Mathematica Bohemica

Kenneth A. Ribet

Wiles dokázal Taniyamovu hypotézu; důsledkem je Fermatova věta

Mathematica Bohemica, Vol. 119 (1994), No. 1, 75–78

Persistent URL: http://dml.cz/dmlcz/126202

119 (1994) MATHEMATICA BOHEMICA No. 1, 75–78

NEWS AND NOTICES

WILES DOKÁZAL TANIYAMOVU HYPOTÉZU; DŮSLEDKEM JE FERMATOVA VĚTA

KENNETH A. RIBET, University of California, Berkeley

Nechť p, u, v a w jsou celá čísla, $p > 1$. Pokud $u^p + v^p + w^p = 0$, pak $uvw = 0$.

Důkazem této podoby Fermatovy věty zakončil svou sérii tří přednášek na konferenci o Iwasawově teorii, automorfních formách a p-adických reprezentacích, uspořádané v červnu 1993 Ústavem Isaaca Newtona pro matematické vědy v Cambridgi (Velká Británie), profesor univerzity v Princetonu Andrew Wiles. Svým přednáškám dal Wiles leccos napovídající, ale nejednoznačný název „Eliptické křivky, modulární křivky a Galoisovy reprezentace", aby jeho posluchači netušili, čím série přednášek vyvrcholí. Přesto vytrvale kolovaly nejrůznější pověsti a napětí se stupňovalo s tím, jak přednášky postupovaly. Třetí přednášku sledovalo více než šedesát matematiků, z nichž mnozí si přinesli fotoaparáty, aby očekávanou událost zachytili.

Ve své závěrečné přednášce Wiles oznámil, že dokázal Taniyamovu hypotézu – nesmírně důležitou domněnku z aritmetické algebraické geometrie – pro obsáhlou třídu eliptických křivek nad tělesem racionálních čísel $\mathbf{Q}$. Jde o tzv. „semistabilní" eliptické křivky, tedy ty, jejichž konduktor je bezkvadrátový. Většina přítomných posluchačů věděla, že Fermatova věta z tohoto výsledku vyplývá. Přestože Fermatova věta vždy fascinovala jak amatéry, tak i profesionální matematiky, v konečném důsledku má Taniyamova hypotéza pro moderní matematiku mnohem větší význam.

Hypotéza Yutaky Taniyamy o tom, že každá eliptická křivka nad $\mathbf{Q}$ je modulární, byla poprvé zformulována v ne zcela úplné podobě na konferenci Tokyo-Nikko v roce 1955. Její tvrzení dále zpřesnili G. Shimura a A. Weil; byla střídavě známa jako Weilova hypotéza, hypotéza Shimury-Taniyamy i pod řadou jiných názvů. Ve své obvyklé formulaci tato hypotéza přiřazuje algebraicko-geometrickým objektům (eliptickým křivkám) objekty teorie reprezentací (modulární formy). Tvrdí, že L-funkce

Translated from *"Wiles Proves Taniyama's Conjecture; Fermat's Last Theorem Follows"*, by Kenneth A. Ribet, Notices of the American Mathematical Society, Volume 40, Number 6, July/August 1993, by permission of the American Mathematical Society.

eliptické křivky nad $\mathbf{Q}$, jež v sobě obsahuje informaci o chování této křivky modulo p pro všechna prvočísla p, je integrální transformací Fourierovy řady jisté modulární formy. Taniyamova hypotéza je speciálním případem „Langlandsovy filosofie", řady navzájem propojených hypotéz, zformulovaných R.P. Langlandsem a jeho kolegy.

Zatímco formulace Langlandsových hypotéz vyžaduje značné zázemí z teorie automorfních forem, Taniyamovu hypotézu se podařilo přeformulovat tak, že v ní vystupují pouze holomorfní zobrazení [7]. Uvažujme eliptické křivky nad $\mathbf{Q}$, až na isomorfismus definovaný nad $\overline{\mathbf{Q}}$: jde o ty Riemannovy plochy rodu jedna, které lze definovat polynomiálními rovnicemi s *racionálními* koeficienty. Taniyamova hypotéza tvrdí, že pro každou takovou plochu S existuje podgrupa $\Gamma \subset \mathbf{SL}(2, \mathbf{Z})$ zadaná kongruencemi a nekonstantní holomorfní zobrazení $\Gamma \setminus \mathcal{H} \longrightarrow S$, kde $\mathcal{H}$ je horní polorovina komplexních čísel s kladnou imaginární částí.

Na souvislost mezi Fermatovou větou a Taniyamovou hypotézou upozornil ve své přednášce v Oberwolfachu v roce 1985 G. Frey; netriviálnímu řešení rovnice $a^p + b^p = c^p$ (kde p je liché prvočíslo) lze přiřadit eliptickou křivku, která se zdála být protipříkladem k Taniyamově hypotéze [2, 3]. Freyova eliptická křivka E je dána zdánlivě jednoduchou rovnicí $y^2 = x(x - a^p)(x + b^p)$. (Předtím, než napíšeme rovnici křivky E, musíme v některých případech provést vhodnou permutaci čísel $(\pm a, \pm b, \pm c)$.) V rukopise, který rozdával v Oberwolfachu, Frey naznačil neúplný důkaz toho, že jeho křivka není modulární, tj. že platí implikace „Taniyama $\Longrightarrow$ Fermat". Očekával, že jeho důkaz bude doveden do konce specialisty na teorii modulárních křivek.

Frey si povšiml toho, že pokud je E modulární, platí totéž o grupě $E[p]$ bodů řádu p na E. To znamená, že $E[p]$ lze vložit (jako algebraickou grupu nad $\mathbf{Q}$) do jacobiánu algebraické křivky odpovídající faktoru $\Gamma \setminus \mathcal{H}$. Podle hypotéz, které Serre zformuloval poté, co se dověděl o Freyově konstrukci, by $E[p]$ měla odpovídat specifické podgrupě $\Gamma_0(2) \subset \mathbf{SL}(2, \mathbf{Z})$ (viz [10, 11]). To vede ke sporu, neboť jacobián křivky $\Gamma_0(2) \setminus \mathcal{H}$ je triviální.

V Serreových hypotézách jsem rozpoznal zobecnění problému, který jsem zformuloval při studiu článku B. Mazura [5]. Podařilo se mi je dokázat v červenci 1986, přibližně rok poté, kdy byly vysloveny [8, 9]. Zpráva o tom, že jsem dokázal „Taniyama $\Longrightarrow$ Fermat", přesvědčila matematické společenství o tom, že Fermatova věta musí platit: všichni jsme očekávali, že se Taniyamova hypotéza jednou stane větou. Všeobecně se ale mělo za to, že důkaz Taniyamovy hypotézy není nikterak nablízku.

Wiles nedal na cizí mínění o tom, že je Taniyamova hypotéza mimo náš dosah, a začal na svém důkazu pracovat v okamžiku, kdy se dověděl, že Fermatova věta je důsledkem této hypotézy. Jeho důkaz bude nakonec v sobě zahrnovat výsledky a technické prostředky z Wilesových dřívějších prací (včetně společných článků s J. Coatesem a Mazurem) a z publikací G. Faltingse, R. Greenberga, H. Hidy, V. Kolyvagina,

Mazura, K. Ribeta, K. Rubina, J. Tilouina, abychom se zmínili alespoň o některých. Jednu zvlášť obtížnou překážku Wiles překonal poté, co obdržel preprint M. Flacha (viz [1]).

V následujících odstavcích naznačíme důkaz v hrubých rysech tak, jak jej Wiles načrtl ve svých přednáškách v Cambridgi. Podrobný důkaz je obsahem dvousetstránkového rukopisu, který Wiles hodlá zpřístupnit matematické veřejnosti v nejbližších týdnech.

Aby ukázal, že semistabilní eliptická křivka $E/\mathbf{Q}$ je modulární, Wiles nejprve zvolí liché prvočíslo ℓ, které pak v praxi bude rovno třem či pěti. Uvážíme-li akci Galoisovy grupy $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ na těch torsních bodech křivky E, jejichž řád je mocninou ℓ, dostaneme ℓ-adickou reprezentaci $\varrho_\ell\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, \mathbf{Z}_\ell)$. (Za bližším vysvětlením se čtenář může obrátit na libovolnou z nedávných publikací o eliptických křivkách, jako je např. [12].) Eliptická křivka E vyhovuje Taniyamově hypotéze právě tehdy, je-li ϱ_ℓ „modulární" v tom smyslu, že je obvyklým způsobem přiřazeno parabolické modulární formě váhy dva. Representace ϱ_ℓ „vypadá" jako modulární v tom, že má správný determinant a vyhovuje jistým nutným lokálním podmínkám v ℓ a v ostatních rozvětvených prvočíslech.

Wiles dokazuje, zhruba řečeno, že Galoisova reprezentace jako ϱ_ℓ je modulární, pokud „vypadá" modulárně a její redukce modulo ℓ je reprezentace $\overline{\varrho}_\ell\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, \mathbf{F}_\ell)$, která je (1) surjektivní a (2) modulární. Podmínka (2) znamená, že $\overline{\varrho}_\ell$ je redukcí *nějaké* reprezentace, která je modulární; jinými slovy, chceme aby ϱ_ℓ bylo kongruentní s nějakou modulární reprezentací. (V mnoha případech lze při studiu $\overline{\varrho}_\ell$ v podmínce (1) zaměnit slovo „surjektivní" na „ireducibilní".)

Wilesův argument je podán v jazyce Mazurovy deformační teorie [6]. Wiles uvažuje deformace reprezentace $\overline{\varrho}$ (která vyhovuje podmínkám (1) a (2)), přičemž si všímá pouze těch deformací, které by teoreticky mohly odpovídat parabolickým formám váhy dvě. (Požaduje, aby determinant deformace byl roven cyklotomickému charakteru a zavádí lokální podmínku v prvočísle ℓ. Pro supersingulární $\overline{\varrho}$ kupříkladu vyžaduje, aby lokálně v ℓ deformace pocházela z Barsotti-Tateovy grupy.) Wiles ukazuje, že univerzální deformace těchto vlastností je modulární, čímž dokazuje hypotézu vyslovenou Mazurem. K tomu musí ukázat, že jisté strukturní zobrazení φ mezi dvěma lokálními okruhy, které je a priori surjektivní, je ve skutečnosti isomorfismem.

Zde Wiles využívá idejí Mazura, Hidy, Tilouina, Flacha, Kolyvagina a dalších. Aby dokázal, že φ je injektivní, Wiles studoval analogii klasické Selmerovy grupy pro druhou symetrickou mocninu modulární deformace ϱ reprezentace $\overline{\varrho}$ a nalezl odhad pro její velikost užitím techniky vycházející z prací Kolyvagina a Flacha. (V mnoha případech Wiles přesně spočítá řád této Selmerovy grupy.)

Poté, co dokázal tuto klíčovou větu, Wiles ukáže, že E je modulární. Nejprve zkoumá případ $\ell = 3$. Podle věty J. Tunnella [13], která v sobě zahrnuje výsledky H. Saito-

T. Shintaniho a Langlandse [4], reprezentace $\overline{\varrho}_3$ splňuje (2), pokud splňuje (1). Odtud vyplývá, že E je modulární, pokud je $\overline{\varrho}_3$ surjektivní.

Problém, o kterém se Wiles zmínil na závěr své druhé přednášky, představuje případ, kdy $\overline{\varrho}_3$ *není* surjektivní. Předpokládejme, kupříkladu, že $\overline{\varrho}_3$ je reducibilní: můžeme i v tomto případě vyhrát koncovku? Wiles vysvětlil své ohromující řešení ve třetí přednášce. S použitím Hilbertovy věty o ireducibilitě a Čebotarevovy věty o hustotě zkonstruuje pomocnou semistabilní eliptickou křivku E', jejíž reprezentace mod 3 splňuje (1) a jejíž reprezentace mod 5 je isomorfní s $\overline{\varrho}_5$. Tuto konstrukci lze provést díky tomu, že modulární křivka $X(5)$ je rodu nula. Wiles použije svou klíčovou větu poprvé k tomu, aby ukázal, že E' je modulární. Proto je i $\overline{\varrho}_5$ modulární, neboť pochází z E'. Druhým použitím klíčové věty, tentokrát pro ϱ_5, Wiles odvozuje, že E je modulární!

Wilesův důkaz Taniyamovy hypotézy představuje pro moderní matematiku obrovský mezník. Na jedné straně názorně ilustruje sílu abstraktní „mašinerie", kterou jsme nashromáždili k řešení konkrétních diofantických problémů. Na straně druhé nás přivádí podstatně blíž k tomu, abychom nalezli souvislost mezi automorfními reprezentacemi a algebraickými varietami.

Literatura

[1] *M. Flach*: A finiteness theorem for the symmetric square of an elliptic curve. Invent. Math. *109* (1992), 307–327.

[2] *G. Frey*: Links between stable elliptic curves and certain diophantine equations. Ann. Univ. Sarav. *1* (1986), 1–40.

[3] *G. Frey*: Links between solutions of $A - B = C$ and elliptic curves. Lecture Notes in Math. *1380* (1989), 31–62.

[4] *R.P. Langlands*: Base change for GL(2). Ann. of Math. Stud., vol. 96, Princeton Univ. Press, Princeton, NJ. 1980.

[5] *B. Mazur*: Modular curves and the Eisenstein ideal. Publ. Math. IHES *47* (1977), 33–186.

[6] *B. Mazur*: Deforming Galois representations. Galois Groups over $\mathbf{Q}$. Math. Sci. Res. Inst. Publ., vol. 16, Springer-Verlag Berlin and New York, 1989, 385–437.

[7] *B. Mazur*: Number theory as gadfly. Amer. Math. Monthly *98* (1991), 593–610.

[8] *K.A. Ribet*: On modular representations of $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ arising from modular forms. Invent. Math. *100* (1990), 431–476.

[9] *K.A. Ribet*: From the Taniyama-Shimura Conjecture to Fermat's Last Theorem. Ann. Fac. Sci. Toulouse Math. *11* (1990), 116–139.

[10] *J.-P. Serre*: Lettre à J.-F. Mestre, 13 Août 1985. Contemp. Math. *67* (1987), 263–268.

[11] *J.-P. Serre*: Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Duke Math. J. *54* (1987), 179–230.

[12] *J.H. Silverman*: The arithmetic of elliptic curves. Graduate Texts in Math., vol. 106, Springer, New York (1986).

[13] *J. Tunnell*: Artin's conjecture for representations of octahedral type. Bull. Amer. Math. Soc. (N.S.) *5* (1981), 173–175.

Přeložil Jan Nekovář