Cahiers du CEFRES
N° 28, Matematik Pierre de Fermat
Alena Šolcová, Michal Křížek, Georges Mink (Ed.)

Guy TERJANIAN
Velká Fermatova věta

Référence électronique / electronic reference :
Guy Terjanian, « Velká Fermatova věta », Cahiers du CEFRES. N° 28, Matematik Pierre de Fermat (ed. Alena Šolcová, Michal Křížek, Georges Mink).
Mis en ligne en / published on : mai 2010 / may 2010
URL : http://www.cefres.cz/pdf/c28/terjanian_2002_velka_fermatova_veta.pdf
Editeur / publisher : CEFRES USR 3138 CNRS-MAEE
http://www.cefres.cz

Velká Fermatova věta

Guy Terjanian, Toulouse

1. Úvod

V roce 1670 Samuel de Fermat, syn Pierra de Fermata, publikoval v Toulouse Diofantovu Aritmetiku rozšířenou o poznámky, které jeho otec připisoval na okraje svého exempláře Bachetova vydání Diofantovy Aritmetiky z roku 1621. V jedné z těchto poznámek Fermat bez důkazu tvrdí, že:

Neexistují přirozená čísla $n \geq 3$, $x \geq 1$, $y \geq 1$ *a* $z \geq 1$ *taková, že*

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

To je Velká Fermatova věta, které se francouzsky též říká „le dernier théorème de Fermat“ (poslední Fermatova věta). Tato poznámka způsobila vznik obrovského množství prací a až v roce 1995 ji dokázali Andrew Wiles a Richard Taylor. V tomto článku se zaměříme na přehled základních výsledků týkajících se tohoto problému, seskupených podle užitých matematických metod.

2. Elementární metody

První výsledky lze odvodit z věty, kterou vyslovil sám Fermat.

Věta 1 (Fermat, 1670). *Obsah pravoúhlého trojúhelníka, jehož délky stran jsou přirozená čísla, není čtvercem přirozeného čísla.*

Fermat ji dokázal pomocí metody nekonečného sestupu. Z věty 1 plyne:

Věta 2.

(i) *Jestliže* x *a* y *jsou přirozená čísla taková, že* $x > y \geq 1$, *pak* $xy(x^2 - y^2)$ *není čtvercem.*

(ii) *Jestliže* x, y, z *jsou celá čísla taková, že* $x^4 - y^4 = z^2$, *pak je* y *nebo* z *rovno nule.*

(iii) *Neexistují přirozená čísla* $x \geq 1$, $y \geq 1$ *a* $z \geq 1$ *taková, že*

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

Z francouzského originálu *Le grand théorème de Fermat* přeložili Michal a Pavel Křížek.

D ů k a z . (i) Jestliže $x > y \geq 1$, pak $(x^2 - y^2,\ 2xy,\ x^2 + y^2)$ jsou strany pravoúhlého trojúhelníka s obsahem $xy(x^2 - y^2)$ a použijeme větu 1.
(ii) Jestliže x, y, z jsou celá čísla taková, že $x^4 - y^4 = z^2$ a že $yz \neq 0$, pak máme $x^2 y^2((x^2)^2 - (y^2)^2) = (xyz)^2$, což je ve sporu s (i).
(iii) Důsledek (ii). □

Velká Fermatova věta tudíž platí pro exponent 4, což nám umožňuje vyšetřovat jen ty případy, kdy je exponent prvočíslem. Zvolme tedy prvočíslo $p \geq 3$ a uvažujme rovnici

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

Stejně tak se můžeme zřejmě zabývat rovnicí

$$x^p - y^p = z^p$$

nebo rovnicí

$$x^p + y^p + z^p = 0 .$$

Pokud Velká Fermatova věta neplatí pro exponent p, pak existují celá čísla x, y, z splňující

$$(H_p)\ \begin{cases} x \geq 1,\ y \geq 1,\ z \geq 1, \\ x, y, z \text{ jsou po dvou nesoudělná,} \\ x^p - y^p = z^p . \end{cases}$$

Vyjděme tedy z této hypotézy (H_p), abychom došli ke sporu.
Zavedeme-li cyklotomický polynom

$$\Phi_p = X^{p-1} + X^{p-2}Y + \cdots + Y^{p-1},$$

dostaneme

$$X^p - Y^p = (X - Y)\Phi_p .$$

Z hypotézy (H_p) vyplývá

$$(x - y)\Phi_p(x, y) = z^p .$$

Jestliže z není dělitelné p, existují přirozená čísla u a v tak, že

$$\begin{aligned} x - y &= u^p, \\ \Phi_p(x, y) &= v^p, \\ z &= uv, \end{aligned}$$

a jestliže z je dělitelné p, existují přirozená čísla r a s tak, že

$$x - y = p^{p-1} r^p,$$
$$\Phi_p(x, y) = ps^p,$$
$$z = prs.$$

To nás přivádí k následujícím vztahům:

$$(R_1) \begin{cases} x \geq 1, \ y \geq 1, \ v \geq 1, \\ (x, y) = 1, \\ \Phi_p(x, y) = v^p \end{cases}$$

a

$$(R_2) \begin{cases} x \geq 1, \ y \geq 1, \ s \geq 1, \\ (x, y) = 1, \\ \Phi_p(x, y) = ps^p. \end{cases}$$

O řešeních (R_1) a (R_2) pro $p \geq 5$ nevíme téměř nic. Víme jen, že (R_2) má řešení $x = y = s = 1$.

Důkaz neplatnosti (H_p) probíhá většinou ve dvou etapách:

První případ: (H_p) neplatí, když p nedělí xyz.
Druhý případ: (H_p) neplatí, když p dělí xyz.

První výsledek týkající se (H_p) pochází od Eulera. V roce 1770 ve svém pojednání s názvem Algebra dokázal Velkou Fermatovu větu pro exponent 3.

Věta 3 (Euler, 1770). *Neexistují přirozená čísla x,y,z tak, že*

$$x^3 + y^3 = z^3.$$

D ů k a z . Použijeme opět metodu nekonečného sestupu. Vyjděme ze vztahů

$$x \geq 1, \ y \geq 1, \ z \geq 1,$$
$$x^3 \pm y^3 = z^3,$$
$$(x, y, z) = 1,$$

kde z je sudé a čísla x a y jsou lichá. Je-li

$$x \pm y = 2p,$$
$$x \mp y = 2q,$$

pak máme

$$2p(p^2 + 3q^2) = z^3$$

a pro $z = 2z_1$ dále dostaneme

$$p(p^2+3q^2)=4z_1^3.$$

Pokud z_1 není dělitelné 3, pak existují přirozená čísla z_2, z_3 tak, že

$$p=4z_2^3,$$
$$p^2+3q^2=z_3^3,$$
$$z_1=z_2z_3.$$

Odtud Euler bez bližšího vysvětlení odvodil, že existují celá čísla t a u taková, že

$$p+q\sqrt{-3}=\left(t+u\sqrt{-3}\right)^3,$$

což dává

$$p=t^3-9u^2t,$$
$$4z_2^3=t(t+3u)(t-3u).$$

Tedy existují celá čísla z_4, z_5, z_6 taková, že

$$t=4z_4^3,$$
$$t+3u=z_5^3,$$
$$t-3u=z_6^3,$$
$$z_2=z_4z_5z_6.$$

Odtud vyplývá, že

$$z_5^3+z_6^3=(2z_4)^3,$$

a také že

$$2|z_4|\le 2z_2<2z_1=z.$$

Jestliže z_1 je dělitelné 3, dojdeme stejným způsobem k rovnosti tvaru

$$a^3+b^3=(2c)^3,$$

kde a, b, c jsou celá čísla a $2|c|<z$. Získáme tak rovnost stejného tvaru jako tu, ze které jsme vyšli, ale s přirozeným číslem z' menším než z, což je spor. □

Euler mohl dokázat platnost rovnosti

$$p+q\sqrt{-3}=\left(t+u\sqrt{-3}\right)^3,$$

neboť to lze udělat použitím vlastností kvadratické formy x^2+3y^2, kterou znal.

Věta 4 (Lejeune Dirichlet, 1825, 1828). *Neexistují přirozená čísla x, y, z taková, že*

$$x^5+y^5=z^5.$$

Důkaz lze opět provést pomocí metody nekonečného sestupu s využitím vztahu

$$4\Phi_5 = (3X^2 + 4XY + 3Y^2)^2 - 5(X + Y)^4$$

a vlastností kvadratické formy $x^2 - 5y^2$.

Věta 5 (Lamé, Lebesgue, 1840). *Neexistují přirozená čísla x, y, z taková, že*

$$x^7 + y^7 = z^7.$$

Důkaz je elementární. Vyjde se ze vztahů

$$x^7 + y^7 + z^7 = 0,$$
$$(x + y + z)^7 = 7(x + y)(x + z)(y + z)[(x^2 + y^2 + z^2 + xy + xz + yz)^2 + xyz(x + y + z)]$$

a přijde se k rovnici

$$p^2 = q^4 - 2^{2a} \cdot 3 \cdot 7^4 q^2 r^2 + 2^{4a+4} \cdot 7^7 r^4,$$

která se opět vyšetřuje pomocí metody nekonečného sestupu.

Věta 6 (Sophie Germain, Legendre, 1823). *Jestliže existuje prvočíslo q tvaru* $2kp+1$ *splňující následující vlastnosti:*

a) $x^p + y^p + z^p \equiv 0 \pmod{q} \Rightarrow q$ *dělí x, y nebo z,*
b) $x^p \equiv p \pmod{q}$ *nemá řešení,*

pak platí první případ Velké Fermatovy věty vzhledem k exponentu p.

Důkaz je poměrně jednoduchý a lze jej nalézt v Ribenboimových knihách [2, 3].

Lze odvodit následující větu:

Věta 7. *Pokud alespoň jedno z čísel* $2p + 1$, $4p + 1$, $8p + 1$, $10p + 1$, $14p + 1$, $16p + 1$ *je prvočíslo, pak první případ Velké Fermatovy věty platí pro exponent p.*

Odtud dostaneme, že první případ platí pro všechny prvočíselné exponenty menší než 100.

Legendre navrhl ještě jinou metodu pro první případ. Jestliže pro jisté prvočíslo p platí

$$x^p + y^p \equiv z^p \pmod{p^2},$$

pak x, y nebo z je dělitelné p a první případ je tak ověřen. To nastane pro $p = 3$ a $p = 5$, ale ne pro $p = 7$. Toto je zajímavá metoda, která byla jen málo studována.

Věta 8 (Terjanian, 1977). *Jestliže x, y, z jsou přirozená čísla taková, že $x^{2p} + y^{2p} = z^{2p}$, pak je x nebo y dělitelné $2p$.*

D ů k a z (sporem). Předpokládejme naopak, že x, y, z jsou taková, že

$x \geq 1, \quad y \geq 1, \quad z \geq 1,$
x, y, z jsou po dvou nesoudělná,
$x^{2p} + y^{2p} = z^{2p},$
$2p$ nedělí ani x ani y.

Jedno z čísel x, y je sudé a jedno liché. Předpokládejme, že x je sudé. Potom platí

$$z^{2p} - y^{2p} = x^{2p},$$
$$(z^2 - y^2)\Phi_p(z^2, y^2) = x^{2p},$$

a protože x není dělitelné p, existuje u tak, že

$$\Phi_p(z^2, y^2) = u^{2p}.$$

Nechť m je prvočíslo takové, že pro Legendrův symbol platí $\left(\frac{p}{m}\right) = -1$. Pak

$$\left(\frac{\Phi_p(z^2, y^2)}{\Phi_m(z^2, y^2)}\right) = \left(\frac{p}{m}\right) = -1,$$

což je ale spor, neboť $\Phi_p(z^2, y^2)$ je čtverec. □

3. Cyklotomie

Cyklotomie je geometrický problém dělení kružnice na stejné části. Gauss se zabýval tímto problémem v roce 1801. Ve svém díle „Disquisitiones arithmeticae“ studoval rozšíření tělesa racionálních čísel Q pomocí p-té odmocniny z jedné, kde p je prvočíslo.

Nechť

p je liché prvočíslo,
$z = e^{2i\pi/p},$

$$K = Q(z) = \{ \sum_{i=0}^{n} a_i z^i \mid \ a_i \in Q; \ n \in N\},$$

$$A = Z(z) = \{ \sum_{i=0}^{n} a_i z^i \mid \ a_i \in Z; \ n \in N\}.$$

Tedy platí

$$\Phi_p(z) = \sum_{i=0}^{p-1} z^i = 0.$$

Gauss ukázal, že polynom Φ_p je ireducibilní, z čehož vyplývá, že K je konečné rozšíření Q stupně $p-1$. Navíc Gauss určil všechna podtělesa tělesa K.

Množina A je podokruhem K, což Gauss nevyšetřoval kromě několika speciálních případů. To ale bylo ústředním bodem výzkumu Kummera, neboť z (H_p) lze odvodit

$$(H_p') \qquad \prod_{i=0}^{p-1} (x - yz^i) = z^p,$$

kde čísla $x - yz^i$ jsou v okruhu A.

Jestliže A je *faktorový okruh*, tj. okruh, v němž rozklad na ireduciblilní prvky je jednoznačný (až na jednotky), a jestliže z není dělitelné p, pak čísla $x - yz^i$ jsou po dvou nesoudělná a pro každé $i = 0, \ldots, p-1$ existuje jednotka ε_i okruhu A a prvek $\alpha_i \in A$ tak, že

$$x - yz^i = \varepsilon_i \alpha_i^p .$$

Pomocí tohoto vztahu matematici útočili na Fermatův problém.

V roce 1844 Kummer naivně věřil, že okruh A je faktorový okruh. Potom výpočtem zjistil, že tomu tak není v případě $p = 23$. Tato obtíž jej neodradila a v říjnu 1845 oznámil svému příteli Kroneckerovi, že problém rozřešil zavedením nového abstraktního konceptu „ideálních prvočísel“ (prvky A se rozkládají jednoznačně na součin ideálních prvočísel). To pomohlo Kummerovi vytvořit algebraickou teorii čísel. Poznamenejme, že Kummerovy ideály nejsou naše dnešní ideály. Jsou to, čemu se dnes říká dělitelé.

Z hypotézy (H_p') dostáváme pro $i = 0, \ldots, p-1$

$$(H_p'') \begin{cases} x - yz^i = \alpha_i^p, & \text{jestliže } p \text{ nedělí } z, \\ x - yz^i = (1-z)\beta_i^p, & \text{jestliže } p \text{ dělí } z, \end{cases}$$

kde α_i a β_i jsou ideály A.

Aby mohl jít Kummer dále, zavedl *grupu tříd ideálů* na A pomocí faktorizace semigrup ideálů A podle semigrupy hlavních ideálů okruhu A. Ukázal, že tato grupa tříd je konečnou grupou. Dále nazval p *regulárním prvočíslem,* jestliže řád grupy tříd ideálů z A není dělitelný p.

Jestliže p je regulární, pak ideály α_i a β_i z (H_p'') jsou hlavní ideály a pro $i = 0, \ldots, p-1$ platí

$$(H_p''') \begin{cases} x - yz^j = \varepsilon_i \alpha_i^p, & \text{jestliže } p \text{ nedělí } z, \\ x - yz^j = \varepsilon_i (1-z) \alpha_i^p, & \text{jestliže } p \text{ dělí } z, \end{cases}$$

kde ε_i je jednotka v okruhu A a α_i je prvek z A.

Kummer předložil také následující kritérium.

Věta 9 (Kummer, 1847). *Pro to, aby p bylo regulárním prvočíslem, je nutné a stačí, aby žádný čitatel Bernoulliho čísel B_2, $B_4, \ldots, B_{p-3}$ nebyl dělitelný p.*

Připomeňme, že *Bernoulliho čísla* jsou racionální čísla taková, že

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

přitom platí

$$B_{2n+1} = 0 \quad \text{pro} \quad n \geq 1,$$
$$B_0 = 1, \; B_1 = -\frac{1}{2}, \; B_2 = \frac{1}{6}, \; B_4 = -\frac{1}{30}, \ldots .$$

Všechna prvočísla menší než 100 jsou regulární kromě čísel 37, 59 a 67. Je známo, že existuje nekonečně mnoho regulárních prvočísel.

Věta 10 (Kummer 1850, Hilbert 1897). *Jestliže p je regulární prvočíslo a jestliže α, β, γ jsou prvky tělesa $K=Q(z)$ takové, že*

$$\alpha^p + \beta^p + \gamma^p = 0,$$

pak alespoň jedno z čísel α, β, γ je nulové.

Kummerův důkaz není zdaleka triviální. Nebyl ani zcela rigorózní, ale Hilbert jej zdokonalil.

Potom Kummer dokázal Velkou Fermatovu větu pro exponenty 37, 59 a 67, a také pro všechny exponenty menší než 100. Další rozvoj cyklotomického přístupu se týkal především prvního případu Velké Fermatovy věty.

Dále si představme *Mirimanoffovy polynomy*. To jsou polynomy definované vztahem

$$f_n = \sum_{r=1}^{p-1} r^{n-1} x^r$$

pro přirozené n.

Věta 11 (Kummer 1857, Mirimanoff 1905). *Předpokládejme, že* $p \geq 5$ *a nechť* x, y, z *jsou celá čísla taková, že*

$$x^p + y^p + z^p = 0 \quad a \quad p \text{ nedělí součin } xyz.$$

Jestliže t *je jedno z čísel*

$$-\frac{x}{y}, -\frac{y}{x}, -\frac{x}{z}, -\frac{z}{x}, -\frac{y}{z}, -\frac{z}{y},$$

pak

$$B_i f_{p-i}(t) \equiv 0 \pmod{p} \quad pro \quad i = 2, 4, \ldots, p-3$$

a také

$$f_{p-1}(t) \equiv 0 \pmod{p}.$$

Věta 12. *Jestliže* $p \geq 11$ *a jestliže existují celá čísla* x, y, z *nesoudělná s* p *taková, že* $x^p + y^p + z^p = 0$, *pak platí*

$$B_{p-3} \equiv B_{p-5} \equiv B_{p-7} \equiv B_{p-9} \equiv 0 \pmod{p}.$$

Tato věta plyne z věty 11. Není známo žádné prvočíslo p, pro které by B_{p-3} a B_{p-5} byla dělitelná p.

Věta 13. *Nechť* $p \geq 5$ *je takové, že existují celá čísla* x, y, z *nesoudělná s* p *tak, že* $x^p + y^p + z^p = 0$. *Pak platí*

(i) $2^{p-1} \equiv 1 \pmod{p^2}$ (*Wieferich*, 1909),

(ii) $3^{p-1} \equiv 1 \pmod{p^2}$ (*Mirimanoff*, 1910).

Důkaz se opírá o větu 11. Pro $p < 4 \cdot 10^9$ jsou známa jen dvě prvočísla p splňující kongruenci $2^{p-1} \equiv 1 \pmod{p^2}$. Jsou to čísla 1093 a 3511. Pokud jde o kongruenci $3^{p-1} \equiv 1 \pmod{p^2}$, jsou také známa jen dvě řešení: 11 a 1006003.

Věta 14 (Furtwängler, 1912). *Nechť $p \geq 5$ a nechť existují celá čísla x, y, z nesoudělná s p taková, že*

$$x^p + y^p + z^p = 0,$$
$$(x, y, z) = 1,$$
$$xyz \neq 0.$$

(i) *Jestliže p nedělí x a jestliže r dělí x, pak $r^{p-1} \equiv 1 \pmod{p^2}$.*

(ii) *Jestliže $x^2 - y^2$ není kongruentní s 0 modulo p a jestliže $r \mid x^2 - y^2$, pak $r^{p-1} \equiv 1 \pmod{p^2}$.*

Důkaz využívá zákona reciprocity p-tých mocnin a je poměrně jednoduchý. Lze jej odvodit okamžitě z věty 13.

Věta 13 zobecnil Frobenius, Vandiver, Pollaczek, Morishima a Granville. Na druhé straně Vandiver podal nová kritéria platnosti Velké Fermatovy věty, která dovolují její ověření pro prvočíselné exponenty menší než $4 \cdot 10^6$.

Zaveďme *index iregularity* p,

$$i(p) = \operatorname{card}\{2 \leq i \leq p-3 \text{ takových, že } i \text{ je sudé a } B_i \equiv 0 \pmod{p}\},$$

kde card označuje počet prvků.

Věta 15 (Eichler, 1965, 1973; Skula 1977; Brückner 1979). *Nechť $p \geq 5$ a nechť existují celá čísla x, y, z nesoudělná s p taková, že $x^p + y^p + z^p = 0$. Pak $i(p) \geq \sqrt{p} - 2$.*

Pro $p < 4 \cdot 10^6$ platí $i(p) \leq \frac{1}{2} \log p < \sqrt{p} - 2$ a tato nerovnost patrně platí pro všechna prvočísla p.

V roce 1989 autor tohoto příspěvku definoval jinou vlastnost prvočísla p. Řekneme, že p má *vlastnost LC* (franc. loi complémentaire), jestliže pro $a \in Z$ jsou obě následující vlastnosti ekvivalentní:

(i) $a \equiv 0$ nebo $-1 \pmod{p}$,

(ii) a není kongruentní s 1 modulo p a pro každou reálnou jednotku ε z $K = Q(z)$ platí

$$\left(\frac{\varepsilon}{a - z}\right) = 1,$$

kde závorky odpovídají zbytkům p-tých mocnin a $a - z$ je celé číslo v tělese K.

Je zřejmé, že z (i) plyne (ii).

Věta 16 (Terjanian 1989; Anglès 2001). *Nechť* $p \geq 5$.
(i) *K tomu, aby* p *splňovalo vlastnost* LC *je nutné a stačí, aby systém kongruencí*

$$B_n f_{p-n}(x) = 0 \pmod{p}, \qquad n = 2, \ldots, p-3,$$

neměl jiná řešení než $x \equiv 0,\ 1$ *nebo* $-1 \pmod{p}$.

(ii) *Jestliže existují celá čísla nesoudělná s p taková, že*

$$x^p + y^p + z^p = 0,$$

pak p nemá vlastnost LC.

(iii) *Jestliže p nemá vlastnost LC , potom platí*

$$B_{p-3} \equiv 0 \pmod{p},$$
$$2^{p-1} \equiv 1 \pmod{p},$$
$$i(p) \geq \sqrt{p} - 2.$$

Tento výsledek implikuje větu 15 a zlepšuje Skulův výsledek z roku 1994.

4. Eliptické křivky

Eliptická křivka na tělese racionálních čísel Q je nesingulární kubická projektivní rovina definovaná na Q a obsahující racionální bod. Jestliže P je racionální bod eliptické křivky E , můžeme na množině racionálních bodů patřících do E zavést strukturu komutativní grupy, jejíž neutrální prvek je P .

Na počátku sedmdesátých let se Děmjaněnko, Frey a Hellegouarch zajímali o grupu torzí eliptických křivek, tj. o podgrupu sestavenou z racionálních bodů konečného řádu. Objevili, že pokud eliptická křivka na Q připouští racionální bod řádu p^2, kde $p \geq 5$ je prvočíslo, pak křivka rovnic

$$x^p - y^p = 1,$$
$$x^p + y^p = z^p$$

obsahuje racionální bod (x, y, z) takový, že $xyz \neq 0$, a proto Fermatova rovnice pro exponent p má netriviální řešení a Velká Fematova věta neplatí (viz [1]).

V roce 1984 Frey přiřadil eliptickou křivku netriviálnímu řešení Fermatovy rovnice. Přesněji řečeno pro

prvočíslo $p \geq 5$,
a, b, c celá čísla
$abc \neq 0$,
$(a, b, c) = 1$,
$a \equiv -1 \pmod 4$,
$b \equiv 0 \pmod 2$

Frey zavedl eliptickou křivku

$$y^2 = x(x - a^p)(x - b^p)$$

a načrtl důkaz faktu, že tato křivka nesplňuje domněnku Tanijamovu-Šimurovu, což bylo dále zdokonaleno Ribetem.

Věta 17 (Ribet, 1990). *Tanijamova-Šimurova domněnka implikuje Velkou Fermatovu větu.*

Tanijamova-Šimurova domněnka byla oznámena v roce 1955 Tanijamou. Tvrdí, že pokud E je eliptická křivka nad Q, l prvočíslo, pro něž E má dobrou redukci, $E(l)$ je počet bodů na E v konečném tělese F_l a pokud $a_l = l + 1 - E(l)$, pak čísla a_l jsou koeficienty indexu l modulární formy s vahou 2.

Věta 18 (Fermat, 1670; Wiles 1995). *Neexistují přirozená čísla* $n \geq 3$, x, y *a* z *taková, že* $x^n + y^n = z^n$.

To je Velká Fermatova věta (srov. obr. 1 a 2). Wiles dokázal Tanijamovu-Šimurovu domněnku pro semistabilní křivky, což stačí k ověření platnosti Velké Fermatovy věty.

Obr. 1. Na podstavci sochy Pierra de Fermata v jeho rodném Beaumontu-de-Lomagne, je vytesán nápis, který tvrdí, že $X^n + Y^n$ se nerovná Z^n pro n větší než 2.

Obr. 2. Česká a francouzská známka věnovaná Velké Fermatově větě.

Další rozvoj těchto metod přivedl Darmona a Mérela k rozřešení rovnic

$$x^n + y^n = z^2,$$
$$x^n + y^n = z^3,$$
$$x^n + y^n = 2z^n.$$

Výzkum eliptických křivek vyústil v zajímavou a překvapivou domněnku:

Hypotéza abc (Masse, Oesterlé, 1985). *Pro každé* $\varepsilon > 0$ *existuje konstanta* $C(\varepsilon)$ *taková, že pro každou trojici přirozených vzájemně nesoudělných čísel* (a, b, c), *pro něž* $a + b = c$, *platí*

$$c \le C(\varepsilon) r^{1+\varepsilon},$$

kde r je součin prvočísel, která dělí abc.

Důsledky domněnky abc jsou následující:

C1. *Existuje prvočíslo p_0 tak, že pro každé prvočíslo $p \geq p_0$ rovnice*

$$\Phi_p(x, y) = z^p,$$

kde $(x, y)=1$, $xy \neq 0$ a x, y, z jsou celá čísla, má jediná dvě řešení $(1,-1,1)$ a $(-1,1,1)$.

C2. *Počet šestic (x, y, z, r, s, t) přirozených čísel, pro něž*

$$x^r + y^s = z^t,$$
$$(x, y, z) = 1,$$
$$\frac{1}{r}+\frac{1}{s}+\frac{1}{t}<1,$$

je konečný.

Zatím nevíme, jak odpovědět na výše uvedené otázky.

Obr. 3. Autor tohoto příspěvku při přednášce o Velké Fermatově větě.

Literatura

[1] Mozzochi, R., *The Fermat diary*, American Mathematical Society, 2000.

[2] Ribenboim, P., *13 lectures on Fermat's last theorem,* Springer, 1979.

[3] Ribenboim, P., *Fermat's last theorem for amateurs,* Springer, 1999.

Adresa: Prof. Dr. Guy Terjanian, Laboratoire de Mathématiques, Emile Picard, CNRS, Université Paul Sabatier, 118 Rue de Narbonne, F-310 62 Toulouse Cedex 04, France.