Pokroky matematiky, fyziky a astronomie

Ladislav Skula

Některé historické aspekty Fermatova problému

Pokroky matematiky, fyziky a astronomie, Vol. 39 (1994), No. 6, 318--330

Persistent URL: http://dml.cz/dmlcz/139546

Některé historické aspekty Fermatova problému

Ladislav Skula, Brno

Dne 23. června 1993 přednesl britský matematik Andrew Wiles v Ústavu Isaaca Newtona pro matematické vědy v Cambridgi (Isaac Newton Institute for Mathematical Sciences in Cambridge) přednášku o vyřešení velmi významné hypotézy japonského matematika Yutaki Taniyamy v aritmetické algebraické geometrii týkající se velké třídy eliptických křivek nad racionálními čísly. Jako důsledek vyplývá odsud vyřešení Fermatova problému, který byl zapsán jako tvrzení bez důkazu vynikajícím francouzským učencem Pierre de Fermatem asi r. 1637. Od té doby se mnoho matematiků profesionálů i amatérů pokoušelo toto tvrzení dokázat. Snad o žádném matematickém problému nebylo napsáno tolik prací, z nichž obrovská část obsahovala závažné chyby nebo důkazy obsahovaly zatím neodstranitelné mezery.

Výsledek Andrewa Wilese vzbudil novou vlnu zájmu o tuto otázku. Cílem tohoto článku je napsat jakousi „prehistorii" Fermatova problému, která v některých směrech (*Fermatovy kvocienty*) zasahuje do současné doby. O Wilesově důkazu, který používá algebraickou geometrii, pojednává článek J. Nekováře ([Ne], 1994).

Zmiňme se na tomto místě ještě o nedávných dvou význačných výsledcích týkajících se Fermatova problému. V r. 1983 dokázal G. Faltings ([Fa]) *Mordellovu hypotézu* z r. 1922:

Nechť K je algebraické číselné těleso. Pak počet K-racionálních bodů nesingulární projektivní křivky nad K, jejíž genus je větší než 1, je konečný.

Z této věty pak plyne, že *pro každé přirozené číslo $n \geq 3$ má Fermatova rovnice $x^n + y^n = z^n$ konečný počet celočíselných řešení (x, y, z)*, tudíž pro přirozené číslo $n \geq 3$ nejvýše konečný počet trojic (x, y, z) narušuje platnost Fermatovy hypotézy.

Druhý významný výsledek plyne z článků Adlemana, Heatha-Browna a Fouvryho ([AH], [Fo], 1985) a týká se platnosti věty o nekonečnosti množiny prvočísel, pro něž platí *první případ Fermatovy hypotézy.*

Můj příspěvek se týká „klasické cesty" užívající ponejvíce algebraickou teorii čísel, kterou se značná část matematiků ubírala v historii tohoto problému. Nemohl jsem popsat všechny výsledky z této oblasti, vybral jsem podle svého názoru jen nejvýznačnější a nejzajímavější. Tento výběr je tedy vysoce subjektivní. Mimo nepochybného příspěvku Fermata samotného považuji za nejvýznačnější přínos v oblasti řešení Fermatova problému výsledky německého matematika Ernsta Kummera z minulého století.

RNDr. Ladislav Skula, DrSc. (1937), je profesorem na katedře aplikované matematiky Přírodovědecké fakulty Masarykovy univerzity, Janáčkovo nám. 2a, 662 95 Brno.

Tato práce byla částečně finančně podporována GA ČR pod grantovým číslem 201/93/2122.

Kummerovy práce značně přesahují význam Fermatova problému, a jejich hodnota značnou měrou ovlivnila vývoj algebry a teorie čísel. Kummerova teorie ideálních čísel dala impuls k vybudování jedné ze základních partií algebry — teorii ideálů. Výsledky prací Ernsta Kummera se stále používají a citují v algebraické teorii čísel a zejména v oblasti kruhových těles. Kummerův příklad ukazuje na vysoce pozitivní úlohu, kterou sehrála Fermatova hypotéza při rozvoji matematiky.

Čtenáře, který projeví hlubší zájem o historii Fermatova problému, odkazuji na Bachmannovu knihu [Ba], která zahrnuje stav bádání o Fermatově hypotéze asi do r. 1917, velmi pěkná monografie P. Ribenboima [R1] udává výsledky z této oblasti ze všech možných hledisek zhruba do konce osmdesátých let.

Kniha H. M. Edwardse [Ed] je zaměřena na velmi detailní historická fakta zasahující do doby Kummerovy a na podrobný výklad Kummerova přínosu. Ve slovenštině existuje zajímavá a poučná kniha Š. Schwarze [Sc], ve které je kladen důraz na teorii ideálů, motivaci jejího vzniku a zákulisí této teorie.

1. Fermat

Pierre de Fermat (1601–1665) patřil ve své době k nejslavnějším matematikům v Evropě. Proslavil se svými výsledky v teorii čísel, analytické geometrii, počtu pravděpodobnosti a dospěl až k základům diferenciálního počtu. Ve fyzice-optice se dodnes používá Fermatův princip.

Jeho vědecká činnost v matematice se vyznačuje třemi kuriozitami. První kuriozitou je skutečnost, že Fermat nebyl žádný profesionální matematik, matematiku pěstoval jako jeden ze svých koníčků, ke kterým patřily též básnictví a řecká filologie. Hlavním jeho oborem byly právní vědy, P. Fermat byl profesí právník a pracoval jako soudce v Toulouse. Často byl nazýván kníže amatérů.

Druhou zvláštností byl fakt, že P. Fermat nikdy neuveřejnil žádnou matematickou práci. Jedinou výjimku tvoří dodatek ke knize jeho kolegy z r. 1660, který byl však napsán anonymně. Jeho matematické výsledky se šířily v tehdejším vědeckém světě prostřednictvím jeho korespondence s jinými vědci a pomocí různých pojednání, které kolovaly v matematické veřejnosti v rukopisné formě. Po jeho smrti zveřejnil jeho syn Samuel de Fermat (1670) mnoho číselně-teoretických výsledků svého otce.

Třetí kuriozitou Fermatovy matematické činnosti je časté uvádění tvrzení bez důkazů. Tím se ovšem stalo, že bylo později zjištěno, že některá Fermatova tvrzení nejsou správná. Fermat např. studoval čísla

$$F_n = 2^{2^n} + 1 \qquad (n = 0, 1, 2, \ldots)$$

(dnes zvaná *Fermatova čísla*) a tvrdil, že všechna tato čísla jsou prvočísla. Toto tvrzení platí pro $0 \leqq n \leqq 4$, neboť $F_0 = 3$, $F_1 = 5$, $F_2 = 17$, $F_3 = 257$, $F_4 = 65\,537$ jsou prvočísla, zatímco Fermatovo číslo

$$F_5 = 2^{32} + 1 = 641 \times 6\,700\,417$$

je složené, což bylo ukázáno Eulerem.

V dnešní době existuje celá literatura o Fermatových číslech ([R2], Chapter 2, VI), nicméně mimo uvedených F_n ($0 \leqq n \leqq 4$) nejsou známá žádná jiná Fermatova čísla, která jsou prvočísla. Nerozřešené jsou zatím otázky, zdali existuje nekonečně mnoho přirozených čísel n tak, že F_n je prvočíslo, resp. složené číslo.

Jiná chybná Fermatova tvrzení je možno nalézt v knížce W. Sierpińského [Sr], odst. 24.

Až do letošního roku (1993) všechny Fermatovy výroky z teorie čísel byly dokázány nebo bylo ukázáno, že neplatí, až na tzv. „*Velkou Fermatovu větu*". Tato věta se v anglicky psaných článcích nazývá převážně „*Fermat's Last Theorem*", stručněji (FLT), což znamená poslední ještě nedokázané nebo nevyvrácené Fermatovo tvrzení. Tato „Velká Fermatova věta" (nebo též „Fermatova hypotéza") je následující matematické tvrzení:

VELKÁ FERMATOVA VĚTA. *Rovnice*

$$x^n + y^n = z^n$$

pro každé přirozené číslo $n \geqq 3$ *je neřešitelná v celých nenulových číslech* x, y, z.

P. Fermat zapsal si tuto větu (latinsky) asi kolem r. 1637 na okraj stránky svého exempláře sebraných spisů řeckého matematika Diofanta (žil asi v 3. stol. n. l. v Alexandrii) s poznámkou, že našel obdivuhodný důkaz tohoto tvrzení, pro který je na okraji málo místa.

K vyslovení této věty byl P. Fermat inspirován studiem části těchto Diofantových spisů týkajících se úlohy nalézt všechna celá čísla x, y, z, pro která platí

$$x^2 + y^2 = z^2.$$

Každá trojice přirozených čísel (x, y, z), která vyhovují uvedené rovnici, se nazývá *pythagorejská trojice*. Nejznámější pythagorejskou trojicí je trojice $(3, 4, 5)$, která byla známa již ve starověku a užívána pro konstrukci pravého úhlu. Další pythagorejskou trojicí je trojice $(5, 12, 13)$.

Erich von Däniken ([Dä], odst. *Ubohý Pythagore!*, str. 103, 104) dává existenci pravoúhlých trojúhelníků s poměrem stran rovným těmto dvěma pythagorejským trojicím ve stavbách z doby kamenné v souvislost se stykem s mimozemskými civilizacemi.

Popis všech pythagorejských trojic je znám a je dán následující větou:

VĚTA *(o pythagorejských trojicích). Řešení rovnice* $x^2 + y^2 = z^2$ *přirozenými čísly* x, y, z, *která jsou nesoudělná a* x *je sudé, je dáno tzv. „indickými formulemi":*

$$x = 2mn, \quad y = m^2 - n^2, \quad z = m^2 + n^2,$$

kde m, n *jsou nesoudělná přirozená čísla různé parity a* $m > n$.

Fermat objevil a často používal důkazovou metodu *descente infinie* (nekonečný sestup), která je založena na tomto principu:

Jestliže $V(n)$ značí nějakou vlastnost pro každé přirozené číslo n a jestliže jsme ukázali, že z předpokladu „přirozené číslo p má vlastnost $V(p)$" plyne existence přirozeného čísla q menšího než p majícího vlastnost $V(q)$, pak žádné přirozené číslo n nemá vlastnost $V(n)$.

Fermatův princip descente infinie je vlastně jakási „indukce směrem dolů" neboli „sestupná indukce". Tento princip využívá skutečnosti, že množina přirozených čísel $\mathbb{N}$ v obvyklém uspořádání je *dobře uspořádaná množina*, tj. každá neprázdná podmnožina $\mathbb{N}$ má nejmenší prvek. Vzhledem k důležitosti této metody ukážeme její důkaz, který je ostatně jediným důkazem v tomto článku:

Důkaz. Nechť jsou splněny uvedené podmínky principu descente infinie. Označme M množinu všech přirozených čísel m, která mají vlastnost $V(m)$. Je-li množina M neprázdná, pak vzhledem k dobrému uspořádání množiny $\mathbb{N}$ existuje přirozené číslo p, které je nejmenším prvkem množiny M. Pak $p \in M$, tudíž p má vlastnost $V(p)$. Podle předpokladu metody descente infinie existuje $q \in \mathbb{N}$, které má vlastnost $V(q)$ a $q < p$. Pak ale $q \in M$, což je spor a tudíž množina M je prázdná, c. b. d.

Na druhé straně z platnosti principu descente infinie plyne, že množina $\mathbb{N}$ je dobře uspořádaná množina. Jsou tedy obě vlastnosti přirozených čísel:

„$\mathbb{N}$ je dobře uspořádaná množina"

a

„platí princip descente infinie"

ekvivalentní. V současné výstavbě přirozených čísel (Peanovy axiomy, kardinální čísla konečných množin) se dokazuje vlastnost: „$\mathbb{N}$ je dobře uspořádaná množina". Ve Fermatově době neexistovala žádná z našeho hlediska precisní výstavba přirozených čísel, tudíž Fermat nemohl svůj princip nekonečného sestupu dokázat. Tento princip byl pokládán za intuitivně správné matematické tvrzení.

Užitím této metody dokázal Fermat *nemožnost řešení rovnice*

$$x^4 + y^4 = z^2$$

přirozenými čísly x, y, z.

V tomto důkaze označme pro přirozené číslo z vlastnost $V(z)$: „existují nesoudělná přirozená čísla x, y (x sudé), taková, že $x^4 + y^4 = z^2$". Jestliže existuje přirozené číslo z mající vlastnost $V(z)$, pak existují nesoudělná přirozená čísla x, y (x sudé) taková, že platí

$$(x^2)^2 + (y^2)^2 = z^2.$$

Trojice (x^2, y^2, z) je pak pythagorejská trojice a z indických formulí se dá odvodit existence přirozeného čísla $z' < z$ majícího vlastnost $V(z')$. Použitím metody descente infinie dostáváme nemožnost řešení rovnice $x^4 + y^4 = z^2$ přirozenými čísly.

Podobným způsobem se dá ukázat nemožnost řešení rovnic

$$\begin{aligned} x^4 - y^4 &= z^2 \\ x^4 + 4y^4 &= z^2, \qquad \text{(Euler)} \\ x^4 - 4y^4 &= \pm z^2 \end{aligned}$$

nenulovými celými čísly x, y, z ([R1], Ch. III, (2B)).

Z tvrzení o rovnici $x^4 + y^4 = z^2$ pak snadno plyne platnost velké Fermatovy věty pro exponent $n = 4$. Jelikož každé přirozené číslo $n \geqq 3$ je buď násobkem lichého prvočísla nebo 4, stačí se při řešení velké Fermatovy věty omezit na exponent $n = l$, kde l je liché prvočíslo. Vyšetřování rovnice ve velké Fermatově větě (*Fermatova rovnice*) pak přejde na vyšetřování rovnice

$$x^l + y^l = z^l,$$

kde l je liché prvočíslo.

Pro $l = 3$ podal Euler v r. 1770 důkaz, který však nebyl úplný a byl později doplněn. Jiný důkaz byl podán Gaussem, který byl publikován až po jeho smrti. Euler užíval čísel tvaru $a^2 + 3b^2$, kdežto Gauss pracoval již s komplexními algebraickými čísly tvaru $a + b\sqrt{-3}$ (v obou případech jsou a, b celá čísla). Oba tyto důkazy užívaly Fermatem objevenou metodu descente infinie.

Dirichlet podal řešení velké Fermatovy věty pro exponent $l = 5$ v r. 1825. Jeho důkaz však byl neúplný; na to poukázal Legendre, který udal vlastní nezávislý a úplný důkaz. Dirichlet pak v r. 1828 uveřejnil svůj doplněný důkaz. Dirichlet vyřešil též případ sudého exponentu $n = 14$ v r. 1832 a Lamé dokázal v r. 1839 Fermatovou hypotézu pro prvočíselný exponent $l = 7$. □

2. Kummer

V roce 1847 oznámil též Lamé, že nalezl důkaz velké Fermatovy věty. Jestliže pro přirození číslo $n \geqq 3$ je $\xi = \xi_n$ n-tá primitivní odmocnina z 1 [např. $\xi = \cos(2\pi/n) + i\sin(2\pi/n)$], pak můžeme Fermatovu rovnici $x^n + y^n = z^n$ psát ve tvaru

$$\prod_{i=0}^{n-1} (x + \xi^i y) = z^n.$$

Fermatův problém formulovaný pro celá čísla přechází tímto způsobem na problém pro speciální prvky kruhového tělesa $Q(\xi)$. *Kruhové těleso* $Q(\xi)$ je definováno jako těleso, které vznikne z tělesa racionálních čísel Q adjunkcí čísla ξ. Prvky kruhového tělesa jsou čísla tvaru $a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{n-1}\xi^{n-1}$, kde $a_0, \ldots, a_n$ jsou racionální čísla. Prvky kruhového tělesa jsou komplexní čísla a operace sčítání a násobení mezi nimi jsou definovány jako tytéž operace pro komplexní čísla. Název kruhové těleso je motivován faktem, že mocniny $1 = \xi^0, \xi, \xi^2, \ldots, \xi^{n-1}$ znázorněné v komplexní rovině tvoří vrcholy pravidelného n-úhelníka na jednotkové kružnici se středem v počátku.

Okruhem celých čísel kruhového tělesa $Q(\xi)$ se rozumí okruh $\mathbb{Z}[\xi]$, jehož prvky jsou čísla tvaru $a_0 + a_1\xi + a_2\xi^2 + \ldots + a_{n-1}\xi^{n-1}$, kde $a_0, \ldots, a_{n-1}$ jsou prvky okruhu celých čísel $\mathbb{Z}$. Okruh $\mathbb{Z}[\xi]$ je podokruhem tělesa $Q(\xi)$.

Lamé předpokládal, že v okruhu $\mathbb{Z}[\xi]$ platí analogické aritmetické zákony jako v okruhu celých čísel $\mathbb{Z}$. Speciálně považoval za platnou *větu o jednoznačnosti rozkladu (prvku) na ireducibilní faktory.* Takový okruh se dnes nazývá *Gaussův okruh.* V okruhu celých čísel $\mathbb{Z}$ tato věta platí a nazývá se *fundamentální věta aritmetiky celých čísel.*

Lamého idea byla ve stručnosti následující: jestliže čísla $\beta_i = x + \xi^i y$ $(0 \leqq i \leqq n-1)$ z Fermatovy rovnice jsou po dvou nesoudělná, dostáváme

$$\beta_0 \cdot \beta_1 \ldots \beta_{n-1} = z^n,$$

kde součin na levé straně je součin po dvou nesoudělných čísel okruhu $\mathbb{Z}[\xi]$. Ze zákona o jednoznačnosti rozkladu prvku na ireducibilní faktory pak plyne, že existují $\alpha_i \in \mathbb{Z}[\xi]$ a jednotky ε_i okruhu $\mathbb{Z}[\xi]$ tak, že

$$\beta_i = \varepsilon_i \alpha_i^n \quad \text{pro každé} \quad 0 \leqq i \leqq n-1.$$

Odtud je možno Fermatovou metodou descente infinie odvodit spor. Podobně by bylo možno postupovat v případě, že čísla β_i nejsou po dvou nesoudělná. (Důkaz je zde technicky náročnější, ale nakonec se zase používá Fermatova metoda descente infinie.)

E. E. Kummer (1810–1893) význačný německý matematik minulého století ale ukázal, že pro prvočíslo $l = 23$ v okruhu $\mathbb{Z}[\xi_{23}]$ neplatí věta o jednoznačnosti rozkladu na ireducibilní faktory. Existují zde čtyři navzájem neasociované ireducibilní prvky $\pi_1, \pi_2, \pi_3, \pi_4$ s vlastností

$$\pi_1\pi_2 = \pi_3\pi_4.$$

Otázka, které okruhy $\mathbb{Z}[\xi_n]$ jsou Gaussovy, byla rozřešena až v dnešní době. J. M. Masley publikoval v r. 1972 ([Ma]) výsledek udávající všechny okruhy $\mathbb{Z}[\xi_n]$, ve kterých platí věta o jednoznačnosti rozkladu na ireducibilní faktory. Těchto okruhů je jen konečně mnoho a jejich počet je roven číslu 29. Pro liché prvočíslo $n = l$ jsou to jen okruhy $\mathbb{Z}[\xi_l]$, kde $l \leqq 19$.

Hlavní zásluha Kummerova spočívá však v tom, že nalezl způsob, jak tento nedostatek odstranit (pro $n = l$ liché prvočíslo). Kummer „dodal" k okruhu $\mathbb{Z}[\xi]$ nové typy komplexních čísel, které nazval „ideální komplexní čísla" (ideale complexe Zahlen) na rozdíl od prvků okruhu $\mathbb{Z}[\xi]$, které nazýval „skutečná komplexní čísla" (wirkliche complexe Zahlen), přičemž tato nová množina je uzavřená k operaci násobení a tvoří tudíž pologrupu. Kummerova konstrukce vytvářela tuto pologrupu s platností věty o jednoznačnosti rozkladu na ireducibilní prvky.

V dnešní terminologii je tato konstrukce nejlépe vyjádřena pojmem „teorie divizorů" zavedeným Borevičem a Šafarevičem ([BŠ]). Kummerova ideální komplexní čísla jsou v podstatě divizory okruhu $\mathbb{Z}[\xi_l]$, které můžeme ztotožnit s ideály tohoto okruhu.

Mezi těmito ideálními komplexními čísly definoval Kummer ekvivalenci, přičemž počet tříd $h = h_l$ této ekvivalence je konečný a udává jakousi „míru odchylky" okruhu

$\mathbf{Z}[\xi_l]$) od jednoznačnosti rozkladu na ireducibilní prvky. Např. $h_l = 1$, právě když okruh $\mathbf{Z}[\xi_l]$ je Gaussův.

Kummerem vybudovaná teorie byla v kompletní formě publikována v jeho článku v r. 1847. Tato teorie dala vznik teorii ideálů obecného okruhu rozpracovanou Dedekindem, Emmy Noetherovou, Krullem, van der Waerdenem a jinými význačnými algebraiky a patří k základům moderní algebry.

Přes velký význam Kummerovy teorie ideálních čísel se Kummerovi nepodařilo obecně dokázat Fermatovu hypotézu. Nicméně odvodil v této oblasti jedno slavné tvrzení vyžadující jím zavedeného pojmu *regulárního* a *iregulárního prvočísla.*

Liché prvočíslo l se nazývá *regulární prvočíslo*, jestliže l nedělí počet tříd h_l okruhu $\mathbf{Z}[\xi_l]$. V opačném případě se liché prvočíslo nazývá *iregulární prvočíslo.*

Hlavní výsledek získaný Kummerem (1850) v oblasti Fermatovy hypotézy je následující:

VĚTA. *Nechť l je regulární prvočíslo. Pak rovnice*

$$\alpha^l + \beta^l + \gamma^l = 0$$

nemá řešení pro $\alpha, \beta, \gamma \in \mathbf{Z}[\xi_l]$, $\alpha \cdot \beta \cdot \gamma \neq 0$.

Poněvadž $\mathbf{Z} \subseteq \mathbf{Z}[\xi_l]$, plyne odtud platnost velké Fermatovy věty pro exponent rovný regulárnímu prvočíslu. Toto tvrzení bylo mnoha autory rozšiřováno na větší třídy prvočíselných exponentů, nejznámější a nejvýznačnější množiny těchto mocnitelů jsou uvedeny v článku matematiků D. H. Lehmera, E. Lehmera a H. S. Vandivera ([LLV], 1954). Pomocí rychlého počítače (v té době) SWAC ukázali zmínění autoři správnost Fermatovy hypotézy pro lichá prvočísla < 2000. S rozvojem počítačů a výpočetních metod byl tento výsledek rozšiřován a v posledních tabulkách iregulárních prvočísel ([BM], 1993) byla platnost Fermatovy hypotézy verifikována pro lichá prvočísla $< 4 \cdot 10^6$.

Ve výsledcích týkajících se Fermatova problému se vyskytují též různé odhady pro řešení Fermatovy rovnice, z nichž mezi nejznámější patří odhad daný touto větou ([IP], 1980):

VĚTA *(Inkeri, van der Poorten). Nechť l je liché prvočíslo a x, y, z jsou navzájem nesoudělná přirozená čísla, $y > x > 0$, která vyhovují rovnici*

$$x^l + y^l = z^l.$$

Pak

$$z - x > l^{2l}.$$

Kummer také zjišťoval, která prvočísla jsou regulární a která iregulární. Nejdříve vypočítal (1850, 1851), že iregulární prvočísla < 100 jsou jen prvočísla 37, 59 a 67, později (1874) určil všechna iregulární prvočísla menší než 164. Jsou to ještě prvočísla 101, 103, 131, 149 a 157. Kummer také objevil metodu, jak zjišťovat početně iregularitu prvočísla. Při této metodě jsou používána *Bernoulliova čísla*, kterými se budeme zabývat v dalším odstavci.

Otázka, zda existuje nekonečně mnoho iregulárních prvočísel, byla pozitivně vyřešena Jensenem ([Je], 1915). Naproti tomu dodnes zůstává otevřený problém, zdali existuje nekonečně mnoho regulárních prvočísel. Kummer sám se domníval, že počet iregulárních a regulárních prvočísel je stejný (asymptoticky). Označíme-li $\pi_i(x)$ počet iregulárních prvočísel menších než reálné číslo x a $\pi(x)$ počet všech prvočísel $< x$, pak Kummerovu domněnku lze vyjádřit vzorcem:

$$\lim_{x\to\infty} \frac{\pi_i(x)}{\pi(x)} = \frac{1}{2}.$$

Naproti tomu Siegel ([Sg], 1964) „heuristicky" dokazuje

$$\lim_{x\to\infty} \frac{\pi_i(x)}{\pi(x)} = 1 - \frac{1}{\sqrt{e}} \doteq 0{,}39.$$

Současné výpočty hodnot $\pi_i(x)$ a $\pi(x)$ jsou velmi blízké Siegelovu vzorci.

3. Bernoulliova čísla

V různých oblastech matematiky se vyskytují a používají *Bernoulliova čísla* B_n ($n \geqq 0$), která se poprvé objevila v knize Jakoba Bernoulliho ([Br], 1713, str. 97) vydané po jeho smrti. Tato čísla jsou definovaná jako koeficienty Taylorova rozvoje

$$\frac{x}{e^x - 1} = \sum_{n=0}^{\infty} B_n \frac{x^n}{n!}.$$

Dá se ukázat, že Bernoulliova čísla jsou čísla racionální a platí:

$$B_0 = 1, \quad B_1 = -\tfrac{1}{2}, \quad B_2 = \tfrac{1}{6}, \quad B_n = 0 \qquad \text{pro liché číslo } n \geqq 3,$$
$$B_n \neq 0 \quad \text{a} \quad \operatorname{sgn} B_n = (-1)^{\frac{n}{2}-1} \qquad \text{pro sudé číslo } n \geqq 2.$$

Bernoulliova čísla se dají také vyjádřit rekurentní formulí

$$(1 + B)^m - B^m = 0 \quad \text{pro } m \geqq 2, \ m \text{ celé č.},$$

kde B^k značí symbolickou mocninu rovnou B_k.

Kummer objevil ekvivalentní podmínku pro iregularitu prvočísla, která je vyjádřena pomocí Bernoulliových čísel. Pro vyjádření Kummerovy podmínky je nutno rozšířit pojem dělitelnosti celého čísla prvočíslem na čísla racionální, což je provedeno přirozeným způsobem.

Řekneme, že *prvočíslo l dělí racionální číslo* α, jestliže l dělí celé číslo a, kde $\alpha = a/b$, b je celé číslo různé od nuly a čísla a, b jsou nesoudělná. Nyní můžeme formulovat Kummerovu podmínku:

VĚTA *(Kummerovo kritérium pro iregularitu prvočísla). Liché prvočíslo l je iregulární, právě když existuje přirozené číslo i $[1 \leqq i \leqq \frac{1}{2}(l-3)]$ tak, že prvočíslo l dělí Bernoulliovo číslo B_{2i}.*

Toto kritérium má značný teoretický i praktický význam a od dob Kummerových se používá pro zjišťování iregularity konkrétních prvočísel. Tak např. pro nejmenší iregulární prvočíslo $l = 37$ máme

$$B_{32} = -\frac{7\,709\,321\,041\,217}{2 \cdot 3 \cdot 5 \cdot 17},$$

kde $7\,709\,321\,041\,217 = 37 \times 208\,360\,028\,141$.

Počet Bernoulliových čísel z Kummerova kritéria iregularity dělitelných prvočíslem l dává jakousi „míru iregularity prvočísla", nazývá se *index iregularity prvočísla* l a značí se symbolem $i(l)$. Tato hodnota je přesně dána formulí

$$i(l) = \#\{1 \leqq i \leqq \tfrac{1}{2}(l-3) : l \text{ dělí } B_{2i}\}.$$

Zřejmě pro regulární prvočíslo l je $i(l) = 0$. Nejmenší iregulární prvočísla $37, \ldots, 131$ mají index iregularity roven 1, naproti tomu $i(157) = 2$. V současné době byly pomocí výkonných počítačů a nejnovějších výpočetních metod (rychlá Fourierova transformace!) získány indexy iregularity pro prvočísla $l < 4 \cdot 10^6$ ([BM], 1993). Pro tato prvočísla l vždy platí $i(l) \leqq 7$, přičemž $i(l) = 7$ jen pro $l = 3\,238\,481$. Tabulky ukazují, že funkce $i(l)$ je proti prvočíslu l velmi malá. Pomocí indexu iregularity se dá odvodit jedno velmi silné kritérium pro tzv. první případ Fermatovy hypotézy.

Fermatova hypotéza se klasicky dělí (pro prvočíselný exponent) na dva případy:

První případ Fermatovy hypotézy (pro prvočíslo l) je tvrzení:
neexistují celá čísla x, y, z nedělitelná prvočíslem l tak, že $x^l + y^l = z^l$.

Druhý případ Fermatovy hypotézy (pro prvočíslo l) je tvrzení:
neexistují celá nenulová čísla x, y, z tak, že prvočíslo l dělí součin xyz a $x^l + y^l = z^l$.

Eichler ([Ei], 1965) publikoval velmi silné tvrzení o prvním případu Fermatovy hypotézy, které lze přepsat pro index iregularity tímto způsobem:

VĚTA *(Eichlerovo kritérium). Jestliže l je liché prvočíslo a platí-li*

$$i(l) < \sqrt{l} - 2,$$

pak platí první případ Fermatovy hypotézy pro prvočíslo l.

Pro první případ Fermatovy hypotézy odvodil Kummer (1857) další vztahy, ze kterých vyplynulo toto tvrzení:

TVRZENÍ. *Neplatí-li první případ Fermatovy hypotézy pro liché prvočíslo l, pak l dělí Bernoulliova čísla B_{l-3}, B_{l-5}.*

Podmínku „l dělí B_{l-3}“ dokázal již dříve jiným způsobem Cauchy. Jak je tato podmínka silná, ukazují již zmíněné tabulky indexu iregularity ([BM]): pro $l < 4 \cdot 10^6$ jen dvě prvočísla l mají vlastnost „l dělí B_{l-3}“, totiž $l = 16\,843$ a $l = 2\,124\,679$. Mimo tento fakt ukazují zmíněné tabulky, že mezi prvočísly $l < 4 \cdot 10^6$ jen pro prvočíslo $l = 37$ platí „l dělí B_{l-5}“.

Cauchyova a Kummerova podmínka pro první případ Fermatovy hypotézy byla dále rozšířena Mirimanoffem a Morishimou na Bernoulliova čísla B_{l-7}, B_{l-9}, B_{l-11}, B_{l-13}. Tuto podmínku velmi silně zostřil v r. 1934 Krasner ([Kr]) následujícím způsobem:

VĚTA *(Krasnerovo kritérium). Nechť* $n_0 = (45\,!)^{88}$. *Jestliže* l *je prvočíslo větší než* n_0, *pro které neplatí první případ Fermatovy hypotézy, pak*

$$l \text{ dělí } B_{l-1-2i}$$

pro každé $1 \leqq i \leqq \left[\sqrt[3]{\log l}\right]$.

Toto kritérium bylo dále zostřováno, podařilo se odstranit předpoklad $l > n_0$ a v podstatě nejsilnější verzi tohoto kritéria podal Granville ([Gr], 1986).

VĚTA *(Granville). Jestliže první případ Fermatovy hypotézy neplatí pro liché prvočíslo* l, *pak*

$$l \text{ dělí } B_{l-1-2i}$$

pro každé $1 \leqq i \leqq \left[(\log l / \log\log l)^{\frac{1}{2}}\right]$.

4. Fermatovy kvocienty

Jedno z nejvýznačnějších tvrzení vyslovené Fermatem v oblasti teorie čísel a používané v různých částí matematiky zejména v algebře (teorie konečných grup) je tzv. *„Malá Fermatova věta“*.

VĚTA *(Malá Fermatova věta). Pro prvočíslo* l *a celé číslo* a *nedělitelné* l *platí:*

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

Symbol $\equiv \pmod{m}$ byl zaveden Gaussem a je definován následovně:

Jsou-li x, y, m celá čísla, $m > 1$, pak řekneme, že *číslo* x *je kongruentní s číslem* y *podle modulu* m (nebo *modulo* m), jestliže m dělí rozdíl $x - y$. Píšeme pak

$$x \equiv y \pmod{m}.$$

Fermat sdělil toto tvrzení v r. 1640 v dopise Freuiclemu de Bessy. Publikováno bylo po jeho smrti až v r. 1679. První uveřejněný důkaz byl podán Eulerem v r. 1736.

Malá Fermatova věta tedy říká, že prvočíslo l dělí rozdíl $a^{l-1} - 1$ pro každé celé číslo a nedělitelné l. Pak číslo $(a^{l-1} - 1)/l$ je číslo celé, které se nazývá *Fermatův kvocient prvočísla* l *o základu* a. Fermatův kvocient označujeme symbolem $q_l(a)$ nebo jen $q(a)$. Tudíž

$$\frac{a^{l-1} - 1}{l} = q_l(a) \qquad \text{pro celé č. } a \text{ nedělitelné } l.$$

Fermatův kvocient má mnoho zajímavých vlastností, zmiňme se o jeho tzv. *„logaritmické vlastnosti“*.

TVRZENÍ *(logaritmická vlastnost Fermatova kvocientu). Nechť l je prvočíslo, které nedělí celá čísla a, b. Pak*

$$q_l(ab) \equiv q_l(a) + q_l(b) \pmod{l}.$$

Budeme se nyní zajímat rolí Fermatova kvocientu při pokusech o řešení prvního případu Fermatovy hypotézy. Vyšetřování tohoto vztahu zahájil A. Wieferich ([Wi], 1909) svou slavnou větou:

VĚTA *(Wieferich). Jestliže neplatí první případ Fermatovy hypotézy pro liché prvočíslo l, pak*

$$q_l(2) \equiv 0 \pmod{l}.$$

Wieferichova věta dala impuls k hledání lichých prvočísel l s vlastností $q_l(2) \equiv 0 \pmod{l}$, neboli

$$2^{l-1} \equiv 1 \pmod{l^2}.$$

Prvočíslo l s touto vlastností se dnes nazývá *Wieferichovo prvočíslo.* Žádné prvočíslo menší než 1000 není Wieferichovo. První Wieferichovo prvočíslo bylo nalezeno Meissnerem ([Me], 1913) a je rovno prvočíslu $l = 1093$. Další Wieferichovo prvočíslo objevil Beeger ([Bg], 1922) a je rovno prvočíslu $l = 3511$. Od té doby nebylo žádné další Wieferichovo prvočíslo nalezeno, D. H. Lehmer ([Lh], 1981) ukázal pomocí počítače, že pro $l < 6 \cdot 10^9$ žádné další Wieferichovo číslo neexistuje. Dosud nerozřešené jsou otázky, zdali existuje nekonečně mnoho Wieferichových prvočísel nebo jen konečně mnoho.

Wieferichovo kritérium dále rozšířili Mirimanoff, Vandiver, Frobenius, Pollaczek, Morishima a poslední výsledek v tomto směru získali Granville a Monagan ([GM], 1988):

VĚTA *(Granville, Monagan). Jestliže první případ Fermatovy hypotézy neplatí pro liché prvočíslo l, pak*

$$q_l(p) \equiv 0 \pmod{l}$$

pro každé prvočíslo $p \leqq 89$.

Jedna ze základních prací týkajících se Fermatových kvocientů byla uveřejněna v r. 1905 (před *Wieferichem*) českým matematikem Matyášem Lerchem ([Le]). V této práci byl udán následující vzorec pro Fermatův kvocient:

VĚTA *(Lerchova formule pro Fermatův kvocient). Nechť l je prvočíslo, a celé číslo nedělitelné l. Pak*

$$q_l(a) \equiv \sum_{x=1}^{l-1} \frac{1}{ax} \left[\frac{ax}{l}\right] \pmod{l}.$$

Zde symbolem $\frac{1}{y}$ pro celé číslo y nedělitelné prvočíslem l můžeme rozumět celé číslo z takové, že $y \cdot z \equiv 1 \pmod{l}$. Takové číslo z existuje a modulo l je určeno jednoznačně. Číslo z můžeme nazývat *inverze y modulo l.*

Buď l liché prvočíslo. Pro přirozené číslo $N < l$ a celé číslo k položme

$$s(k, N) = \sum_{k\frac{l}{N} < x < (k+1)\frac{l}{N}} \frac{1}{x},$$

kde výrazy $\frac{1}{x}$ značí inverze čísel x modulo l. Lerchovu formuli pak můžeme psát takto:

$$N \cdot q_l(N) \equiv \sum_{k=0}^{N-1} k s(k, N) \pmod{l}.$$

Jsou tedy hodnoty $N \cdot q_l(N)$ „lineárními kombinacemi" čísel $s(k, N)$. Nabízí se otázka, co lze říci o číslech $s(k, N)$ v souvislosti s prvním případem Fermatovy hypotézy. Autor tohoto článku publikoval ([Sk], 1992) obecnou větu, která tuto otázku řeší. Nicméně pro konkrétní hodnoty N je nutno vypočítat hodnoty speciálních determinantů modulo l. Ručním výpočtem bylo v článku [Sk] ukázáno, že v případě neplatnosti prvního případu Fermatovy hypotézy pro prvočíslo l máme

$$s(k, N) \equiv 0 \pmod{l}$$

pro každé $N \in \{2, 3, \ldots, 10\} \cup \{12\}$ a každé celé číslo k $(0 \leqq k \leqq N - 1)$.

Tento výsledek byl autorem ve spolupráci s kanadským kolegou K. Dilcherem za použití moderní výpočetní techniky vylepšen na toto tvrzení ([DS]):

VĚTA *(Dilcher, Skula). Jestliže l je liché prvočíslo, pro které neplatí první případ Fermatovy hypotézy, pak*

$$s(k, N) \equiv 0 \pmod{l}$$

pro každé přirozené číslo $N \leqq 46$ a každé celé číslo k $(0 \leqq k \leqq N - 1)$.

P. Cikánek (autorův spolupracovník) dokázal vztah $s(k, N) \equiv 0 \pmod{l}$ za předpokladu předcházející věty pro všechna přirozená čísla $N \leqq 94$, ale pro dostatečně velká prvočísla l ([Ci]).

Literatura

[AH] L. M. ADLEMAN, D. R. HEATH-BROWN: *The first case of Fermat's last theorem.* Invent. Math. *79* (1985), 409–416.

[Ba] P. BACHMANN: *Das Fermatproblem in seiner bisheringen Entwicklung.* W. de Gruyter, Berlin und Leipzig, 1919.

[Bg] N. G. W. H. BEEGER: *On a new case of the congruence* $2^{p-1} \equiv 1$ (p^2). Messenger of Math. *51* (1922), 149–150.

[Br] J. BERNOULLI: *Ars Conjectandi.* Basel, 1713.

[BŠ] I. BOREVIČ, I. P. ŠAFAREVIČ: *Těorija čisel.* Moskva, 1985, 3. vydání.

[BM] J. BUHLER, R. CRANDALL, R. ERNVALL, and T. METSÄNKYLÄ: *Irregular primes and cyclotomoic invariants to four million.* Mathematics of Computation *621* No. 203 (1993), 151–154.

[Ci] P. CIKÁNEK: *Special extension of Wieferich criterion.* Math. of Comp. *62* (1994), 923–930.
[Dä] E. VON DÄNIKEN: *Doba kamenná byla docela jiná.* Český překlad, Praha, 1993.
[DS] K. DILCHER, L. SKULA: *A new criterion for the first case of Fermat's last theorem.* Math. of Comp., v tisku.
[Ed] H. M. EDWARDS: *Fermat's Last Theorem, A Genetic Introducition to Algebraic Number Theory.* Springer-Verlag, 1977.
[Ei] M. EICHLER: *Eine Bemerkung zur Fermatschen Vermutung.* Acta Arithm. *11* (1965), 129–131 (Errata, 261).
[Fa] G. FALTINGS: *Endlichkeitssätze für abelsche Varietäten über Zahlkörpern.* Invent. Math. *73* (1983), 349–366.
[Fo] E. FOUVRY: *Théorème de Brun-Titchmarsh, application an théorème de Fermat.* Invent. Math. *79* (1985), 383–407.
[Gr] A. GRANVILLE: *On Krasner's criteria for the first case of Fermat's last theorem.* Manuscripta mathematica *56* (1986), 67–70.
[GM] A. GRANVILLE, M. B. MONAGAN: *The first case of Fermat's last theorem is true for all prime exponents up to 714, 591, 416, 091, 389.* Trans. Amer. Math. Soc. *306* (1988), 320–359.
[JP] K. INKERI, A. J. VAN DER POORTEN: *Some remarks on Fermat's conjecture.* Acta Arith. *XXXVI* (1980), 107–111.
[Je] K. L. JENSEN: *Om talteoretiske Egenskaber ved de Bernoulliske tal.* Dánsky, Nyt Tidsskript f. Math. *26* (1915), 73–83.
[Kr] M. KRASNER: *Sur le premiér cas du théorème de Fermat.* C. R. Acad. Sci. Paris *199* (1934), 256–258.
[Ku] ERNST EDUARD KUMMER: *Collected Papers.* Vol. I, *Contributions to Number Theory.* Edited by ANDRÉ WEIL, Springer Verlag, 1975.
[LLV] D. H. LEHMER, E. LEHMER, H. S. VANDIVER: *An application of high-speed computing to Fermat's last theorem.* Proc. Nat. Acad. Sci. U.S.A. *40* (1954), 25–33.
[Lh] H. D. LEHMER: *On Fermat's quotient, base two.* Math. Comp. *36* (1981), 289–290.
[Le] M. LERCH: *Zur Theorie des Fermatschen Quotienten* $(a^{p-1} - 1)/p = q(a)$. Math. Annalen, *B60* (1905), 471–490.
[Ma] J. M. MASLEY: *On the Class Number of Cyclotomic Fields.* Thesis, Princeton University, 1972.
[Me] W. MEISSNER: *Über die Teilbarkeit von* $2^p - 2$ *durch das Quadrat der Primzahl* $p =$ $= 1093$. Sitzungsberichte Akad. d. Wiss., Berlin (1913), 663–667.
[Ne] J. NEKOVÁŘ: *Modulární křivky a Fermatova věta.* Mathematica Bohemica č. 1 (1994).
[R1] P. RIBENBOIM: *13 Lectures on Fermat's Last Theorem.* Springer-Verlag, 1979.
[R2] P. RIBENBOIM: *The Book of Prime Number Records.* Springer-Verlag, 1988.
[Sc] Š. SCHWARZ: *Algebraické čísla.* Praha, 1950.
[Sg] C. L. SIEGEL: *Zu zwei Bemerkungen Kummers.* Nachr. Akad. Wiss. Göttingen, Math. Phys. Kl. II, (1964), 51–57.
[Sr] W. SIERPIŃSKI: *Co víme a co nevíme o prvočíslech* (český překlad). Praha 1966.
[Sk] L. SKULA: *Fermat's Last Theorem and the Fermat Quotients.* Comm. Math. Univ. Sancti Pauli (Tokyo), Vol. *41* (1992), 35–54.
[Wi] A. WIEFERICH: *Zum letzten Fermat'schen Theorem.* Journal für reine u. angew. Math. *136* (1909), 293–302.