6. Fermatova prvočísla

PIERRE FERMAT (1601 -- 1665) byl jedním z matematických géniů 17.století. Celý život prožil v jihofrancouzském Toulouse a jeho nejbližším okolí, nikdy dokonce ani nenavštívil Paříž, ačkoliv si s tamější vědeckou komunitou dopisoval. Nebyl dokonce ani povoláním matematik, těch ostatně bylo v té době nemnoho. Nevíme ani, zda jeho nejbližší okolí za jeho života tušilo, že jedna ze zálib ctihodného soudního rady, pana P. de Fermat, jak byl někdy též titulován, ho zařadí mezi nejvýznamnější světové matematiky všech dob. S největší pravděpodobností spíše oceňovalo jeho vynikající klasické vzdělání, dokonalou znalost latiny, řečtiny, italštiny a španělštiny; tyto jazyky znal natolik dobře, že v nich psal i verše a na překlady z řečtiny byl vyhlášeným expertem.

Rekapitulujeme-li jeho matematické výsledky, musíme se zmínit o tom, že dosáhl významných výsledků v **matematické analýze**, jimiž připravoval půdu k založeni infinitesimálního počtu o několik desetiletí později; že společně s DESCARTEM položil základy **analytické geometrie** a že je považován za zakladatele **teorie čísel**. Fermatova intuice a jasnozřivost byla opravdu mimořádná. (Jedním z nejznámějších dokladů je tzv. **Velká Fermatova věta**, tj. tvrzení, že rovnice $x^n + y^n = z^n$ nemá pro $n > 2$ netriviální celočíselné řešení. Důkaz této věty byl po staletích marného snažení proveden až v r. 1995.

O to zajímavější je následující případ, v němž se Fermat spletl a to naprosto zásadně. Jak k tomu došlo?

Fermat studoval dokonalá čísla. Jak již víme, souvisejí tato čísla bezprostředně s Mersennovými prvočísly, tj. prvočísly tvaru $2^n - 1$. Není tedy překvapující, že si položil otázku, kdy jsou prvočísly čísla podobného tvaru: $2^n + 1$. Fermat vyslovil, že čísla tvaru

$$F_m = 2^{2^m} + 1$$

jsou pro m = 0, 1, 2, …prvočísla.

Jak na tuto hypotézu Fermat přišel? Platí následující evidentní tvrzení, které Fermat bezesporu znal (nebo si je odvodil):

Je-li p *přirozené a* q > 1 *liché, platí*

$$2^{pq}+1 = (2^p+1)(2^{p(q-1)} - 2^{p(q-2)} + .. - 2^p + 1) .$$

Odtud okamžitě plyne, že číslo tvaru $2^n + 1$ může být pro $n > 1$ prvočíslem pouze tehdy, když exponent n nemá lichého prvočinitele, tj. je tvaru 2^m. Fermat navíc spočítal pět prvních čísel F_m:

$$F_0 = 3, \quad F_1 = 5, \quad F_2 = 17, \quad F_3 = 257, \quad F_4 = 65\,537$$

a zjistil, že jsou to vesměs prvočísla. Formulace výše uvedené hypotézy se tedy zdá naprosto logická.

Fermat sám několikrát ve své korespondenci uvedl, že obecný důkaz této hypotézy se mu sice nepodařilo nalézt, věnoval však problematice tolik úsilí a provedl tolik namáhavých výpočtů, že je o pravdivosti této hypotézy zcela přesvědčen. (Poznamenejme, že Fermat své výsledky -- až na čestné výjimky -- nepublikoval a zachovaly se jen v jeho četné korespondenci nebo jako vpisky do literatury, kterou studoval. Za zachování většiny výsledků tak vděčíme Fermatovu synovi Samuelovi, rovněž soudnímu radovi v Toulouse, který se po otcově smrti vydání jeho díla intenzívně věnoval.)

Fermat tedy zemřel v domnění, že jeho hypotéza je pravdivá, že všechna čísla F_m jsou prvočísla. Další vývoj byl zajímavý a v mnoha ohledech poučný.

Fermatovo dílo, alespoň v oblasti teorie čísel, upadalo po jeho smrti v zapomnění; zřejmě předběhl dobu a matematika nebyla na rozvoj této disciplíny připravena. Až o necelé století později se o definitivní zrod teorie čísel zasloužil největší matematik 18. století, LEONHARD EULER. Ten řadu Fermatových výsledků znovuobjevil, v mnohém na Fermata navázal a jako první zasáhl do historie Fermatových čísel F_m, když v r. 1832 dokázal, že **číslo F_5 je složené**! Nalezl totiž faktorizaci

$$F_5 = 2^{32} + 1 = 4\,294\,967\,297 = 641 \times 6\,700\,417 .$$

$$

Tím byla samozřejmě Fermatova hypotéza vyvrácena, nebylo však ani zdaleka jasné, jak je to s dalšími čísly F_m. (V dalším budeme *Fermatovým prvočíslem* rozumět číslo F_m, které je prvočíslem.)

Carl Friedrich Gauss

Zájem o Fermatova prvočísla výrazně vzrostl koncem 18. století, kdy německý matematik CARL FRIEDRICH GAUSS (1777 -- 1855) odvodil následující překvapující souvislost Fermatových prvočísel s pravidelnými mnohoúhelníky:

Pravidelný mnohoúhelník je eukleidovsky konstruovatelný právě tehdy, když počet jeho vrcholů je roven číslu

$$n = 2^k \cdot p_1 \cdot p_2 \cdot \ldots \cdot p_s$$

kde $p_1, p_2, \ldots, p_s$ jsou navzájem různá Fermatova prvočísla.

Odtud okamžitě vyplývá, že pravidelné *n*-úhelníky jsou eukleidovsky konstruovatelné například pro n = 3, 4, 5, 6, 8, 10, 12, 15, 16, 17,… a nejsou eukleidovsky konstruovatelné například pro n = 7, 9, 11, 13, 14,….

Protože Fermatových prvočísel bylo v onu chvíli známo pouze 5 (a jak uvidíme, tento počet se dodnes nezvýšil), bylo podle Gausse možno dokázat existenci eukleidovské konstrukce pouze pro $2^5 - 1 = 31$ pravidelných mnohoúhelníků s **lichým** počtem vrcholů.

Další krok v poznávání Fermatových čísel se podařilo udělat až za 150 let po Eulerovi, v roce 1880, kdy F. LANDRY dokázal, že F_6 je součinem dvou prvočísel:

$$F_6 = 2^{64} + 1 = 274\,147 \times 67\,280\,421\,310\,721.$$

Ani další číslo tedy nesplňovalo Fermatovu předpověď!

A vývoj byl i nadále k Fermatově hypotéze neúprosný. V .1897 dokázal FELIX KLEIN (1849 -- 1925), že číslo F_7 je složené, nenašel však žádného dělitele. V roce 1909 dokázali analogický výsledek pro číslo F_8 J.C. MOREHEARD a A. E. WESTERN.

Faktorizaci čísla F_7 se podařilo nalézt až v r. 1970:

$$F_7 = (2^9 \times 116\,503\,103\,764\,643+1) \times (2^9 \times 1\,141\,971\,095\,088\,142\,685+1),$$

jednoho dělitele čísla F_8 nalezli BRENT a POLLARD až v roce 1981; je jím číslo

$$1\,238\,926\,361\,552\,897.$$

Abychom mohli docenit jak obtížné bylo uvedené výsledky získat, stačí si uvědomit, jak rychle posloupnost Fermatových čísel roste.

Podívejme se, jak bychom zjišťovali „standardními“ metodami, zda je například F_m prvočíslo. Víme, že k tomu je stačí dělit všemi prvočísly, která nepřevyšují číslo $\sqrt{F_m}$. Jak dlouho bychom tedy prověřovali například číslo F_8?

Celá část čísla $\sqrt{F_8}$ má 39 cifer, takže lze vcelku snadno odvodit, že před ním je cca

$$\frac{10^{38}}{38 \cdot \ln 10} \quad 10^{36}$$

prvočísel. Vzhledem k tomu, že rok má cca 3.2×10^7 sekund, potřebovali bychom při miliardě dělení za sekundu k provedení potřebných výpočtů přibližně 3×10^{19} let. Jen pro porovnání: stáří vesmíru odhadujeme na cca 15×10^9 let.

Pokusme se -- pod dojmem právě uvedených odhadů – alespoň představit, jakými metodami mohl polský matematik WACLAW SIERPINSKI (1882 -- 1969) v roce 1962, bez využití výpočetní techniky, dokázat, že číslo F_{1945} není prvočíslo.

Dekadický zápis tohoto čísla zcela jistě nikdy nikdo nenapíše, protože počet jeho číslic je 10^{582}.

Ještě neuvěřitelnější je fakt, že v r. 1983 W. KELLER odvodil, že číslo $F_{23\,471}$ je dělitelné číslem $5 \times 2^{23\,473} + 1$. Toto Fermatovo číslo má více než $10^{7\,000}$ cifer. **Pozor**: velikost posledního čísla si nesmíme plést s číslem $10^{7\,000}$. Toto číslo má „jen“ 7001 cifer.)

Nyní již můžeme uzavřít historii probírané Fermatovy hypotézy. Zdá se, že Fermat se v tomto případě mýlil naprosto fatálně. **Všechna** dosud prozkoumaná Fermatova čísla, kromě prvních pěti, **jsou složená**. Dodnes sice není dokázáno, že žádné další Fermatovo prvočíslo neexistuje, mnohé však tomu nasvědčuje.

Téměř šokující je přitom skutečnost, že teoreticky se Fermat vlastně **vůbec neměl splést**. Z výsledků, které sám odvodil a dokázal, totiž plynulo, že číslo F_5, které posléze rozložil Euler, může mít prvočíselné dělitele pouze tvaru 64n+1 a číslo 641, o němž Fermat bezpochyby i zpaměti věděl, že je prvočíslem, je opravdu dělitelem. Zdá se téměř neuvěřitelné, že tento fakt Fermat, který byl v praktických výpočtech mimořádně zběhlý a i mnohem větší čísla faktorizoval prakticky obratem, mohl přehlédnout. A přitom, jak jsme již uvedli, sám napsal, že výpočtům v tomto směru věnoval mnoho úsilí! Jediné vysvětlení je, že se prostě při pokusu o faktorizaci čísla F_5 spletl a svůj výpočet již nikdy neprověřoval.

Kdyby této Fermatovy pravděpodobné chyby nebylo, nikdy by nezformuloval onu hypotézu. Vývoj teorie čísel by možná v některých ohledech byl jiný. Ona osudná chyba však rozhodně nesnižuje Fermatovu genialitu a možná paradoxně přispěla k mnoha zajímavým objevům v této oblasti.