Pokroky matematiky, fyziky a astronomie

Michal Křížek; Lawrence Somer

Pseudoprvočísla

Pokroky matematiky, fyziky a astronomie, Vol. 48 (2003), No. 2, 143–151

Persistent URL: http://dml.cz/dmlcz/141171

Pseudoprvočísla

Michal Křížek, Praha, a Lawrence Somer, Washington

Čísla jsou jediná univerzální řeč ve vesmíru.
NATHANAEL WEST

1. Úvod

Studiem prvočísel a jejich mnohdy překvapivými vlastnostmi se zabývá lidstvo už několik tisíciletí. Teprve ve 20. století se však přišlo na to, že prvočísla mají také řadu užitečných aplikací. Např. rodná čísla od roku 1986 jsou utvářena tak, aby byla dělitelná prvočíslem 11. Počítač totiž okamžitě odhalí chybu, jakmile se při zadávání rodného čísla zmýlíme v jedné jeho cifře.[1]) To je jeden z příkladů tzv. samodetekujících se kódů. Poněkud komplikovanějším jedenáctkovým kódem jsou chráněna proti případné chybě i čísla bankovních účtů, identifikační čísla organizací, čísla ISSN časopisů, čísla ISBN publikací aj. Větší prvočísla, jež mají až sto cifer, se používají v moderních kryptografických systémech s veřejným šifrovacím klíčem (např. v metodě RSA pro přenos tajných zpráv). Také digitální podpis, jehož zavedení do života nedávno schválil náš parlament, je založen na velkých prvočíslech. Pomocí prvočísel lze konstruovat efektivní generátory pseudonáhodných čísel nebo navrhovat algoritmy pro velmi rychlé násobení velkých čísel. Prvočísla mají řadu aplikací i při zpracování signálu pomocí číselně teoretických transformací a byla již několikrát použita v poselstvích mimozemským civilizacím. Jejich další aplikace lze nalézt např. v [17].

V tomto článku si představíme speciální třídu složených čísel — pseudoprvočísla, která vykazují některé vlastnosti jako prvočísla. Podáme přehled jejich základních charakteristik, uvedeme mj. tvrzení o jejich asymptotické hustotě a ukážeme, že jejich výskyt je mnohem vzácnější než výskyt prvočísel. Například jen 3 pseudoprvočísla jsou menší než 1000, zatímco ve stejném intervalu je 168 prvočísel. Zavedeme také zajímavou množinu Carmichaelových čísel a popíšeme některé algoritmy pro generování pseudoprvočísel.

[1]) Pak rozdíl mezi správným a špatně zadaným číslem bude $\pm c \cdot 10^k$, kde $c \in \{1, 2, \ldots, 9\}$, což nikdy není dělitelné 11 (ale může být dělitelné složenými čísly 12, 14, 15, 16, ..., a proto složená čísla nejsou pro tyto účely vhodná). Jestliže se zmýlíme ve více cifrách, potom s velkou pravděpodobností přibližně 10/11 počítač rovněž odhalí chybu.

Prof. RNDr. MICHAL KŘÍŽEK, DrSc. (1952), Matematický ústav Akademie věd ČR, Žitná 25, 115 67 Praha 1, e-mail: krizek@math.cas.cz

Prof. Dr. LAWRENCE SOMER (1948), Department of Mathematics, Catholic University of America, Washington, D. C., 20064, USA, e-mail: somer@cua.edu

Předneseno na semináři *Dějiny matematiky* na Stavební fakultě ČVUT dne 25. února 2003.

2. Co je pseudoprvočíslo?

Pro definování pojmu „pseudoprvočíslo“ budeme potřebovat Malou Fermatovu větu, která určuje základní vlastnosti prvočísel a na níž je založena většina pravděpodobnostních algoritmů pro testování prvočíselnosti.[2]) Malá Fermatova věta tak hraje klíčovou roli v teorii čísel. Většinou se uvádí ve dvou ekvivalentních verzích. První verze říká, že pokud p je prvočíslo, pak

$$a^p \equiv a \pmod{p}$$

pro všechna celá čísla a (jinými slovy, p dělí $a^p - a$ beze zbytku). Podle druhé verze, když p je prvočíslo nesoudělné s a, pak

$$a^{p-1} \equiv 1 \pmod{p}. \tag{1}$$

Obrácené tvrzení k Malé Fermatově větě bohužel neplatí. Pro libovolný základ $a > 1$ existuje složené číslo n nesoudělné s a tak, že

$$a^n \equiv a \pmod{n}. \tag{2}$$

Například složené číslo $n = 341 = 31 \times 11$ splňuje (2) pro $a = 2$. Snadno totiž vypočteme, že $2^{10} \equiv 1 \pmod{341}$. Umocněním na třicátou čtvrtou dostaneme $2^{340} \equiv 1 \pmod{341}$, tj. platí (1). Vynásobíme-li ještě poslední kongruenci dvěma, dostaneme

$$2^{341} \equiv 2 \pmod{341}, \tag{3}$$

tj. platí i vztah (2). Pro jiný základ $a = 3$ lze odvodit, že $3^{340} \equiv 56 \pmod{341}$, což podle (1) znamená, že 341 je složené číslo (aniž bychom prováděli jeho rozklad na prvočísla).

Definice. Složené přirozené číslo n se nazývá *pseudoprvočíslo o základu* a, pokud platí (2), tj. jestliže n dělí $a^n - a$.

Poznamenejme ještě, že pokud jsou čísla a a n nesoudělná, pak (2) platí, právě když

$$a^{n-1} \equiv 1 \pmod{n}. \tag{4}$$

3. Několik historických poznámek

První pseudoprvočíslo 341 o základu 2 bylo nalezeno v roce 1819 Pierrem F. Sarrusem[3]) (viz [8, s. 92] nebo Annales de Math. *10* (1819), 184–187), který ukázal platnost kongruence (3).

[2]) V roce 2002 M. Agrawal, N. Kayal a N. Saxena zveřejnili článek *Primes is in P*, kde je popsán nový deterministický algoritmus pro testování prvočíselnosti, který je polynomiální v čase. Pro zadané číslo n je jeho výpočetní složitost $\mathcal{O}((\log n)^{12})$, a proto se zatím pro praktické účely nepoužívá.

[3]) Pierre Frédérique Sarrus je známý zejména svými jednoduchými vztahy pro výpočet determinantů čtvercových matic řádu 2 nebo 3.

Podle [26] vlastnost (3) čísla 341 byla rovněž zaznamenána anonymním autorem článku *Théorèmes et problèmes sur les nombres*, který byl publikován v Journal für die reine und angewandte Mathematik *6* (1830), 100–106.

Také János Bolyai (1802–1860), jeden ze zakladatelů neeuklidovských geometrií, informoval svého otce (viz [14]) o objevu pseudoprvočísla 341 v dopise z května 1855. Navíc podle [14, s. 72] Bolyai byl první, kdo ukázal, že Fermatovo číslo $F_5 = 2^{32} + 1 = 641 \times 6700417$ je pseudoprvočíslo o základu 2. Jeho důkaz byl založen na kongruenci

$$2^{2^{32}} \equiv 1 \pmod{F_5}.$$

V roce 1909 T. Banachiewicz publikoval 5 pseudoprvočísel o základu 2 menších než 2000 a později objevil ještě dvě zbývající v tomto intervalu (viz [3], [8, s. 94], [35]). Jejich (úplný) seznam má tvar:

$$\begin{aligned} 341 &= 11 \times 31, \\ 561 &= 3 \times 11 \times 17, \\ 645 &= 3 \times 5 \times 43, \\ 1105 &= 5 \times 13 \times 17, \\ 1387 &= 19 \times 73, \\ 1729 &= 7 \times 13 \times 19, \\ 1905 &= 3 \times 5 \times 127. \end{aligned}$$

Pseudoprvočísla o základu 2 byla objevena nejdříve a jsou také nejčastěji studována (viz např. monografie [33]). Proto pro jednoduchost budeme pseudoprvočísla o základu 2 nazývat jen *pseudoprvočísla*.[4])

Pseudoprvočíslům se kdysi také říkalo „skoro prvočísla“ (angl. almost primes) (viz [10]) nebo též *Pouletova čísla* (viz [9]), neboť byla intenzivně studována P. Pouletem v [27], kde jsou tabelována všechna pseudoprvočísla až do 10^8. Viz též [18].

V řadě publikací (viz např. [3], [8, s. 59], [12]) se uvádí, že staří Číňané již 500 let př. n. l. věřili, že

$$2^n \equiv 2 \pmod{n} \tag{5}$$

platí, právě když je n prvočíslo. Zajímavé vysvětlení, jak tato téměř jistě nepravdivá historka vznikla, je popsáno v [29, s. 103–105] či v [28, s. 86]. Hlavní protiargument je ten, že staří Číňané nikdy neformulovali pojem „prvočísla“. Tato chyba se poprvé objevila pravděpodobně v článku [12] a byla pak opakována mnoha autory.

Podle D. Mahnkeho (viz [19]) v letech 1680–1681 G. W. Leibniz rovněž chybně tvrdil, že kongruence (5) platí, jen když je n prvočíslo.

Následující větu, jež je uvedena v [35] a [38], lze použít k rekurzivnímu generování nekonečně mnoha pseudoprvočísel.

[4]) Pseudoprvočísla o jiných základech jsou tabelována např. v [29].

Věta 1. *Jestliže n je liché pseudoprvočíslo, pak $2^n - 1$ je také liché pseudoprvočíslo.*

Důkaz. Protože n je složené, existuje přirozené číslo c, $1 < c < n$, které dělí n. Pak $2^c - 1$ dělí číslo $2^n - 1$, tj.

$$2^c - 1 \mid 2^n - 1,$$

a tudíž $2^n - 1$ je také složené. Nyní stačí dokázat, že

$$2^n - 1 \mid 2^{2^n - 2} - 1. \tag{6}$$

Jelikož n je liché pseudoprvočíslo, podle kongruence (4) platí

$$(2^n - 2)/2 = 2^{n-1} - 1 = kn$$

pro nějaké celé číslo k. Potom

$$2^n - 1 \mid 2^{kn} - 1 = 2^{(2^n-2)/2} - 1$$

a vztah (6) je tedy splněn, neboť $2^{2^n-2} - 1 = (2^{(2^n-2)/2} - 1)(2^{(2^n-2)/2} + 1)$. □

Díky této větě můžeme explicitně stanovit pseudoprvočíslo, které je větší než libovolné předem zadané přirozené číslo. Podobné tvrzení pro prvočísla prozatím není známo, i když víme, že prvočísel je nekonečně mnoho. Do roku 2002 největší známé prvočíslo bylo Mersennovo prvočíslo $2^{13466917} - 1$, jež má více než 4 miliony cifer. Poznamenejme ještě, že v roce 1903 větu 1 dokázal E. Malo (viz [21]) pro případ, že n je prvočíslo a $2^n - 1$ je složené.

První sudé pseudoprvočíslo (o základu 2)

$$161\,038 = 2 \times 73 \times 1103$$

bylo nalezeno D. H. Lehmerem v roce 1950 (viz [10]). O rok později N. G. W. H. Beeger dokázal, že existuje nekonečně mnoho sudých pseudoprvočísel (viz [4]).

4. Hustota a rozložení pseudoprvočísel

I když je pseudoprvočísel nekonečně mnoho (viz věta 1), je jich mnohem méně než prvočísel. Například K. Szymiczek [40] dokázal, že pokud n-té pseudoprvočíslo (o základu 2) označíme P_n, pak je řada

$$\sum_{n=1}^{\infty} \frac{1}{P_n}$$

konvergentní, zatímco je dobře známo, že pokud p_n značí n-té prvočíslo, pak je řada

$$\sum_{n=1}^{\infty} \frac{1}{p_n}$$

divergentní. Později však A. Mąkowski v [20] pro pseudoprvočísla ukázal, že řada

$$\sum_{n=1}^{\infty} \frac{1}{\log P_n}$$

je divergentní.

Nechť $\pi(x)$ označuje počet prvočísel nepřevyšujících x. Pak podle známé prvočíselné věty, kterou formuloval C. F. Gauss a kterou až v r. 1896 dokázal J. Hadamard a nezávisle též Ch. de la Vallée Poussin, je

$$\pi(x) \approx \frac{x}{\log x} \quad \text{pro } x \to \infty.$$

Označme dále $\Pi_a(x)$ počet pseudoprvočísel o základu a, která nepřevyšují x. Potom nejlepší známý odhad hodnoty $\Pi_a(x)$ pro dostatečně velká x je

$$\mathrm{e}^{(\log x/\log a)^{\alpha}} \leqq \Pi_a(x) \leqq \frac{x}{\big(\ell(x)\big)^{1/2}}\,, \tag{7}$$

kde $\ell(x) = \mathrm{e}^{\log x \log\log\log x/\log\log x}$ a α lze zvolit jako $0{,}68/1{,}68 > 2/5$ (viz [23], [24] a [29, s. 312–313]). Horní odhad v (7) je mnohem menší než $x/\log x$ pro dostatečně velká x. Poznamenejme ještě, že tabulka v [25, s. 1005] uvádí, že $\Pi_2(10^{10}) = 14884$, zatímco podle tabulky v [29, s. 237] je $\pi(10^{10}) = 455052511$. Jestliže tedy náhodně zvolíme číslo $n \leqq 10^{10}$, pro něž $2^{n-1} \equiv 1 \pmod{n}$, pak pravděpodobnost, že n je prvočíslo, bude více než 30 000krát větší než pravděpodobnost toho, že n je pseudoprvočíslo.

Další vlastnost, která je společná jak prvočíslům, tak i psedoprvočíslům, je vyjádřena v následující větě, kterou dokázal A. Rotkiewicz v [30] a [32].

Věta 2 (Rotkiewiczova). *Jestliže $a \geqq 1$ a $d \geqq 1$ jsou nesoudělná čísla, pak existuje nekonečně mnoho pseudoprvočísel v aritmetické posloupnosti $\{a + kd\}_{k=0}^{\infty}$.*

Podobný výsledek pro prvočísla udává známá Dirichletova věta, která má stejné znění jako věta 2, když vypustíme předponu „pseudo“.

5. Carmichaelova čísla

Obrovská řídkost pseudoprvočísel o pevném základu a ve srovnání s prvočísly poskytuje rozumný důvod používat Malou Fermatovu větu pro testování prvočíselnosti (viz [26, s. 81]). Existují však složená čísla n, nazývaná *Carmichaelova čísla* nebo též *absolutní pseudoprvočísla*, která jsou pseudoprvočísly pro každý základ a, tj. kongruence

$$a^n \equiv a \pmod{n}$$

platí pro všechna přirozená čísla a.

Počítačová prvočíselná síta založená na Malé Fermatově větě nám tedy kromě prvočísel propustí[5]) i složená Carmichaelova čísla. Proto se příslušné testy prvočíselnosti musí jistým způsobem modifikovat (viz např. [17]).

V roce 1899 A. Korselt dokázal následující nutnou a postačující podmínku pro to, aby složené přirozené číslo n bylo absolutním pseudoprvočíslem (viz [16]).

Věta 3 (Korseltova). *Složené číslo n je absolutní pseudoprvočíslo, právě když n není dělitelné čtvercem žádného přirozeného čísla (většího než jedna) a $p-1$ dělí $n-1$ pro všechny prvočinitele p čísla n.*

Z Korseltovy věty 3 například okamžitě plyne, že $561 = 3 \times 11 \times 17$ je absolutní pseudoprvočíslo, neboť $3-1=2$, $11-1=10$, $17-1=16$ a všechna tato tři čísla dělí 560.

Označme $\gcd(m,n)$ největší společný dělitel přirozených čísel m a n. Potom můžeme modifikovat známou Eulerovu funkci

$$\varphi(n) = \operatorname{card}\{m \in \mathbb{N} : \gcd(m,n) = 1\}$$

na tzv. Carmichaelovu lambda funkci $\lambda(n)$, která byla poprvé definována v roce 1912 (viz [6]).

Definice. Nechť n je přirozené číslo. Pak *Carmichaelova lambda funkce* $\lambda(n)$ je definována takto:

$$\begin{aligned}
\lambda(1) &= 1 = \varphi(1),\\
\lambda(2) &= 1 = \varphi(2),\\
\lambda(4) &= 2 = \varphi(4),\\
\lambda(2^k) &= 2^{k-2} = \tfrac{1}{2}\varphi(2^k) \quad \text{pro } k \geqq 3,\\
\lambda(p^k) &= (p-1)p^{k-1} = \varphi(p^k) \quad \text{pro každé liché prvočíslo } p \text{ a } k \geqq 1,\\
\lambda(p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}) &= \operatorname{lcm}\big(\lambda(p_1^{k_1}),\, \lambda(p_2^{k_2}),\, \ldots,\, \lambda(p_r^{k_r})\big),
\end{aligned}$$

kde $p_1, p_2, \ldots, p_r$ jsou vzájemně různá prvočísla, $k_i \geqq 1$ pro $1 \leqq i \leqq r$ a lcm označuje nejmenší společný násobek.

Z definice funkce $\lambda(n)$ vidíme, že $\lambda(n) \mid \varphi(n)$. Následující ekvivalence (viz [17]) je zobecněním slavné Eulerovy-Fermatovy věty: *Čísla $a \in \mathbb{N}$ a $n \in \mathbb{N}$ jsou nesoudělná, právě když*

$$a^{\lambda(n)} \equiv 1 \pmod{n}$$

(srov. (1)).

Je zajímavé, že když Korselt dokázal větu 3, neuvedl ani jeden příklad absolutního pseudoprvočísla. V roce 1910 R. D. Carmichael nezávisle objevil uvedené Korseltovo kritérium a přeformuloval je následujícím způsobem, i když nepoužil termínu „Carmichaelovo číslo“ (viz [5]):

[5]) Známá Wilsonova ekvivalence: „*p je prvočíslo* $\iff$ $(p-1)! \equiv -1 \pmod{p}$“ se k testování prvočíselnosti nehodí, neboť není znám efektivní způsob výpočtu faktoriálu modulo p.

Věta 4 (Carmichaelova). *Složené číslo n je Carmichaelovo číslo, právě když n není dělitelné čtvercem žádného přirozeného čísla (většího než jedna) a $\lambda(n) \mid n-1$.*

V článku [5] Carmichael také ukázal, že každé Carmichaelovo číslo má alespoň tři prvočíselné dělitele, a uvedl čtyři příklady Carmichaelových čísel, které obsahovaly i dvě nejmenší: 561 a 1105. V jeho dalším článku [6] je uvedeno již patnáct Carmichaelových čísel. Podle [25] existuje jen 2163 Carmichaelových čísel menších než $25 \cdot 10^9$.

V práci [1] je ukázáno, že existuje nekonečně mnoho Carmichaelových čísel. Navíc je dokázáno, že pokud $C(x)$ označuje počet Carmichaelových čísel nepřevyšujících x, pak pro dostatečně velké x platí

$$C(x) > x^{2/7}.$$

6. Závěrečné poznámky

Existuje několik zajímavých souvislostí mezi *Fermatovými čísly* $F_m = 2^{2^m} + 1$, $m = 0, 1, 2, \ldots$, a pseudoprvočísly. V roce 1904 M. Cipolla dokázal, že $n \mid 2^n - 2$ pro $n = 2^{2^m} + 1$, $m = 0, 1, 2, \ldots$. O pět let později Banachiewicz konstatoval, že všechna Fermatova čísla jsou buď prvočísla, anebo pseudoprvočísla o základu 2 (důkaz je uveden např. v [17, s. 36]). Možná, že právě tento fakt vedl Fermata k jeho nesprávné domněnce, že všechna Fermatova čísla jsou prvočísla. Poznamenejme ještě, že rovněž každé složené *Mersennovo číslo* $M_p = 2^p - 1$, kde p je prvočíslo, je pseudoprvočíslo (důkaz je uveden např. v [17, s. 44]).

Fermatova čísla použilo několik autorů (viz [7], [11], [12], [31] a [39]) ke generování nekonečně mnoha pseudoprvočísel. Následující věta z roku 1904 dokázaná v [7] ukazuje, jak lze Fermatova čísla použít k vytvoření nekonečně mnoha pseudoprvočísel, která mají libovolně velký počet prvočinitelů.

Věta 5 (Cipollova). *Jestliže $a > b > \cdots > s > 1$ a $n = F_a F_b \cdots F_s$, pak n je pseudoprvočíslo, právě když $2^s > a$. Pro libovolně velké $m > 1$ tedy existuje nekonečně mnoho pseudoprvočísel, která mají alespoň m různých prvočinitelů.*

V roce 1949 P. Erdős dokázal, že pro každé $m > 1$ existuje nekonečně mnoho pseudoprvočísel, která mají právě m různých prvočinitelů. Je zajímavé, že první důkaz nekonečného počtu pseudoprvočísel podal J. H. Jeans už v roce 1897. V práci [12] ukázal, že když $a > b$ a $2^b > a$, pak $F_a F_b$ je pseudoprvočíslo. Tento výsledek je speciálním případem věty 5.

Poznamenejme ještě, že pro libovolné složené přirozené číslo n je podle binomické věty rozdíl $a^n - a$ dělitelný n pro $a = n + 1$. Odtud a ze vztahu (2) plyne, že n je pseudoprvočíslo o základu $n + 1$.

Výzkum v oblasti pseudoprvočísel je nyní značně rozsáhlý. Existuje celá řada rozličných tříd pseudoprvočísel (viz [2], [13], [15], [17], [22], [34], [36], [39]), např. již zmíněná absolutní pseudoprvočísla, Eulerova pseudoprvočísla, Fermatova d-pseudoprvočísla,

Frobeniova pseudoprvočísla, Lehmerova pseudoprvočísla a Lehmerova superpseudoprvočísla, Lucasova pseudoprvočísla, Lucasova d-pseudoprvočísla a Lucasova superpseudoprvočísla, silná pseudoprvočísla, superpseudoprvočísla aj. Teprve čas ukáže, zda někdy najdou uplatnění také v praktických situacích podobně jako prvočísla.

Poděkování. Práce byla podpořena grantem A 1019201 GA Akademie věd ČR. Autoři děkují Mgr. Heleně Holovské, RNDr. Karlu Mickovi, DrSc., a Mgr. Ing. Jakubu Šolcovi za cenné připomínky.

L i t e r a t u r a

[1] Alford, W. R., Granville, A., Pomerance, C.: *There are infinitely many Carmichael numbers.* Ann. of Math. *140* (1994), 703–722.
[2] Baillie, R., Wagstaff, S. S.: *Lucas pseudoprimes.* Math. Comp. *35* (1980), 1391 až 1417.
[3] Banachiewicz, T.: *O związku pomiędzy pewnym twierdzeniem matematyków chińskich a formą Fermata na liczby pierwsze.* Spraw. Tow. Nauk, Warszawa *2* (1909), 7–11.
[4] Beeger, N. G. W. H.: *On even numbers m dividing $2^m - 2$.* Amer. Math. Monthly *58* (1951), 553–555.
[5] Carmichael, R. D.: *Note on a new number theory function.* Bull. Amer. Math. Soc. *16* (1910), 232–238.
[6] Carmichael, R. D.: *On composite numbers P which satisfy the Fermat congruence $a^{P-1} \equiv 1 \pmod{P}$.* Amer. Math. Monthly *19* (1912), 22–27.
[7] Cipolla, M.: *Sui numeri composti P, che verificano la congruenza di Fermat $a^{P-1} \equiv 1 \pmod{P}$.* Annali di Matematica (3) *9* (1904), 139–160.
[8] Dickson, L. E.: *History of the theory of numbers, vol. I, Divisibility and primality.* Carnegie Inst., Washington 1919.
[9] Duparc, H. J. A.: *On Carmichael numbers, Poulet numbers, Mersenne numbers and Fermat numbers.* Rapport ZW 1953-004, Math. Centrum Amsterdam 1953, 1–7.
[10] Erdős, P.: *On almost primes.* Amer. Math. Monthly *57* (1950), 404–407.
[11] Jarden, D.: *Existence of an infinitude of composite n for which $2^{n-1} \equiv 1 \pmod{n}$* (Hebrew, Engl. Summary). Riveon Lematematika *4* (1950), 65–67.
[12] Jeans, J. H.: *The converse of Fermat's theorem.* Messenger of Mathematics *27* (1897/98), 174.
[13] Joo, I., Phong, B. M.: *On super Lehmer pseudoprimes.* Studia Sci. Math. Hungar. *25* (1990), 121–124.
[14] Kiss, E.: *Notes on János Bolyai's researches in number theory.* Historia Math. *26* (1999), 68–76.
[15] Kiss, P.: *Some results on Lucas pseudoprimes.* Ann. Univ. Sci. Budapest. Eötvös Sect. Math. *28* (1985), 153–159.
[16] Korselt, A.: *Problème chinois.* L'Interm. des Math. *6* (1899), 143.
[17] Křížek, M., Luca, F., Somer, L.: *17 lectures on Fermat numbers: From number theory to geometry.* CMS Books in Mathematics, vol. 9, Springer-Verlag, New York 2001.
[18] Lehmer, D. H.: *On the converse of Fermat's theorem.* Amer. Math. Monthly *43* (1936), 346–354.
[19] Mahnke, D.: *Leibniz auf der Suche nach einer allgemeinen Primzahlgleichung.* Bibliotheca Math. *13* (1913), 29–61.
[20] Mąkowski, A.: *On a problem of Rotkiewicz on pseudoprime numbers.* Elem. Math. *29* (1974), 13.

[21] Malo, E.: *Nombres qui sans être premiers, verifient exceptionnellement une congruence de Fermat.* L'Interm. des Math. *10* (1903), 88.
[22] Phong, B. M.: *On super Lucas and super Lehmer pseudoprimes.* Studia Sci. Math. Hungar. *23* (1988), 435–442.
[23] Pomerance, C.: *On the distribution of pseudoprimes.* Math. Comp. *37* (1981), 587–593.
[24] Pomerance, C.: *A new lower bound for the pseudoprime counting function.* Illinois J. Math. *26* (1982), 4–9.
[25] Pomerance, C., Selfridge, J. L., Wagstaff, S. S.: *The pseudoprimes to* $25 \cdot 10^9$. Math. Comp. *35* (1980), 1003–1026.
[26] Porubský, Š.: *Fermat a teorie čísel aneb Problematika dělitelů a dokonalá čísla.* In: *Matematik Pierre de Fermat* (eds. A. Šolcová et al.), Cahiers du CEFRES *28* (2002), 49–86.
[27] Poulet, P.: *Table des nombres composés vérifiant le théeorème de Fermat pour le module* 2 *jusqu'à* 100.000.000. Sphinx *8* (1938), 42–52. Errata in Math. Comp. *25* (1971), 944–945, Math. Comp. *26* (1972), 814.
[28] Ribenboim, P.: *The book of prime number records.* Springer, New York 1988, 1989.
[29] Ribenboim, P.: *The new book of prime number records.* Springer, New York 1996.
[30] Rotkiewicz, A.: *Sur les nombres pseudopremiers de la forme* $ax + b$. C. R. Acad. Sci. Paris Sér. I Math. *257* (1963), 2601–2604.
[31] Rotkiewicz, A.: *Sur les formules donnant des nombres pseudopremiers.* Colloq. Math. *12* (1964), 69–72.
[32] Rotkiewicz, A.: *On the pseudoprimes of the form* $ax + b$. Proc. Cambridge Philos. Soc. *63* (1967), 389–392.
[33] Rotkiewicz, A.: *Pseudoprime numbers and their generalizations.* Stud. Assoc. Fac. Sci. Univ. Novi Sad 1972.
[34] Rotkiewicz, A.: *Lucas and Frobenius pseudoprimes.* Proc. of the 10th Internat. Conf. on Fibonacci Numbers and their Applications, Flagstaff, Arizona, 2002 (to appear in Kluwer), 1–21.
[35] Sierpiński, W.: *Remarque sur une hypothèse des Chinois concernant les nombres* $(2^n - 2)/n$. Colloq. Math. *1* (1948), 9.
[36] Somer, L.: *On Fermat d-pseudoprimes.* In: Théorie des nombres (éd. J.-M. De Koninck, C. Levesque), Walter de Gruyter, Berlin, New York, 1989, 841–860.
[37] Somer, L.: *On Lucas d-pseudoprimes.* In: *Applications of Fibonacci numbers*, vol. 7 (eds. G. E. Bergum, A. N. Philippou, A. F. Horadam), Kluwer Academic Publishers, Dordrecht 1998, 369–375.
[38] Steuerwald, R.: *Über die Kongruenz* $2^{n-1} \equiv 1 \pmod{n}$. S.-B. Math.-Nat. Kl., Bayer. Akad. Wiss. 1947, 177.
[39] Szymiczek, K.: *Note on Fermat numbers.* Elem. Math. *21* (1966), 59.
[40] Szymiczek, K.: *On pseudoprimes which are products of distinct primes.* Amer. Math. Monthly *74* (1967), 35–37.