Pokroky matematiky, fyziky a astronomie

Michal Křížek

O Fermatových číslech

Pokroky matematiky, fyziky a astronomie, Vol. 40 (1995), No. 5, 243--253

Persistent URL: http://dml.cz/dmlcz/138304

[SY1] T. SAUER and J. A. YORKE: *Shadowing trajectories of dynamical systems.* In „Computer-Aided Proofs in Analysis" (eds. K. Meyer and D. Schmidt), Springer-Verlag, Berlin 1990, 229–234.

[SY2] T. SAUER and J. A. YORKE: *Rigorous verification of trajectories for the computer simulation of dynamical systems.* Nonlinearity *4* (1991), 961–979.

[Š] A. N. ŠARKOVSKIJ: *Koexistencija ciklov nepreryvnogo otobraženia prjamoj na sebja.* Ukrainskij matematičeskij žurnal *16* (1964), 61–71.

O Fermatových číslech

Michal Křížek, Praha

1. Úvod

Francouzský matematik Pierre Fermat (1601–1665) se proslavil nejen svou velkou a malou větou Fermatovou, ale také hypotézou, že všechna čísla tvaru

$$F_m = 2^{2^m} + 1 \quad \text{pro } m = 0, 1, 2, \ldots \tag{1}$$

jsou prvočísla. Ani jedno z těchto tří tvrzení však pravděpodobně nedokázal. Přiznával ale, že s důkazem domněnky o prvočíselnosti F_m si neví rady. Čísla F_m se po něm nazývají Fermatova čísla.

Pokud je F_m prvočíslo, říkáme, že je Fermatovým prvočíslem. Prvních pět členů posloupnosti (1), tj.

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65537, \tag{2}$$

jsou prvočísla. K tomu, aby číslo $2^n + 1$ pro n přirozené bylo prvočíslem, je nutné, aby byl exponent n tvaru 2^m pro $m \in \{0, 1, 2, \ldots\}$. Je-li totiž k přirozené a $l \geqq 3$ liché, pak

$$2^{kl} + 1 = (2^k + 1)(2^{k(l-1)} - 2^{k(l-2)} + \ldots - 2^k + 1). \tag{3}$$

Odtud plyne, že číslo $2^n + 1$ je složené, jestliže je exponent n dělitelný lichým číslem $l \geqq 3$. To však v posloupnosti (1) nenastane.

RNDr. MICHAL KŘÍŽEK, DrSc. (1952), je pracovníkem Matematického ústavu AV ČR, Žitná 25, 11 567 Praha 1 (e-mail: krizek@earn.cvut.cz). Tato práce byla částečně podpořena grantem č. 201/94/1067 GA ČR.

V roce 1732 Leonhard Euler zjistil, že $F_5 = 641 \cdot 6700417$, a tím vyvrátil Fermatovu hypotézu. Vyvstala ovšem otázka, zda vůbec existuje nekonečně mnoho prvočísel tvaru (1).

Zájem o Fermatova prvočísla vzrostl zejména poté, co německý matematik Carl Friedrich Gauss (1777–1855) dokázal studiem kořenů binomické rovnice $x^k = 1$ větu, která vyjadřuje až neuvěřitelnou souvislost mezi geometrií a teorií čísel.

Gaussova věta. *Pravidelný mnohoúhelník je eukleidovsky konstruovatelný (tj. pomocí kružítka a pravítka) tehdy a jen tehdy, když počet jeho vrcholů je roven číslu* $k = 2^i p_1 p_2 \dots p_j$, *kde* $i \geqq 0$, $j \geqq 0$, $k \geqq 3$ *jsou celá čísla a* $p_1, p_2, \dots, p_j$ *navzájem různá Fermatova prvočísla.*

Vidíme tedy, že pravidelný mnohoúhelník je eukleidovsky konstruovatelný pro $k = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17, \dots$ a není konstruovatelný pro $k = 7, 9, 11, 13, 14, \dots$. Pravidelný pětiúhelník uměli zkonstruovat již staří Řekové. Marně však hledali postup, jak narýsovat pravidelný sedmiúhelník či devítiúhelník. Konstrukci pravidelného sedmnáctiúhelníku (tj. pro $i = 0$, $j = 1$, $k = p_1 = 17$) podal sám Gauss [26]. Je popsána i konstrukce pravidelných mnohoúhelníků s 257 a 65537 vrcholy [21]. Protože není dokázáno, zda (2) obsahuje všechna Fermatova prvočísla (žádné jiné totiž dosud nebylo objeveno), nevíme vlastně, kolik existuje pravidelných mnohoúhelníků, které lze teoreticky zkonstruovat pomocí pravítka a kružítka. Podle Gaussovy věty zatím známe $31 = 2^5 - 1$ eukleidovsky konstruovatelných pravidelných mnohoúhelníků s lichým počtem vrcholů.

Šesté Fermatovo číslo F_6 rozložil na součin dvou činitelů F. Landry v roce 1880 ve věku svých osmdesáti dvou let (viz [28]). F. Klein v roce 1897 ukázal, že číslo F_7 je složené, aniž by znal nějakého jeho dělitele. Podobně J. C. Moreheard a A. E. Western dokázali v roce 1909, že F_8 je složené. Dnes je již prověřeno, že F_m jsou složená pro $5 \leqq m \leqq 23$. U čísel F_{14}, F_{20} a F_{22} zatím sice není znám žádný netriviální dělitel, ale jejich neprvočíselnost lze na počítači dokázat postupy popsanými v [4, 27]. Pro $m > 23$ je známo přes 100 dalších Fermatových čísel, která jsou složená. Zatím největší složené Fermatovo číslo F_{23471} objevil W. Keller [8]. Počítačovou analýzou dokázal, že je dělitelné číslem $5 \cdot 2^{23473} + 1$. Číslo F_{23471} má více než 10^{7000} cifer. Velikost tohoto Fermatova čísla ale nesmíme zaměňovat s relativně malým číslem 10^{7000}, které má „jen“ 7001 cifer.

Je dokázáno (viz např. [7, str. 15]), že Fermatových prvočísel je s pravděpodobností 1 konečně mnoho. S jistotou ovšem nemůžeme tvrdit, že jich je skutečně jen konečně mnoho. (Např. pravděpodobnost, že náhodně zvolené reálné číslo bude iracionální, je také 1, a přesto se může stát, že při náhodném výběru zvolíme právě číslo racionální.)

Fermatova čísla se používají při konstrukci některých generátorů pseudonáhodných čísel. Například v kdysi oblíbeném počítači ZX Spectrum jsou pseudonáhodná čísla definována pomocí zbytků při postupném dělení $F_4 = 2^{16} + 1$ mocninami $75, 75^2, 75^3, \dots$. Analogicky se používá $F_5 = 2^{32} + 1$ v TURBO PASCALU pro PC. Poznamenejme ještě, že ve dvojkové soustavě mají Fermatova čísla tvar $1000\dots0001$ s $2^m - 1$ nulami uprostřed.

Kdybychom zkoušeli prvočíselnost F_m tak, že bychom F_m dělili všemi prvočísly menšími než $\sqrt{F_m}$, byl by to časově nezvládnutelný algoritmus i pro relativně malá m. Předpokládejme například, že provedeme miliardu dělení za sekundu. Pak bychom pro rozklad nevinně vyhlížejícího čísla F_8 potřebovali mnohem více času, než je stáří vesmíru ($\approx 15 \cdot 10^9$ let). Podle Gaussova vztahu [7, 21] je počet prvočísel menších než n přibližně[1]) roven $n/\ln n$. Protože celá část čísla $\sqrt{F_8}$ má 39 cifer, je před $\sqrt{F_8}$ alespoň $10^{38}/(38 \ln 10) \doteq 10^{36}$ prvočísel. Uvážíme-li, že rok má asi $3{,}2 \cdot 10^7$ sekund, dostaneme, že bychom pro rozklad F_8 potřebovali alespoň $3 \cdot 10^{19}$ let. Takový algoritmus matematici přirovnávají ke snaze rozbít atom kladivem.

Pokud o rozkládaném čísle máme nějakou informaci navíc, může se nám podařit najít hledaný rozklad podstatně rychleji. V další kapitole ukážeme, jak lze předem množinu případných dělitelů F_m podstatně zredukovat. Klíčovou roli přitom bude hrát věta Lucasova, která udává nutnou podmínku pro tvar těch prvočísel, která dělí F_m.

2. Obecný tvar prvočíselných dělitelů Fermatových čísel

Cílem této kapitoly bude dokázat elementárními prostředky Lucasovu větu. K tomu účelu připomeneme základní definice a vyslovíme několik pomocných tvrzení. Nadále budeme pracovat jen s celými čísly. Největšího společného dělitele přirozených čísel k a b budeme označovat (k, b) a symbol $k \mid b$ bude znamenat, že k dělí b beze zbytku. Pokud b vydělíme k a dostaneme zbytek z, $0 \leqq z < k$, budeme to zapisovat takto: $z = \langle b \rangle_k$, tj. pro b, z, k je splněna kongruence $b \equiv z \bmod k$. Platí tedy například rovnost

$$\langle \langle a \rangle_k \langle b \rangle_k \rangle_k = \langle ab \rangle_k. \tag{4}$$

Je-li totiž $a = a' + a''k$ a $b = b' + b''k$, pak $ab = a'b' + (a'b'' + a''b' + a''b''k)k$, a tedy $\langle ab \rangle_k = \langle a'b' \rangle_k$. Odtud již plyne (4).

Malá Fermatova věta. *Je-li b přirozené číslo a p prvočíslo, pak $p \mid b^p - b$.*

DŮKAZ. Jestliže $p \mid b$, pak p dělí i $b^p - b = b(b^{p-1} - 1)$. Nechť tedy

$$(p, b) = 1. \tag{5}$$

Ukážeme, že pak $p \mid b^{p-1} - 1$. Uvažujme konečnou posloupnost

$$b, 2b, 3b, \ldots, (p-1)b, pb. \tag{6}$$

Dvě různá čísla ib a jb (např. pro $i > j$) nemohou dát stejný zbytek při dělení p, protože pak by $p \mid b(i-j)$, což by byl spor s (5). Posloupnost (6) dává tedy p různých zbytků při dělení p. Poslední člen v (6), který dává zbytek 0, odstraníme. Stejné zbytky (až na pořadí) obdržíme při dělení posloupnosti $1, \ldots, p-1$ číslem p. Odtud a indukcí pomocí

[1]) Chyba je menší než 15 % pro každé $n \geqq 3000$; Hadamard a de la Vallée Poussin dokázali asymptotickou rovnost pro $n \to \infty$.

(4) dostaneme, že $b^{p-1}(p-1)! \equiv (p-1)! \bmod p$. Čili $(b^{p-1}-1)(p-1)! \equiv 0 \bmod p$ a první činitel vlevo je tedy dělitelný p. □

Malá Fermatova věta se někdy formuluje i takto: Jestliže p je prvočíslo a platí (5), pak

$$b^{p-1} \equiv 1 \mod p. \tag{7}$$

Známá Eulerova věta z teorie čísel (viz např. [21, 22]) je zobecněním (7).

Úmluva. Do konce této kapitoly bude p označovat liché prvočíslo.

Definice. *Je-li b přirozené číslo, pak nejmenší přirozený exponent e, pro který $p \mid b^e - 1$ (tj. $b^e \equiv 1 \bmod p$), se nazývá multiplikativní řád čísla b modulo p, což budeme zapisovat takto: $e = \operatorname{ord}_p b$.*

Podle malé Fermatovy věty $p \mid b^{p-1} - 1$, pokud platí (5). Odtud plyne existence řádu $e \leqq p-1$. (Pro b i p sudé by ovšem žádné takové přirozené e neexistovalo.) Můžete si např. ověřit, že $\operatorname{ord}_7 2 = 3$, $\operatorname{ord}_5 3 = 4$ apod.

Lemma. *Je-li $e = \operatorname{ord}_p b$, pak*

$$p \mid b^n - 1 \tag{8}$$

pro $n = ke$, $k \in \{1, 2, \ldots\}$, a (8) platí jen pro tyto exponenty a žádné jiné.

DŮKAZ. Jestliže $n = ke$, pak

$$b^n - 1 = b^{ke} - 1 = (b^e - 1)(b^{e(k-1)} + \ldots + b^e + 1), \tag{9}$$

a tedy (8) platí podle předchozí definice.

Předpokládejme na okamžik, že $p \mid b^{ke+h} - 1$ pro nějaké $k \in \{1, 2, \ldots\}$ a $0 < h < e$. Pak

$$(b^{ke+h} - 1) - (b^{ke} - 1) = b^{ke}(b^h - 1).$$

Protože jsou obě čísla v závorkách vlevo dělitelná p a podle (8) p nedělí b^{ke}, musí být $b^h - 1$ dělitelné p. To je ale spor s minimalitou e. □

Věta. *Jestliže $p \mid F_m$, pak p je tvaru $p = k2^{m+1} + 1$, kde k je přirozené číslo.*

Důkaz se opírá o rovnost $\operatorname{ord}_p 2 = 2^{m+1}$, ale nebudeme jej uvádět, protože plyne z (10). V literatuře se uvádí (viz např. [12]), že tvrzení věty možná znal už Fermat, ačkoliv důkaz předložil teprve Euler. Není však jasné, proč v tom případě Fermat nepoužil větu k rozkladu čísla F_5. Stačilo totiž vyzkoušet vydělit číslo F_5 pouze prvočísly tvaru $64k+1$ a pro $k = 10$ se Fermat mohl sám přesvědčit, že jeho hypotéza o prvočíselnosti F_m neplatí.

V roce 1878 francouzský matematik Édouard A. Lucas dokázal, že číslo k v předchozí větě je vždy sudé.

Lucasova věta. *Jestliže $p \mid F_m$, pak p je tvaru*

$$p = k2^{m+2} + 1, \tag{10}$$

kde k je přirozené číslo.

DŮKAZ. Nechť $b = 2^{2^{m-2}}\left(2^{2^{m-1}} - 1\right)$. Protože

$$2^{2^m} + 1 \equiv 0 \mod p, \tag{11}$$

máme

$$\langle b^2\rangle_p = \langle 2^{2^{m-1}}\left(2^{2^m} - 2\cdot 2^{2^{m-1}} + 1\right)\rangle_p = \langle -2\cdot 2^{2^m}\rangle_p = \langle -2\cdot 2^{2^m} + 2(2^{2^m} + 1)\rangle_p = 2. \tag{12}$$

Jinými slovy, $b^2 \equiv 2 \mod p$. Odtud a z (11) plyne, že $b^{2^{m+1}} \equiv 2^{2^m} \equiv -1 \mod p$, a proto $b^{2^{m+2}} \equiv 1 \mod p$. Podle lemmatu je tedy $\operatorname{ord}_p b = 2^j$ pro $j \leqq m + 2$. Kdyby však $j < m + 2$, pak by opět podle lemmatu bylo i číslo

$$2^{e2^{m-j}} - 1 = 2^{2^m} - 1$$

dělitelné lichým prvočíslem p, což je spor s (11). Tudíž

$$\operatorname{ord}_p b = 2^{m+2}. \tag{13}$$

Podle (12) jsou čísla p a b nesoudělná. Užijeme-li tedy vztah (7), pak podle lemmatu a (13) obdržíme, že $p - 1 = k \operatorname{ord}_p b = k2^{m+2}$. □

Užitečnost Lucasovy věty si ilustrujme na úloze, jíž se zabýval A. E. Western roku 1903. Hledal k takové, aby $k2^{20} + 1 \mid F_{18}$. Dělitelnost stačí prověřovat jen pro ta k, pro něž je $k2^{20} + 1$ prvočíslo. Western takto poměrně snadno zjistil, že hledané číslo je $k = 13$, protože pro všechna menší k, kromě případu $k = 7$, jsou čísla $k2^{20} + 1$ složená.

3. Další vlastnosti Fermatových čísel

Snadno nahlédneme (viz (2)), že F_m pro $m \geqq 2$ končí na 7, protože 2^{2^m} končí na 6. Poslední dvojčíslí F_m může končit jen na 17, 37, 57 a 97 pro $m \geqq 2$.

Z (1) je patrno, že platí rekurentní vztah

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

a tak

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

Odtud indukcí dostáváme zajímavou vlastnost

$$F_{m+1} - 2 = F_m F_{m-1} \ldots F_1 F_0,$$

ze které plyne, že $F_{m+1} - 2$ je dělitelné všemi menšími Fermatovými čísly. Tedy

$$F_{m-k} \mid F_m - 2 \quad \text{pro všechna } k = 1, \ldots, m. \tag{14}$$

Mocniny dvojky zvětšené o jedničku se mohou vzájemně dělit, např. $2 + 1 \mid 8 + 1$ nebo $4+1 \mid 64+1$. Pro Fermatova čísla však Eulerův vrstevník Ch. Goldbach dokázal, že jsou po dvou nesoudělná.

Goldbachova věta. *Žádná dvě různá Fermatova čísla nemají společného dělitele většího než* 1.

DŮKAZ. Předpokládejme, že

$$q \mid F_m \quad \text{a} \quad q \mid F_{m-k}. \tag{15}$$

Odtud a z (14) plyne, že $q \mid F_m - 2$. Podle (15) tedy máme $q \mid 2$. Protože však je F_m liché, je $q = 1$. □

Podle Goldbachovy věty je tedy každé z čísel $F_0, F_1, \ldots, F_m$ dělitelné prvočíslem, které ostatní Fermatova čísla nedělí. Proto existuje alespoň $m + 1$ různých prvočísel nepřevyšujících F_m. Odtud mj. vyplývá, že prvočísel je nekonečně mnoho (tzv. Euklidova věta).

Pomocí Goldbachovy a Lucasovy věty lze dokázat následující tvrzení (viz [10]). Nechť F_m je složené,

$$F_m = (k2^n + 1)(l2^j + 1),$$

kde k a l jsou lichá čísla. Pak

$$k \geqq 3, \quad l \geqq 3, \quad n = j \geqq m + 2, \tag{16}$$

čísla k a l jsou nesoudělná a buď $3 \mid k$, anebo $3 \mid l$. Čísla k a l nemohou být současně obě „malá“, neboť, jak ukázal J. Chleboun, platí nerovnost

$$\max(k, l) \geqq F_{m-2}.$$

J. C. Moreheard navíc odvodil, že jestliže

$$p = 3 \cdot 2^n + 1$$

je prvočíslo, které dělí F_m, pak je n liché.

Od zveřejnění Lucasova výsledku byla věnována velká pozornost studiu prvočísel tvaru (10). W. Sierpiński v roce 1960 dokázal, že existuje nekonečně mnoho k, pro něž jsou čísla $k2^n + 1$ složená pro libovolné n přirozené — viz [8]. Žádné takové k sice neobjevil, ale dnes je známo, že například všechna čísla tvaru $78557 \cdot 2^n + 1$ jsou složená. Nicméně dosud nevíme, které je nejmenší k s touto vlastností.

4. Rozklady Fermatových čísel na počítačích

Zásluhou výkonných počítačů je dnes známo přes 160 prvočíselných dělitelů asi sto dvaceti Fermatových čísel [3, 9]. Morrison a Brillhart rozložili na prvočinitele číslo F_7 v roce 1970 [16], Brent a Pollard F_8 v roce 1980 [2] a Lenstra, Lenstra (ml.), Manasse, Pollard F_9 v roce 1990 [12]. Problém rozkladu čísla F_9 byl rozdělen na

množství samostatných úloh, které řešilo 700 pracovních stanic po celém světě celkem 4 měsíce, přičemž v závěru byl použit superpočítač. Toto číslo je mnohem větší, než je počet elementárních částic v pozorovatelné části našeho vesmíru. Úplný rozklad F_{11} na prvočinitele se podařil Brentovi [1] překvapivě již v roce 1988. Pomohlo mu, že F_{11} má 4 prvočinitele poměrně malé (viz tab. 1) a jen jednoho prvočinitele velkého s 564 ciframi. Test prvočíselnosti si ovšem vyžádal 30 dní strojového času. Číslo F_{11} je zatím největší úplně rozložené Fermatovo číslo.

Číslo F_{10} je zatím rozloženo na tři činitele. Dva jsou prvočíselní a o třetím je dokázáno, že je složený.

Podle [5, str. 376] anonymní pisatel v roce 1828 vyslovil hypotézu, že všechna čísla tvaru

$$2+1,\ 2^2+1,\ 2^{2^2}+1,\ 2^{2^{2^2}}+1,\ldots$$

jsou prvočísla (viz též [22, str. 21]). V roce 1953 však J. L. Selfridge na počítači ukázal, že $3150 \cdot 2^{18}+1 \mid F_{16}$, čímž tuto starou hypotézu vyvrátil.

Tabulka 1 obsahuje všechny dosud získané prvočinitele čísel F_m pro $5 \leqq m \leqq 20$. Označíme-li Ω_m počet prvočinitelů F_m (započítávaných včetně násobnosti), pak platí

$$1 = \Omega_0 = \ldots = \Omega_4 < 2 = \Omega_5 = \ldots = \Omega_8 < 3 = \Omega_9 < 5 = \Omega_{11} < 6 < \Omega_{12}. \qquad (17)$$

Z malé Fermatovy věty vidíme, že jestliže p nedělí $b^p - b$ pro nějaké b, pak p je složené. Můžeme tak zjistit, že dané číslo je složené, aniž bychom znali nějakého jeho dělitele. Jestliže například ukážeme, že p nedělí $2^{p-1}-1$, pak p není prvočíslo.

Poznamenejme, že rozkládat čísla na prvočinitele je mnohem náročnější na počet operací než pouze ověřovat jejich prvočíselnost [13, 17]. Na tomto faktu je založeno moderní šifrování zpráv pomocí velkých prvočísel — viz např. [18]. Počet operací k rozložení čísla, které je součinem dvou velkých prvočísel (o nichž předem nic nevíme), roste exponenciálně s počtem jeho cifer. Pokud má takové číslo přes 200 cifer, je pomocí dnešních prostředků prakticky nerozložitelné. Naproti tomu test prvočíselnosti libovolného dvěstěciferného čísla netrvá na superpočítači déle než několik minut.

Přehled současně používaných algoritmů na rozklady velkých čísel lze nalézt v [12]. Např. Pollardův algoritmus [19] je vhodný pro rozklad těch čísel, pro jejichž nějakého dělitele existuje „blízké“ číslo (± 10) složené pouze z „malých“ činitelů (nepřevyšujících 20 000). Za jeden z nejúčinnějších algoritmů je v současné době považován Lenstrův algoritmus (a jeho rozmanité modifikace), v němž je grupa čísel modulo p nahrazena grupou bodů na eliptické křivce [11, 24]. Všechny tyto algoritmy patří do třídy NP (nondeterministic polynomial — viz [18]), tzn., že obsahují generátory náhodných čísel. Poznamenejme ještě, že pokud najdeme rozklad nějakého čísla q na dva činitele q_1 a q_2, pak zpětné ověření, že $q = q_1 q_2$, trvá na počítači jen zlomky sekundy. Pro problémy třídy NP totiž platí, že když nám někdo zadá řešení, tak jsme schopni ověřit v polynomiálním čase (vzhledem k velikosti vstupních dat), že to řešení skutečně je.

m	prvočíselný dělitel	rok	objevitel
5	641	1732	Euler
5	6700417	1732	Euler
6	274177	1880	Landry
6	67280421310721*	1880	Landry
7	59649589127497217	1970	Morrison, Brillhart
7	5704689200685129054721	1970	Morrison, Brillhart
8	1238926361552897	1980	Brent, Pollard
8	p_{62} — viz [2]	1980	Brent, Pollard
9	2424833	1903	Western
9	p_{49} — viz [12]**	1990	Lenstra, Lenstra, Jr., Manasse, Pollard
9	p_{99} — viz [12]**	1990	Lenstra, Lenstra, Jr., Manasse, Pollard
10	45592577	1953	Selfridge
10	6487031809	1962	Brillhart
11	319489	1899	Cunningham
11	974849	1899	Cunningham
11	167988556341760475137	1988	Brent
11	3560841906445833920513	1988	Brent
11	p_{564} — viz [1]***	1988	Brent
12	114689	1877	Lucas, Pervouchine
12	26017793	1903	Western
12	63766529	1903	Western
12	190274191361	1974	Hallyburton, Brillhart
12	1256132134125569	1986	Baillie
13	2710954639361	1974	Hallyburton, Brillhart
13	2663848877152141313	1991	Crandall
13	3603109844542291969	1991	Crandall
14	číslo je složené	1961	Selfridge, Hurwitz
15	1214251009	1925	Kraïtchik
15	2327042503868417	1987	Gosper
16	825753601	1953	Selfridge
17	31065037602817	1979	Gostin
18	13631489	1903	Western
19	70525124609	1962	Reisel
19	646730219521	1963	Wrathall
20	číslo je složené	1987	Young, Buell

Tab. 1. Známí dělitelé Fermatových čísel F_m, $5 \leqq m \leqq 20$. Symbol p_j označuje prvočíslo o j cifrách. Prvočíselnost dokázal * Laundry, Le Lasseur a Gérardin, ** Odlyzko, *** Morain.

K tomu, abychom okamžitě zjistili, zda nalezený dělitel čísla F_m je prvočíselný, se nám může hodit Suyamova věta. Její předpoklady jsou splněny pro převážnou většinu (asi 88 %) všech známých prvočíselných dělitelů Fermatových čísel.

Věta (Suyama). *Nechť* $p = k2^n + 1$ *dělí* F_m *a nechť* $k2^{n-(m+2)} < 9 \cdot 2^{m+2} + 6$. *Pak* p *je prvočíslo.*

DŮKAZ. Předpokládejme naopak, že p je součinem dvou činitelů. Pro každý činitel platí (16), a tak $k2^n + 1 \geqq (3 \cdot 2^{m+2} + 1)^2$. Tedy $k2^{n-(m+2)} \geqq 9 \cdot 2^{m+2} + 6$. □

Například pro dělitele $45592577 = 11131 \cdot 2^{12} + 1$ čísla F_{10} máme $n = 12$, $m = 10$ a $n - (m + 2) = 0$. Protože $k = 11131$ je menší než $9 \cdot 2^{12} + 6 = 36870$, musí tento dělitel být prvočíslem.

F. Proth dokázal větu, pomocí které lze rovněž snadno zjistit prvočíselnost dělitelů Fermatových čísel pro $k < 2^n$ (viz [20]). Uveďme ještě jedno zajímavé a užitečné tvrzení týkající se prvočíselnosti, které bylo použito k důkazu, že Fermatovo číslo F_{20} je složené [27].

Věta (Pepinův test [5, 12]). *Pro* $m \geqq 1$ *je* F_m *prvočíslo tehdy a jen tehdy, když* $3^{(F_m-1)/2} \equiv -1 \mod F_m$.

5. Zobecnění Fermatových čísel

Zajímavé zobecnění Fermatových čísel našli Ligh a Jones [14]. Studovali čísla tvaru

$$L_{p,m} = \frac{2^{p^{m+1}} - 1}{2^{p^m} - 1} = \sum_{j=1}^{p} 2^{p^m(j-1)},$$

odkud vidíme, že $F_m = L_{2,m} = 2^{2^m} + 1$. Pro $m = 0$ zase máme $M_p = L_{p,0} = 2^p - 1$, což jsou tzv. Mersenneova čísla — viz [25]. Tudíž $L_{p,m}$ zobecňují jak Fermatova, tak Mersenneova čísla.

Počátkem tohoto století byl zahájen velký projekt, který se zabývá rozklady Cunninghamových čísel, tj. čísel tvaru $b^n \pm 1$, kde b je „malé“ a n „velké“.

Je-li $b \geqq 2$ a $b^n + 1$ je prvočíslo, pak nutně $n = 2^m$. To plyne ze vztahu (3), kde zaměníme základ 2 za b.

Podobně ze vztahu (9) pro $k \geqq 2$ a $e \geqq 2$ plyne, že k tomu, aby bylo číslo $b^n - 1$ prvočíslem, je nutné, aby byl exponent n prvočíslem.

Tzv. zobecněná Fermatova čísla jsou definována vztahem $F_{b,m} = b^{2^m} + 1$. Je patrno, že $F_m = F_{2,m}$.

V současnosti je každý měsíc nalezeno zhruba 25 nových prvočíselných dělitelů Cunninghamových čísel. Tabulky jejich dělitelů pro $b \leqq 12$ jsou obsahem knihy [3]. Největší přínos Cunninghamova projektu ale spočívá v tom, že dal podnět k vytváření nových vysoce efektivních metod pro testování prvočíselnosti, hledání prvočíselných rozkladů apod.

6. Otevřené problémy

Na závěr uveďme nejdůležitější nerozřešené problémy týkající se Fermatových čísel.

1) Je prvočísel F_m konečně mnoho?
2) Je složených čísel F_m nekonečně mnoho?
3) Jsou prvočísla v (2) všechna Fermatova prvočísla?
4) Které pravidelné mnohoúhelníky jsou eukleidovsky konstruovatelné?
5) Existuje obecný vzorec rozkladu F_m pro $m \geqq 5$ podobně jako v (3)?
6) Je posloupnost $\{\Omega_m\}_{m=0}^{\infty}$ (viz (17)) monotónní?
7) Jaký je úplný rozklad čísel F_{10}, F_{12}, F_{13} atd. na prvočísla?
8) Jaký je nejmenší prvočinitel složených čísel F_{14}, F_{20} a F_{22}?
9) Existuje pro každé $m \geqq 5$ přirozené číslo h tak, že $5h2^{m+2} + 1 \mid F_m$?
10) Existuje F_m, které je dělitelné druhou mocninou nějakého prvočísla?

K problému 10) poznamenejme, že existuje domněnka, podložená pravděpodobnostním důkazem, že žádné Fermatovo číslo není dělitelné čtvercem žádného prvočísla. Tato hypotéza se prověřovala na počítačích téměř pro všechny známé dělitele F_m a zatím se ji nepodařilo vyvrátit. K jejímu prověřování se většinou používá následující věty (viz [9]):

Věta. *Jestliže prvočíslo p dělí F_m, pak*

$$p^2 \mid F_m \iff 2^{p-1} \equiv 1 \bmod p^2 \qquad \textit{(Wieferichova kongruence).} \tag{18}$$

Například test, zda čtverec prvočísla $p = 85 \cdot 2^{2458} + 1$ dělí F_{2456}, si vyžádal 165 hodin strojového času [6]. Přes veškeré úsilí počítačů jsou dodnes známa jen dvě prvočísla ($p = 1093$ a $p = 3511$ — viz [15]), která splňují Wieferichovu kongruenci v (18). Tato prvočísla ale nedělí žádné F_m, protože nejsou tvaru (10) pro $m \geqq 5$. Úzkou souvislost kongruence $2^{p-1} \equiv 1 \mod p^2$ s platností velké věty Fermatovy udává Wieferichova věta — viz článek [23], který nedávno vyšel v PMFA.

Závěrem mi dovolte poděkovat Mgr. Janě Daňkové, která svými cennými připomínkami přispěla ke zlepšení obsahu článku.

Literatura

[1] R. P. Brent: *Factorization of the eleventh Fermat number.* Abstracts Amer. Math. Soc. *10* (1989), 176–177.
[2] R. P. Brent, J. M. Pollard: *Factorization of the eighth Fermat number.* Math. Comp. *36* (1981), 627–630.
[3] J. Brillhart, D. H. Lehmer, J. L. Selfridge, B. Tuckerman, S. S. Wagstaff: *Factorization of $b^n \pm 1$, $b = 2, 3, 5, 6, 7, 10, 11, 12$ up to high powers.* Contemporary Math. vol. 22, Amer. Math. Soc., Providence 1988.
[4] R. Crandall, J. Doenias, C. Norrie, J. Young: *The twenty-second Fermat number is composite.* Math. Comp. *64* (1995), 863–868.
[5] L. E. Dickson: *History of the theory of numbers: Divisibility and primality.* Carnegie Inst. of Washington 1919.

[6] G. B. GOSTIN, P. B. MCLAUGHLIN, JR.: *Six new factors of Fermat numbers.* Math. Comp. *38* (1982), 645–649.

[7] G. H. HARDY, E. M. WRIGHT: *An introduction to the theory of numbers.* Clarendon Press, Oxford 1945.

[8] W. KELLER: *Factors of Fermat numbers and large primes of the form* $k \cdot 2^n + 1$. Math. Comp. *41* (1983), 661–673.

[9] W. KELLER: *Factors of Fermat numbers and large primes of the form* $k \cdot 2^n + 1$. *II.* Preprint Univ. of Hamburg (1992), 1-40.

[10] M. KŘÍŽEK, J. CHLEBOUN: *A note on factorization of the Fermat numbers and their factors of the form* $3h2^n + 1$. Math. Bohem. *119* (1994), 437–445.

[11] H. W. LENSTRA: *Factoring integers with elliptic curves.* Ann. of Math. *126* (1987), 649–673.

[12] A. K. LENSTRA, H. W. LENSTRA, JR., M. S. MANASSE, J. M. POLLARD: *The factorization of the ninth Fermat number.* Math. Comp. *61* (1993), 319–349.

[13] H. W. LENSTRA, C. POMERANCE: *A rigorous time bound for factoring integers.* J. Amer. Math. Soc. *5* (1992), 483–516.

[14] S. LIGH, P. JONES: *Generalized Fermat and Mersenne numbers.* Fibonacci Quart. *20* (1982), 12–16 .

[15] P. L. MONTGOMERY: *New solutions of* $a^{p-1} \equiv 1 \pmod{p}^2$. Math. Comp. *61* (1993), 361–363.

[16] M. A. MORRISON, J. BRILLHART: *A method of factoring and factorization of* F_7. Math. Comp. *29* (1975), 183–205.

[17] J. M. POLLARD: *Theorems on factorization and primality testing.* Math. Proc. Cambridge Philos. Soc. *76* (1974), 521–528.

[18] P. PUDLÁK: *O složitosti.* PMFA *33* (1988), 20–34.

[19] H. REISEL: *Prime numbers and computer methods for factorization.* Birkhäuser, Boston-Basel-Stuttgart 1985.

[20] R. M. ROBINSON: *The converse of Fermat's theorem.* Amer. Math. Monthly *64* (1957), 703–710.

[21] M. R. SCHROEDER: *Number theory in science and communication.* Springer-Verlag 1990.

[22] W. SIERPIŃSKI: *Teorija liczb.* Warszawa 1950.

[23] L. SKULA: *Některé historické aspekty Fermatova problému.* PMFA *39* (1994), 318–330.

[24] I. STEWART: *Geometry finds factors faster.* Nature *325* (1987), 199.

[25] T. ŠALÁT: *O dokonalých číslach.* PMFA *IX* (1964), 1–13.

[26] B. ŠOFR: *Euklidovské geometrické konštrukcie.* ALFA, Bratislava 1976.

[27] J. YOUNG, D. A. BUELL: *The twentieth Fermat number is composite.* Math. Comp. *50* (1988), 261–263.

[28] H. C. WILLIAMS: *How was* F_6 *factored?* Math. Comp. *61* (1993), 463–474.