$ *a* $S_{k+1} = S_k^2 - 2$ *pro* $k = 1, 2, 3, \ldots$. *Je-li* p *liché prvočíslo, pak* M_p *je prvočíslo právě tehdy, když* M_p *dělí* S_{p-1}.

Lucasův-Lehmerův výsledek je používán k testování prvočíselnosti Mersennových čísel i v současné době. Další zajímavá vlastnost čísel M_n byla dokázána v [43, str. 91]:

$$\textit{Pokud } n \textit{ dělí } M_p\textit{, pak } n \equiv \pm 1 \pmod 8 \textit{ a } n \equiv 1 \pmod p.$$

Náročnost problému rozložit Mersennova čísla na součin prvočísel přiblížíme čtenáři na příkladech exponentů $n = 67$ a $n = 257$. V roce 1903 Frank Nelson Cole (1861–1926) rozložil na zasedání Americké matematické společnosti v New Yorku číslo M_{67} na součin dvou prvočísel [16, str. 17] a tím dokázal, že číslo M_{67} je složené:

$$2^{67} - 1 = 147573952589676412927 = 193707721 \times 761838257287.$$

Důkaz, že číslo M_{257} je složené, objevil Lehmer v roce 1927. Kompletní rozklad čísla M_{257} na součin tří prvočísel byl nalezen teprve v roce 1980 [16, str. 27]. Číslo M_{257} tvoří 78 cifer a jeho prvočíselný rozklad má tvar:

$$\begin{aligned} M_{257} &= 231584178474632390847141970017375815706539969331281128078915168015826259279871 \\ &= 535006138814359 \times 1155685395246619182673033\times \\ &\quad \times 374550598501810936581776630096313181393. \end{aligned}$$

Podrobnosti o objevech týkajících se Mersennových čísel do roku 1935, včetně kompletní bibliografie, lze nalézt v článku [2], jehož autorem je Raymond Clare Archibald (1875–1955). Čtenáři lze rovněž doporučit historické pojednání [52] z roku 1952, které sepsal Horace Scudder Uhler (1872–1956). Chronologický vývoj jednotlivých objevů týkajících se faktorizace Mersennových čísel až do roku 1990 lze nalézt ve velmi obsáhlé práci [16], jejímž autorem je Haworth Guy.

V roce 1996 založil George Woltman projekt GIMPS [15] (Great Internet Mersenne Prime Search), jehož cílem je hledání dalších Mersennových prvočísel. Do dnešní doby (září 2021), je známo 51 Mersennových prvočísel. Seznam (3), který

vznikal v období let 1644–1947 má následující, aktuální pokračování:

$$\begin{aligned}&521, 607, 1279, 2203, 2281, 3217, 4253, 4423, 9689, 9941, 11213, 19937, 21701,\\&23209, 44497, 86243, 110503, 132049, 216091, 756839, 859433, 1257787,\\&1398269, 2976221, 3021377, 6972593, 13466917, 20996011, 24036583,\\&25964951, 30402457, 32582657, 37156667, 42643801, 43112609, 57885161,\\&74207281, 77232917, 82589933.\end{aligned} \tag{5}$$

V letech 1948–2021 tedy bylo nalezeno dalších 39 Mersennových prvočísel. Největší v současnosti známé Mersennovo prvočíslo M_n bylo objeveno v roce 2018 a má exponent $n = 82589933$. Zda je však seznam (5) mezi hodnotami $n = 43112609$ a $n = 82589933$ kompletní, není prozatím ověřeno. Je tedy možné, že mezi uvedenými hodnotami existují další, prozatím neznámá, Mesennova prvočísla. Aktuální informace o vývoji problematiky lze sledovat na internetové stránce GIMPS [15].

Mersennova čísla jsou v současnosti studována především v souvislosti s aplikacemi velkých prvočísel v teorii kódování. Strategický význam tohoto oboru matematiky pro přenos utajovaných zpráv, bankovních transakcí a bezpečnost internetu vyvolává intenzivní snahu pochopit hlubší zákonitosti světa prvočísel.

2. Jakóbczykova hypotéza

V roce 1951 publikoval polský kněz a matematik Franciszek Jakóbczyk (1905–1992) následující zajímavou hypotézu [20, str. 127] týkající se dělitelů Mersennových čísel s prvočíselými exponenty.

Hypotéza 2.1. *Buď p libovolné prvočíslo. Pak Mersennovo číslo M_p není dělitelné čtvercem žádného prvočísla.*

Jinak formulováno, je-li p prvočíslo, pak prvočíselný rozklad Mersennova čísla M_p má tvar $M_p = p_1 \times p_2 \times \cdots \times p_k$, kde $k \in \mathbb{N}$ a $p_1, p_2, \ldots, p_k$ jsou navzájem různá lichá prvočísla. Na Jakóbczykovu hypotézu upozorňuje rovněž Wacław Sierpiński (1882–1969) v knize *Co wiemy a czego nie wiemy o liczbach pierwszych* [47, str. 70], která vyšla ve Varšavě v roce 1961. Ruský překlad knihy [47] vyšel v Moskvě v roce 1963. Jakóbczykovo jméno se v souvislosti s Hypotézou 2.1 vyskytuje rovněž v Sierpińského knize *A Selection of Problems in the Theory of Numbers* [48, str. 92], která vyšla v New Yorku v roce 1964. Ve skutečnosti druhá část knihy [48, str. 25–97] obsahuje anglický překlad polského vydání [47]. Český překlad knihy [47] pak vyšel v roce 1966.

V kontextu uvedených informací je zarážející, že v současné době Jakóbczykovo jméno jako autora Hypotézy 2.1 není vůbec zmiňováno a je prakticky zapomenuto. Podrobnosti o životě a díle Franciszka Jakóbczyka může čtenář nalézt v článku [40].

Pro zajímavost uveďme, že ani Richard Kenneth Guy (1916–2020), autor známé knihy *Unsolved Problems in Number Theory* [17] se o Jakóbczykově práci nezmiňuje. Stojí ale za povšimnutí, že Guy zaujímá k Jakóbczykově hypotéze velmi vyhraněný a odmítavý postoj. Píše, cituji [17, str. 7]: *If p is a prime, is $2^p - 1$ always squarefree? This seems to be another unanswerable question. It is safe to*

conjecture that the answer is "No!"This could be settled by computer if you were lucky.

V knize [48, str. 102], část *One hundred elementary but difficult problems in arithmetic*, položil polský matematik Andrzej Schinzel následující otázku P_{10}^2.

Problém 2.2 (Schinzel, 1964)**.** Existuje nekonečně mnoho Mesennových čísel která nejsou dělitelná čtvercem žádného přirozeného čísla většího než 1?

Je zřejmé, že pravdivost Jakóbczykovy Hypotézy 2.1 implikuje kladnou odpověď na Schinzelovu otázku formulovanou v Problému 2.2. Zda je však odpověď na Schinzelovu otázku kladná nebo záporná není do dnešní doby známo.

3. Eulerův a Fermatův kvocient

V této kapitole připomeneme několik základních tvrzení a pojmů z teorie čísel, které souvisí s naší problematikou. Pro libovolné $m \in \mathbb{N}$ nechť $\varphi(m)$ označuje počet všech $k \in \mathbb{N}$, kde $1 \leq k \leq m$, která jsou nesoudělná s m. Funkci $\varphi(m)$ zavedl již v roce 1763 švýcarský matematik Leonhard Euler (1707–1783), který rovněž dokázal, že

$$\varphi(m) = m \prod_{p|m} \left(1 - \frac{1}{p}\right), \tag{6}$$

přičemž součin v (6) probíhá přes všechna různá prvočísla p, která dělí m. Funkce $\varphi(m)$ se nazývá Eulerova funkce. Speciálně, pokud $m = p^n$, kde p je prvočíslo a n je libovolné přirozené číslo, pak $\varphi(p^n) = p^n - p^{n-1}$. Euler rovněž dokázal, že pro libovolná nesoudělná čísla $a, m \in \mathbb{Z}$, $m > 1$ platí

$$a^{\varphi(m)} \equiv 1 \pmod{m}. \tag{7}$$

Z (7) ihned plyne, že číslo $q_m(a)$ definované vztahem

$$q_m(a) = \frac{a^{\varphi(m)} - 1}{m} \tag{8}$$

je vždy celé číslo. V roce 1997 navrhla trojice autorů Takashi Agoh, Karl Dilcher a Ladislav Skula [1, str. 31] používat pro číslo (8) název Eulerův kvocient čísla m se základem a.

Speciálním případem Eulerova kvocientu, pro $m = p$, kde p je prvočíslo, je Fermatův kvocient

$$q_p(a) = \frac{a^{p-1} - 1}{p}. \tag{9}$$

Název Fermatův kvocient použil poprvé v roce 1861 James Joseph Sylvester (1814–1897) v *Comptes Rendus de l'Académie des Sciences* [50, str. 161]. Pojmenování, které Sylvester pro podíl (9) použil, má připomínat skutečnost, že podle malé Fermatovy věty je $q_p(a)$ celé číslo. Aritmetické vlastnosti čísel $q_p(a)$ byly od roku 1828 detailně studovány celou řadou autorů. Podrobnosti o dosažených výsledcích může čtenář nalézt v [10, str. 105–112] nebo též v publikaci Karla Lepky [31, str. 29–73]. Je vhodné zmínit, že některé důležité vlastnosti Fermatova kvocientu objevil v letech 1905–1906 český matematik Matyáš Lerch (1860–1922) v článcích [32] a [33].

Vlastnosti Eulerova kvocientu byly pak podrobně studovány v [1]. Eulerova funkce $\varphi(m)$ úzce souvisí s teorií konečných cyklických grup. Pro potřeby tohoto článku však bude stačit připomenout pouze několik základních skutečností. Pro libovolné prvočíslo p a pro libovolné $n \in \mathbb{N}$ nechť $(\mathbb{Z}/p^n\mathbb{Z})^\times$ označuje multiplikativní grupu jednotek okruhu $\mathbb{Z}/p^n\mathbb{Z}$. Grupa $(\mathbb{Z}/p^n\mathbb{Z})^\times$ je konečná a má $\varphi(p^n)$ prvků. Je-li p liché prvočíslo, pak $(\mathbb{Z}/p^n\mathbb{Z})^\times$ je cyklická. Je-li $p = 2$, pak $(\mathbb{Z}/2^n\mathbb{Z})^\times$ je cyklická právě tehdy, když $n = 1$ nebo $n = 2$. Dále, pro libovolné $a \in (\mathbb{Z}/p^n\mathbb{Z})^\times$ označme $\mathrm{ord}_{p^n}(a)$ řád prvku a v grupě $(\mathbb{Z}/p^n\mathbb{Z})^\times$, tj. nejmenší přirozené číslo k takové, že $a^k \equiv 1 \pmod{p^n}$. Uvedené pojmy budou užitečné již v následující kapitole.

4. Wieferichova prvočísla

V roce 1909 dokázal německý matematik Arthur Wieferich (1884–1954) pozoruhodné tvrzení, týkající se prvního případu velké Fermatovy věty [54].

Věta 4.1 (Wieferich, 1909)**.** *Nechť p je liché prvočíslo a nechť x, y, z jsou celá čísla nedělitelná p, vyhovující rovnici $x^p + y^p = z^p$. Pak $2^{p-1} \equiv 1 \pmod{p^2}$.*

Na počest Wieferichova objevu jsou prvočísla p splňující kongruenci $2^{p-1} \equiv 1 \pmod{p^2}$ nazývána Wieferichova prvočísla. Pomocí pojmů zavedených v předchozí kapitole je snadné dokázat, že následující podmínky jsou ekvivalentní:

$$\begin{aligned} &\text{(i)} \quad 2^{p-1} \equiv 1 \pmod{p^2}, \\ &\text{(ii)} \quad q_p(2) \equiv 0 \pmod{p}, \\ &\text{(iii)} \quad \mathrm{ord}_{p^2}(2) = \mathrm{ord}_p(2). \end{aligned} \tag{10}$$

Z historického hlediska je zajímavé zmínit, že v době publikace Wieferichovy věty nebylo známo žádné prvočíslo splňující (10). Již v roce 1910 Waldemar Meissner (1852–1928) prozkoumal všechna prvočísla $p \leq 1000$ ale žádné, které by mělo vlastnost (10), nenalezl. Ke stejnému závěru dospěl také ukrajinský matematik Dmitry Grawe (1863–1939). V roce 1913 došlo k prvnímu důležitému objevu. Meissner rozšířil svoje předchozí výpočty pro všechna prvočísla $p \leq 2000$ a nalezl první Wieferichovo prvočíslo $w_1 = 1093$. Svůj výsledek publikoval v článku [36]. Ke druhému objevu došlo v roce 1922. Holandský matematik Nicolas Beeger (1884–1965) prozkoumal všechna prvočísla $p \leq 3700$ a nalezl druhé Wieferichovo prvočíslo $w_2 = 3511$. Objev publikoval v článku [3]. V roce 1927 Robert Haußner (1863–1948) provedl výpočty pro všechna prvočísla $p \leq 10000$, ale žádné další Wieferichovo prvočíslo neobjevil [18]. Již o dva roky dříve Nicolas Beeger [4] informoval, že bez úspěchu prohledal všechna prvočísla po hranici $p \leq 14000$. Beeger pokračoval v hledání třetího Wieferichova prvočísla až do začátku druhé světové války. V roce 1939 publikoval závěr [5], že ani pro $p \leq 16000$ neexistuje žádné další Wieferichovo prvočíslo.

V [5, str. 52] vyslovuje Beeger zajímavý názor, že kromě nalezených Wieferichových prvočísel 1093 a 3511 již žádné další neexistuje. Dokázat tuto domněnku by však v důsledku znamenalo nalézt důkaz prvního případu velké Fermatovy věty. Možná bude zajímavé uvést přesné znění Beegerova názoru z roku 1939: *The fact that there are only* 2 *primes* < 16000 *satisfying* $2^{p-1} \equiv 1 \pmod{p^2}$ *and that there*

is no such prime between 3511 *and* 16000 *may give rise to the conjecture that others do not exist and that the first case of Fermat's last theorem can be proved in showing that* $(2^{p-1}-1) : p^2$ *is, for large values of p, not a whole number.*

Výrazný pokrok v hledání Wieferichových prvočísel nastal s příchodem počítačů po druhé světové válce. V roce 1958 Carl Erik Fröberg [13] rozšířil hledání pro $p \leq 50000$, ale žádné nové Wieferichovo prvočíslo neobjevil. Sidney Kravitz [25] v roce 1960 zjistil, že ani pro $p \leq 100000$ žádné další Wieferichovo prvočíslo neexistuje. Neúspěšné byly rovněž výpočty, které v roce 1964 provedli Erna H. Pearson [39] pro $p \leq 200183$ a Hans Riesel [44] pro $p \leq 500000$. V roce 1963 Melvin Hausner a David Sachs [19] dospěli s využitím počítače IBM 7090 k výsledku, že jedinými Wieferichovými prvočísly $p \leq 10^6$ jsou 1093 a 3511. Další pokroky v pátrání po třetím Wieferichovu prvočíslu souvisí zejména s technologickým rozvojem počítačů a konstrukcí efektivnějších algoritmů. Připomeňme alespoň některé.

Již v roce 1968 Fröberg [14, str. 84–88] podstatným způsobem rozšířil svůj výsledek z roku 1958. Avšak ani pro $p \leq 3 \times 10^7$ další Wieferichovo prvočíslo nenalezl. V roce 1971 trojice autorů Brillhart, Tonascia a Weinberger [6, str. 213–222] podala zprávu, že pro $p \leq 3 \times 10^9$ žádné další Wieferichovo prvočíslo neexistuje. V roce 1981 Lehmer [30] informoval, že ani pro $p \leq 6 \times 10^9$ nebylo další Wieferichovo prvočíslo objeveno. O 17 let později, v roce 1997, Richard Crandall, Karl Dilcher a Carl Pomerance publikovali závěr [9], že pro $p \leq 4 \times 10^{12}$ žádné nové Wieferichovo prvočíslo neexistuje. V roce 2005 pokračovali v hledání Wieferichových prvočísel Joshua Knauer a Jörg Richstein. Podle jejich výsledku prezentovaného v článku [24] neexistuje žádné další Wieferichovo prvočíslo pro $p \leq 1{,}25 \times 10^{15}$.

Novou nadějí na nalezení třetího Wieferichova prvočísla se stala metoda založená na nečekaném objevu Larryho Washingtona [21, str. 198]. Pokud obě známá Wieferichova prvočísla 1093 a 3511 zmenšíme o jedničku, pak binární rozvoj vzniklých čísel je periodický:

$$1092 = 0100\,0100\,0100_2 = 444_{16} \quad \text{a} \quad 3510 = 110\,110\,110\,110\,110_2 = 6666_8. \tag{11}$$

Dolní indexy 2, 8 a 16 ve vztahu (11) znamenají vyjádření čísla ve dvojkové, osmičkové a šestnáctkové číselné soustavě. Tento objev se stal inspirací pro hledání třetího Wieferichova prvočísla ve tvaru s periodickým binárním rozvojem. Podrobnosti může čtenář nalézt v článku Miroslava Kureše a Jana Dobeše [11]. Projekt Wieferich@Home založený na této myšlence probíhal v letech 2007–2016. Objev třetího Wieferichova prvočísla však nepřinesl.

V roce 2011 Francois G. Dorais a Dominic Klyve [12] publikovali výsledek, že ani pro $p \leq 6 \times 10^{15}$ neexistuje žádné další Wieferichovo prvočíslo. Od roku 2011, nezávisle na projektu Wieferich@Home, probíhal také jiný projekt pro hledání Wieferichových prvočísel s názvem PrimeGrid. Tento projekt dosáhl v roce 2017 hranice $p \leq 10^{17}$ a byl ukončen aniž by nalezl třetí Wieferichovo prvočíslo.

Konečně v roce 2020 byl zahájen nový projekt PrimeGrid [42], který spojil hledání Wieferichových prvočísel s hledáním Fibonacci–Wieferichových prvočísel [23]. Současný stav (září 2021) dosažený v rámci tohoto projektu můžeme formulovat jako tvrzení, které shrnuje 112 let výzkumu Wieferichových prvočísel: *V intervalu* $[2, 3 \times 10^{18}]$ *existují pouze dvě Wieferichova prvočísla:* 1093 *a* 3511.

Je vhodné poznamenat, že intenzivní snaha nalézt třetí Wieferichovo prvočíslo byla od roku 1997 podporována domněnkou, že množina všech Wieferichových prvočísel je nekonečná a že počet Wieferichových prvočísel ležících v intervalu $[x, y]$ je přibližně roven číslu

$$\sum_{p\in[x,y]} \frac{1}{p} \approx \ln\left(\frac{\ln(y)}{\ln(x)}\right). \tag{12}$$

Tato domněnka je založena na statistických argumentech prezentovaných v [9, str. 446]. Otázkou zůstává, zda vztah (12) opravdu platí, protože podle (12) by se měla v intervalu $[2, 3 \times 10^{18}]$ vyskytovat aspoň čtyři Wieferichova prvočísla. Tato předpověď se ale v období následujících let 1997–2021 nepotvrdila. Do dnešní doby není známo, zda množina všech Wieferichových prvočísel je konečná nebo nekonečná množina.

Je naprosto fascinující si uvědomit, že za posledních 57 let (1964–2021) vzrostly výpočetní schopnosti počítačů o více než 12 řádů. Výrazného zrychlení výpočtů bylo po roce 1997 dosaženo také díky využití internetu a strategii distribuovaných výpočtů. Základní myšlenkou distribuovaných výpočtů je rozložit rozsáhlý výpočetní problém na mnoho různých částí. Jednotlivé části jsou pak prostřednictvím internetu přiděleny různým počítačům po celém světě a ty dílčí úlohy zpracují.

Na závěr kapitoly ještě poznamenejme, že hledání Wieferichových prvočísel je často spojováno s řešením obecnějšího problému, totiž určit prvočísla p splňující podmínku $a^{p-1} \equiv 1 \pmod{p^2}$, kde $a \geq 2$ je dané přirozené číslo. Tato problematika je studována například v článcích [22, 34, 38, 44].

5. Souvislost Jakóbczykovy hypotézy s Wieferichovými prvočísly

První souvislost mezi Wieferichovými prvočísly a Mersennovými čísly objevil v roce 1965 polský matematik Andrzej Rotkiewicz (1931–2016). V článku [45] dokázal Rotkiewicz následující čtyři tvrzení.

Věta 5.1 (Rotkiewicz, 1965)**.** *Platí:*

(i) *Nechť existuje nekonečně mnoho Mersennových čísel M_q, kde q je prvočíslo, které nemají čtvercové dělitele větší než 1. Pak existuje nekonečně mnoho prvočísel p s vlastností $2^{p-1} \not\equiv 1 \pmod{p^2}$.*

(ii) *Nechť existuje pouze konečně mnoho prvočísel p s vlastností $2^{p-1} \equiv 1 \pmod{p^2}$. Pak pro libovolné, dostatečně velké prvočíslo q a libovolné přirozené číslo n nemá Mersennovo číslo M_{q^n} čtvercové dělitele větší než 1.*

(iii) *Nekonečně mnoho přirozených čísel n s vlastností $n^2|2^n - 2$ existuje právě tehdy, když existuje nekonečně mnoho prvočísel p s vlastností $p^2|2^{p-1} - 1$.*

(iv) *Nekonečně mnoho přirozených čísel $n^2 > 1$ s vlastností $n^2|2^{n^2} - 2$ existuje právě tehdy, když existuje nekonečně mnoho prvočísel p s vlastností $p^2|2^{p-1} - 1$.*

Je zřejmé, že tvrzení (i) Věty 5.1 dává částečnou odpověď na Schinzelovu otázku P_{10}^2 uvedenou ve druhé kapitole. Tvrzení (iii) pak dává částečnou odpověď na

otázku P_{43}^2 v [48, str. 109]:

Existuje nekonečně mnoho přirozených čísel n, pro která $2^n - 2$ je dělitelné n^2?

V roce 1967 Le Roy J. Warren a Henry G. Bray [53] dokázali následující implikaci.

Věta 5.2 (Warren, Bray, 1967)**.** *Buďte p, q libovolná lichá prvočísla.*

$$\text{Jestliže } p \text{ dělí } M_q, \text{ pak } 2^{\frac{p-1}{2}} \equiv 1 \pmod{M_q}.$$

Z Věty 5.2 bezprostředně plyne následující důsledek.

Důsledek 5.3. *Buďte p, q libovolná lichá prvočísla.*

$$\text{Jestliže } p^2 \text{ dělí } M_q, \text{ pak } 2^{p-1} \equiv 1 \pmod{p^2}.$$

Jinak formulováno, existuje-li Mersennovo číslo s prvočíselným exponentem, které je dělitelné čtvercem prvočísla p, pak p je Wieferichovo prvočíslo. Alternativní důkaz tvrzení Věty 5.2 předložil Chris K. Caldwell [8]. Existují-li pouze dvě Wieferichova prvočísla, 1093 a 3511, pak tato skutečnost spolu s Větou 5.2 implikuje správnost Jakóbczykovy hypotézy.

V roce 2019 publikoval Ladislav Skula článek [49], v němž studoval Wieferichova prvočísla vyšších řádů a jejich souvislost s Mersennovými čísly. Bude vhodné připomenout definici [49, str. 2]: Řekneme, že Wieferichovo prvočíslo p je řádu $n \in \mathbb{N}$, když

$$q_{p^n}(2) \equiv 0 \pmod{p^n}, \quad \text{nebo ekvivalentně, } 2^{p^{n-1}(p-1)} \equiv 1 \pmod{p^{2n}}.$$

Důkaz následující věty využívá některých výsledků dosažených v [1, str. 44–47].

Věta 5.4 (Skula, 2019)**.** *Nechť p a q jsou libovolná prvočísla, $n \in \mathbb{N}$ a nechť p^n dělí Mersennovo číslo M_q. Pak následující jsou tvrzení ekvivalentní:*

(i) p^{n+1} *dělí* M_q,
(ii) p *je Wieferichovo prvočíslo řádu* n,
(iii) $\operatorname{ord}_{p^{n+1}}(2) = q$,
(iv) $2^{p-1} \equiv 1 \pmod{p^{n+1}}$,
(v) $\operatorname{Ord}_p(q_p(2)) \geq n$.[1]

Studii o Mersennových číslech a Jakóbczykově hypotéze zakončíme krátkou poznámkou.

Poznámka 5.5. Franciszek Jakóbczyk [20, str. 127] vyslovil rovněž analogickou hypotézu k Hypotéze 2.1, která se týká Frematových čísel. Základní informace o Fermatových číslech může čtenář nalézt v [26] a [27]. Jakóbczykova hypotéza o Fermatových číslech zasluhuje podobnou pozornost jako Hypotéza 2.1 a je vhodným námětem pro volné pokračování tohoto článku. Konečně problémem podobného typu jako Hypotéza 2.1 je také otázka existence Fibonacci–Wieferichových prvočísel, kterou v roce 1960 formuloval americký matematik Donald Dines Wall (1921–2000). Podrobnosti o tomto problému lze nalézt v autorově článku [23].

[1] Pro každé $x \in \mathbb{N}$ a každé prvočíslo p klademe $\operatorname{Ord}_p(x) = a \in \mathbb{N} \cup \{0\} \iff p^a \mid x$ a $p^{a+1} \nmid x$, $\operatorname{Ord}_p(0) = \infty$.

Reference

[1] T. Agoh, K. Dilcher, L. Skula: *Fermat quotients for composite moduli*, Journal of number theory **66** (1997), 29–50.

[2] R. C. Archibald: *Mersenne's numbers*, Scripta Mathematica **3** (1935), 112–119.

[3] N. Beeger: *On a new case of the congruence* $2^{p-1} \equiv 1 \pmod{p^2}$, Messenger of Mathematics **51** (1922), 149–150.

[4] N. Beeger: *On the congruence* $2^{p-1} \equiv 1 \pmod{p^2}$ *and Fermat's last theorem*, Messenger of Mathematics **55** (1925), 17–26.

[5] N. Beeger: *On the congruence* $2^{p-1} \equiv 1 \pmod{p^2}$ *and Fermat's last theorem*, Nieuw Archief Voor Wiskunde **20** (1939), 51–54.

[6] J. Brillhart, J. Tonascia, P. Weinberger: *On the Fermat quotient*, Computers in Number Theory (1971), 213–222.

[7] P. Bungus: *Numerorum Mysteria*, Bergamo, 1591.

[8] Ch. K. Caldwell: *Proof that all prime-sqared Mersenne divisors are Wieferich*, online `https://primes.utm.edu/notes/proofs/SquareMerDiv.html`.

[9] R. E. Crandall, K. Dilcher, C. Pomerance: *A search for Wieferich and Wilson primes*, Mathematics of Computation **66** (1997), 433–449.

[10] L. E. Dickson: *History of the Theory of Numbers, Vol. I*, Dover Publications, Mineola, 2005.

[11] J. Dobeš, M. Kureš: *Search for Wieferich primes through the use of periodic binary strings*, Serdica Journal of Computing **4** (2010), 293–300.

[12] F. G. Dorais, D. Klyve: *A Wieferich prime search up to* 6.7×10^{15}, Journal of Integer Sequences **14** (2011), Article 11.9.2.

[13] C. E. Fröberg: *Some computations of Wilson and Fermat remainddres*, Mathematics of Computation **12** (1958), 281.

[14] C. E. Fröberg: *On some number-theoretical problems treated with computers*, Computers in Mathematical Research, Amsterdam, 1968.

[15] GIMPS, online `https://www.mersenne.org`.

[16] H. Guy: *Mersenne numbers*, Berkshire, 1990.

[17] R. K. Guy: *Unsolved Problems in Number Theory*, Springer-Verlag, New York, 1981.

[18] R. Haußner: *Über numerische Lösungen der Kongruenz* $u^{p-1} - 1 \equiv 0 \pmod{p^2}$, Journal für die Reine und Angewandte Mathematik **156** (1927), 223–226.

[19] M. Hausner, D. Sachs: *On the congruence* $2^p \equiv 2 \pmod{p^2}$, American Mathematical Monthly **70** (1963), 996.

[20] F. Jakóbczyk: *Les applications de la fonction* $\lambda_g(n)$ *à l'étude des fractions périodiques et de la congruence chinoise* $2^n - 2 \equiv 0 \pmod{n}$, Annales Universitatis Mariae Curie-Skłodowska **5** (1951), 97–138.

[21] W. Johnson: *On the nonvanishing of Fermat quotients* $\pmod{p}$, Journal für die Reine und Angewandte Mathematik **292** (1977), 196–200.

[22] W. Keller, J. Richstein: *Solutions of the congruence* $a^{p-1} \equiv 1 \pmod{p^r}$, Mathematics of Computation **74** (2005), 927–936.

[23] J. Klaška: *Donald Dines Wall's conjecture*, The Fibonacci Quarterly **56** (2018), No. 1, 43–51.

[24] J. Knauer, J. Richstein: *The continuing search for Wieferich primes*, Mathematics of Computation **74** (2005), 1559–1563.

[25] S. Kravitz: *The congruence* $2^{p-1} \equiv 1 \pmod{p^2}$ *for* $p < 100,000$, Mathematics of Computation **14** (1960), 378.

[26] M. Křížek: *O Fermatových číslech*, Pokroky matematiky, fyziky a astronomie **40** (1995), No. 5, 243–253.

[27] M. Křížek, F. Luca, L. Somer: 17 *Lectures on Fermat Numbers, From Number Theory to Geometry*, Canadian Mathematical Society, Springer, 2001.

[28] D. H. Lehmer: *An extended theory of Lucas function*, Annals of Mathematics **31** (1930), 419–448.

[29] D. H. Lehmer: *On Lucas' test for the primality of Mersenne's numbers*, Journal of the London Mathematical Society **10** (1935), 162–165.
[30] D. H. Lehmer: *On Fermat's quotient, base two*, Mathematics of Computation **36** (1981), 289–290.
[31] K. Lepka: *Historie Fermatových kvocientů*, Prometheus, Praha, 2000.
[32] M. Lerch: *Zur Theorie des Fermatschen Quotienten* $(a^{p-1}-1)/p = q(a)$, Mathematische Annalen **60** (1905), 471–490.
[33] M. Lerch: *Sur les théorèmes de Sylvester concernant le quotient de Fermat*, Comptes Rendus de l'Académie des Sciences **142** (1906), 35–38.
[34] P. Ležák: *Hledání Wieferichových prvočísel*, Kvaternion **2** (2013), 103–109.
[35] E. Lucas: *Théorie des fonctions numériques simplement périodiques*, American Journal of Mathematics **1** (1878), 184–240, 289–321.
[36] W. Meissner: *Über die Teilbarkeit von* $2^p - 2$ *durch das Quadrat der Primzahl* $p = 1093$, Sitzungsberichte der Königlich Preußischen Akademie der Wissenschaften, Berlin, 1913, 663–667.
[37] E. M. Mersenne: *Cogitata Physico - Mathematica, in quibustam naturae quam artis effectus admirandi certissimis demonstrationibus explicantur, Praefatio Generalis XIX*, Bertier, Paris, 1644.
[38] P. L. Montgomery: *New solutions of* $a^{p-1} \equiv 1 \pmod{p^2}$, Mathematics of Computation **61** (1993), 361–363.
[39] E. H. Pearson: *On the congruences* $(p-1)! \equiv -1$ *and* $2^{p-1} \equiv 1 \pmod{p^2}$, Mathematics of Computation **17** (1963), 194–195.
[40] H. Piersa: *Śp. Ksiądz dr Franciszek Jakóbczyk (9 X 1905 – 3 VI 1992)*, Roczniki Filozoficzne **39–40** (1991–1992), spis 3, 5–7.
[41] Š. Porubský: *Fermat a teorie čísel aneb problematika dělitelů a dokonalá čísla*, Cahiers du CEFRES (2002), 49–86.
[42] PrimeGrid, online `https://www.primegrid.com`.
[43] P. Ribenboim: *The new Book of Prime Number Records*, Springer-Verlag, New York, 1996.
[44] H. Riesel: *Note on the congruence* $a^{p-1} \equiv 1 \pmod{p^2}$, Mathematics of Computation **18** (1964), 149–150.
[45] A. Rotkiewicz: *Sur les nombres de Mersenne depourves de diviseurs carres et sur les nombres naturels n, tels que* $n^2|2^n - 2$, Matematičeski vestnik **17** (1965), No. 2, 78–80.
[46] F. Servít: *Eukleidovy Základy (Elementa)*, Jednota českých matematiků, Praha, 1907.
[47] W. Sierpiński: *Co wiemy, a czego nie wiemy o liczbach pierwszych*, Warszawa, 1961.
[48] W. Sierpiński: *A Selection of Problems in the Theory of Numbers*, New York, 1964.
[49] L. Skula: *Prime power divisors of Mersenne numbers and Wieferich primes of higher order*, Integers, Electronic Journal of Combinatorial Number Theory **19** (2019).
[50] J. J. Sylvester: *Sur une propriété des nombres premiers qui se rattache au théorème de Fermat*, Comptes Rendus de l'Académie des Sciences **52** (1861), 161–163.
[51] T. Šalát: *O dokonalých číslach*, Pokroky matematiky, fyziky a astronomie **9** (1964), No. 1, 1–13.
[52] H. S. Uhler: *A brief history of the investigations on Mersenne's numbers and the latest immense primes*, Scripta Mathematica **18** (1952), 121–131.
[53] L. R. Warren, H. G. Bray: *On the squar-freeness of Fermat and Mersenne numbers*, Pacific Journal of Mathematics **22** (1967), 563–564.
[54] A. Wieferich: *Zum letzten Fermat'schen Theorem*, Journal für die Reine und und Angewandte Mathematik **136** (1909), 293–302.

Jiří Klaška, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 616 69 Brno, Česká republika,
e-mail: `klaska@fme.vutbr.cz`