JAKÓBCZYKOVA HYPOTÉZA O FERMATOVÝCH ČÍSLECH

JIŘÍ KLAŠKA

Věnováno profesoru Michalu Křížkovi

Abstrakt. Článek je volným pokračováním předchozí autorovy studie [15], která byla věnována hypotéze polského matematika Franciszka Jakóbczyka (1905-1992) o Mersennových číslech. Neméně zajímavá je Jakóbczykova hypotéza o Fermatových číslech, která tvrdí, že každé Fermatovo číslo je buď prvočíslo, nebo je součinem různých prvočísel. Hypotéza byla poprvé publikována v roce 1951 a její důkaz nebyl do dnešní doby nalezen.

1. Fermatova čísla

Fermatova čísla jsou přirozená čísla tvaru

$$F_n = 2^{2^n} + 1, \text{ kde } n \in \mathbb{N} \cup \{0\}. \tag{1.1}$$

Na základě definice (1.1) můžeme snadno určit hodnoty prvních pěti Fermatových čísel:

$$F_0 = 3,\ F_1 = 5,\ F_2 = 17,\ F_3 = 257,\ F_4 = 65537. \tag{1.2}$$

Čísla F_n poprvé podrobně studoval francouzský matematik Pierre de Fermat (1601–1665) v souvislosti s otázkou, která z čísel tvaru $2^m + 1$, $m \in \mathbb{N} \cup \{0\}$, mohou být prvočísla. Tento problém byl přirozeným rozšířením Fermatových úvah o prvočíselnosti Mersennových čísel, to je čísel $M_m = 2^m - 1$, kde $m \in \mathbb{N} \cup \{0\}$. Připomeňme, že pro Mersennova čísla platí následující zajímavá implikace:

$$\textit{Je-li } 2^m - 1 \textit{ prvočíslo, pak } m \textit{ je prvočíslo.} \tag{1.3}$$

Opačná implikace k implikaci (1.3) ale neplatí, protože například $2^{11} - 1 = 23 \cdot 89$. Ve skutečnosti je do roku 2023 známo pouze 51 Mersennových prvočísel a další se intenzivně hledají [13]. Více podrobností o Mersennových číslech lze nalézt v knihách [7] a [20] nebo též v autorově článku [15].

Pro čísla $2^m + 1$ platí následující tvrzení:

$$\textit{Je-li } 2^m + 1 \textit{ prvočíslo a } m > 1\textit{, pak } m = 2^n \textit{ pro nějaké } n \in \mathbb{N}. \tag{1.4}$$

Je zřejmé, že právě objev implikace (1.4) vedl Fermata ke studiu čísel (1.1), která dnes nazýváme jeho jménem. Další částí příběhu Fermatových čísel bylo zjištění, že

2020 *MSC.* Primární 11A41; Sekundární 11A07, 11-02.
Klíčová slova. Fermatova čísla, Franciszek Jakóbczyk, Wieferichova prvočísla.

všechna čísla uvedená v seznamu (1.2) jsou prvočísla. To vedlo Fermata k formulaci Hypotézy 1.1.

Hypotéza 1.1 (Fermat, 1640)**.** *Každé Fermatovo číslo* $F_n = 2^{2^n} + 1$ *je prvočíslo.*

I když byl Fermat o správnosti Hypotézy 1.1 zcela přesvědčen, její důkaz nepředložil. Naznačoval však, že Hypotézu 1.1 bude možné dokázat metodou nekonečného sestupu [8, str. 375]. Na základě dochované korespondence se rovněž zdá, že další významný francouzský matematik Bernard Frénicle de Bessy (1604–1674) s Fermatovým tvrzením souhlasil. Historické podrobnosti o korespondenci mezi Fermatem a Fréniclem z roku 1640 lze nalézt v Fletcherově článku [11]. Navíc Marin Mersenne (1588–1648) v knize *Novarum Physico-Matematicarum* z roku 1647 uvedl, že každé Fermatovo číslo je prvočíslo. Uvedené skutečnosti byly příčinou, že Hypotéza 1.1 byla považována za dokázané tvrzení a téměř sto následujících let se problémem nikdo nezabýval. Teprve v roce 1732 švýcarský matematik Leonhard Euler (1707–1783) pomocí protipříkladu dokázal, že tvrzení Hypotézy 1.1 není pravdivé. Euler nalezl rozklad čísla

$$F_5 = 4294967297 = 641 \cdot 6700417.$$

Tento objev oživil zájem matematiků o studium Fermatových čísel a jejich vlastností. Eulerovým objevem také vznikla nová otázka, totiž zda Fermatových prvočísel je konečně nebo nekonečně mnoho.

Mezi nejkrásnější doposud dokázaná tvrzení o Fermatových číslech patří věta, kterou dokázal švýcarský matematik Christian Goldbach (1690–1764) a kterou dnes nazýváme Goldbachova věta.

Věta 1.2 (Goldbach, 1730)**.** *Žádná dvě různá Fermatova čísla nejsou dělitelná stejným prvočíslem (tj. nemají společného dělitele většího než jedna).*

Snadným důsledkem Goldbachovy věty je fundamentální matematické tvrzení, totiž že množina všech prvočísel je nekonečná. Další krásné a zcela mimořádné tvrzení objevil a dokázal německý matematik Carl Friedrich Gauss (1777–1855). Toto tvrzení nečekaným způsobem propojilo problematiku Fermatových prvočísel s geometrií.

Věta 1.3 (Gauss, 1796)**.** *Pravidelný mnohoúhelník je eukleidovsky konstruovatelný (tj. pouze pomocí pravítka a kružítka) právě tehdy, když počet jeho vrcholů je roven číslu* $n = 2^r \cdot p_1 \cdots p_s$*, kde* $n \in \mathbb{N}$*,* $n \geq 3$*,* $r, s \in \mathbb{N} \cup \{0\}$ *a* $p_1, \ldots, p_s$ *jsou navzájem různá Fermatova prvočísla.*

Protože doposud nevíme, zda seznam (1.2) obsahuje všechna Fermatova prvočísla, nevíme ani kolik existuje pravidelných mnohoúhelníků, které lze eukleidovsky zkonstruovat. Na základě Gaussovy věty ale víme, že existuje aspoň 31 pravidelných mnohoúhelníků s lichým počtem vrcholů, které lze zkonstruovat pomocí pravítka a kružítka.

V roce 1854 nalezl dánský matematik Thomas Clausen (1801–1885) rozklad čísla

$$F_6 = 18446744073709551617 = 274177 \cdot 67280421310721.$$

Clausen o svém výsledku informoval Gausse v korespondenci ze dne 1. ledna 1855, tedy krátce před Gaussovou smrtí. Gauss zemřel 23. února 1885. Clausenův důležitý objev nebyl nikdy publikován, až v roce 1964 Kurtem Reinhardem Biermannem v historické studii [1, str. 185]. Tato skutečnost vysvětluje, proč jako objevitel rozkladu čísla F_6 je ve většině článků [4, str. 431], [6, str. 175] i knih [7, str. 172], [8, str. 377] uváděn francouzský matematik Fortuné Landry (1799–1895), který rozklad nalezl v roce 1880 a publikoval v *Comptes rendus* [21]. Analýzou Landryho výsledku se podrobně věnoval H. C. Williams v článku [39]. Mezi literární zdroje, které uvádí informaci o prvním objeviteli rozkladu Fermatova čísla F_6 správně, jsou například velmi obsažné a kvalitní knihy [20, 32]. To, že se informace o Biermannově článku šíří matematickou komunitou jen pomalu, svědčí poznámka v knize Paula Ribenboima [32, str. 85] z roku 1996, kde sděluje, že na Biermannovu studii ho upozornil jeho kolega A. Hinz.

Důležitou větu, která popisuje tvar prvočíselných dělitelů Fermatových čísel publikoval v roce 1878 [24] francouzský matematik François Édouard Anatole Lucas (1842–1891).

Věta 1.4 (Lucas, 1878)**.** *Nechť $m \in \mathbb{N}$, $m > 1$ a nechť p je libovolné prvočíslo takové, že $p \mid F_m$. Pak $p \equiv 1 \pmod{2^{m+2}}$. To znamená, že p je tvaru $p = k \cdot 2^n + 1$, kde $k, n \in \mathbb{N}$ a $n \geq m + 2$.*

V roce 1903 Alfred Edward Western [6] úspěšně použil Lucasovu větu k nalezení prvočíselných dělitelů několika Fermatových čísel:

$$37 \cdot 2^{16} + 1 \mid F_9,\ 397 \cdot 2^{16} + 1 \mid F_{12},\ 7 \cdot 139 \cdot 2^{16} + 1 \mid F_{12},\ 13 \cdot 2^{20} + 1 \mid F_{18}. \quad (1.5)$$

Do druhé světové války pak bylo nalezeno několik dalších dělitelů Fermatových čísel, ale žádný výrazný pokrok ve studiu problematiky Fermatových čísel nenastal. S nástupem počítačů bylo logické očekávat, že nové výpočetní možnosti přinesou nové výsledky a další kompletní rozklady Fermatových čísel. To nastalo až v roce 1970, kdy Michael A. Morrison a John Brillhart [26] objevili rozklad Fermatova čísla F_7:

$$F_7 = 59649589127497217 \cdot 5704689200685129054721.$$

Pro další výklad bude vhodné zavést, v souladu s označením [4, str. 429], následující konvenci. Pro dané $n \in \mathbb{N}$ nechť P_n označuje prvočíslo mající v dekadické soustavě právě n cifer a a C_n nechť označuje složené přirozené číslo mající právě n cifer. Bude-li v dalším textu třeba rozlišit dvě různá prvočísla se stejným počtem cifer, použijeme u jednoho z čísel jako horní index symbol hvězdička. Zavedenou konvenci použijeme již při formulaci následujícího objevu. V roce 1980 nalezli Richard P. Brent a John M. Pollard [3] kompletní rozklad Fermatova čísla F_8:

$$F_8 = 1238926361552897 \cdot P_{62},$$

kde

$$P_{62} = 93461639715357977769163558199606896585051237541638188580280321.$$

V roce 1990 A. K. Lestra, H. W. Lestra, M. S. Manasse a J. M. Pollard [23] za asistence mnoha spolupracovníků a využití přibližně různých 700 pracovišť dokončili rozklad Fermatova čísla F_9:

$$F_9 = 2424833 \cdot 7455602825647884208337395736200454918783366342657 \cdot P_{99},$$

kde

$$\begin{aligned} P_{99} = {} & 7416400626275308015247871419019374740599407810975 1 \\ & 9023905821316144415759504705008092818711693940737. \end{aligned}$$

Připomeňme, že faktor $2424833 = 37 \cdot 2^{16} + 1$ objevil již Western v roce 1903, viz (1.5).

V roce 1995 nalezl Richard P. Brand [4] kompletní rozklad čísla F_{10}:

$$F_{10} = 45592577 \cdot 6487031809 \cdot 4659775785220018543264560743076778192897 \cdot P_{252},$$

kde

$$\begin{aligned} P_{252} = {} & 1304398744054881897274847687965099039466085308416118921868952957 \\ & 7768324162514718635741402279775731048958987839288429238448311497 \\ & 0329137987290886016179460941194490105959067101305319061710183547 \\ & 4916096191939124885381160807122996723228062178207531270144245777. \end{aligned}$$

Pro úplnost poznamenejme, že faktor 45592577 objevil již v roce 1953 Selfridge a faktor 6487031809 nalezl Brillhart v roce 1962.

Je jistě pozoruhodné, že rozklad Fermatova čísla F_{11} byl znám dříve než kompletní rozklady čísel F_9 a F_{10}. Rozklad čísla F_{11} byl nalezen již v roce 1988 a má tvar

$$F_{11} = 319489 \cdot 974849 \cdot 167988556341760475137 \cdot 3560841906445833920513 \cdot P_{564}.$$

Faktory 319489 a 974849 čísla F_{11} objevil již v roce 1899 Cunningham [6, str. 175]. Hlavní, zbývající část rozkladu čísla F_{11} nalezl Richard P. Brand [2]. Přesnou hodnotu velkého prvočísla P_{564} může čtenář nalézt například v knize [20, str. 209].

Kompletní rozklad čísla F_{12} a ani žádného dalšího Fermatova čísla není do roku 2023 znám. Částečný rozklad čísla F_{12} má tvar

$$\begin{aligned} F_{12} = {} & 114689 \cdot 26017793 \cdot 63766529 \cdot 190274191361 \cdot 1256132134125569 \cdot \\ & 5686306475353569551690334109408678048393607420608184 33 \cdot C_{1133}. \end{aligned}$$

Faktor 114689 objevili v roce 1877 Lucas a Pervouchine, faktory 26017793 a 63766529 nalezl v roce 1903 Western, faktor 190274191361 objevili v roce 1974 Hallyburton a Brillhart a faktor 1256132134125569 nalezl v roce 1986 Baillie. Poslední pokrok v rozkladu čísla F_{12} nastal v roce 2010, kdy Michael Vang objevil faktor

$$P_{54} = 5686306475353569551690334109408678048393607420608184 33.$$

Problém určit všechny prvočíselné dělitele složeného čísla C_{1133} je jednou z velkých výzev před kterými výzkumníci Fermatových čísel v současné době stojí. Pokud je

číslo C_{1133} rovno součinu dvou přibližně stejně velkých prvočísel, pak může nalezení jeho rozkladu trvat ještě velmi dlouhou dobu. Na druhé straně nelze vyloučit, že pokrok v konstrukci kvantových počítačů spolu s objevy nových postupů faktorizace přirozených čísel umožní rozložit toto číslo mnohem rychleji, než si dnes dokážeme představit. Sledovat další vývoj faktorizace čísla C_{1133} může být proto velmi zajímavé a poučné. Aktuální informace o nově nalezených dělitelích Fermatových čísel F_n je možné sledovat například na internetové stránce *Distributed Search for Fermat Number Divisors* [9] nebo na stránce *Prime factors* $k \cdot 2^n + 1$ *of Fermat numbers* F_m *and complete factoring status* [29]. Internetové stránky [9] a [29] nejsou jedinými stránkami, které se Fermatovými čísly zabývají. Seznam dalších stránek lze nalézt v [20, str. 243].

Vědomosti dosažené o prvočíselných rozkladech Fermatových čísel $F_5, \cdots, F_{12}$ za 383 let jejich výzkumu (1640–2023) lze shrnout do následujícího chronologického přehledu.

$$\begin{aligned}
F_5 &= P_3 \cdot P_7, && (1732)\\
F_6 &= P_6 \cdot P_{14}, && (1854)\\
F_7 &= P_{17} \cdot P_{22}, && (1970)\\
F_8 &= P_{16} \cdot P_{62}, && (1980)\\
F_9 &= P_7 \cdot P_{49} \cdot P_{99}, && (1990)\\
F_{10} &= P_8 \cdot P_{10} \cdot P_{40} \cdot P_{252}, && (1995)\\
F_{11} &= P_6 \cdot P_6^* \cdot P_{21} \cdot P_{22} \cdot P_{564}, && (1988)\\
F_{12} &= P_6 \cdot P_8 \cdot P_8^* \cdot P_{12} \cdot P_{16} \cdot P_{54} \cdot C_{1133}. && (2023)
\end{aligned} \tag{1.6}$$

Připomeňme také, že již v roce 1925 byl zahájen obecněji zaměřený projekt, který se zabývá prvočíselnými rozklady čísel tvaru $b^n \pm 1$, která se nazývají Cunninghamova čísla. Tento název byl zaveden na počest Allana J. C. Cunninghama (1842–1928), který spolu s Herbertem J. Woodallem tento projekt založili. Výsledkem jejich snažení je, že v dnešní době existují již tři tištěné verze tabulek rozkladů čísel $b^n \pm 1$, z nichž nejnovější je z roku 2002. Největší přínos projektů [9, 13, 29] a jim podobným, spočívá ve vytváření nových efektivních metod pro testování prvočíselnosti a pro hledání kompletních prvočíselných rozkladů přirozených čísel. Tyto metody mají v dnešní době velký strategický význam.

Konečně je vhodné připomenout, že o problematice Fermatových čísel byly napsány stovky publikací. Čtenáře lze odkázat například na patnáctou kapitolu prvního svazku známé Dicksonovy *Historie teorie čísel* [8], ve které jsou shrnuty nejdůležitější objevy o Fermatových číslech do roku 1919. Dále pak na knihy [7, 20], nebo na články našich autorů Eduarda Fuchse [12, str. 70–74], Michala Křížka [18, 19], Karla Lepky [22, str. 148] a Štefana Porubského [28].

2. Jakóbczykova hypotéza

V roce 1951 publikoval polský kněz a matematik Franciszek Jakóbczyk (1905–1992) dva zajímavé a obtížné problémy týkající Fermatových a Mersennových čísel. Původní formulace hypotéz byla uveřejněna ve francouzštině [14, str. 127]:

Hypothèse. *Les nombres de Fermat et de Mersenne sont des nombres impairs du type* $n = p_1 \cdot p_2 \cdots p_k$ *où* $k \geq 1$.

O Jakóbczykově hypotéze, která se týká Mersennových čísel se zmiňuje známý polský matematik Wacław Sierpiński (1882–1969) v knize *Co wiemy a czego nie wiemy o liczbach pierwszych* [33, str. 70], která byla publikována ve Varšavě v roce 1961. Tuto hypotézu lze rovněž nalézt v Sierpińského knize *A Selection of Problems in the Theory of Numbers* [34, str. 92], která vyšla v New Yorku v roce 1964. Ve skutečnosti druhá část knihy [34, str. 25–97] obsahuje anglický překlad polského originálu [33]. Je zajímavé, že Sierpiński do svých knih nezařadil také formulaci Jakóbczykovy hypotézy o Fermatových číslech. Tato skutečnost je možná jednou z příčin, proč dodnes není Jakóbczykovo jméno v souvislosti s jeho hypotézou o Fermatových číslech uváděno. Podrobnosti o životě a díle Franciszka Jakóbczyka může čtenář nalézt v článku [27].

Připomeňme, že Jakóbczykově hypotéze týkající se případu Mersennových čísel je věnována samostatná přehledová studie [15]. V souvislosti s Mersennovými čísly je také vhodné upozornit na dvě nedávné autorovy publikace [16] a [17]. Článek [16] je věnován alternativnímu důkazu hlavní Skulovy věty prezentované v [35]. Viz též [15, str. 55]. V [17] je pak Skulova věta zobecněna pro případ Cunninghamových čísel $b^n \pm 1$.

Zaměřme nyní pozornost na Jakóbczykovu hypotézu o Fermatových číslech.

Hypotéza 2.1 (Jakóbczyk, 1951)**.** *Každé Fermatovo číslo* $F_n = 2^{2^n} + 1$ *je buď prvočíslo nebo je součinem různých prvočísel.*

Je zřejmé, že Hypotézu 2.1 lze formulovat následujícím ekvivalentním způsobem:

Žádné Fermatovo číslo není dělitelné druhou mocninou prvočísla.

I když se Hypotéza 2.1 objevuje ve známých knihách [7, str. 192], [20, str. 160] a [32, str. 88], z nichž [7] a [20] jsou speciálně věnovány Fermatovým číslům, neobsahují tyto publikace žádné informace o jejím autoru, ani o době jejího vzniku.

Pro formulaci hlavních výsledků dosažených o Hypotéze 2.1 bude vhodné připomenout některé základní definice. Nechť $a, m \in \mathbb{N}$, $m \geq 2$ a nechť $\gcd(a, m) = 1$. Pak číslo

$$q_m(a) = \frac{a^{\varphi(m)} - 1}{m} \tag{2.1}$$

se nazývá Eulerův kvocient čísla m se základem a. Číslo $\varphi(m)$ vyskytující se v definičním vztahu (2.1) je rovno počtu všech $k \in \mathbb{N}$, kde $1 \leq k \leq m$, která jsou nesoudělná s m. Funkce φ se nazývá Eulerova funkce. Podle Eulerovy věty (viz například [7, str. 14], [20, str. 20]) platí, že $a^{\varphi(m)} \equiv 1 \pmod{m}$. Odtud plyne, že $q_m(a)$ je celé číslo. Je-li m prvočíslo, pak $\varphi(m) = m - 1$ a kvocient (2.1) se nazývá Fermatův kvocient. Podrobnější informace může čtenář nalézt v [15, str. 51–52]. Dále, nejmenší číslo $k \in \mathbb{N}$ takové, že $a^k \equiv 1 \pmod{m}$ se nazývá multiplikativní řád čísla a modulo m a označuje se $\operatorname{ord}_m(a)$. Základní vlastnosti multiplikativního řádu lze nalézt například v [7, str. 30] nebo v [17, str. 3–4].

V roce 1909 dokázal německý matematik Arthur Wieferich (1884–1954) pozoruhodné tvrzení, týkající se prvního případu velké Fermatovy věty [38].

Věta 2.2 (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. Na základě výše uvedených definic není obtížné dokázat, že podmínky (i)–(iii) jsou ekvivalentní:

$$\begin{aligned} &\text{(i)} \quad 2^{p-1} \equiv 1 \pmod{p^2}, \\ &\text{(ii)} \quad q_p(2) \equiv 0 \pmod{p}, \\ &\text{(iii)} \quad \operatorname{ord}_{p^2}(2) = \operatorname{ord}_p(2). \end{aligned} \tag{2.2}$$

Je jistě zajímavé, že v roce 1909, kdy Arthur Wieferich svoje slavné tvrzení dokázal, nebylo žádné Wieferichovo prvočíslo ještě známo. Do dnešní doby byla objevena pouze dvě prvočísla splňující (2.2). První, $w_1 = 1093$, objevil v roce 1913 Waldemar Meissner [25] a druhé, $w_2 = 3511$, objevil v roce 1922 Nicolas Beeger [5]. Podrobná historická fakta týkající se Wieferichových prvočísel jsou uvedena v článku [15, str. 52–54]. Připomeňme, že nedávný projekt *PrimeGrid* [30] zaměřený na hledání Wieferichových prvočísel prokázal, že třetí Wieferichovo prvočíslo, pokud existuje, musí být větší než

$$2^{64} = 18446744073709551616 \doteq 1{,}8 \cdot 10^{19}. \tag{2.3}$$

Projekt *PrimeGrid* byl ukončen v prosinci 2022. Tedy ani po sto letech od Beegerova objevu nebylo přes velkou snahu mnoha matematiků další Wieferichovo prvočíslo nalezeno. Sám Beeger v roce 1939 vyslovil domněnku, že žádné další Wieferichovo prvočíslo již neexistuje.

První důležité tvrzení, které propojilo Jakóbczykovu hypotézu o Fermatových číslech s Wieferichovými prvočísly dokázali v roce 1967 Le Roy J. Warren a Henry G. Bray [37].

Věta 2.3 (Warren, Bray, 1967)**.** *Nechť $n \in \mathbb{N}$, $n > 1$ a nechť p je libovolné liché prvočíslo. Jestliže $p \mid F_n$, pak*

$$2^{\frac{p-1}{2}} \equiv 1 \pmod{F_n}.$$

Z Věty 2.3 snadno plyne následující důsledek.

Důsledek 2.4. *Nechť $n \in \mathbb{N}$, $n > 1$ a nechť p je libovolné liché prvočíslo. Jestliže $p^2 \mid F_n$, pak p je Wieferichovo prvočíslo, tj. $2^{p-1} \equiv 1 \pmod{p^2}$.*

Protože v článku [37] není důkaz Důsledku 2.4 uveden, uvedeme důkaz nyní.

Důkaz. Předpokládejme, že $p^2 \mid F_n$. Pak $p \mid F_n$ a podle Věty 2.3 platí $2^{(p-1)/2} \equiv 1 \pmod{F_n}$. To však znamená, že $F_n \mid (2^{(p-1)/2} - 1)(2^{(p-1)/2} + 1) = 2^{p-1} - 1$. Protože relace dělitelnosti $\mid$ je tranzitivní, konjunkce podmínek $p^2 \mid F_n$ a $F_n \mid 2^{p-1} - 1$ implikuje $p^2 \mid 2^{p-1} - 1$. Tato relace ale podle části (i) vztahu (2.2) znamená, že p je Wieferichovo prvočíslo. □

V roce 1979 Paulo Ribenboim [31, str. 86–88] publikoval následující dvě tvrzení.

Věta 2.5 (Ribenboim, 1979)**.** *Nechť $n \in \mathbb{N}$, $n \geq 2$ a nechť p je libovolné prvočíslo. Jestliže $p^2 \mid F_n$, pak $p = k \cdot 2^r + 1$, kde $k, r \in \mathbb{N}$, $r \geq n+2$, k je liché a*

$$q_p(k) = \frac{k^{p-1} - 1}{p} \equiv 1 \pmod{p}.$$

Věta 2.6 (Ribenboim, 1979)**.** *Nechť $a, n \in \mathbb{N}$, $a \geq 2$ a nechť p je libovolné liché prvočíslo. Jestliže $p \mid F_{a,n} = a^{a^n} + 1$ a $q_p(a) \equiv 0 \pmod{p}$, pak $p^2 \mid F_{a,n}$.*

Speciálně, je-li $a = 2$, pak Věta 2.6, společně s částí (ii) vztahu (2.2), zaručuje platnost následující implikace:

$$\text{Jestliže } p \mid F_n \text{ a } 2^{p-1} \equiv 1 \pmod{p^2}, \text{ pak } p^2 \mid F_n. \tag{2.4}$$

Důsledek 2.4 spolu s implikací (2.4) pak dokazuje platnost Věty 2.7.

Věta 2.7. *Nechť $n \in \mathbb{N} \cup \{0\}$, $a \geq 2$ a nechť p je libovolné liché prvočíslo. Jestliže $p \mid F_n$, pak $p^2 \mid F_n$ právě tehdy, když $2^{p-1} \equiv 1 \pmod{p^2}$.*

Kompletní důkaz Věty 2.7 lze nalézt v [20, str. 68]. Z důvodu historické korektnosti poznamenejme, že autorství implikace (2.4) není zcela zřejmé. Michal Křížek v článku [18, str. 252] nepřímo uvádí jako autora Věty 2.7 Wilfrida Kellera a odkazuje zde čtenáře na nepublikovaný Kellerův rukopis. Také odkazy uvedené v [20, str. 68] původ implikace (2.4) neobjasňují. Kromě toho, Paulo Ribenboim v [31, str. 87] uvádí, že jeho Věta 2.6 je přeformulováním výsledků uvedených v článku [10], jehož autorkou je Jeanne Ferentinou–Nicolacopoulou.

V souvislosti s Větou 2.7 je rovněž vhodné zmínit, že v roce 2023 autor tohoto článku publikoval tvrzení (viz [17, str. 19]), které zjednodušuje logickou strukturu Věty 2.7 následujícím způsobem:

Věta 2.8 (Klaška, 2023)**.** *Nechť $n \in \mathbb{N} \cup \{0\}$ a nechť p je libovolné liché prvočíslo. Pak $p^2 \mid F_n$ právě tehdy, když p je Wieferichovo prvočíslo a $\operatorname{ord}_p(2) = 2^{n+1}$.*

Není obtížné ověřit, že pro jediná dvě známá Wieferichova prvočísla platí

$$\operatorname{ord}_{1093}(2) = \operatorname{ord}_{1093^2}(2) = 364 = 2^2 \cdot 7 \cdot 13,$$
$$\operatorname{ord}_{3511}(2) = \operatorname{ord}_{3511^2}(2) = 1755 = 3^3 \cdot 5 \cdot 13.$$

Odtud a z (2.3) nyní plyne, že žádné Fermatovo číslo není dělitelné druhou mocninou žádného prvočísla p, kde $p < 1{,}8 \cdot 10^{19}$. Zkoumání četnosti výskytu prvočísel p splňujících podmínku $\operatorname{ord}_p(2) = 2^k$ pro nějaké $k \in \mathbb{N}$ vede rovněž k zajímavým závěrům. Například je známo, že pro $p < 4{,}18 \cdot 10^{18}$ existuje pouze padesát prvočísel splňujících podmínku $\operatorname{ord}_p(2) = 2^k$ pro nějaké $k \in \mathbb{N}$. Seznam těchto prvočísel je následující:

3, 5, 17, 257, 641, 65537, 114689, 274177, 319489, 974849, 2424833, 6700417, 13631489, 26017793, 45592577, 63766529, 167772161, 825753601, 1214251009, 6487031809, 70525124609, 190274191361, 646730219521, 2710954639361, 2748779069441, 4485296422913, 6597069766657, 25409026523137, 25991531462657, 31065037602817, 46179488366593, 67280421310721,

76861124116481, 151413703311361, 640126220763137, 1095981164658689, 1238926361552897, 1256132134125569, 2327042503868417, 2405286912458753, 2917004348489729, 59649589127497217, 204393464266227713, 231292694251438081, 1033434552359452673, 1529992420282859521, 2170072644496392193, 2663848877152141313, 3603109844542291969, 4179340454199820289.

Dále je možné dokázat [20, str. 37], že prvočísla uvedená v tomto seznamu jsou právě ta prvočísla, která dělí některé z Fermatových čísel. Přesněji formulováno, platí Věta 2.9.

Věta 2.9. *Nechť $n \in \mathbb{N} \cup \{0\}$ a nechť p je libovolné liché prvočíslo. Pak $p \mid F_n$ právě tehdy, když* $\operatorname{ord}_p(2) = 2^{n+1}$.

Více informací o posloupnosti prvočíselných dělitelů Fermatových čísel lze nalézt na webové stránce *The On-Line Encyclopedia of Integer Sequences* [36, A023394] a také v knize [20, str. 37].

Článek zakončíme formulací Problému 2.10, který byl inspirován přehledem známých rozkladů Fermatových čísel uvedených v (1.6), viz [20, str. 159] a [18, str. 249].

Problém 2.10 (Křížek, 1995)**.** *Dokažte nebo vyvraťte následující tvrzení. Nechť $\delta(F_n)$ označuje počet všech prvočíselných dělitelů Fermatova čísla F_n. Pak pro každé $n \in \mathbb{N} \cup \{0\}$ platí $\delta(F_n) \leq \delta(F_{n+1})$.*

Z přehledu (1.6) okamžitě vidíme, že

$$(\delta(F_n))_{n=0}^{\infty} = (1, 1, 1, 1, 1, 2, 2, 2, 2, 3, 4, 5, \ldots).$$

Je zřejmé, že pokud je posloupnost $(\delta(F_n))_{n=0}^{\infty}$ neklesající, pak seznam (1.2) obsahuje všechna Fermatova prvočísla. Speciální část Problému 2.10, která se týká výskytu prvočísel v posloupnosti $(F_n)_{n=0}^{\infty}$, lze formulovat jako samostatnou hypotézu, viz [20, str. 163].

Hypotéza 2.11 (Křížek, 1995)**.** $\delta(F_n) = 1$ *právě tehdy, když* $n \leq 4$.

Na základě našich současných vědomostí můžeme předpokládat, že řešení problémů formulovaných Michalem Křížkem a nalezení důkazu Jakóbczykovy hypotézy bude velmi obtížné. Nelze ani vyloučit, že řešení těchto jednoduše formulovatelných problémů leží zcela mimo hranice lidských možností.

Reference

[1] K. R. Biermann: *Thomas Clausen, Mathematiker und Astronom*, Journal für die Reine und Angewandte Mathematik **216** (1964), 159–198.

[2] R. P. Brent: *Factorization of the eleventh Fermat number*, Abstracts Amer. Math. Soc. **10** (1989), 176–177.

[3] R. P. Brent, J. M. Pollard: *Factorization of the eighth Fermat number*, Mathematics of Computation **36** (1981), 627–630.

[4] R. P. Brent: *Factorization of the tenth Fermat number*, Mathematics of Computation **68** (1999), 429–451.
[5] N. Beeger: *On a new case of the congruence* $2^{p-1} \equiv 1 \pmod{p^2}$, Messenger of Mathematics **51** (1922), 149–150.
[6] A. J. Cunningham, A. E. Western: *On Fermats numbers*, Proc. London Math. Soc. **(2)1** (1904), 175.
[7] E. Deza: *Mersenne Numbers and Fermat Numbers, Selected Chapters of Number Theory: Special Numbers*, World Scientific, 2021.
[8] L. E. Dickson: *History of the Theory of Numbers*, Vol. I, Dover Publications, 2005.
[9] Distributed Search for Fermat Number Divisors, online http://www.fermatsearch.org.
[10] J. Ferentinou–Nicolacopoulou: *Une propriété des diviseurs du nombre* $r^{r^m}+1$. *Applications au dernier théorème de Fermat*, Bulletin of the Greek Mathematical Society **4** (1963), 121–126.
[11] C. R. Fletcher: *A reconstruction Frenicle–Fermat correspondence of 1640*, Historia Mathematica **18.4** (1991), 344–351.
[12] E. Fuchs: *Co ještě nevíme o přirozených číslech (2) aneb Od dokonalých čísel k Fermatovým prvočíslům*, Učitel matematiky **7.2** (1999), 65–74.
[13] Great Internet Mersenne Prime Search, online https://www.mersenne.org.
[14] 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.
[15] J. Klaška: *Hypotéza Franciszka Jakóbczyka o Mersennových číslech*, Kvaternion (2021), 47–57.
[16] J. Klaška: *A simple proof of Skula's theorem on prime power divisors of Mersenne numbers*, Journal of Integer Sequences **25** (2022), Article 22.4.3.
[17] J. Klaška: *Jakóbczyk's hypothesis on Mersenne numbers and generalizations of Skula's theorem*, Journal of Integer Sequences **26** (2023), Article 23.3.8.
[18] M. Křížek: *O Fermatových číslech*, Pokroky matematiky, fyziky a astronomie **40.5** (1995), 243–253.
[19] M. Křížek: *Od Fermatových prvočísel ke geometrii*, Cahiers du CEFRES, (2002), 131–161.
[20] M. Křížek, F. Luca, L. Somer: 17 *Lectures on Fermat Numbers, From Number Theory to Geometry*, Canadian Mathematical Society, Springer, 2001.
[21] F. Landry: *Note sur la décomposition du nombre* $2^{64}+1$, Comptes rendus de l'Académie des Sciences A **91** (1880), 138.
[22] K. Lepka: *Malá Fermatova věta*, Učitel matematiky **5.3** (1997), 143–150.
[23] A. K. Lenstra, H. W. Lenstra, M. S. Manasse, J. M. Pollard: *The factorization of the ninth Fermat number*, Mathematics of Computation **61** (1993), 319–349.
[24] E. Lucas: *Théorèmes d'arithmétique*, Atti della Reale Accademia delle Scienze di Torino **13** (1878), 271–284.
[25] 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.
[26] M. A. Morrison, J. Brillhart: *The factorization of* F_7, Bull. Amer. Math. Soc. **77** (1971), 264.
[27] H. Piersa: *Śp. Ksiądz dr Franciszek Jakóbczyk (9 X 1905 – 3 VI 1992)*, Roczniki Filozoficzne **39–40**, spis 3, (1991–1992), 5–7.
[28] Š. Porubský: *Fermat a teorie čísel aneb problematika dělitelů a dokonalá čísla*, Cahiers du CEFRES, 2002, 49–86.
[29] Prime factors $k \cdot 2^n + 1$ of Fermat numbers F_m and complete factoring status (compiled by Wilfrid Keller), online http://www.prothsearch.com/fermat.html.
[30] PrimeGrid, online https://www.primegrid.com.
[31] P. Ribenboim: *On the square factors of the numbers of Fermat and Ferentinou- Nicolacopoulou*, Bulletin of the Greek Mathematical Society **20** (1979), 81–92.

[32] P. Ribenboim: *The new Book of Prime Number Records*, Springer-Verlag, New York, 1996.
[33] W. Sierpiński: *Co wiemy, a czego nie wiemy o liczbach pierwszych*, Warszawa, 1961.
[34] W. Sierpiński: *A Selection of Problems in the Theory of Numbers*, New York, 1964.
[35] L. Skula: *Prime power divisors of Mersenne numbers and Wieferich primes of higher order*, Integers, Electronic Journal of Combinatorial Number Theory **19** (2019).
[36] The On-Line Encyclopedia of Integer Sequences (OEIS), online https://oeis.org.
[37] L. R. Warren, H. G. Bray: *On the square-freeness of Fermat and Mersenne numbers*, Pacific Journal of Mathematics **22** (1967), 563–564.
[38] A. Wieferich: *Zum letzten Fermat'schen Theorem*, Journal für die Reine und und Angewandte Mathematik **136** (1909), 293–302.
[39] H. C. Williams: *How was F_6 factored?*, Mathematics of Computation **61** (1993), 463–474.

Jiří Klaška, Ústav matematiky, Fakulta strojního inženýrství, Vysoké učení technické v Brně, Technická 2, 61669 Brno, Česká republika,
e-mail: klaska@fme.vutbr.cz