Karel Lepka
Malá Fermatova věta

Učitel matematiky, Vol. 5 (1997), No. 3, 143–150

Persistent URL: http://dml.cz/dmlcz/151388

MALÁ FERMATOVA VĚTA

KAREL LEPKA

Úvod

Vynikající francouzský matematik *Pierre de Fermat* (1601 – 1665) patřil k předním vědcům první poloviny 17. století a k nejpozoruhodnějším postavám v dějinách matematiky. V tomto článku chceme seznámit čtenáře s jedním jeho významným objevem, který je v naší odborné literatuře znám jako Malá Fermatova věta a který patří k fundamentálním tvrzením v elementární teorii čísel. K tomuto objevu dospěl Fermat na přelomu třicátých a čtyřicátých let 17. století. V této době byla ve velké oblibě tzv. *dokonalá čísla*. Zkoumání těchto čísel se věnovali všichni přední francouzští matematikové té doby; mimo Fermata jmenujme ještě *Descarta, Mersenna a Frenicla de Bessy*. Protože tato čísla s Fermatovým objevem úzce souvisejí, zmíníme se nejdříve o nich.

Dokonalá čísla

Označme $s(n)$ součet všech dělitelů čísla n s výjimkou n samotného a $S(n)$ součet všech dělitelů čísla n. Potom číslo n, které splňuje podmínku $s(n) = n$, resp. $S(n) = 2n$ se nazývá *dokonalé*.

Pro nesoudělná čísla a, b zřejmě platí následující tvrzení:

Věta: *Nechť* $n = ab$, *přičemž* $(a, b) = 1$. *Potom*

$$S(n) = S(ab) = S(a)S(b).$$

Nyní uvedeme a dokážeme nutnou a postačující podmínku toho, aby sudé číslo bylo dokonalé.

Věta: *Sudé číslo* n *je dokonalé právě tehdy, když je lze psát ve tvaru* $n = 2^{k-1}(2^k - 1)$, *kde* k *je přirozené číslo,* $k > 1$ *a* $2^k - 1$ *je prvočíslo.*

Důkaz: Předpokládejme, že sudé číslo $n = 2^{k-1}l$, kde l je liché číslo, je dokonalé. Potom platí $S(n) = S(2^{k-1})S(l) = 2^k l$.

Využijeme-li známý vzorec pro součet geometrické posloupnosti, obdržíme

$$S(n) = (2^k - 1)S(l) = 2^k l.$$

Protože $(2^k - 1, 2^k) = 1$, je $S(l) = 2^s q$, kde q je přirozené číslo. Odtud obdržíme $(2^s - 1)q = l$ a po úpravě $S(l) = l + q$, kde $q|l$ a $q < l$. Číslo l má tedy právě dva dělitele a proto $q = 1$ a l je prvočíslo tvaru $2^k - 1$.

Nyní předpokládejme, že $n = 2^{k-1}(2^k - 1)$, přičemž $2^k - 1$ je prvočíslo. Potom

$$S(n) = S(2^{k-1})S(2^k - 1).$$

První činitel je využitím vzorce pro součet geometrické posloupnosti roven $2^k - 1$ a druhý činitel je vzhledem k předpokladu roven 2^k. Je tedy $S(n) = 2n$ a číslo n je dokonalé.

Toto tvrzení, včetně důkazu dostatečnosti, uvádí už *Eukleides* ve svých Základech(IX, 36). Tato věta neudává funkci, která by generovala sudá dokonalá čísla[5], ale redukuje tento problém na rozřešení otázky, zda číslo $M_n = 2^n - 1$ je prvočíslo nebo číslo složené. Tato čísla byla na Mersennovu počest nazvána *Mersennova čísla*. Vzhledem ke známé identitě

$$2^n - 1 = (2^a - 1)(1 + 2^a + 2^{2a} + \cdots + 2^{(b-1)a}), \qquad (1)$$

kde $n = ab$, je zřejmé, že Mersennovo číslo M_n může být prvočíslo pouze tehdy, je-li i n prvočíslo.

V roce 1640 se Frenicle otázal Fermata prostřednictvím Mersenna, zda existuje dokonalé číslo mezi 10^{20} a 10^{22}. Fermat byl při řešení této úlohy úspěšný. Jak oznámil v červnu roku 1640 v dopise Mersennovi, jeho metoda byla založena na následujících třech předpokladech:

(I) Je-li n složené, je i $2^n - 1$ složené.

(II) Je-li n prvočíslo, potom $2^n - 2$ je násobek $2n$.

[5]Existence lichých dokonalých čísel nebyla dosud ani potvrzena, ani vyvrácena. Takové číslo by však muselo být větší než 10^{50} a muselo by mít nejméně 8 různých prvočinitelů.

(III) Je-li n prvočíslo a p je prvočíselný dělitel $2^n - 1$, potom $p - 1$ je násobek n.

Podmínka (I) je důsledek již zmíněné identity (1). Skutečnost, že to Fermat uvádí jako objev, svědčí o tom, že znalosti algebry nebyly v té době příliš velké. Podmínky (II) a (III) jsou ovšem typické případy toho, co se dnes označuje jako *Malá Fermatova věta.* Tato tvrzení uvádí Fermat bez důkazu. V dopise Freniclovi z 18. října 1640, v němž Fermat píše o „la propositon fondamentale de parties aliquotes" neboli o základní větě o dělitelích, Fermat poodhalil i způsob, kterým ke svým závěrům přišel: *Je dáno libovolné prvočíslo p a libovolná geometrická posloupnost $1, a, a^2$, etc., p musí dělit některé číslo $a^n - 1$ pro něž n dělí $p - 1$; jestliže potom N je libovolný násobek nejmenšího n pro něž toto platí, p dělí také $a^N - 1$. Toto tvrzení platí pro všechny řady a všechna prvočísla. Poslal bych Vám jeho důkaz, ale obávám se, že je příliš dlouhý.*

Důkazy Malé Fermatovy věty

V dnešní době se Malá Fermatova věta uvádí v následujícím znění:

Věta: *Nechť p je prvočíslo. Pak pro všechna přirozená čísla a platí*

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

Je-li navíc $(a, p) = 1$, platí

$$a^{p-1} \equiv 1 \pmod{p} \tag{3}$$

Symbol kongruence zavedl *Gauss.* Jestliže čísla a a b dávají po dělení číslem p stejný zbytek, píšeme $a \equiv b \pmod{p}$.

Vezmeme-li v úvahu tuto formulaci (2), lze provést tzv. *aditivní důkaz.* Použijeme binomickou větu

$$(x + y)^p = x^p + \binom{p}{1} x^{p-1} y + \cdots + \binom{p}{p-1} x y^{p-1} + y^n.$$

Položíme $x = y = 1$ a jelikož všechny binomické koeficienty s výjimkou $\binom{p}{0}$ a $\binom{p}{p}$ jsou násobky p, obdržíme

$$2^p \equiv 2 \pmod{p}.$$

Nyní můžeme předpokládat, že existuje alespoň jedno číslo a, které splňuje podmínku $a^p \equiv a \pmod{p}$ a použijeme-li opět binomickou větu s volbou $x = a, y = 1$, obdržíme

$$(a+1)^p = a^p + \binom{p}{1} a^{p-1} + \cdots + \binom{p}{p-1} a + 1.$$

Přejdeme-li ke kongruenci a vezmeme-li do úvahy indukční předpoklad, obdržíme

$$(a+1)^p \equiv a + 1 \pmod{p}.$$

Vzhledem k tomu, co Fermat bezpečně znal o binomických koeficientech již v roce 1636, lze předpokládat, že Fermat tento důkaz, přinejmenším pro případ $a = 2$, který je pro hledání dokonalých čísel rozhodující, znal. Tento důkaz však prakticky nesouvisí s dělitelností čísel a jak ukazuje již citovaný dopis Freniclovi, Fermatovy úvahy se ubíraly poněkud jiným směrem.

Fermat si zřejmě uvědomil, že při dělení členů posloupnosti $1, a, a^2, \ldots$ prvočíslem p se zbytky opakují. Je totiž možných nejvýše $p - 1$ zbytků, existují tedy nejméně dva exponenty, řekněme n a $n + m$, které dávají týž zbytek. Platí tedy

$$a^{m+n} - a^n \equiv 0 \pmod{p}.$$

S ohledem na předpoklad $(a, p) = 1$ dostáváme

$$a^m \equiv 1 \pmod{p},$$

takže číslo 1 je vždy členem posloupnosti zbytků. Nechť d je nejmenší exponent, který při dělení dává zbytek 1. Potom i jeho libovolný násobek md dává zbytek 1, neboť

$$a^{md} - 1 = (a^d - 1)(a^{(m-1)d} + \cdots + a^d + 1)$$

je dělitelný p. Naopak jedinými mocniteli čísla a, které při dělení číslem p dávají zbytek 1 jsou násobky d. Nechť

$$m = qd + r, \quad q \geq 0, \quad 0 \leq r < d$$

dá při dělení p rovněž zbytek 1. Jelikož $a^m \doteq a^{qd}a^r$ a a^{qd} dávají zbytek 1, musí být jejich rozdíl $a^{qd}(a^r - 1)$ dělitelný p. Protože a^{qd} není dělitelné p, musí být dělitelné p číslo $a^r - 1$, což je však spor s definicí čísla d s výjimkou $r = 0$, tedy m je násobkem d. Navíc čísla a^{n+m} a a^n dávají týž zbytek pouze v případě, že a^m dává zbytek 1. Jinými slovy, při dělení čísel a^n prvočíslem d dostaneme d zbytků, které se cyklicky opakují. Pokud $d = p - 1$, potom samozřejmě platí $d|p - 1$. V opačném případě existuje alespoň jedno číslo k, které není členem posloupnosti zbytků. Uvažujme množinu zbytků, které obdržíme při dělení čísel $k, ka, ka^2, \ldots$ prvočíslem p. Tato množina má opět d prvků, neboť čísla ka^{m+n} a ka^n dají týž zbytek tehdy a jen tehdy, když $p|ka^n(a^m - 1)$ a to platí pouze v případě $d|m$. Navíc ani jeden z těchto zbytků není prvkem původní množiny, což dokážeme sporem. Předpokládejme, že a^n a ka^m dávají týž zbytek. Potom stejnou vlastnost mají i čísla a^{n+1} a ka^{m+1}, neboť $a^n - a^m k$ je dělitelné p pouze tehdy, když $a(a^n - a^m k)$ je dělitelné p. Tak postupujeme dál, až narazíme na případ, kdy $d|m+j$. Potom ovšem čísla a^{n+j} a k dávají týž zbytek, což je spor s definicí čísla k. Pokud jsme nevyčerpali všechny možné zbytky, volíme k', které nepatří do žádné z výše uvedených množin a postupujeme stejným způsobem, dokud nevyčerpáme všechny možné zbytky. Musí tedy platit $d|p - 1$, což jsme chtěli dokázat. Tento důkaz bývá označován jako *multiplikativní.*

Je-li $a = 2$, potom lze dokázat následující tvrzení:

Věta: *Nechť n a p jsou lichá prvočísla, přičemž $p|2^{n-1} - 1$. Potom $p = 2kn + 1$.*

Důkaz: Je-li $n > 2$ prvočíslo a výraz $2^{n-1} - 1$ je dělitelný lichým prvočíslem p, potom platí $p - 1 = k'n$, kde k' je přirozené číslo. Jelikož p je liché, je $p - 1$ sudé a $2|k'n$. Protože n je liché, je k' sudé a $k' = 2k$. Prvočíselní dělitelé čísel $2^n - 1$ jsou tudíž tvaru $p = 2kn + 1$.

Jak vyplývá z Fermatova dopisu Freniclovi, tento důsledek znal a nebylo pro něho problém faktorizovat číslo $2^{37} - 1$. Pokud

existuje prvočíselný dělitel p, potom 37 musí dělit $p-1$. Jelikož p je liché, musíme je hledat mezi prvočísly tvaru $74n+1$, první kandidát 149 nevyhovuje, ale druhý 223 ano.

Fermatova čísla

Fermat se také zabýval otázkou, kdy je 2^n+1 prvočíslo. Toto nemůže nastat, jestliže n má lichého dělitele $d>1$. Platí-li totiž $n=ed$ a položíme-li $N=2^e$, potom $2^n+1=N^d+1$ a toto číslo je dělitelné $N+1$. K důkazu stačí použít známé identity

$$x^n+1=(x+1)(x^{n-1}-x^{n-2}+\cdots+1)$$

V případě, že n nemá lichého dělitele, je $n=2^r$ a pro $r=0,1,2,3,4$ je číslo 2^n+1 prvočíslo. V dopise Freniclovi z roku 1640 vypočítal všechna tato čísla až po $r=6$ a odhaduje, že se jedná o prvočísla. Nechce se až věřit, že se Fermat nepokusil faktorizovat alespoň číslo pro $r=5$. Podle jím objevené metody mezi možné dělitele tohoto čísla připadají pouze prvočísla tvaru $64n+1$, z nichž 641 toto číslo skutečně dělí. Ani Frenicle se nepokusil toto číslo rozložit, přestože Fermat v dopise vyslovil přání, aby tak učinil; naopak s tímto Fermatovým závěrem vyslovil souhlas. Fermat až do konce života věřil, že tento jeho závěr je správný, ačkoliv obvykle udával, že pro to nemá důkaz. Můžeme si představit, že když poprvé formuloval svůj závěr, byl jím tak unesen, že si nevšiml numerické chyby a své výpočty si nepřekontroloval. Číslo $2^{64}+1$, které má dělitele 274177 bylo za hranicemi Fermatových možností a můžeme říci i Freniclových, přestože byl vytrvalejším a lepším počtářem.

Přínos L. Eulera

Fermat se problémy dělitelnosti ve čtyřicátých letech přestal zabývat. *Leibniz* kolem roku 1680 dokázal malou Fermatovu větu pomocí formule

$$(1+1+\cdots+1)^p=1+1+\cdots+1+\sum_{q+r+\cdots+s=p}\frac{p!}{q!r!\ldots s!},$$

svůj důkaz však nikdy neuveřejnil. Ten byl objeven až v jeho pozůstalosti a poprvé publikován Goldbachem (1690 – 1764).

Dalším matematikem, který se věnoval těmto problémům byl *Leonhard Euler*. K zájmu o tuto problematiku ho zřejmě přivedla Fermatova čísla. Podařilo se mu najít dělitele 641 čísla $2^{2^5}+1$ a vyvrátil tak Fermatovu domněnku, že se jedná o prvočísla. V roce 1736 publikoval první důkaz malé Fermatovy věty, který byl aplikací binomické věty. O tom, jak hluboce Fermatovo dílo z teorie čísel upadlo v zapomnění, svědčí skutečnost, že Euler považoval Malou Fermatovu větu za svůj objev, teprve později přiznal Fermatovo prvenství. V roce 1761 podal i multiplikativní důkaz této věty, který vzápětí rozšířil i pro složená čísla m.

Věta: *Nechť* $(a,m)=1$ *a* $\varphi(m)$ *značí počet čísel, která nedělí číslo* m *a která jsou menší než* m. *Potom platí*

$$a^{\varphi(m)} \equiv 1 \pmod{p}.$$

Funkce $\varphi(m)$ se nazývá *Eulerova funkce*. Jestliže známe prvočíselný rozklad čísla m, není obtížné stanovit funkci $\varphi(m)$.

Věta:*Nechť* $m = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_k^{\alpha_k}$, *kde* $p_1, p_2 \ldots p_k$ *jsou navzájem různá prvočísla. Potom platí:*

$$\varphi(m) = m\left(1-\frac{1}{p_1}\right)\left(1-\frac{1}{p_2}\right)\cdots\left(1-\frac{1}{p_k}\right).$$

Důkaz této věty lze nalézt např. v [Si].

Malá Fermatova věta nebyla jediným problémem, kterým se Euler zabýval. Dokázal[6] Velkou Fermatovu větu pro $n=3$, zabýval se diofantickými rovnicemi a rozkládáním čísla na součet druhých mocnin, položil základy teorie eliptických integrálů atd. Na rozdíl od Fermata nalezl pochopení u svých současníků, takže se jeho zásluhou stala teorie čísel trvalou součástí matematiky.

[6]V jeho důkaze se vyskytly drobné nepřesnosti, které později odstranil Gauss. Pozn. red.

Závěr

Později byly podány další důkazy a objeveny souvislosti s dalšími tvrzeními z teorie čísel. Je rovněž možné, že Fermat nebyl první, kdo toto tvrzení objevil, viz [Di], vol. I, str. 59. Fermat však při řešení problému dokonalých čísel a jiných starých úloh použil nové netradiční metody a položil základy nového odvětví matematiky—teorie čísel.

LITERATURA:

[Di] Leonard E. Dickson, *History of the theory of numbers*, Carnegie Institution of Washington, Washington, 1919.

[Ed] Harold M. Edwards, *Posledňaja těorema Ferma*, Mir, Moskva, 1980. (ruský překlad)

[Fu] Eduard Fuchs, *Co ještě nevíme o prvočíslech*, in Historie matematiky I (Sborník) (1994), JČMF, Brno, 140–161.

[Ma] Michael Sean Mahoney, *The Mathematical Career of Pierre de Fermat*, 2. vydání., Princeton University Press, Princeton, New Jersey, 1994.

[Si] Wacław Sierpiński, *Elementary Theory of Numbers*, Polish Scientific Publishers, Warszawa, 1987.

[Sk1] Ladislav Skula, *Některé historické aspekty Fermatova problému*, Pokroky matematiky, fyziky a astronomie **39** (1994), 318 – 330.

[Sk2] Ladislav Skula, *Co je to diskrétní matematika?*, in Sborník VIII. brněnské konference o vyučování matematice (1992), 7–10.

[We] André Weil, *Number Theory*, Birkhäuser, Boston, 1987.