Michal Křížek

Od Fermatových čísel ke geometrii

*Pokroky matematiky, fyziky a astronomie*, Vol. 46 (2001), No. 3, 179--191

Persistent URL: http://dml.cz/dmlcz/141082

# Od Fermatových čísel ke geometrii

Věnováno prof. O. Kowalskému k jeho 65. narozeninám.

*Michal Křížek, Praha*

## 1. Úvod

V letošním roce si připomínáme 400. výročí narození velkého francouzského matematika Pierra de Fermata (1601–1665). Jedno z jeho mylných tvrzení doslova způsobilo revoluci v teorii čísel i geometrii. Fermat se totiž domníval, že všechna čísla tvaru

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

jsou prvočísla. Prvních pět členů této posloupnosti $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$ a $F_4 = 65537$ prvočísla skutečně jsou. Avšak už číslo $F_5$ je složené, jak v roce 1732 zjistil Leonhard Euler (viz obr. 1). Čísla $F_m$ se nazývají *Fermatova čísla*. Je-li $F_m$ prvočíslo, říkáme, že je *Fermatovým prvočíslem*.

EUKLEIDES (4.–3. stol. př. n. l.):

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

PIERRE DE FERMAT (1601–1665):

*Pro* $m = 0, 1, 2, \ldots$ *je posloupnost* $F_m = 2^{2^m} + 1$ *tvořena prvočísly* (mylné tvrzení).

LEONHARD EULER (1707–1783):

$F_5 = 641 \times 6700417$.

CARL FRIEDRICH GAUSS (1777–1855):

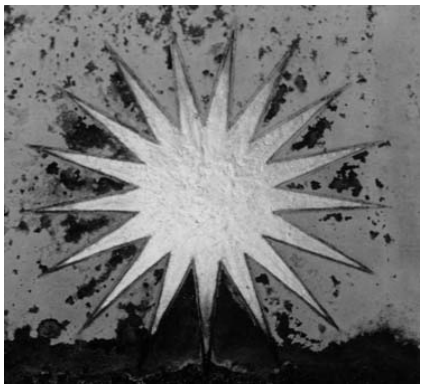
*Pravidelný n-úhelník lze zkonstruovat pomocí pravítka a kružítka právě tehdy, když platí* $n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j}$, *kde* $n \geqq 3$, $i \geqq 0$, $j \geqq 0$ *a* $F_{m_1}, F_{m_2}, \ldots, F_{m_j}$ *jsou vzájemně různá Fermatova prvočísla.*

Obr. 1. Historické milníky eukleidovské konstrukce pravidelných mnohoúhelníků.

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

## 2. Konstrukce pravidelných mnohoúhelníků

Do roku 1796 byla Fermatova čísla spíše matematickou kuriozitou. Zájem o ně vzrostl, když Carl Friedrich Gauss objevil až neuvěřitelnou souvislost mezi Fermatovými prvočísly a eukleidovskou konstrukcí (tj. pomocí kružítka a pravítka) pravidelných mnohoúhelníků. Gauss ve svých devatenácti letech zcela nečekaně nalezl eukleidovskou konstrukci pravidelného sedmnáctiúhelníka. Na počest tohoto fundamentálního objevu je na podstavci Gaussovy sochy (viz obr. 2) v jeho rodném Braunschweigu znázorněna pravidelná sedmnácticípá hvězda (nikoli na jeho hrobce v Göttingen, jak si Gauss původně přál).



Obr. 2. Zlatá sedmnácticípá hvězda na podstavci Gaussovy sochy v Braunschweigu.

O několik let později pak Gauss formuloval nutnou a postačující podmínku (viz obr. 1) udávající, kdy je pravidelný mnohoúhelník eukleidovsky konstruovatelný. Její původní důkaz, který má více než 50 stránek (viz [10, Sect. VII]), však není zcela úplný. Nutnost Gaussovy podmínky byla dokázána později, v roce 1837 Wantzelem [22] (viz též [17]). Pravidelný $n$-úhelník s lichým počtem vrcholů lze tedy zkonstruovat pro

$$n = 3, 5, 15, 17, 51, 85, 255, 257, \ldots, \tag{1}$$

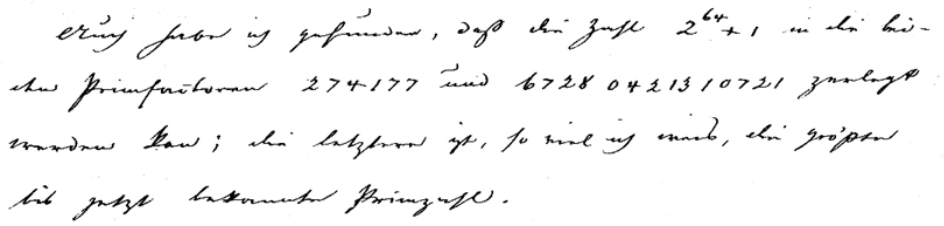
kde $15 = 3 \cdot 5$, $51 = 3 \cdot 17$, $85 = 5 \cdot 17$, $255 = 3 \cdot 5 \cdot 17$, ... jsou součiny Fermatových prvočísel.

Vyšetřování prvočíselnosti Fermatových čísel se tak stalo důležitým úkolem. Německý astronom Thomas Clausen píše 1. ledna 1855 Gaussovi (viz [3, str. 185]), že číslo $F_6$ je složené. Na obr. 3 je kopie části jeho dopisu, který je uložen v knihovně univerzity v Göttingen. Stejný výsledek publikoval nezávisle Landry až v roce 1880 (viz [15]).

V roce 1878 François Édouard Anatole Lucas dokázal (viz [16]) následující větu, která se stala mocným nástrojem pro hledání prvočinitelů Fermatových čísel.

*Jestliže prvočíslo $p$ dělí $F_m$ pro $m > 1$, pak existuje přirozené číslo $k$ tak, že*

$$p = k \cdot 2^{m+2} + 1.$$



Obr. 3. Část dopisu T. Clausena, ve kterém Gaussovi oznamuje, že se mu podařilo najít rozklad čísla $F_6$: *„Auch habe ich gefunden, daß die Zahl* $2^{64}+1$ *in die beiden Primfactoren* 274177 *und* 67280421310721 *zerlegt werden kann; die letztere ist, so viel ich weiß, die größte bis jetzt bekannte Primzahl.“*

Užitečnost Lucasovy věty si ukažme na úloze, kterou se zabýval A. E. Western v roce 1903. Šlo o to zjistit, zda $F_{18}$ je číslo složené. Počet jeho cifer je úctyhodný — téměř 80 000, protože

$$\log_{10}(2^{2^{18}}+1)+1 \approx \log_{10} 2^{2^{18}}+1 = 2^{18}\log_{10} 2+1 \doteq 78\,914.$$

Podle Lucasovy věty je třeba najít přirozené číslo $k$ tak, aby $k\cdot 2^{20}+1$ dělilo $F_{18}$ a aby $k\cdot 2^{20}+1$ bylo prvočíslo. Tímto způsobem Western poměrně snadno zjistil, že hledané číslo $k$ je 13, protože pro menší hodnoty $k$ (kromě případu $k=7$) jsou čísla $k\cdot 2^{20}+1$ složená.

Jak ale můžeme ověřit, že $p = 13\cdot 2^{20}+1 = 13631489$ skutečně dělí obrovské Fermatovo číslo $F_{18}$? To lze snadno zjistit pomocí následujícího řetězce kongruencí:

$$\begin{aligned}
2^{2^5} &\equiv 65536^2 \equiv 1048261 \pmod p,\\
2^{2^6} &\equiv 1048261^2 \equiv 3164342 \pmod p,\\
2^{2^7} &\equiv 3164342^2 \equiv 9153547 \pmod p,\\
&\vdots \qquad\qquad \vdots\\
2^{2^{17}} &\equiv 1598622^2 \equiv 1635631 \pmod p,\\
2^{2^{18}} &\equiv 1635631^2 \equiv 13631488 \pmod p,
\end{aligned}$$

kde na pravých stranách stojí zbytky při dělení prvočíslem $p$. Tudíž

$$2^{2^{18}}+1 \equiv 0 \pmod{13631489}.$$

Díky moderním matematickým metodám a výkonné výpočetní technice dnes již víme, že

$$F_m \text{ je složené pro } 5 \leqq m \leqq 30,$$

i když pro $F_{14}$, $F_{20}$, $F_{22}$ a $F_{24}$ zatím neznáme žádného netriviálního dělitele (viz [12]). Číslo $F_{24}$ má přes 5 miliónů cifer. Důkaz toho, že je to číslo složené, si vyžádal provedení $10^{17}$ aritmetických operací (viz [6]). Byl to zatím nejrozsáhlejší výpočet, jehož výsledkem byla jednobitová informace typu ANO/NE. Zatím není známo, zda

$F_{31}$ je číslo složené či prvočíslo. Nevíme tedy, zda je současný seznam eukleidovsky konstruovatelných pravidelných mnohoúhelníků již úplný.

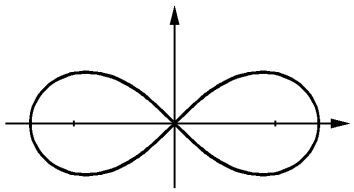
Přestože je dnes známo přes dvě stě prvočinitelů (viz [23]) různých Fermatových čísel, stále se nedaří vysledovat mezi nimi takovou zákonitost, která by vedla k definitivní odpovědi na to, zda je $F_4$ největší Fermatovo prvočíslo. Otevřeným problémem také stále zůstává, zda je Fermatových prvočísel konečně či nekonečně mnoho.

## 3. O dalších souvislostech Fermatových čísel s geometrií

C. F. Gauss rovněž objevil způsob, jak rozdělit lemniskátu na pět stejně dlouhých částí (viz [20]). Jeho výsledek později zobecnil Niels Henrik Abel takto:

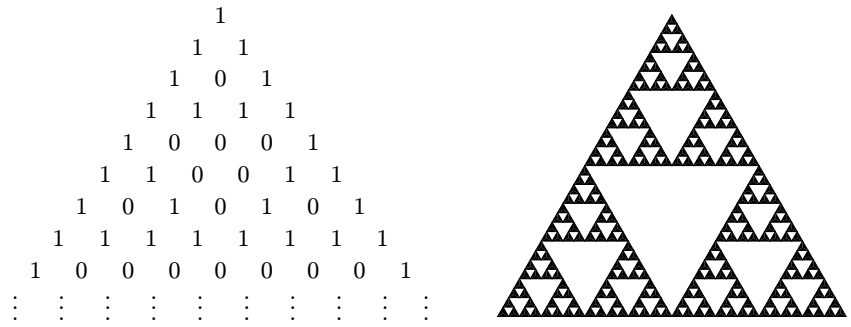
*Lemniskáta může být rozdělena na $n$ stejně dlouhých částí pomocí pravítka a kružítka, když $n = 2^i F_{m_1} F_{m_2} \cdots F_{m_j}$, kde $i \geqq 0$ a $j \geqq 0$ jsou celá čísla a $F_{m_1}$, $F_{m_2}$, …, $F_{m_j}$ jsou vzájemně různá Fermatova prvočísla.*

Podrobný důkaz tohoto tvrzení je uveden v [20]. Připomeňme, že (Bernoulliho) lemniskáta je uzavřená křivka, jejíž body mají od dvou pevných bodů $\left(\pm(a/2)\sqrt{2},\, 0\right)$ konstantní součin vzdáleností rovný $a^2/2$, kde $a > 0$ je reálný parametr ($a = \sqrt{2}$ na obr. 4).



Obr. 4. Lemniskáta $(x^2 + y^2)^2 = a^2(x^2 - y^2)$.

Ukažme si další pozoruhodný vztah mezi teorií čísel a konstrukcí pravidelných mnohoúhelníků. Uvažujme známý Pascalův trojúhelník modulo 2, tj. sudá čísla v Pascalově trojúhelníku nahradíme nulou a lichá jedničkou (viz levá část obr. 5):




Obr. 5. Pascalův trojúhelník modulo 2 a Sierpińského fraktální množina.

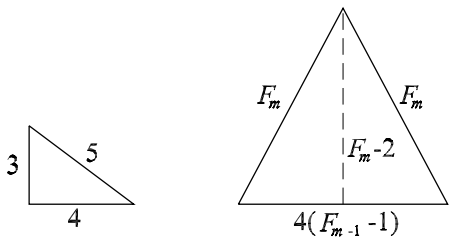
Každý řádek tak představuje číslo zapsané ve dvojkové soustavě. Převedeme-li nyní tato čísla do desítkové soustavy, dostaneme posloupnost

$$1, 3, 5, 15, 17, 51, 85, 255, 257, \ldots, \tag{2}$$

která je rostoucí, protože každý řádek v trojúhelníku z obr. 5 začíná 1 a je o jednu dvojkovou cifru delší než předchozí řádek. Porovnejme nyní posloupnosti (1) a (2). Není to malý zázrak? Důkaz této zajímavé shody je uveden v [9] (viz též [14, str. 81]). Povšimněte si ještě, že Pascalův trojúhelník modulo 2 má podobnou strukturu jako známá Sierpińského fraktální množina (srov. obr. 5).

I Heronův trojúhelník souvisí s Fermatovými prvočísly. Připomeňme, že trojúhelník, jehož délky stran i obsah jsou celočíselné, se nazývá *Heronův trojúhelník*. Následující tvrzení je dokázáno v [14].

*Nechť délky stran Heronova trojúhelníku jsou mocniny prvočísel. Pak jsou tyto délky stran buď rovny* 3, 4, 5, *anebo* $F_m$, $F_m$, $4(F_{m-1}-1)$ *pro nějaké* $m \geqq 1$, *pro něž je* $F_m$ *prvočíslo* (viz obr. 6).




Obr. 6. Jediné možné Heronovy trojúhelníky, jejichž délky stran jsou mocniny prvočísel.

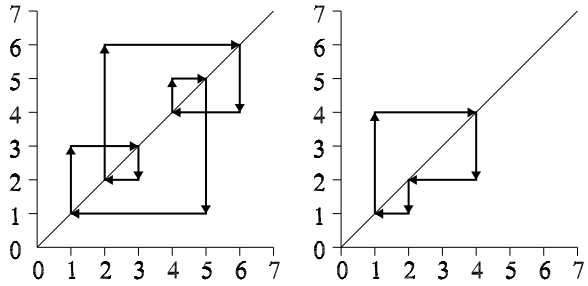
Prvočíselnost $F_m$ má překrásnou geometrickou interpretaci, kterou v roce 2000 objevili Jones a Pearce (viz [11]). Nejprve si ale popíšeme algoritmus, jak lze graficky zobrazovat zlomky tvaru $1/n$.

Nechť $b > 1$ a $n$ jsou celá čísla. Jestliže $r_i$ je zbytek v $i$-tém kroku při dělení $1/n$ vzhledem k základu $b$, pak zbytek v následujícím kroku $i+1$ splňuje kongruenci

$$r_{i+1} \equiv b r_i \pmod{n}.$$

Začneme-li s $r_0 = 1$, dostaneme posloupnost zbytků $r_0$, $r_1$, $r_2$, ... pro $1/n$ odpovídajících základu $b$. Tuto skutečnost můžeme v rovině graficky znázornit takto (viz obr. 7): z bodu $(r_0, r_0)$ veďme úsečku nejprve vertikálně a pak horizontálně do bodu $(r_1, r_1)$. Odtud opět vedeme úsečku nejprve vertikálně a pak horizontálně do bodu $(r_2, r_2)$ atd. Pokud v $i$-tém kroku dostaneme nulový zbytek, algoritmus ukončíme. Posloupnost zbytků tak jednoznačně určuje výsledný graf.

Uvažujme například zlomek $\frac{1}{7}$, který má při základu 10 rozvoj $0{,}\overline{142857}$. Odpovídající posloupnost zbytků je periodická, $r_0 = 1$, $r_1 = 3 \equiv 10 \pmod{7}$, $r_2 = 2 \equiv 30$




$b = 10$ $b = 11$

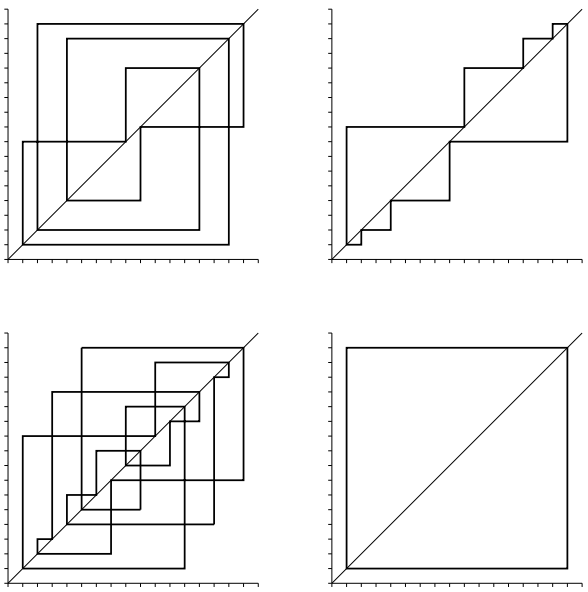
Obr. 7. Grafické znázornění zlomku $\frac{1}{7}$ pro dva různé základy.

(mod 7), $r_3 = 6 \equiv 20 \pmod 7$, $r_4 = 4 \equiv 60 \pmod 7$, $r_5 = 5 \equiv 40 \pmod 7$, $r_0 = r_6 = 1 \equiv 50 \pmod 7$ atd. Z obr. 7 je patrno, že příslušný graf je středově symetrický vzhledem k bodu $\left(\frac{7}{2}, \frac{7}{2}\right)$ při základu $b = 10$, ale je nesymetrický při základu $b = 11$.

Přirozené číslo $n > 1$ nazveme *perfektně symetrické*, jestliže graf odpovídající zlomku $1/n$ je středově symetrický vzhledem k bodu $(n/2, n/2)$ pro každý základ $b$, pro který $b \not\equiv 0 \pmod n$ a $b \not\equiv 1 \pmod n$. Jones a Pearce v [11] dokazují následující nutnou a postačující podmínku:

*Přirozené číslo $n > 1$ je perfektně symetrické právě tehdy, když $n$ je Fermatovo prvočíslo nebo $n = 2$.*

Na obrázku 8 jsou znázorněny grafy odpovídající zlomku $1/F_2$ pro několik různých základů.



Obr. 8. Grafy odpovídající zlomku $\frac{1}{17}$ při základech $b = 8$, 9, 10 a 16.

V [14] je dokázáno patnáct dalších nutných a postačujících podmínek na prvočíselnost $F_m$. O souvislosti Fermatových prvočísel s pěti platonskými tělesy (pravidelnými mnohostěny) se můžete dočíst v [13].

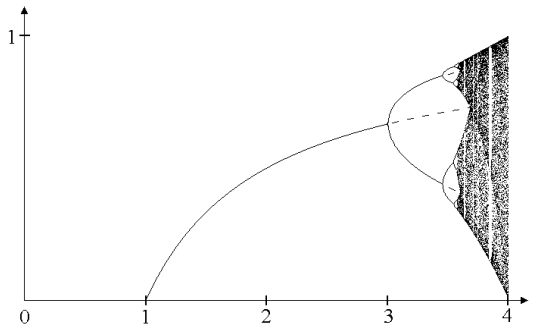
## 4. Fermatova čísla a bifurkace logistické rovnice

V této kapitole se zmíníme o překvapivé souvislosti (viz [2]) Fermatových čísel s logistickou rovnicí, která zapříčinila bouřlivý rozvoj teorie chaosu. V sedmdesátých letech M. J. Feigenbaum řešil iteračně na běžné kapesní kalkulačce tzv. *logistickou rovnici* (viz [8])

$$x_{n+1} = \lambda x_n(1 - x_n), \quad n = 1, 2, \ldots, \tag{3}$$

jež popisuje například evoluci dynamického biologického systému. Lineární člen $\lambda x_n$ charakterizuje růst jisté populace, zatímco kvadratický člen $(-\lambda x_n^2)$ reprezentuje její úbytek v důsledku nějakého procesu. Pro pevný parametr $\lambda$ a zadanou počáteční hodnotu $x_1 \in [0, 1]$ může mít posloupnost $\{x_n\}$ různý počet hromadných bodů.

Jak je patrno z obr. 9, řešení jednoduchého nelineárního matematického modelu (3) mají značně komplikovanou strukturu s množstvím bifurkací. První z nich je v bodě $\lambda_1 = 1$. Odpovídající „větev řešení“ je dána funkcí $f(\lambda) = 1 - 1/\lambda$ pro $\lambda \in [1, 4]$, která popisuje stabilní rovnovážný stav až do druhého bifurkačního bodu $\lambda_2 = 3$. Další bifurkační body jsou v $\lambda_3 \doteq 3{,}44949$, $\lambda_4 \doteq 3{,}54409$ atd. V nich dochází k tzv. „zdvojování period“, o čemž se zmíníme později.




Obr. 9. Feigenbaumova cesta k chaosu. Pro vzrůstající hodnotu řídicího parametru $\lambda \in [0, 4]$ obrázek ilustruje množinu odpovídajících hromadných bodů všech posloupností $\{x_n\}$ pro všechny počáteční hodnoty $x_1 \in [0, 1]$.

Pro $\lambda > \lambda_2$ existuje konstantní (ale nestabilní) řešení s počáteční podmínkou $x_1 = x_1(\lambda)$ ležící na grafu funkce $f$, např. $x_n = 0{,}7$ pro všechna přirozená $n$ a $\lambda = \frac{10}{3}$. Podobně pro $\lambda > \lambda_3$ existují další nestabilní řešení. Například $x_n = \frac{6}{7}$ pro $n$ liché, $x_n = \frac{3}{7}$ pro $n$ sudé a $\lambda = \frac{7}{2}$. Tato nestabilní řešení jsou znázorněna v obr. 9 přerušovanou čarou.

Jestliže počáteční hodnota $x_1 \in (0, 1]$ neleží na grafu funkce $f$, dostaneme 2 hromadné body pro $\lambda \in (\lambda_2, \lambda_3]$. Podobně hodnotě $\lambda \in (\lambda_3, \lambda_4]$ obecně odpovídají 4 hromadné body atd. Jak uvidíme později, tyto hromadné body budou generovat nekonstantní periodická řešení. Zvolíme-li například $\lambda \in (\lambda_2, \lambda_3]$ a počáteční hodnotu $x_1$ na horní nebo dolní větvi, bude odpovídající posloupnost $\{x_n\}$ oscilovat mezi těmito dvěma hodnotami.

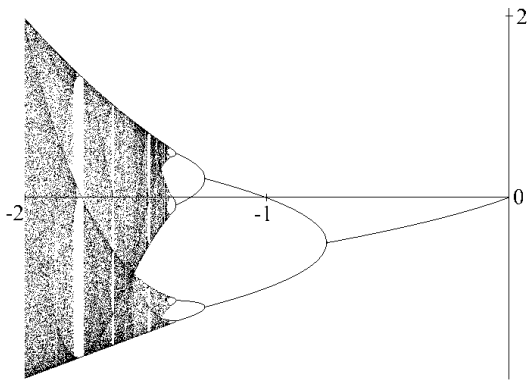
Pomocí jednoduché transformace

$$x_n = \frac{1}{2} - \frac{y_n}{\lambda} \tag{4}$$

lze logistickou rovnici (3) přepsat do kanonického tvaru (srov. obr. 10)

$$y_{n+1} = y_n^2 + b, \tag{5}$$

kde $b = \lambda/2 - \lambda^2/4$.



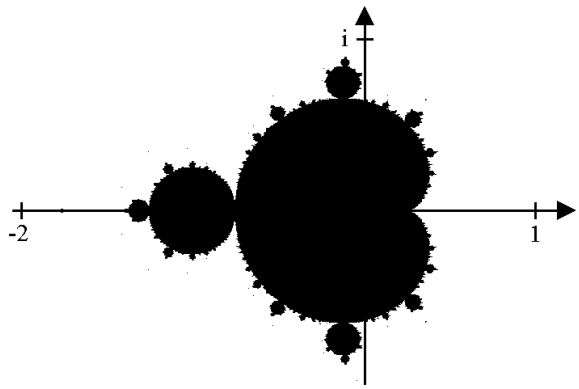

Obr. 10. Hromadné body posloupností $\{y_n\}$ pro parametr $b \in [-2, 0]$ a pro všechny počáteční hodnoty $y_1 \in [-2, 2]$. Nestabilní řešení nejsou znázorněna.

Rovnici (5) je výhodné vyšetřovat v komplexní rovině $\mathbb{C}$, tj. $b$, $y_n \in \mathbb{C}$. Poznamenejme, že některé fraktální objekty v komplexní rovině jsou popsány pomocí stejné rovnice jako chaos v reálné proměnné. Označme závislost posloupnosti (5) na parametru $b$ obvyklým způsobem: $y_n = y_n(b)$. Pak pro počáteční podmínky $y_1(b) = 0$ pro všechna $b \in \mathbb{C}$ je množina $M$ všech ohraničených posloupností $\{y_n(b)\}_{n=1}^{\infty}$ *Mandelbrotova množina*, tj.

$$M = \left\{ b \in \mathbb{C} \mid \exists c > 0 \ \forall n \in \{1, 2, \ldots\} : |y_n(b)| \leqq c \right\}$$

(viz obr. 11). Pokud každému bodu $b \in \mathbb{C} \setminus M$ přiřadíme jistý barevný odstín podle „rychlosti divergence“ posloupnosti $\{y_n(b)\}_{n=1}^{\infty}$, získáme tak známé barevné obrázky okolí Mandelbrotovy množiny.

Řešení $\{y_n\}_{n=1}^{\infty}$ rovnice (5) se nazývá *periodické*, jestliže existuje přirozené číslo $p$ tak, že $y_{n+p} = y_n$ pro všechna přirozená $n$ a $y_{n+r} \neq y_n$ pro všechna $r \in \{1, \ldots, p-1\}$.




Obr. 11. Mandelbrotova množina všech komplexních čísel $b$, pro něž je posloupnost $y_1(b) = 0$, $y_2(b)$, $y_3(b)$, ... definovaná vztahem (5) ohraničená.

Číslo $p$ se pak nazývá *minimální perioda* a jakýkoliv její přirozený násobek *perioda*. Ostatní řešení se nazývají *neperiodická*. Periodická a neperiodická řešení rovnice (3) se definují analogicky.

Antonjuk a Stanjukovič v článku [2] nejprve vyšetřují nejjednodušší případ rovnice (5) pro $b = 0$, tj.

$$y_{n+1} = y_n^2. \tag{6}$$

Všechna řešení (periodická i neperiodická) rovnice (6) mají tvar

$$y_n = a^{2^n}, \quad a \in \mathbb{C}.$$

Všechna řešení s periodou $p$ (ale i periodou $q$, která dělí $p$) splňují vztah

$$y^{2^p} - y = 0.$$

Při tzv. zdvojování period se vyšetřují všechna periodická řešení s periodou $p = 2^m$, $m = 0, 1, 2, \ldots$ (nebo periodou $q$, která dělí $p$). Ta jsou definována rovnicí

$$y^{2^{2^m}} - y = 0.$$

Vyloučíme-li triviální řešení $y_n = 0$, dostaneme

$$y^{2^{2^m}-1} - 1 = 0. \tag{7}$$

Periodická řešení splňující (7) zřejmě musí ležet na jednotkové kružnici v komplexní rovině.

Matematickou indukcí lze snadno odvodit velice užitečný vztah (viz např. [14])

$$F_m - 2 = 2^{2^m} - 1 = \prod_{k=0}^{m-1} (2^{2^k} + 1) = \prod_{k=0}^{m-1} F_k. \tag{8}$$

Exponent v rovnici (7) lze tedy napsat jako součin Fermatových čísel. To nám umožňuje rozložit polynom na levé straně (7) na ireducibilní cyklotomické polynomy nižšího řádu. Hledání těchto polynomů je proto spojeno s rozkladem Fermatových čísel z pravé strany rovnice (8) na prvočísla.

Pokud $F_m$ a $F_{m+1}$ jsou dvě po sobě následující prvočísla, počet „bifurkačních větví“ se zdvojnásobí. To nastává pro hodnoty $p = 2,\ 4,\ 8,\ 16,\ 32$. Fermatovo číslo $F_5$ je ale složené, proto pro periodu $p = 2^6 = 64$ nastává zajímavý úkaz, kdy se počet bifurkačních větví zešestinásobí (viz [2]). Pro další čísla $F_6$, $F_7$ a $F_8$ se počet větví zečtyřnásobí. Značně komplikovaná situace nastává pro další Fermatova čísla, která mají více netriviálních dělitelů.

Případ rovnice (5) pro $b \neq 0$ se v [2] vyšetřuje pomocí teorie perturbací. Opět existuje vzájemně jednoznačný vztah mezi jednotlivými bifurkačními větvemi a cyklotomickými polynomy. Užijeme-li zpětně transformaci (4), dostaneme analogické výsledky také pro rovnici (3). To znamená, že v bifurkačním bodě $\lambda_6$ se každá větev rozdělí na šest dalších větví. Pouze některé z nich se chovají jako atraktory. Ostatní větve se chovají jako repelory, a proto je velice obtížné je spočítat numericky. V bodě $\lambda_7$ se každá větev rozdělí na čtyři větve atd.

## 5. Fermatova transformace a další aplikace Fermatových čísel

Na závěr se krátce zmíníme o některých technických aplikacích $F_m$. Fermatova čísla mají zajímavé použití při digitálním zpracování signálů. Pro jednoduchost předpokládejme, že $F_m$ je prvočíslo. Nechť $\alpha \in \{2, 3, \dots, F_m - 1\}$ je dáno a nechť $N$ je zvoleno tak, že $N$ dělí tzv. řád $e = \operatorname{ord}_{F_m} \alpha$, tj. nejmenší exponent, pro který $\alpha^e \equiv 1 \pmod{F_m}$.

Číslo $N$ se nazývá *délka transformace* a $\operatorname{ord}_{F_m} \alpha$ *maximální délka transformace*. Například pro $m \geqq 1$ a $\alpha = 3$ je maximální délka transformace rovna $2^{2^m}$, jak plyne z Pepinova testu, o němž jsme již psali ve [12]. Jestliže $\alpha = 2$, pak je $\operatorname{ord}_{F_m} \alpha = 2^{m+1}$ pro $m = 0,\ 1,\ \dots$ .

Fermatova transformace pro rychlé zpracování digitálních signálů byla poprvé navržena v [1]. Digitální signál je reprezentován vektorem $x = \big(x(0), x(1), \dots, x(N-1)\big)$ celých čísel takových, že $x(k) \in \{0,\ 1,\ \dots,\ F_m - 1\}$ pro $k = 0,\ 1,\ \dots,\ N-1$. Jednorozměrná *Fermatova transformace* a její inverze jsou pak definovány vztahy

$$\begin{aligned} X(j) &\equiv \sum_{k=0}^{N-1} x(k)\alpha^{jk} \pmod{F_m}, && j = 0, 1, \dots, N-1, \\ x(k) &\equiv N^{-1} \sum_{j=0}^{N-1} X(j)\alpha^{-jk} \pmod{F_m}, && k = 0, 1, \dots, N-1, \end{aligned} \tag{9}$$

kde $X(j) \in \{0,\ 1,\ \dots,\ F_m - 1\}$ pro všechna $j \in \{0,\ 1,\ \dots,\ N-1\}$ a $N^{-1}$ označuje celé číslo, pro něž $NN^{-1} \equiv 1 \pmod{F_m}$.

Jak známo, Fourierova a Laplaceova transformace jsou definovány pro spojité signály, které musí být pro počítačovou implementaci diskretizovány. Pro porovnání

s (9) připomeňme, že *diskrétní Fourierova transformace* a její inverze jsou definovány v komplexním oboru podobnými vztahy

$$Y(j) = \sum_{k=0}^{N-1} y(k)\,\mathrm{e}^{-2\pi\mathrm{i}jk/N}, \qquad j = 0, 1, \ldots, N-1,$$

$$y(k) = N^{-1} \sum_{j=0}^{N-1} Y(j)\,\mathrm{e}^{2\pi\mathrm{i}jk/N}, \quad k = 0, 1, \ldots, N-1,$$

kde $N^{-1} = 1/N$ je nyní na rozdíl od (9) reálné číslo. Diskrétní Fourierova transformace vyžaduje $N^2$ násobení komplexních čísel. Poznamenejme, že počet násobení lze zredukovat na $\mathcal{O}(N \log N)$, pokud $N$ je mocnina 2 (viz tzv. rychlá Fourierova transformace zavedená v [5]). Naproti tomu Fermatova transformace a její inverze vyžadují provedení pouze $\mathcal{O}(N \log N)$ sčítání, odečítání, posunů o bit, ale žádné násobení. V počítačové aritmetice modulo $F_m$ lze totiž převést příslušná násobení na „bitové“ posuny (viz [14]).

Fermatova transformace umožňuje jednoduše počítat konvoluce digitálních signálů (viz [1]) pomocí podobných vztahů jako pro diskrétní Fourierovu transformaci. Důležité však je, že nedochází k žádným zaokrouhlovacím chybám, protože výpočet probíhá v celočíselné aritmetice.

V roce 1978 Reed, Truong a Welch publikovali efektivní algoritmus pro rychlé dekódování Reedových-Solomonových kódů pomocí Fermatovy transformace (viz [18]). Poznamenejme, že například kompaktní disky CD jsou chráněny proti drobnému poškrábání pomocí známých Reedových-Solomonových samoopravujících se kódů, které umožňují dodatečně vypočítat ztracenou informaci. Samoopravující se kódy se také používají např. při přenosu dat z meziplanetárních sond.

Schönhage a Strassen[1]) v roce 1971 předložili rychlý algoritmus pro násobení velkých čísel o $N$ cifrách, který vyžaduje provedení jen $\mathcal{O}(N \log N \log\log N)$ aritmetických operací (viz [21]). Tento algoritmus je založen na aritmetice modulo $F_m$. Poznamenejme, že běžný algoritmus pro násobení dvou čísel, který se děti učí ve škole, vyžaduje $\mathcal{O}(N^2)$ operací.

Pro výpočet Fermatovy transformace (9) se používá binární aritmetika modulo $F_m$. V [7] je podrobně popsáno, jak efektivně provádět základní operace v této aritmetice.

V článku [4] je uvedena další zajímavá aplikace Fermatových čísel při vytváření hešovacích funkcí (angl. hashing functions), které každé hodnotě ukládané v paměti počítače přiřadí adresu, kam se má tato hodnota uložit.

Fermatova čísla lze také použít ke konstrukci generátorů pseudonáhodných čísel. Posloupnost pseudonáhodných čísel $X_i \in [0, 1)$ lze definovat např. takto (viz [19, str. 40])

$$X_i = \frac{r_i - 1}{F_4 - 1} \quad \text{pro} \quad i = 1, 2, \ldots,$$

[1]) V. Strassen se již dříve proslavil překvapivým výsledkem, že Gaussova eliminace není optimální vzhledem k asymptotickému počtu operací — viz Numer. Math. *13* (1969), 354–356.

kde $r_i \in \{1, \ldots, F_4 - 1\}$ je zbytek takový, že

$$r_i \equiv 75 r_{i-1} \pmod{F_4} \quad \text{a} \quad r_0 = 1.$$

Délka periody této posloupnosti je 65 536, což je maximální možná délka pro číslo $F_4$ (viz [14]). Poznamenejme ještě, že generátory pseudonáhodných čísel se používají k získání prvočíselných rozkladů, při testování prvočíselnosti, při simulaci některých fyzikálních procesů, při řešení parciálních diferenciálních rovnic metodou Monte Carlo (zejména ve vícerozměrném prostoru), v kryptografii pro generování pseudonáhodných posloupností bitů, ve všech počítačových hrách, kde je zapotřebí nějaké nahodilosti, aj.

V monografii [14] uvádíme některé další aplikace Fermatových čísel.

**Poděkování.** Autor děkuje paní Baerbel Mund z Niedersaechsische Staats- und Universitätsbibliothek v Göttingen za laskavé zaslání kopie dopisu Thomase Clausena z obr. 3 a F. Lucovi, L. Somerovi a A. Šolcové za cenné připomínky.

L i t e r a t u r a

[1] Agarwal, R. C., Burrus, C. S.: *Fast convolution using Fermat number transforms with applications to digital filtering.* IEEE Trans. Acoust. Speech Signal Processing *22* (1974), 87–97.

[2] Antonjuk, P. N., Stanjukovič, K. P.: *The logistic difference equation. Period doublings and Fermat numbers* (Russian). Dokl. Akad. Nauk SSSR *313* (1990), 1289–1292.

[3] Biermann, K.-R.: *Thomas Clausen, Mathematiker und Astronom.* J. Reine Angew. Math. *216* (1964), 159–198.

[4] Chang, C. C.: *An ordered minimal perfect hashing scheme based upon Euler's theorem.* Inform. Sci. *32* (1984), 165–172.

[5] Cooley, J. W., Tukey, J. W.: *An algorithm for the machine calculation of complex Fourier series.* Math. Comp. *19* (1965), 297–301.

[6] Crandall, R. E., Mayer, E., Papadopoulos, J.: *The twenty-fourth Fermat number is composite.* Math. Comp., submitted (1999), 1–21.

[7] Creutzburg, R., Grundmann, H.-J.: *Fast digital convolution via Fermat number transform* (German). Elektron. Informationsverarb. Kybernet. *21* (1985), 35–46.

[8] Feigenbaum, M. J.: *Quantitative universality for a class of nonlinear transformations.* J. Stat. Phys. *19* (1978), 25–52.

[9] Hewgill, D.: *A relationship between Pascal's triangle and Fermat's numbers.* Fibonacci Quart. *15* (1977), 183–184.

[10] Gauss, C. F.: *Disquisitiones arithmeticae* (přeloženo z latinského originálu z r. 1801). Springer, Berlin 1986.

[11] Jones, R., Pearce, J.: *A postmodern view of fractions and the reciprocals of Fermat primes.* Math. Mag. *73* (2000), 83–97.

[12] Křížek, M.: *O Fermatových číslech.* PMFA *40* (1995), 243–253.

[13] Křížek, M., Křížek, P.: *Kouzelný dvanáctistěn pětiúhelníkový.* Rozhledy mat.-fyz. *74* (1997), 234–238.

[14] Křížek, M., Luca, F., Somer, L.: *17 lectures on Fermat numbers: From number theory to geometry.* Springer-Verlag, New York 2001.

[15] Landry, F.: *Sur la décomposition du nombre* $2^{64} + 1$. C. R. Acad. Sci. Paris *91* (1880), 138.

[16] Lucas, E.: *Théorèmes d'arithmétique.* Atti della Realle Accademia delle Scienze di Torino *13* (1878), 271–284.
[17] Pierpont, J.: *On an undemostrated theorem of the Disquisitiones Arithmeticæ.* Bull. Amer. Math. Soc. *2* (1895/96), 77–83.
[18] Reed, I. S., Truong, T. K., Welch, L. R.: *The fast decoding of Reed-Solomon codes using Fermat transforms.* IEEE Trans. Inform. Theory *24* (1978), 497–499.
[19] Ripley, B. D.: *Stochastic simulations.* John Wiley & Sons, New York 1987.
[20] Rosen, M.: *Abel's theorem on the lemniscate.* Amer. Math. Monthly *88* (1981), 387–395.
[21] Schönhage, A., Strassen, V.: *Fast multiplication of large numbers* (German). Computing *7* (1971), 281–292.
[22] Wantzel, P. L.: *Recherches sur les moyens de reconnaître si un Problème de Géométrie peut se résoudre avec la règle at le compas.* J. Math. *2* (1837), 366–372.
[23] `http://www.prothsearch.net/fermat.html`

# Padesát let výpočtů koeficientů vnitřní konverze záření gama

*Otokar Dragoun a Miloš Ryšavý, Praha*

Podobně jako excitované atomy přecházejí i vzbuzená atomová jádra do nižších energetických stavů často emisí monoenergetických fotonů. V obou případech jsou tyto přechody vyvolány elektromagnetickou interakcí a platí při nich zákony zachování energie, hybnosti, momentu hybnosti a parity. Spektroskopie rentgenovských i měkčích fotonů a stejně tak i spektroskopie jaderného záření gama to využívají ke stanovení kvantových charakteristik vzbuzených stavů zkoumaných objektů.

Při výzkumu atomů se však setkáváme i s neradiačním deexcitačním procesem, při kterém jsou emitovány skupiny monoenergetických Augerových elektronů. Již při prvních měřeních magnetickými spektrometry na začátku 20. století se ukázalo, že k emisi monoenergetických elektronů dochází i při radioaktivních přeměnách. V té době již bylo známo Roentgenovo záření i Einsteinova rovnice fotoelektrického jevu. Bylo proto přirozené předpokládat, že dochází k „vnitřní konverzi záření gama“: jádro emituje foton, který vyvolá fotoefekt na některém z elektronů vlastního atomového obalu (foton se tedy uvnitř atomu „konvertuje“ na elektron). Ze změřené energie vzniklého fotoelektronu lze pak stanovit energii jaderného přechodu.

Brzy se však ukázalo [1], že představa vnitřního fotoefektu je nesprávná a že proces probíhá přímou elektromagnetickou interakcí mezi vzbuzeným jádrem a některým

Ing. Otokar Dragoun, DrSc. (1937), a RNDr. Miloš Ryšavý, CSc. (1947), Ústav jaderné fyziky AVČR, 250 68 Řež, e-mail: `dragoun@ujf.cas.cz`, `rysavy@ujf.cas.cz`