Jan Nekovář
Modulární křivky a Fermatova věta

Mathematica Bohemica, Vol. 119 (1994), No. 1, 79–96

Persistent URL: http://dml.cz/dmlcz/126199

119 (1994) MATHEMATICA BOHEMICA No. 1, 79–96

MODULÁRNÍ KŘIVKY A FERMATOVA VĚTA

JAN NEKOVÁŘ, Matematický ústav Karlovy university Praha

Cílem tohoto článku je doplnit zprávu K. Ribeta o Wilesově důkazu Fermatovy věty[1] o trochu podrobnější vysvětlení některých geometrických pojmů a konstrukcí vyskytujících se v důkazu. Protože Wilesův rukopis je stále ještě v recenzním řízení a není přístupný veřejnosti,[2] autor se mohl opírat pouze o převzaté informace; ty čerpal především z přednášek K. Ribeta a K. Rubina v MSRI v Berkeley (červenec 1993) a ze zápisů Wilesových přednášek na konferenci v Cambridgi (červen 1993).

Tento článek vychází z autorovy přednášky pro doktorandy MFF UK v září 1993. Je určen především studentům a profesionálním matematikům a předpokládá u čtenáře či čtenářky jisté základní algebraické vzdělání.

Několik slov o označení: $\mathbf{Z}$ resp. $\mathbf{Q}$ je okruh celých čísel resp. těleso racionálních čísel. Pro prvočíslo ℓ značí $\mathbf{F}_\ell$ konečné těleso s ℓ prvky, $\mathbf{Z}_\ell$ okruh celých ℓ-adických čísel (je definován níže) a $\mathbf{Q}_\ell$ těleso ℓ-adických čísel (podílové těleso okruhu $\mathbf{Z}_\ell$). Symbolem $\overline{k}$ značíme algebraický uzávěr komutativního tělesa k a uvažujeme $\overline{\mathbf{Q}}$ jako podtěleso tělesa komplexních čísel $\mathbf{C}$. Pro libovolný komutativní okruh R označuje $\mathbf{GL}(n, R)$ grupu invertibilních matic řádu n s prvky ležícími v R; $\mathbf{SL}(n, R)$ pak podgrupu matic s determinantem rovným jedné.

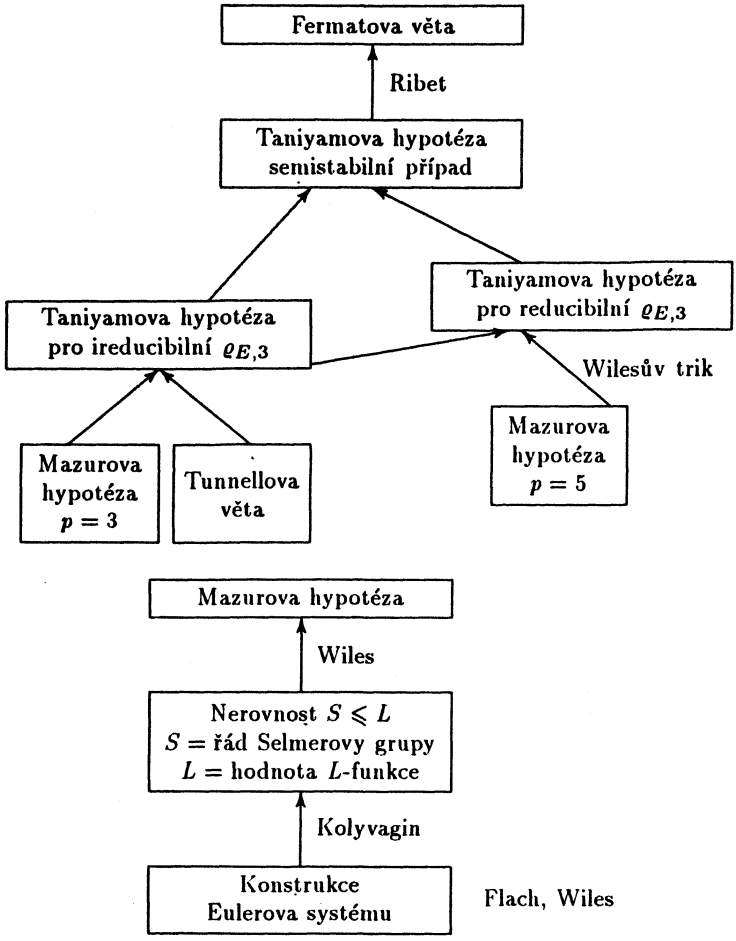
1. STRUKTURA DŮKAZU FERMATOVY VĚTY

Následující vývojový diagram, který shrnuje schéma důkazu, je převzat z přednášky K. Rubina v MSRI.

Několik poznámek k jednotlivým částem diagramu: Wiles dokazuje Taniyamovu hypotézu pro semistabilní eliptické křivky nad $\mathbf{Q}$; Fermatova věta pak odtud vyplývá díky práci Ribeta [26], [27]. Klíčovým krokem je důkaz tzv. Mazurovy hypotézy o deformacích Galoisových reprezentací. Pro její platnost se Wilesovi podařilo nalézt

[1] Viz předchodzí článek

[2] Psáno v listopadu 1993; podle posledních zpráv byl Wilesovi rukopis vrácen, aby v něm opravil několik nepřesností. Bude zajímavé sledovat, zda se mu to podaří.



explicitní numerické kritérium – velikost jistého aritmetického objektu (Selmerovy grupy) nemá být větší než je hodnota odpovídající L-funkce. K tomu použil výsledků a metod řady autorů zabývajících se studiem kongruencí mezi modulárními formami (viz [28]). Nerovnost $S \leqslant L$ pak Wiles dokázal užitím Kolyvaginovy techniky Eulerových systémů ([12], [13], [14]). Nejrozsáhlejší část Wilesova rukopisu je věnována konstrukci příslušného Eulerova systému a vyšetřování jeho vlastností (první krok v tomto směru byl učiněn Flachem [6]).[3]

[3] V prosinci 1933 vydal Wiles prohlášení, podle něhož se mu prý podařilo odstranit všechny mezery, na které ho upozornili recenzenti, kromě jedné, a to v důkazu nerovnosti $S \leqslant L$. Implikace „$S \leqslant L \Rightarrow$ Fermat" je prý v pořádku.

2. Pravidelné mnohoúhelníky

Jádrem Wilesova důkazu je studium Galoisových reprezentací nad $\mathbf{Q}$, tj. reprezentací Galoisovy grupy $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Ty se poprvé objevily (v přestrojení) v pracích Gausse o pravidelných mnohoúhelnících. Gauss přeformuloval problém konstrukce pravidelného n-úhelníku algebraicky a to ho vedlo k vyšetřování rozšíření těles $\mathbf{Q} \subset \mathbf{Q}(\mu_n)$, kde $\mu_n \subset \mathbf{C}$ označuje grupu n-tých odmocnin z jedné. Podařilo se mu vyčíslit Galoisovu grupu $\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$ (grupu automorfismů tělesa $\mathbf{Q}(\mu_n)$ ponechávajících prvky $\mathbf{Q}$ na místě) následujícím způsobem: každý automorfismus $g \in \mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$ zobrazuje μ_n do sebe a zachovává multiplikativní strukturu komutativní grupy μ_n. Odtud dostaneme injektivní homomorfismus

$$\mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q}) \longrightarrow \mathrm{Aut}(\mu_n) \xrightarrow{\sim} (\mathbf{Z}/n\mathbf{Z})^*. \tag{1}$$

Hlavní Gaussův výsledek tvrdí, že zobrazení (1) je isomorfismem. Odtud vyplývá existence surjektivního homomorfismu (jenž vznikne složením (1) a kanonické projekce $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Gal}(\mathbf{Q}(\mu_n)/\mathbf{Q})$)

$$\chi_n : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow (\mathbf{Z}/n\mathbf{Z})^*$$

s jádrem $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\mu_n))$, charakterizovaný vztahem

$$g(\zeta) = \zeta^{\chi_n(g)}, \qquad \forall \zeta \in \mu_n.$$

Obdobně dostaneme (pro každé prvočíslo p) p-adickou reprezentaci

$$\chi_{p^\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Aut}(\mu_{p^\infty}) \xrightarrow{\sim} \mathbf{Z}_p^*$$

s jádrem $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\mu_{p^\infty}))$, kde

$$\mu_{p^\infty} = \bigcup_{n \geqslant 1} \mu_{p^n}$$

a $\mathbf{Z}_p = \mathrm{End}(\mu_{p^\infty})$ je okruh celých p-adických čísel.

Reprezentace χ_n v sobě obsahuje mnoho užitečné informace o aritmetice rozšíření $\mathbf{Q}(\mu_n)/\mathbf{Q}$. Nás bude zvláště zajímat větvení daného rozšíření (přesněji řečeno odpovídajícího rozšíření okruhů celých čísel $\mathbf{Z}[\mu_n]/\mathbf{Z}$). Tento pojem je dobře znám z teorie Riemannových ploch: je-li $P(w, z)$ mnohočlen s komplexními koeficienty, pak projekce množiny komplexních řešení rovnice $P(w, z) = 0$ na rovinu proměnné z je rozvětvena právě v těch $z_0 \in \mathbf{C}$, pro která má $P(w, z_0)$ vícenásobný kořen.

V aritmetické situaci je dán nenulový mnohočlen $P(x)$ s celočíselnými koeficienty, který definuje rozšíření okruhů $\mathbf{Z} \subset R = \mathbf{Z}[x]/(P(x))$. Řekneme, že prvočíslo ℓ je v tomto rozšíření rozvětvené, pokud ℓ dělí diskriminant mnohočlenu $P(x)$, tj. pokud má redukce mnohočlenu $P(x)$ modulo ℓ vícenásobný kořen (v $\overline{\mathbf{F}}_\ell$).

V rozšíření $\mathbf{Z}[\mu_n]/\mathbf{Z}$ jsou rozvětvena právě prvočísla dělící n. To lze zjistit z reprezentace χ_n takto: pro dané ℓ existuje vložení Galoisových grup (určené jednoznačně až na konjugaci)

$$D_\ell = \mathrm{Gal}(\overline{\mathbf{Q}}_\ell/\mathbf{Q}_\ell) \hookrightarrow \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$$

a kanonický epimorfismus $D_\ell \longrightarrow \mathrm{Gal}(\overline{\mathbf{F}}_\ell/\mathbf{F}_\ell)$ s jádrem I_ℓ. Prvočíslo ℓ je pak nerozvětvené v $\mathbf{Z}[\mu_n]/\mathbf{Z}$ právě tehdy, když $\chi_n(I_\ell) = \{1\}$.

V obecném případě řekneme, že reprezentace $\varrho\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow G$ je nerozvětvená v ℓ, pokud $\varrho(I_\ell) = \{1\}$. To nastane právě tehdy, je-li ℓ nerozvětvené v $R/\mathbf{Z}$, kde R je okruh celých čísel v tělese K, které odpovídá podgrupě $\mathrm{Ker}(\varrho)$.

Připomeňme, že podle Kroneckerovy-Weberovy věty je každé konečné Galoisovo rozšíření $K/\mathbf{Q}$ s komutativní Galoisovou grupou podtělesem $\mathbf{Q}(\mu_n)$ pro nějaké n. Minimální n této vlastnosti lze určit právě pomocí větvení. Jak uvidíme v odstavci 5, Taniyamova hypotéza je jistou nekomutativní verzí Kroneckerovy-Weberovy věty.

3. Eliptické funkce a křivky

Odmocniny z jedné si obvykle představujeme jako body na kružnici $K\colon x^2+y^2 = 1$. Dvojice funkcí (cos, sin) zadává parametrizaci reálných i komplexních bodů kružnice K:

$$\begin{aligned} \mathbf{R}/2\pi\mathbf{Z} &\xrightarrow{\sim} K(\mathbf{R}), \\ \mathbf{C}/2\pi\mathbf{Z} &\xrightarrow{\sim} K(\mathbf{C}). \end{aligned} \tag{2}$$

Křivka K má strukturu komutativní algebraické grupy s operací

$$[x_1, y_1] + [x_2, y_2] = [x_1x_2 - y_1y_2, x_1y_2 + y_1x_2].$$

Parametrizace (2) je isomorfismem grup (vzpomeňme si na součtové vzorce pro trigonometrické funkce!) a grupa n-tých odmocnin z jedné $\mu_n = K(\mathbf{R})_n = K(\mathbf{C})_n$ je grupou bodů řádu n na křivce K.

Obdobná situace nastává v teorii eliptických funkcí: jsou-li ω_1, ω_2 komplexní čísla lineárně nezávislá nad $\mathbf{R}$, pak je Weierstrassova $\wp$-funkce

$$\wp(z) = \frac{1}{z^2} + \sum_{u \in L - \{0\}} \left(\frac{1}{(z-u)^2} - \frac{1}{u^2} \right)$$

dvouperiodickou meromorfní funkcí s mřížkou period $L = \mathbf{Z}\omega_1 + \mathbf{Z}\omega_2$. Dvojice funkcí $(\wp, \wp'/2)$ pak zadává parametrizaci

$$\mathbf{C}/L \xrightarrow{\sim} E(\mathbf{C}) \tag{3}$$

komplexních bodů kubické křivky

$$E\colon y^2 = x^3 + Ax + B \tag{4}$$

pro určitá $A, B \in \mathbf{C}$ (ke křivce E patří bod v nekonečnu $O = [0 : 1 : 0]$, který odpovídá hodnotě $z = 0$, kde má funkce $\wp$ pól). Naopak pro každou dvojici komplexních čísel A, B takovou, že mnohočlen $x^3 + Ax + B$ má tři různé kořeny, existuje jednoznačně určená mřížka $L \subset \mathbf{C}$, pro kterou příslušná Weierstrassova funkce splňuje (4).

Podle klasické terminologie je E *eliptická křivka*, neboť je parametrizována eliptickými (tj. dvouperiodickými) funkcemi. Křivka E má rovněž strukturu komutativní algebraické grupy, pro kterou je (3) isomorfismem grup. Geometricky lze grupovou operaci popsat takto: O je neutrální prvek a pro tři body P, Q, R na křivce E platí $P + Q + R = O$ právě tehdy, jsou-li P, Q, R průsečíky E s nějakou přímkou.

Pokud $A, B \in \mathbf{Q}$, je grupová operace na E zadána (v homogenních souřadnicích) mnohočleny s racionálními koeficienty. Z toho plyne, že rozšíření $\mathbf{Q}(E_n)/\mathbf{Q}$ (kde E_n označuje grupu bodů řádu n na E) je Galoisovo a jeho automorfismy komutují s grupovou operací na E_n. Protože $E_n = E(\mathbf{C})_n = E(\overline{\mathbf{Q}})_n$ je podle (3) isomorfní s $(\mathbf{Z}/n\mathbf{Z})^2$, dostaneme – podobně jako v minulém odstavci – homomorfismy

$$\varrho_{E,n}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Gal}(\mathbf{Q}(E_n)/\mathbf{Q}) \longrightarrow \mathrm{Aut}(E_n) \xrightarrow{\sim} \mathbf{GL}(2, \mathbf{Z}/n\mathbf{Z}),$$
$$\varrho_{E,p^\infty}\colon \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, \mathbf{Z}_p).$$

Mnohočlen $x^3 + Ax + B$ má nenulový diskriminant $\Delta = -4A^3 - 27B^2$ a reprezentace $\varrho_{E,n}$ (resp. ϱ_{E,p^∞}) je nerozvětvená v prvočíslech ℓ nesoudělných s $n\Delta$ (resp. s $p\Delta$).

4. Modulární křivky

Eliptická křivka nad $\mathbf{C}$ je zadána svou mřížkou period L. Dvě křivky jsou isomorfní (tj. lze je na sebe převést vzájemně jednoznačnou záměnou souřadnic) právě tehdy, jsou-li příslušné mřížky podobné, tj. liší-li se vynásobením na skalár $\lambda \in \mathbf{C}^*$. Pro každou mřížku existuje mřížka jí podobná s bází $1, z$, kde z leží v horní polorovině

$$\mathcal{H} = \{z = x + \mathrm{i}y \mid y > 0\}.$$

Jiná volba báze vede k podobné mřížce s bází $1, (az+b)(cz+d)^{-1}$, kde

$$\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL(2,\mathbf{Z}), \quad \text{tj. } a,b,c,d \in \mathbf{Z}, \quad ad-bc=1.$$

Odtud dostáváme bijekce mezi množinami

$$\begin{array}{c} \{\text{eliptické křivky nad } \mathbf{C}\}/\text{isomorfismus} \\ \downarrow \\ \{\text{mřížky } L \subset \mathbf{C}\}/\mathbf{C}^* \\ \downarrow \\ \mathbf{SL}(2,\mathbf{Z}) \setminus \mathcal{H} \end{array} \tag{5}$$

Všechny tři lze ztotožnit s množinou všech komplexních čísel pomocí modulárního invariantu

$$j(E) = -2^8 \cdot 3^3 \frac{A^3}{\Delta} \in \mathbf{C}.$$

Užijeme-li souřadnice $z \in \mathcal{H}$, pak je

$$j(z) = q^{-1} + 744 + 196\,884q + \ldots, \qquad q = e^{2\pi i z}.$$

Často je užitečné uvažovat eliptické křivky s nějakou další strukturou. Nás bude zajímat následující zobecnění (5):

$$\left\{ \begin{array}{c} \text{eliptická křivka E nad } \mathbf{C} \\ \text{podgrupa } C \subset E, C \simeq \mathbf{Z}/N\mathbf{Z} \end{array} \right\} \Big/ \text{isomorfismus}$$

$$\downarrow$$

$$\{ \text{mřížky } L' \subset L \subset \mathbf{C}, L/L' \simeq \mathbf{Z}/N\mathbf{Z}\}/\mathbf{C}^* \qquad \longleftrightarrow \qquad \Gamma_0(N) \setminus \mathcal{H}$$

Zde $\Gamma_0(N)$ označuje grupu matic

$$\Gamma_0(N) = \left\{ \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathbf{SL}(2,\mathbf{Z}) \mid c \equiv 0 \pmod{N} \right\}.$$

Všechny tři množiny pak lze ztotožnit s komplexními body jisté nesingulární afinní křivky $Y_0(N)$ (pro $N=1$ je $Y_0(1)$ afinní přímkou se souřadnicí j). Křivka $Y_0(N)$ je ve skutečnosti definována nad $\mathbf{Q}$ a její těleso funkcí je isomorfní s $\mathbf{Q}(j(z), j(Nz))$.

Křivka $Y_0(N)$ má kanonickou nesingulární kompaktifikaci $X_0(N)$, která je rovněž definována nad $\mathbf{Q}$. Každé takové křivce je přiřazena její *Jacobiho varieta* $J_0(N)$. Konstrukce této variety nad $\mathbf{C}$ pomocí komplexně analytických metod je obsahem klasické teorie Abelových integrálů ([9], kap. 2). Připomeňme jen, že $J_0(N)$ je projektivní varietou dimenze g, kde g je rod křivky $X_0(N)$, a má strukturu komutativní

algebraické grupy. Intuitivně si ji můžeme představovat jako součin g eliptických křivek (eliptická křivka je svou vlastní Jacobiho varietou). Abelova-Jacobiho věta ztotožňuje komplexní body $J_0(N)$ s komplexním torem dimenze g:

$$J_0(N)(\mathbf{C}) \xrightarrow{\sim} \mathbf{C}^g \Big/ \bigoplus_1^{2g} \mathbf{Z}\omega_i.$$

Body řádu n na $J_0(N)$ proto tvoří grupu isomorfní s $(\mathbf{Z}/n\mathbf{Z})^{2g}$; tak jako předtím máme Galoisovy representace

$$\varrho_{J_0(N),n} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2g, \mathbf{Z}/n\mathbf{Z})$$
$$\varrho_{J_0(N),p^\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2g, \mathbf{Z}_p),$$

které jsou nerozvětvené v prvočíslech ℓ nesoudělných s nN (resp. s pN).

5. Taniyamova hypotéza

Abychom mohli zformulovat Taniyamovu hypotézu (v několika verzích), potřebujeme k tomu pojem modulární Galoisovy reprezentace, který není totožný s tím, co obvykle nazýváme modulární reprezentací v teorii grup.

Galoisova reprezentace $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(n, R)$ (kde R je libovolná $\mathbf{Z}_p$-algebra) se nazývá *modulární* (úrovně N), pokud se vyskytuje v $\varrho_{J_0(N),p^\infty}$, tj. pokud ji lze rozložit jako

$$\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathrm{Im}(\varrho_{J_0(N),p^\infty}) \longrightarrow \mathbf{GL}(n, R).$$

Taniyamova hypotéza (I). *Pro každou eliptickou křivku E nad $\mathbf{Q}$ existuje pro určité N nekonstantní zobrazení*[4] $Y_0(N) \longrightarrow E$.

Taniyamova hypotéza (II). *Pro každou eliptickou křivku E nad $\mathbf{Q}$ existuje prvočíslo p, pro něž je Galoisova reprezentace ϱ_{E,p^∞} modulární (pak jsou reprezentace ϱ_{E,p^∞} modulární pro všechna p).*

Obě tyto formulace jsou ekvivalentní, dokonce se stejným N. Implikace (I) $\Longrightarrow$ (II) je elementární, kdežto (II) $\Longrightarrow$ (I) je důsledkem Tateovy hypotézy, dokázané Faltingsem [5].

Všimněme si, že existuje kanonické zobrazení $X_0(N) \longrightarrow X_0(M)$ kdykoliv M dělí N. Z toho plyne, že eliptická křivka E je modulární úrovně N (tj. splňuje závěr

[4] Máme na mysli zobrazení definované nad $\mathbf{Q}$; podle [20] však stačí, aby bylo definováno nad $\mathbf{C}$

(I) nebo (II)), pokud je modulární úrovně M. V následujícím odstavci definujeme přirozené číslo N_E, o němž lze dokázat následující tvrzení: je-li E modulární nějaké úrovně, pak je modulární úrovně N právě tehdy, pokud N_E dělí N. Proto lze ve všech verzích Taniyamovy hypotézy zformulovaných v tomto článku nahradit výraz „existuje N" slovy „pro $N = N_E$".

Buď E eliptická křivka nad $\mathbf{Q}$ definovaná rovnicí (4) s $A, B \in \mathbf{Q}$. Modelem křivky E nad $\mathbf{Z}$ rozumíme libovolnou křivku

$$\mathcal{E}: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6 \tag{6}$$

s koeficienty $a_i \in \mathbf{Z}$, která je nad $\mathbf{Q}$ isomorfní s E, tj. kterou lze převést na E lineární záměnou souřadnic. Existuje celočíselná verze diskriminantu Δ pro křivku $\mathcal{E}$. Jeho hodnotu $\Delta(\mathcal{E}) \in \mathbf{Z} - \{0\}$ získáme dosazením koeficientů $a_1, \ldots, a_6$ do jistého mnohočlenu $\Delta \in \mathbf{Z}[b_1, b_2, b_3, b_4, b_6]$. Pro $a_1 = a_2 = a_3 = 0$ je $\Delta(\mathcal{E}) = -4a_4^3 - 27a_6^2$.

Pro nás je podstatné, že pro dané E existuje *minimální model* $\mathcal{E}$ nad $\mathbf{Z}$ (určený jednoznačně až na isomorfismus nad $\mathbf{Z}$), pro který je hodnota $|\Delta(\mathcal{E})|$ minimální. Zvolme prvočíslo ℓ a uvažujme redukci $\mathcal{E}_{/\mathbf{F}_\ell}$ křivky modulo ℓ, tj. křivku danou rovnicí (6) nad tělesem $\mathbf{F}_\ell$. Z geometrického hlediska křivka $\mathcal{E}_{/\mathbf{F}_\ell}$ patří k jednomu ze tří typů:

(a) nesingulární křivka ($\Longleftrightarrow \ell \nmid \Delta(\mathcal{E})$)
(b) křivka s dvojnásobným bodem, ve kterém má dvě různé tečny
(c) křivka s dvojnásobným bodem, ve kterém má dvojnásobnou tečnu

Podle toho, který případ nastane, řekneme, že E má v ℓ: (a) dobrou redukci; (b) semistabilní redukci; (c) nestabilní redukci. Všimněme si, že pokud $A, B \in \mathbf{Z}$, pak má E dobrou redukci ve všech ℓ nesoudělných s 6Δ. Typy redukce lze rozlišit pomocí Galoisových reprezentací (Néron, Ogg, Šafarevič, Grothendieck, Serre, Tate): zvolme prvočíslo $p \neq \ell$ a označme $I := \varrho_{E,p^\infty}(I_\ell) \subseteq \mathbf{GL}(2, \mathbf{Z}_p)$. Pak platí

$$\begin{aligned} E \text{ má dobrou redukci v } \ell &\Longleftrightarrow I = \{1\}, \\ E \text{ má semistabilní redukci v } \ell &\Longleftrightarrow |I| = \infty, \\ E \text{ má nestabilní redukci v } \ell &\Longleftrightarrow 1 < |I| < \infty. \end{aligned}$$

Existuje numerický invariant („konduktor křivky E"), který měří redukci E:

$$N_E = \prod_{\ell} \ell^{n(\ell)} = \prod_{\ell \mid \Delta(\mathcal{E})} \ell^{n(\ell)},$$

kde

$$n(\ell) = \begin{cases} 0 & \text{dobrá redukce v } \ell, \\ 1 & \text{semistabilní redukce v } \ell, \\ 2\ (\geqslant 2) & \text{nestabilní redukce v } \ell > 3\ (\text{v } \ell = 2, 3). \end{cases}$$

Křivka E se nazývá *semistabilní*, má-li v každém prvočísle dobrou nebo semistabilní redukci ($\Longleftrightarrow N_E$ je bezkvadrátové číslo).

Očekává se, že veškerá aritmetická informace o křivce E je obsažena v jeho L-funkci, která je definována jako formální Dirichletova řada vztahem

$$L(E,s) = \prod_{\ell}[(1-\alpha_\ell \ell^{-s})(1-\beta_\ell \ell^{-s})]^{-1} = \sum_{n=1}^{\infty} a_n(E) n^{-s},$$

kde pro každé prvočíslo ℓ je dvojice komplexních čísel α_ℓ, β_ℓ určena vztahy

$$\alpha_\ell + \beta_\ell = \ell + 1 - |\mathcal{E}(\mathbf{F}_\ell)|,$$
$$\alpha_\ell \beta_\ell = \begin{cases} \ell & \ell \nmid N_E, \\ 0 & \ell \mid N_E. \end{cases}$$

Hasse [10] dokázal hypotézu E. Artina, podle níž pro $\ell \nmid N_E$ platí $|\alpha_\ell| = |\beta_\ell| = \ell^{1/2}$. Z ní vyplývá, že $L(E,s)$ je absolutně konvergentní pro $\mathrm{Re}(s) > \frac{3}{2}$.

6. Modulární formy

Podívejme se na křivku $X_0(N)$ nad $\mathbf{C}$ z analytického hlediska, tj. jako na kompaktní Riemannovu plochu. Zvláště nás budou zajímat holomorfní diferenciály na této křivce. Každý takový diferenciál lze zapsat pomocí souřadnice $z \in \mathcal{H}$ ve tvaru

$$\omega = f(z)\,\mathrm{d}z = \left(\sum_{n=1}^{\infty} a_n(f) \mathrm{e}^{2\pi \mathrm{i} n z}\right) \mathrm{d}z,$$

kde f je (a) holomorfní v $\mathcal{H}$; (b) splňuje jisté podmínky regularity pro $z \longrightarrow r \in \mathbf{Q}$. Invarianci diferenciálu ω vůči $\Gamma_0(N)$ lze přepsat jako

$$\text{(c)} \qquad f\left(\tfrac{az+b}{cz+d}\right) = (cz+d)^2 f(z) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Funkce f splňující (a)–(c) se nazývají *parabolické modulární formy* typu $(N,2,1)$ a tvoří konečněrozměrný prostor nad $\mathbf{C}$, isomorfní s prostorem holomorfních diferenciálů na $X_0(N)$.

Obecněji, pro celá čísla $k, N \geqslant 1$ a Dirichletův charakter $\chi\colon (\mathbf{Z}/N\mathbf{Z})^* \longrightarrow \mathbf{C}^*$ definujeme parabolickou modulární formu typu (N,k,χ) podmínkami (a),(b) a

$$\text{(c')} \qquad f\left(\tfrac{az+b}{cz+d}\right) = \chi(d)(cz+d)^k f(z) \qquad \forall \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \Gamma_0(N).$$

Každou parabolickou formu lze zapsat ve tvaru Fourierovy řady

$$f(z) = \sum_{n=1}^{\infty} a_n(f) e^{2\pi i n z}.$$

Její L-funkci definujeme jako

$$L(f, s) = \sum_{n=1}^{\infty} a_n(f) n^{-s}.$$

Taniyamova hypotéza (III). *Pro každou eliptickou křivku E nad $\mathbb{Q}$ existuje pro nějaké N parabolická modulární forma f typu $(N, 2, 1)$, pro kterou platí*

$$L(E, s) = L(f, s).$$

Poněkud oslabenou implikaci (I) $\Longrightarrow$ (III) dokázali Eichler [4] a Shimura [33], (III) $\Longrightarrow$ (II) pak Shimura [34].

7. Taniyamova hypotéza a Fermatova věta

Na tuto souvislost poprvé upozornil v roce 1985 Gerhard Frey. Předpokládejme, že pro prvočíslo $p > 3$ existuje celočíselné řešení rovnice

$$a^p + b^p = c^p$$

s $abc \neq 0$. Bez újmy na obecnosti můžeme předpokládat, že $a \equiv -1 \pmod 4$, $b \equiv 0 \pmod 2$. Uvažujme eliptickou křivku

$$E\colon y^2 = x(x - a^p)(x + b^p).$$

Tato křivka má diskriminant $\Delta = (abc)^{2p}$ a transformací souřadnic $x = 4X$, $y = 8Y + 4X$ dostaneme její minimální model

$$\mathcal{E}\colon Y^2 + XY = X^3 + \frac{b^p - a^p - 1}{4} X^2 - \frac{a^p b^p}{16} X$$

s diskriminantem $\Delta(\mathcal{E}) = 2^{-8}(abc)^{2p}$. Křivka E je semistabilní a má konduktor

$$N_E = \prod_{\ell \mid abc} \ell.$$

Frey [7], [8] zformuloval následující tvrzení, které posléze dokázal Ribet [26], [27]:

Věta. *Reprezentace* $\varrho_{E,p^\infty} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, \mathbf{Z}_p)$ *není modulární. Pro křivku* E *tedy neplatí Taniyamova hypotéza.*

Důkaz. Předpokládejme, že ϱ_{E,p^∞} je modulární. Potom je modulární úrovně N_E, a totéž tedy platí i o $\varrho_{E,p}$. Víme, že ϱ_{E,p^∞} je nerozvětvené v prvočíslech ℓ nesoudělných s pN_E. Protože E je semistabilní a $\Delta(\mathcal{E})$ je p-tou mocninou (až na mocninu dvou), reprezentace $\varrho_{E,p}$ se chová mnohem lépe: $\varrho_{E,p}$ je nerozvětvená ve všech $\ell \neq 2, p$ a v určitém smyslu je „hezká" v $\ell = p$.

Podobně se chovají modulární Galoisovy reprezentace úrovně 2. V obecné situaci Serre [31], [32] zformuloval následující hypotézu:

Serreova hypotéza. *Je-li reprezentace* ϱ: $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow GL(2, \mathbf{Z}/p\mathbf{Z})$ *modulární úrovně* N *a* ℓ *prvočíslo dělící* N *v první mocnině takové, že* ϱ *je nerozvětvené (resp. „hezké") v* ℓ *pokud* $\ell \neq p$ *(resp. pokud* $\ell = p$*), pak je* ϱ *modulární úrovně* N/ℓ.

Tuto hypotézu dokázal Mazur [19] pro $\ell \not\equiv 1 \pmod{p}$ a Ribet [26] v plné obecnosti. Použijeme-li tento výsledek pro $\varrho = \varrho_{E,p}$, zjistíme, že ϱ je modulární úrovně 2. To ale není možné, neboť křivka $X_0(2)$ má rod nula a její Jacobiho varieta $J_0(2)$ je triviální. Proto ϱ_{E,p^∞} nemůže být modulární. □

Důsledek. *Platí-li Taniyamova hypotéza pro semistabilní eliptické křivky nad* $\mathbf{Q}$, *platí i Fermatova věta.*

8. Deformace Galoisových reprezentací

Nyní již můžeme popsat Wilesovu strategii, jak dokázat Taniyamovu hypotézu pro semistabilní eliptické křivky, a tím i Fermatovu větu.

Buď E eliptická křivka nad $\mathbf{Q}$ a $p > 2$ prvočíslo. Budeme uvažovat Galoisovu reprezentaci

$$\varrho_{E,p} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, \mathbf{Z}/p\mathbf{Z})$$

a její deformace (viz [18]), tj. spojité reprezentace

$$\varrho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, R),$$

kde R je dostatečně rozumný lokální okruh[5] s tělesem zbytků $R/m = \mathbf{Z}/p\mathbf{Z}$ a kompozice ϱ s kanonickou projekcí $\mathbf{GL}(2, R) \longrightarrow \mathbf{GL}(2, R/m) = \mathbf{GL}(2, \mathbf{Z}/p\mathbf{Z})$ je rovna

[5] R je úplná lokální noetherovská $\mathbf{Z}_p$-algebra

$\varrho_{E,p}$. Jednou takovou deformací je ϱ_{E,p^∞} (pro $R = \mathbf{Z}_p$). Wilesovým cílem je ukázat, že pokud je $\varrho_{E,p}$ modulární (a splňuje některé další podmínky), pak jsou modulární i všechny jeho deformace určitého typu (mezi něž patří i ϱ_{E,p^∞}).

Přesněji řečeno, je třeba uvažovat pouze deformace daného typu $\mathcal{D}$, který v sobě zahrnuje:

(i) Konečnou množinu prvočísel S obsahující p takovou, že ϱ je nerozvětvené ve všech $\ell \notin S$.

(ii) Podmínky na $\varrho|D_p$

(iii) Podmínky na $\varrho|D_\ell$ pro všechna ℓ z jisté podmnožiny $T \subseteq S - \{p\}$.

(iv) Volba determinantu $\det(\varrho)$.

Lze ukázat, že pokud je $\varrho_{E,p}$ ireducibilní, jsou deformace typu $\mathcal{D}$ reprezentovatelné jistým lokálním okruhem $R_\mathcal{D}$ (viz [18] pro podmínku (i)). Znamená to, že existuje univerzální deformace

$$\varrho_\mathcal{D} : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, R_\mathcal{D})$$

taková, že pro každou deformaci ϱ typu $\mathcal{D}$ existuje jednoznačně určený homomorfismus $\mathbf{Z}_p$-algeber $f : R_\mathcal{D} \longrightarrow R$ takový, že $f \circ \varrho_\mathcal{D} = \varrho$.

Předpokládejme navíc, že $\varrho_{E,p}$ je modulární typu $\mathcal{D}$, tj. že má deformaci typu $\mathcal{D}$ $\varrho : \mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}) \longrightarrow \mathbf{GL}(2, \mathcal{O})$ ($\mathcal{O}$ je okruh celých čísel v konečném rozšíření K tělesa $\mathbf{Q}_p$), které je modulární. Pro zjednodušení budeme v dalším uvažovat pouze případ $\mathcal{O} = \mathbf{Z}_p$. Existuje maximální faktoralgebra

$$R_\mathcal{D} \longrightarrow \mathbf{T}_\mathcal{D},$$

která reprezentuje modulární deformace typu $\mathcal{D}$. Algebru $\mathbf{T}_\mathcal{D}$ lze explicitně popsat pomocí tzv. Heckeho operátorů působících v prostoru parabolických modulárních forem. Odtud vyplývá, mimo jiné, že $\mathbf{T}_\mathcal{D}$ je volný modul konečného typu nad $\mathbf{Z}_p$.

Mazurova hypotéza. *Kanonický surjektivní homomorfismus $R_\mathcal{D} \longrightarrow \mathbf{T}_\mathcal{D}$ je isomorfismem. Jinak řečeno, pokud má $\varrho_{E,p}$ modulární deformaci typu $\mathcal{D}$, jsou všechny jeho deformace typu $\mathcal{D}$ modulární.*

Z Mazurovy hypotézy vyplývá, že okruh $R_\mathcal{D}$ by měl být konečný nad $\mathbf{Z}_p$. Uvažujeme-li deformace splňující pouze podmínku (i), je univerzální deformační okruh obvykle isomorfní s $\mathbf{Z}_p[X, Y, Z]$ ([18]); podmínka (iv) pak ubere jednu proměnnou. Znamená to, že o zbylé dvě proměnné se tedy musí postarat podmínka (ii), neboť (iii) nemění dimenzi okruhu $R_\mathcal{D}$.

Klíčem k důkazu Taniyamovy hypotézy je následující

Hlavní věta (Wiles). *Buď E semistabilní eliptická křivka nad $\mathbf{Q}$, $p > 2$ prvočíslo, pro které je $\varrho_{E,p}$ ireducibilní a modulární (a splňuje ještě několik dalších technických podmínek). Pak Mazurova hypotéza platí pro každé $\mathcal{D}$, pro něž je $\varrho_{E,p}$ typu $\mathcal{D}$.*

9. Důkaz Taniyamovy hypotézy v semistabilním případě

Věta (Wiles). *Každá semistabilní eliptická křivka nad* $\mathbf{Q}$ *je modulární.*

Důkaz. Rozlišme několik případů:

(I) $\varrho_{E,3}$ je ireducibilní.

Ze semistability vyplývá, že v tomto případě je $\mathrm{Im}(\varrho_{E,3}) = \mathbf{GL}(2, \mathbf{Z}/3\mathbf{Z})$ a podle Tunnellovy věty [36] je $\varrho_{E,3}$ modulární (podle [36] odpovídá $\varrho_{E,3}$ modulární formě typu $(N, 1, \chi)$, lze však ukázat, že $\varrho_{E,3}$ je pak modulární i v našem smyslu). Podle Hlavní věty (pro $p = 3$) pak je $\varrho_{E,3^\infty}$ rovněž modulární.

(II) $\varrho_{E,3}$ je reducibilní.

V tomto případě existuje podgrupa $C \subset E$, $C \xrightarrow{\sim} \mathbf{Z}/3\mathbf{Z}$, racionální nad $\mathbf{Q}$. Opět rozlišme dva případy:

(IIa) $\varrho_{E,5}$ je reducibilní, tj. existuje podgrupa $C' \subset E$, $C' \xrightarrow{\sim} \mathbf{Z}/5\mathbf{Z}$, definovaná nad $\mathbf{Q}$. Pak $(E, C \oplus C')$ odpovídá racionálnímu bodu křivky $Y_0(15)$. Tato křivka však má pouze čtyři racionální body, a všechny čtyři příslušné eliptické křivky jsou modulární.

(IIb) $\varrho_{E,5}$ je ireducibilní. Uvažujme modulární křivku X parametrizující dvojice (E', λ) (až na isomorfismus), kde E' je eliptická křivka a λ je isomorfismus $\lambda\colon E_5 \xrightarrow{\sim} E'_5$. Tato křivka je rodu nula a obsahuje racionální bod (E, id). Proto je na ní nekonečně racionálních bodů. Pomocí jistého triku Wiles ukazuje, že na X existuje racionální bod, který odpovídá semistabilní eliptické křivce E', pro kterou je $\varrho_{E',3}$ ireducibilní. Díky (I) je E' modulární, a tudíž je i $\varrho_{E',5} = \varrho_{E,5}$ modulární. Podle Hlavní věty (pro $p = 5$) je pak $\varrho_{E,5^\infty}$ modulární. □

Stojí za povšimnutí, že tento důkaz stojí a padá s tím, že 3 a 5 mají mezi všemi prvočísly velmi výsadní postavení:

Tunnellova věta je založena na tom, že $\mathbf{PGL}(2, \mathbf{Z}/3\mathbf{Z}) \xrightarrow{\sim} S_4$ je řešitelná grupa, což neplatí, pokud trojku nahradíme libovolným větším prvočíslem.

Stejně tak má křivka parametrizující dvojice (E', λ), $\lambda\colon E_p \xrightarrow{\sim} E'_p$, pro $p > 5$ rod větší než jedna.

Nedávno se objevil preprint Elkiese, ve kterém je ukázáno, že pro Freyovu křivku E z odstavce 7 (anebo pro nějakou příbuznou křivku) musí být $\varrho_{E,3}$ ireducibilní. To znamená, že pokud nás zajímá pouze Fermatova věta a nikoliv Taniyamova hypotéza, můžeme se obejít bez Wilesova triku pro $p = 5$.

10. Důkaz Mazurovy hypotézy

Na Mazurovu hypotézu lze pohlížet jako na problém z komutativní algebry: jsou dány lokální $\mathbf{Z}_p$-algebry $R_{\mathcal{D}}, \mathbf{T}_{\mathcal{D}}$ a surjektivní homomorfismy

$$R_{\mathcal{D}} \xrightarrow{\alpha} \mathbf{T}_{\mathcal{D}} \xrightarrow{\beta} \mathbf{Z}_p,$$

kde β pochází z modulární deformace ϱ (jejíž existenci předpokládáme). Je třeba ukázat, že α je isomorfismem. Přitom je známo, že $\mathbf{T}_{\mathcal{D}}$ je volný modul konečného typu nad $\mathbf{Z}_p$ a navíc je *Gorensteinovým okruhem* (za tento netriviální výsledek vděčíme především Mazurovi [17], [22]). To znamená, že existuje isomorfismus $\mathbf{T}_{\mathcal{D}}$-modulů

$$\mathbf{T}_{\mathcal{D}} \xrightarrow{\sim} \mathrm{Hom}_{\mathbf{Z}_p}(\mathbf{T}_{\mathcal{D}}, \mathbf{Z}_p). \tag{7}$$

Homomorfismus β v této dualitě odpovídá prvku $\widehat{\beta} \in \mathbf{T}_{\mathcal{D}}$; položíme-li $\eta := \beta(\widehat{\beta}) \in \mathbf{Z}_p$, pak je ideál $\eta\mathbf{Z}_p$ dobře definován (nezávisí na výběru isomorfismu (7)).

Wiles nalezl numerické kritérium pro platnost Mazurovy hypotézy:

Hlavní lemma (Wiles). *Pokud ideál* $\wp_R := \mathrm{Ker}(\beta\alpha)$ *splňuje*

$$\#(\wp_R/\wp_R^2) \leqslant \#(\mathbf{Z}_p/\eta\mathbf{Z}_p), \tag{8}$$

pak je α *isomorfismem a ve skutečnosti nastává rovnost*

$$\#(\wp_R/\wp_R^2) = \#(\mathbf{Z}_p/\eta\mathbf{Z}_p). \tag{9}$$

Obě strany nerovnosti (8) mají aritmetický význam. Levá strana je rovna řádu Selmerovy grupy $S_{\mathcal{D}}$ pro adjungovanou reprezentaci $\mathrm{Ad}(\varrho)$. Přesněji řečeno, $S_{\mathcal{D}}$ je podgrupou grupy Galoisových kohomologií

$$S_{\mathcal{D}} \subset H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), M_2^0(\mathbf{Z}_p) \otimes \mathbf{Q}_p/\mathbf{Z}_p)$$

charakterizovanou lokálními podmínkami typu $\mathcal{D}$. Zde $M_2^0(\mathbf{Z}_p)$ označuje grupu matic řádu 2×2 nad $\mathbf{Z}_p$ s nulovou stopou, na které Galoisova grupa $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ působí adjungovanou reprezentací $g(M) = \varrho(g)M\varrho(g)^{-1}$. Klasické Selmerovy grupy (a s nimi úzce spřízněné Tate-Šafarevičovy grupy) se vyskytují při studiu aritmetiky eliptických křivek. Jejich obecné kohomologické verze definovali Bloch a Kato [1]. Rovnost (9) se zdá být speciálním případem hypotéz Blocha a Kato o hodnotách L-funkcí.

Pravou stranu nerovnosti (8) lze rovněž popsat explicitně. V případě, kdy je modulární samo $\varrho_{E,p^\infty} = \varrho$, je $\eta = \deg(\varphi)$ rovno minimálnímu stupni modulární parametrizace $\varphi\colon X_0(N) \longrightarrow E$. Lze ji rovněž interpretovat jako racionální faktor hodnoty jisté L-funkce (odtud souvislost s hypotézou Blocha-Kato).

Wiles dokazuje nerovnost (8) Kolyvaginovou metodou Eulerových systémů (viz souborné články [21], [24]). Touto metodou Kolyvagin dokázal nerovnosti typu

$$\#S \mid \text{apriorní konstanta}$$

pro klasické Selmerovy a Tate-Šafarevičovy grupy [12], [13], [14].

Ve Wilesově situaci je Eulerův systém tvořen prvky grupy kohomologií

$$c(n) \in H^1(\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}), \mathrm{Sym}^2(\varrho^*))$$

s koeficienty v symetrickém čtverci reprezentace duální k ϱ. První úroveň tohoto Eulerova systému sestrojil Flach [6], který s její pomocí dokázal, že za jistých příznivých okolností

$$\#(\mathbf{Z}_p/\eta\mathbf{Z}_p) \cdot \quad \text{anuluje grupu} \quad S_{\mathcal{D}}.$$

Konstrukci vyšších úrovní Eulerova systému a vyšetřování jejich vlastností prý zabírá největší část Wilesova doposud nezveřejněného rukopisu. Použití Kolyvaginovy metody k důkazu nerovnosti (8) je potom čistě formální.

Kromě toho je ovšem třeba překonat několik technických obtíží. Je to způsobeno tím, že Kolyvaginova metoda umožňuje dokázat (8) pouze pro nejsilnější možné lokální podmínky $\mathcal{D}_{min}$, kterým $\varrho_{E,p}$ vyhovuje. Problém je v tom, že přímé použití Eulerových systémů pro ostatní $\mathcal{D}$ dokazuje pouze poněkud oslabenou nerovnost (8). Wiles proto postupuje nepřímo:

(1) Pokud existuje modulární deformace ϱ nějakého typu $\mathcal{D}$, existuje i modulární deformace ϱ' vyhovující nejsilnějším lokálním podmínkám $\mathcal{D}_{min}$.

Toto tvrzení zobecňuje Serreovu hypotézu z odstavce 7 a bylo dokázáno kolektivním úsilím řady autorů (N. Boston, H. Carayol, F. Diamond, B. Edixhoven, G. Faltings, B. H. Gross, B. Jordan, H. W. Lenstra, R. Livné, B. Mazur, K. A. Ribet, J.-P. Serre, A. Wiles ...; viz též [28]). Drobná potíž spočívá v tom, že v řadě míst [28] se předpokládá, že $p \geqslant 5$. Proto je třeba zvlášť vyšetřovat případ $p = 3$.

(2) Použitím Eulerova systému sestrojeného pro ϱ dokázat (8) pro $\mathcal{D}_{min}$.

(3) Platí-li (8) pro $\mathcal{D}_{min}$, pak platí i pro všechny slabší lokální podmínky $\mathcal{D}$.

Tuto implikaci lze přeformulovat jako výrok o kongruencích mezi modulárními formami. Ten pak Wiles dokazuje zobecněním Ribetových metod z důkazu Serreovy hypotézy (H).

Celá tato dlouhá procedura úspěšně funguje pouze tehdy, pokud Galoisova reprezentace $\varrho_{E,p}$ splňuje řadu podmínek. K důkazu Taniyamovy hypotézy (v semistabilním případě) to stačí; přesto by bylo žádoucí, abychom měli důkaz Mazurovy hypotézy v co největší obecnosti. Ve speciálním případě tzv. diedrálních reprezentací $\varrho_{E,p}$ Wiles dokázal Mazurovu hypotézu pomocí Hlavní hypotézy Iwasawovy teorie pro imaginární kvadratická tělesa, dokázanou Rubinem [29] (rovněž pomocí vhodného Eulerova systému). Teprve práce Flacha [6] naznačila, jak postupovat v obecném případě.

11. Závěrečné poznámky

Bez nadsázky lze říci, že Wiles využívá skoro všeho (s výjimkou Arakelovovy geometrie), co se v posledních dvaceti letech objevilo nového v algebraické teorii čísel (či jak se dnes s oblibou říká, v aritmetické algebraické geometrii). V omezeném prostoru tohoto článku jsme se mohli pouze dotknout těch nejzávažnějších myšlenek a pojmů, které se v důkazu Fermatovy věty objevují.

Jak zdůraznil Ken Ribet v předchozím článku, pro teorii čísel má mnohem větší význam Taniyamova hypotéza, která je nejjednodušším případem obecných Langlandsových hypotéz. Řada pesimistů (mezi něž patřil i autor tohoto článku) měla za to, že tyto hypotézy nám budou ještě dlouho nedostupné. Wilesův výsledek v tomto směru otevírá netušené možnosti. Lze jen doufat, že poslouží motivací pro nejbystřejší ze současných studentů matematiky, aby se začali věnovat oné neobyčejně fascinující disciplíně, kterou teorie čísel vždy byla a je.

Několik slov k literatuře: o eliptických křivkách a funkcích se lze dočíst v [15], [35], [37], [38]; o modulárních křivkách a formách v [16], [25], [34]. Aritmetiku, geometrii i teorii funkcí v jednom najdeme ve vynikajících knihách [2], [11], [30].

Na závěr ještě malý komentář o nejvýznamnějších pracích Andrewa Wilese: ve společné práci s J. Coatesem [3] dokázali první netriviální výsledek o hypotéze Birche a Swinnertona-Dyera. Původní verze důkazu se opírala o „explicitní zákon reciprocity", dokázaný v [39]. V práci [23] B. Mazur a A. Wiles dokázali Hlavní hypotézu Iwasawovy teorie nad $\mathbf{Q}$ a jeho komutativními totálně reálnými rozšířeními (jejich důkaz byl založen na studiu aritmetiky modulárních křivek). Wiles tento výsledek rozšířil na všechna totálně reálná tělesa v [41], [42]. To vyžadovalo zcela jiné metody, zejména pak konstrukci Galoisových reprezentací pro Hilbertovy modulární formy [40]. Již těmito výsledky se Wiles nepochybně zařadil na číselně teoretický Olymp.

[1] *S. Bloch, K. Kato*: L-functions and Tamagawa numbers of motives. In: The Grothendieck Festschrift I, Progress in Mathematics 86. Birkhäuser, Boston, Basel, Berlin, 1990, pp. 333–400.

[2] *H. C. Clemens*: A scrapbook of complex curve theory. Plenum Press, New York, London, 1980.

[3] *J. Coates, A. Wiles*: On the Conjecture of Birch and Swinnerton-Dyer. Invent. Math. *39* (1977), 223–251.

[4] *M. Eichler*: Quaternare quadratische Formen und die Riemannsche Vermutung für die Kongruenzzetafunktion. Arch. Math. *5* (1954), 355–366.

[5] *G. Faltings*: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern. Invent. Math. *73* (1983), 349–366.

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

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

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

[9] *P. Griffiths, J. Harris*: Principles of Algebraic Geometry. Wiley, New York, 1978.

[10] *H. Hasse*: Beweis des Analogons der Riemannschen Vermutung für die Artinschen und F.K. Schmidtschen Kongruenzzetafunktionen in gewissen elliptischen Fällen. Nachr. Ges. Wiss. Göttingen, Math.-Phys. Kl. (1933, 253–262.

[11] *K. Ireland, M. Rosen*: A Classical Introduction to Modern Number Theory. Graduate Texts in Mathematics 84, Springer, New York, Heidelberg, Berlin, 1982.

[12] *V. A. Kolyvagin*: Konečnosť $E(\mathbf{Q})$ i Ш$(E, \mathbf{Q})$ dlja podklassa krivych Vejlja. Izv. Akad. Nauk SSSR, Ser. Mat. *52* (1988), 522–540.

[13] *V. A. Kolyvagin*: O gruppach Mordella-Vejlja i Šafareviča-Tejta dlja elliptičeskich krivych Vejlja. zv. Akad. Nauk SSSR, Ser. Mat. *52* (1988), 1156–1180.

[14] *V. A. Kolyvagin*: Euler Systems. In: The Grothendieck Festschrift II, Progress in Mathematics 87. Birkhäuser, Boston, Basel, Berlin, 1990, pp. 435–483.

[15] *S. Lang*: Elliptic Functions. Addison-Wesley, Reading, Mass., 1973.

[16] *S. Lang*: Introduction to Modular Forms. Springer, Berlin, Heidelberg, New York, 1976.

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

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

[19] *B. Mazur*: Letter to J.-F. Mestre (16 August 1985).

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

[21] *B. Mazur*: On the passage from local to global in number theory. Bulletin AMS *29* (1993), no. 1, 14–50.

[22] *B. Mazur, K. Ribet*: Two-dimensional representations in the arithmetic of modular curves. In: Astérisque 196/197, S.M.F.. 1991, pp. 215–255.

[23] *B. Mazur, A. Wiles*: Class fields of abelian extensions of $\mathbf{Q}$. Invent. Math. *76* (1984), 179–330.

[24] *J. Nekovář*: Values of L-functions and p-adic cohomology. In: Proceedings ECM 1992 Paris. to appear.

[25] *A. Ogg*: Modular forms and Dirichlet series. Benjamin, 1969.

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

[27] *K. A. Ribet*: From the Taniyama-Shimura Conjecture to Fermat's Last Theorem. Ann. Fac. Sci. Toulouse Math. *11* (1990), 116–139.
[28] *K. A. Ribet*: Report on mod ℓ representations of Gal($\overline{\mathbf{Q}}/\mathbf{Q}$). In: Proceedings of the "Motives" conference, Seattle 1991. to appearin Proc. Symp. Pure Math.
[29] *K. Rubin*: The "main conjecture" of Iwasawa theory for imaginary quadratic fields. Invent. Math. *103* (1991), 25–68.
[30] *J.-P. Serre*: A Course in Arithmetic. Springer, New York, 1973.
[31] *J.-P. Serre*: Lettre à J.-F. Mestre, (13 Août 1985). Contemp. Math. *67* (1987), 263–268.
[32] *J.-P. Serre*: Sur les représentations modulaires de degré 2 de Gal. Duke Math. J. *54* (1987), 179–230.
[33] *G. Shimura*: Correspondences modulaires et les fonctions ζ de courbes algébriques. J. Math. Soc. Japan *10* (1958), 1–28.
[34] *G. Shimura*: Introduction to the Arithmetic Theory of Automorphic Functions. Princeton University Press, 1971.
[35] *J.H. Silverman*: The arithmetic of elliptic curves. Graduate Texts in Math., vol. 106, Springer, New York, 1986.
[36] *J. Tunnell*: Artin's conjecture for representations of octahedral type. Bull. Amer. Math. Soc. (N.S.) *5* (1981), 173–175.
[37] *H. Weber*: Lehrbuch der Algebra, III. 1908.
[38] *A. Weil*: Elliptic functions according to Eisenstein and Kronecker. Springer, New Yorkyr 1976.
[39] *A. Wiles*: Higher explicit reciprocity laws. Ann. of Math. *107* (1978), 235–254.
[40] *A. Wiles*: On ordinary λ-adic representations associated to modular forms. Invent. Math. *94* (1988), 529–573.
[41] *A. Wiles*: The Iwasawa conjecture for totally real fields. Ann. of Math. *131* (1990), 493–540.
[42] *A. Wiles*: On a conjecture of Brumer. Ann. of Math. *131* (1990), 555–565.