Karel Lepka

Velká Fermatova věta

In: Jindřich Bečvář (editor); Eduard Fuchs (editor): Historie matematiky. II. Seminář pro vyučující na středních školách, Jevíčko, 21. 8. – 24. 8. 1995, Sborník. (Czech). Praha: Prometheus, 1997.
pp. 161–168.

Persistent URL: http://dml.cz/dmlcz/401042

VELKÁ FERMATOVA VĚTA

KAREL LEPKA

1. Úvod

Pierre de Fermat (1601–1665) patřil k nejvýznamnějším osobnostem první poloviny 17. století. Žil v jihofrancouzském městě Toulouse, kde od roku 1631 až do své smrti působil jako soudce. Dostalo se mu výborného vzdělání, byl vynikajícím právníkem, ovládal kromě řečtiny a latiny i italštinu a španělštinu, psal verše, byl vyhledávaným znalcem starých řeckých textů. Koncem dvacátých let se začal zabývat i přírodními vědami a zejména v matematice dosáhl skvělých výsledků. Nezávisle na *Descartovi*[1] položil základy analytické geometrie, společně s *B. Pascalem*[2] je zakladatelem teorie pravděpodobnosti. Věnoval se rovněž matematické analýze a řešil i problémy z mechaniky a optiky.

Fermat nebyl sice profesionálním matematikem v dnešním slova smyslu, avšak je nutné si uvědomit, že v 17. století to nebyla žádná výjimka, spíše naopak. Styl jeho práce však vykazuje několik pozoruhodných rysů. Fermat své práce prakticky nepublikoval. Důvodem byla nejen velká časová náročnost, neboť autor musel úzce spolupracovat s tiskařem, ale především obava z negativních ohlasů po vyjití knihy. Je však třeba si uvědomit, že v té době neexistovaly vědecké časopisy a publikace byly možné jen v knižní formě. Na sklonku svého života snad zamýšlel vydat své dílo knižně, nikdy k tomu však nedošlo. V roce 1637 se připojil ke skupině učenců sdružených kolem známého organizátora vědeckého života pátera *Mersenna*[3] a od té doby začala jeho vědecká korespondence s mnoha významnými matematiky té doby. Tato korespondence, pokud se zachovala, umožnila později rekonstruovat z větší části jeho dílo. Paradoxní je, že tato korespondence představovala jeho jediný kontakt s vůdčími osobnostmi tehdejší vědy, neboť během svého života nenavštívil ani Paříž. Fermat měl rovněž ve zvyku dělat si poznámky na okrajích knih, které právě studoval. Za to, že jeho dílo neupadlo v zapomenutí, vděčíme jeho synu Samuelovi, který je po otcově smrti shromáždil, pokud to ovšem bylo možné, a vydal knižně.

2. Vznik teorie čísel

Zatím jsme se nezmínili o jedné matematické disciplíně, u jejíhož počátku stál právě Fermat, a tou je teorie čísel. Fermat vyšel z díla alexandrijského

[1] René Descartes (1596–1650), latinsky Renatus Cartesius, francouzský matematik, fyzik a filozof.

[2] Blaise Pascal (1623–1662), francouzský matematik, fyzik a filozof.

[3] Marin Mersenne (1588–1648), francouzský hudební teoretik, matematik a fyzik. Jeho prostřednictvím probíhala vědecká korespondence mezi tehdejšími učenci.

matematika *Diofanta*,[4] především z jeho spisu *Aritmetika*. Zamýšlel obnovit aritmetiku v tom smyslu, jak ji chápal Platón, to jest jako nauku o celých číslech a jejich vlastnostech. Přes svůj obdiv k Diofantovi se od něho začal vzdalovat. Zatímco Diofantos dával přednost racionálnímu řešení, Fermat pracoval především s celými čísly a zaváděl nové metody, především algebraické, které se vymykaly klasickému pojetí aritmetiky. Vytvořil tak novou matematickou disciplínu, avšak v tomto svém úsilí zůstal osamocen a svými současníky nepochopen. Snad i to je jeden z důvodů, proč sděloval své výsledky bez důkazů a metody, kterými k nim došel, pečlivě utajoval. Přitom je mimo jakoukoliv pochybnost, že svá tvrzení dokazoval v tom smyslu, v jakém chápeme matematický důkaz dnes.

Fermat se věnoval především dvěma okruhům problémů. První se týkal dělitelů čísel a jejich vlastností; vyvrcholením jeho práce je „malá Fermatova věta":

Věta: *Nechť p je prvočíslo a a libovolné celé číslo nesoudělné s p. Potom platí*

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

Druhý okruh problémů se týkal tvoření pythagorejských trojic splňujících různé podmínky; o některých Fermatových výsledcích pojednává tento článek. Po jeho smrti teorie čísel upadla takřka v zapomnění. K jejímu dalšímu rozvoji došlo až v 18. století; znovuzrození této disciplíny je spojeno především s *Eulerem*,[5] který dokázal (případně vyvrátil) většinu Fermatových tvrzení a dále je rozvinul. Přesto však zůstal jeden problém, který vzdoroval úsilí mnoha generací matematiků a který se stal ne-li největší, tak určitě nejznámější záhadou v dějinách matematiky.

3. Velká Fermatova věta

Jak již bylo řečeno, Fermat měl ve zvyku psát poznámky v jím studovaných knihách. Problém č. 8 ve druhém díle Diofantovy Aritmetiky se týká řešení neurčité rovnice

$$x^2 + y^2 = z^2 \tag{1}$$

v oboru racionálních čísel. Fermat na okraj připsal následující poznámku: *Naopak je nemožné rozdělit krychli na dvě krychle, čtvrtou mocninu ve dvě čtvrté mocniny nebo obecně jakoukoliv mocninu vyšší než dvě ve dvě mocniny téhož stupně. Pro toto tvrzení jsem nalezl opravdu podivuhodný důkaz, ale tento okraj je příliš úzký, aby zde mohl být napsán.* Jinými slovy, neurčitá (diofantická) rovnice

$$x^n + y^n = z^n \tag{2}$$

[4] Diofantos z Alexandrie, latinsky Diophantus, 3. stol., řecký matematik, který se zabýval řešením neurčitých (diofantických) rovnic.

[5] Leonhard Euler (1707–1783), švýcarský matematik, fyzik a astronom, působil v Berlíně a v Petrohradě. Více než 800 původními pracemi výrazně ovlivnil téměř všechny oblasti těchto věd.

nemá pro $n > 2$ řešení v oboru kladných celých čísel. (Fermat, stejně jako Diofantos pracoval pouze s kladnými čísly.)

4. Pythagorejské trojice

Pomineme-li triviální případ $n = 1$, lze celkem snadno dokázat, že rovnice (2) má nekonečně mnoho řešení. Trojice čísel, které tuto rovnici splňují, nazýváme *pythagorejské trojice*. Jak dokládá tzv. *plimptonská tabulka* č. 322 (1900–1600 př. n. l.), nalézt takové trojice uměli už ve staré Babylonii.

Je zřejmé, že pokud x, y, z je pythagorejská trojice, je $kx, ky, kz; k \in \mathbb{N}$, kde $\mathbb{N}$ je množina přirozených čísel, také pythagorejská trojice. Jestliže $(x, y) = (y, z) = (x, z) = 1$, mluvíme o tzv. *primitivní* pythagorejské trojici. Dále ukážeme, jak nalézt libovolnou primitivní pythagorejskou trojici. Z vlastností sudých a lichých čísel plyne, že dvě čísla z této trojice jsou lichá a jedno sudé a že tím sudým číslem nemůže být číslo z. Nechť sudým číslem z trojice je číslo x. Potom lze psát

$$x^2 = z^2 - y^2 = (z + y)(z - y) \,. \tag{3}$$

Jelikož součet, resp. rozdíl dvou lichých čísel je číslo sudé, můžeme položit $x = 2u, z + y = 2v, z - y = 2w$ a dosazením do (3) obdržíme

$$u^2 = vw, \qquad \text{přičemž } (v, w) = 1 \,.$$

Z věty o jednoznačnosti rozkladu celého čísla na prvočinitele plyne následující tvrzení:

Věta: *Nechť platí* $u^2 = vw$ *a* $(v, w) = 1$. *Potom čísla* v, w *jsou druhými mocninami.*

Platí tedy

$$z = v + w = p^2 + q^2, \quad y = v - w = p^2 - q^2, \quad x = 2pq, \quad p > q \tag{4}$$

a čísla p, q mají opačnou paritu.

5. Metoda nekonečného sestupu

Právě s Velkou Fermatovou větou je spojena zajímavá metoda, která se latinsky nazývá *descende infinite* čili metoda nekonečného sestupu a kterou Fermat objevil zřejmě intuitivně a velmi si na ní zakládal. Její podstata se dá vyjádřit následujícím tvrzením.

Věta: *Nechť dané kladné celé číslo* n *má vlastnost* V. *Jestliže z tohoto předpokladu plyne, že existuje celé kladné číslo* $n_1 < n$ *s vlastností* V, *potom ani jedno celé kladné číslo nemá vlastnost* V.

Tato metoda je vlastně „indukce opačným směrem" a souvisí s tím, že množina $\mathbb{N}$ je *dobře uspořádaná*. Lze totiž snadno dokázat, že dobré uspořádání

a princip nekonečného sestupu jsou ekvivalentní. Jak Fermat zdůraznil, tato metoda dokazuje *neexistenci*.

Využitím této metody lze dokázat Velkou Fermatovu větu pro $n = 4$. Protože tento důkaz není příliš obtížný ani dlouhý, uvedeme ho celý.

Předpokládejme, že x, y, z jsou řešením rovnice

$$x^4 + y^4 = z^4 \,. \tag{5}$$

Bez újmy na obecnosti můžeme předpokládat, že $(x, y) = (x, z) = (y, z) = 1$. Vzhledem k tomu, že rovnici (5) můžeme psát ve tvaru

$$(x^2)^2 + (y^2)^2 = (z^2)^2 \,,$$

je zřejmé, že čísla x^2, y^2, z^2 tvoří primitivní pythagorejskou trojici, tedy

$$x^2 = 2pq, \quad y^2 = p^2 - q^2, \quad z^2 = p^2 + q^2, \quad 0 < q < p \,,$$

a čísla p, q mají opačnou paritu. Rovnici

$$y^2 = p^2 - q^2$$

lze psát ve tvaru

$$y^2 + q^2 = p^2$$

a jelikož $(p, q) = 1$, tvoří i čísla z, p, q primitivní pythagorejskou trojici a q je sudé. Je tedy

$$q = 2ab, \quad y = a^2 - b^2, \quad p = a^2 + b^2, \quad 0 < b < a, \quad (a, b) = 1 \,,$$

a čísla a, b jsou opačné parity. Odtud plyne

$$x^2 = 2pq = 4ab(a^2 + b^2),$$

a po úpravě

$$(\frac{x}{2})^2 = ab(a^2 + b^2).$$

Protože $(ab, a^2 + b^2) = 1$, čísla ab a $a^2 + b^2$ musí být druhé mocniny. Vzhledem k tomu, že $(a, b) = 1$ a součin ab je druhá mocnina, musí být také čísla a a b druhé mocniny, tedy $a = X^2$ a $b = Y^2$. Odtud plyne, že výraz $X^4 + Y^4$ je druhá mocnina. Navíc platí

$$X^4 + Y^4 = a^2 + b^2 < p < p^2 + q^2 = z^2 < x^4 + y^4.$$

Podle metody nekonečného sestupu nemůže být výraz $x^4 + y^4$ druhá mocnina, není tedy ani čtvrtá mocnina, čímž je velká Fermatova věta dokázána pro $n = 4$.

Je nutné si uvědomit, že tím je současně dokázána platnost této věty i pro libovolné číslo dělitelné 4. Skutečně, kdyby platilo $x^{4m} + y^{4m} = z^{4m}$, byla by

čísla x^m, y^m, z^m řešením rovnice $x^4 + y^4 = z^4$, které však neexistuje. Navíc je třeba si uvědomit, že každé přirozené číslo $n > 2$, které není dělitelné číslem 4, musí být dělitelné nějakým prvočíslem $p > 2$. Abychom dokázali obecně Velkou Fermatovu větu, stačí ji dokázat pouze pro prvočísla.

6. Případ $n = 3$

Prvním matematikem, který se po Fermatově smrti věnoval tomuto problému, byl Euler, který v dopise *Goldbachovi*[6] oznamuje, že našel řešení tohoto problému pro $n = 3$. Jak naznačoval o několik let později, byl tento důkaz založen na teorii kvadratických forem tvaru $x^2 + 3y^2$; i když tento důkaz ještě nebyl kompletní, byl značným pokrokem. Později se ho Goldbach rozhodl uveřejnit v posledním oddíle své *Algebry*, kde vypracoval novou techniku pro práci s kvadratickými iracionalitami a jejich použití v teorii binárních kvadratických forem.

Tento důkaz je poměrně dlouhý, proto uvedeme pouze hlavní myšlenky. Kompletní důkaz může čtenář najít v [Ed]. Je zřejmé, že nejvýše jedno z čísel x, y, z může být sudé; nechť je to z. Potom čísla $x + y$ a $x - y$ jsou sudá, tedy $x + y = 2p$, $x - y = 2q$ a odtud plyne, že $x = p + q$ a $y = p - q$. Dosadíme-li za x a y do (2) a položíme-li $n = 3$, obdržíme

$$z^3 = x^3 + y^3 = (x + y)(x^2 - xy + y^2) = 2p(p^2 + 3q^2).$$

Čísla p a q mají opačnou paritu a jsou nesoudělná. Navíc můžeme předpokládat, že jsou kladná a $x \neq y$. Předpoklad, že x, y a z jsou lichá, vede ke stejnému výsledku. Platí-li tedy Velká Fermatova věta, musí existovat celá čísla p, q taková, že $(p, q) = 1$ a výraz $2p(p^2 + 3q)$ je třetí mocninou celého čísla.

Protože čísla $2p$ a $p^2 + 3q^2$ jsou buď nesoudělná nebo mají společný dělitel rovný číslu 3, dělí se důkaz na dva případy. V obou případech však dospíváme k závěru, že lze najít čísla a, b taková, že

$$p = a^3 - 9ab^2, \qquad q = 3a^2 - 3b^2$$

a

$$p^2 + 3q^2 = (a^2 + 3b^2)^3, \qquad 2p = 2a(a^2 - 9b^2)$$

jsou třetí mocniny. Využijeme-li metodu nekonečného sestupu, lze dokázat platnost Velké Fermatovy věty pro $n = 3$.

Hlavní nedostatek tohoto důkazu spočívá v tom, že je nutné navíc dokázat existenci čísel a a b. Vzhledem k tomu, že Fermat pracoval s kvadratickými formami tvaru $x^2 + ay^2$, je možné, že znal, alespoň v hrubých rysech, důkaz pro $n = 3$. Mahoney se domnívá ([Ma]), že právě úspěch v těchto dvou případech mohl vést Fermata k zobecnění tohoto tvrzení a že právě metoda nekonečného sestupu by mohla být oním podivuhodným důkazem.

[6] Christian Goldbach (1690–1764), německý matematik.

Použití kvadratických forem však není jedinou možností jak dokázat Velkou Fermatovu větu pro $n = 3$. Uvažujme výrazy $v = a + b\sqrt{-3}$, $a, b \in \mathbb{Z}$. Snadno se dokáže, že součet, rozdíl a součin těchto výrazů je rovněž výraz tohoto typu a navíc platí $1 \cdot (a + b\sqrt{-3}) = (a + b\sqrt{-3})$. Řečeno slovy dnešní algebry, výrazy tohoto tvaru tvoří komutativní okruh s jedničkou. Euler jako první použil smělou myšlenku přenést zákony aritmetiky celých čísel na čísla tvaru $a + b\sqrt{-3}$. Jinými slovy, Euler byl první, kdo začal pracovat s komplexními čísly jako s čísly.

Rozložíme-li totiž výraz

$$p^2 + 3q^2 = (p + q\sqrt{-3})(p - q\sqrt{-3}),$$

lze dokázat, že k tomu, abychom našli třetí mocninu tvaru $p^2 + 3q^2$ stačí položit

$$p + q\sqrt{-3} = (a + b\sqrt{-3})^3.$$

7. Události roku 1847

Euler při řešení případu $n = 5$ neuspěl. Důkaz podal až v roce 1825 *Dirichlet*;[7] tento důkaz však byl neúplný, na což poukázal *Legendre*,[8] který současně uvedl vlastní nezávislý a úplný důkaz. Dirichlet v roce 1828 svůj důkaz doplnil a o čtyři roky později se mu podařilo vyřešit případ $n = 14$. V roce 1839 dokázal platnost pro $n = 7$ *Lamé*.[9] Tyto důkazy však byly čím dál tím složitější a případ od případu se značně lišily. Proto úsilí matematiků, kteří se zabývali tímto problémem, směřovalo k nalezení metody, která by Velkou Fermatovu větu řešila obecně.

Dne 1. března 1847 oznámil Lamé na zasedání Pařížské akademie, že našel obecný důkaz Velké Fermatovy věty. Lamé v podstatě zobecnil myšlenky důkazů pro $n = 3, 4, 5, 7$. Zavedl komplexní čísla a rozložil výraz $x^n + y^n$ na n lineárních činitelů.

$$x^n + y^n = (x + y)(x + ry)(x + r^2y) \cdots (x + r^{n-1}y), \quad n \text{ liché}.$$

Komplexní číslo r musí splňovat podmínku $r^n = 1$. Jsou-li činitelé na pravé straně po dvou nesoudělní, musí každý z nich být n-tou mocninou a lze použít metodu nekonečného sestupu. Lamé tak místo s celými čísly pracoval se speciálními čísly tvaru

$$a_0 + a_1\zeta + \cdots + a_{\lambda-1}\zeta^{\lambda-1}, \quad a_0, a_1, \ldots, a_{\lambda-1} \in \mathbb{Z}.$$

[7] Peter Gustav Lejeune-Dirichlet (1805–1859), německý matematik, Gaussův nástupce na univerzitě v Göttingenu.

[8] Adrien Marie Legendre (1752–1833), francouzský matematik a geodet.

[9] Gabriel Lamé (1795–1870), francouzský matematik a geofyzik, člen Francouzské Akademie věd.

Tato čísla tvoří kruhové těleso $Q(\zeta)$. Název kruhové těleso vznikl z toho, že mocniny čísla ζ znázorněné v komplexní rovině jsou vrcholy pravidelného n-úhelníka vepsaného jednotkové kružnici se středem v počátku. Podobnými úvahami se zabýval i *Cauchy*.[10] Oba dva deponovali u Pařížské akademie zapečetěné obálky.[11] Lamého nadšení však nesdílel *Liouville*,[12] který ve svém vystoupení poukázal na skutečnost, že Lamé mechanicky přenesl vlastnosti celých čísel na prvky tělesa $Q(\zeta)$. V okruhu celých čísel platí věta o jednoznačnosti rozkladu čísla na prvočinitele.

24. května zveřejnil Liouville dopis, ve kterém *Kummer*[13] z Wroclavi píše, že pro $n = 37$ není tento rozklad jednoznačný a uvedená metoda se nedá obecně použít. Kummer dále píše, že tento nedostatek je možné odstranit zavedením nového typu komplexních čísel, které nazval *ideální komplexní čísla*. Nakonec uvedl, že výsledky této nové teorie byly předneseny na zasedání Berlínské akademie věd v roce 1846 a publikovány ve Zprávách této Akademie. V roce 1847 publikoval v časopise *Journal für die reine und angewandte Mathematik* další dva články, v nichž podává úplné vysvětlení své nové teorie. Kummerovy práce se staly základem nově vzniklé teorie ideálů obecného okruhu, která byla rozvinuta *Dedekindem*[14] a dalšími význačnými matematiky.

8. Závěr

I přes velký význam Kummerovy teorie se však nepodařilo obecně Fermatovu hypotézu dokázat, i když zejména v posledních letech byly do řešení tohoto problému zapojeny i nejvýkonnější počítače, s jejichž pomocí byla tato hypotéza ověřena pro všechna lichá čísla menší než $4 \cdot 10^6$. Teprve v roce 1993 se podařilo tento problém, který více než 300 let odolával úsilí mnoha světových profesionálních i amatérských matematiků a který se několikrát stal i motorem pokroku v matematice, vyřešit. Dne 23. června 1993 přednesl britský matematik *Andrew Wiles* přednášku o vyřešení významné hypotézy japonského matematika Zutaki Taniyamy v aritmetické algebraické geometrii týkající se velké třídy eliptických křivek nad racionálními čísly. Jako důsledek odtud vyplývá nemožnost řešení rovnice (2) v oboru přirozených čísel. Tento důkaz je však daleko za hranicemi Fermatových možností, takže to, jaký důkaz měl Fermat na mysli, už asi zůstane navždy tajemstvím.

[10] Augustin Louis Cauchy (1789–1857), francouzský matematik. Po revoluci v roce 1830 pobýval několik roků v exilu v Praze.

[11] Pokud někdo přišel na nový objev, který bylo nutno ještě dopracovat, mohl u Pařížské akademie uložit zapečetěnou obálku, kde popsal hlavní myšlenku svého objevu.

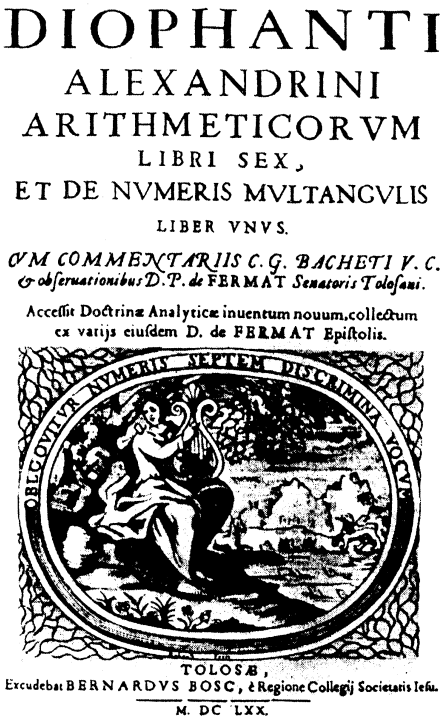
[12] Joseph Liouville (1809–1882), francouzský matematik, profesor na Sorbonně.

[13] Ernst Eduard Kummer (1810–1893), německý matematik.

[14] Richard Dedekind (1831–1916), německý matematik, položil základy teorie ideálů.

LITERATURA

[Bo] Boyer, C. B., *A History of Mathematics*, John Wiley & Sons, Inc., New York, 1968.
[Ed] Edwards, H. M., *Fermat's Last Theorem*, Springer-Verlag, 1977.
[Ko] Kolmogorov A. N., Juškevič A. P., *Matematika 19. veka*, Nauka, Moskva, 1978.
[Ma] Mahoney S., *The mathematical career of Pierre de Fermat*, Princeton University Press, Princeton, New Jersey, 1994.
[Ri] Ribenboim, P., *The Little Book of Big Primes*, Springer-Verlag, New York, 1991.
[Sk] Skula L., *Některé historické aspekty Fermatova problému*, Pokroky matematiky, fyziky a astronomie **39** (1994), 318–329.
[We] Weil A., *Number Theory*, Birkhäuser, Boston, 1987.


DIOPHANTI
ALEXANDRINI
ARITHMETICORVM
LIBRI SEX,
ET DE NVMERIS MVLTANGVLIS
LIBER VNVS.
CVM COMMENTARIIS C. G. BACHETI V. C.
& obſeruationibus D. P. de FERMAT Senatoris Toloſani.
Acceſſit Doctrinæ Analyticæ inuentum nouum, collectum
ex variis eiuſdem D. de FERMAT Epiſtolis.
OBLONGUM NVMERIS SEPTEM DISCRIMINA VOLVM
TOLOSÆ,
Excudebat BERNARDVS BOSC, è Regione Collegij Societatis Ieſu.
M. DC LXX.

Titulní list latinského vydání Diofantovy *Aritmetiky*
s komentáři Bacheta de Méziriac a Fermatovými poznámkami