Michal Křížek; Lawrence Somer
John Tate získal Abelovu cenu za rok 2010

Pokroky matematiky, fyziky a astronomie, Vol. 55 (2010), No. 2, 89–96

Persistent URL: http://dml.cz/dmlcz/141943

John Tate získal Abelovu cenu za rok 2010

Michal Křížek, Praha, Lawrence Somer, Washington

1. Úvod

Abelova cena je považována za „Nobelovu cenu“ za matematiku. Její finanční ohodnocení kolem 1 miliónu dolarů je stejné jako u Nobelovy ceny za fyziku. Abelova cena se uděluje za výjimečně hluboké výsledky, které významně ovlivnily matematické vědy. V letošním roce ji získal americký matematik prof. John Tate z University of Texas v Austinu za práce v oblasti algebraické teorie čísel (viz [18]). Dne 25. května byl přijat k audienci v královském paláci v Oslu. Poté v hlavní aule univerzity v Oslu převzal Abelovu cenu z rukou norského krále Haralda V. Při této příležitosti přednesl slavnostní proslov předseda Norské akademie věd (Norwegian Academy of Science and Letters) Nils Ch. Stenseth a předseda výběrové komise (Abel Committee) Kristian Seip. Další den pak pronesl prof. Tate laureátskou přednášku na téma:

The arithmetic of elliptic curves.

O eliptických křivkách pojednáme ve 4. kapitole. Připomeneme i některé jejich aplikace v kryptografii.

Tateovy výsledky z teorie eliptických křivek podstatně přispěly k důkazu Velké Fermatovy věty[1]) — jednoho z nejslavnějších matematických problémů (viz např. [10], [12], [13], [14]). Tato věta říká, že neexistují přirozená čísla $n > 2$ a a, b, c tak, že

$$a^n + b^n = c^n. \tag{1}$$

Abelovskou přednášku při předání ceny měl proto čest proslovit Richard Taylor na téma: *The Tate Conjecture*. Připomeňme, že to byl právě Taylor, který společně s A. Wilesem dokázali Velkou Fermatovu větu (viz [17]). Další přehledovou přednášku měl Andreas Enge na téma: *The Queen of Mathematics in Communication Security*, v níž poukázal na překvapivé aplikace teorie čísel v kryptografii.[2]) Na večerním banketu pak promluvil mj. Michael Atiyah, který získal Abelovu cenu v roce 2004.

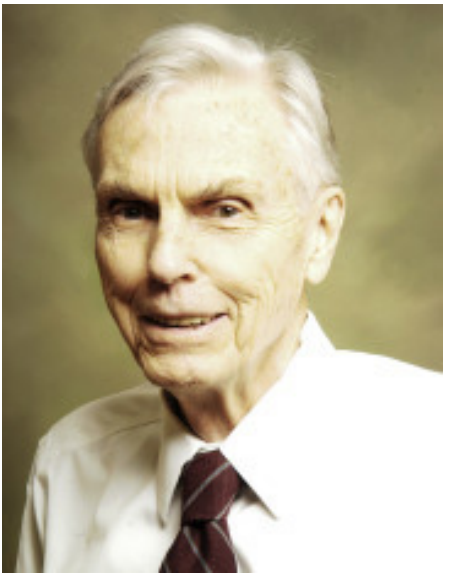
[1]) V originále „Fermat's Last Theorem“, což se většinou interpretuje jako „poslední nevyřešený z Fermatových problémů“. Poznamenejme ale, že např. problém, zda je Fermatových prvočísel nekonečně mnoho, dodnes nebyl vyřešen [5].

[2]) Článek [7] na podobné téma vyšel nedávno i v PMFA (viz též [19]).

Prof. RNDr. Michal Křížek, DrSc., Matematický ústav Akademie věd ČR, v.v.i., Žitná 25, 115 67 Praha 1, e-mail: krizek@math.cas.cz, Prof. Lawrence Somer, PhD., Department of Mathematics, Catholic University of America, Washington, D.C. 20064, U.S.A., e-mail: somer@cua.edu.

2. Kdo je John Tate?

John Tate se narodil 13. března 1925 v Minneapolis. Titul bakaláře získal na Harvardově univerzitě a doktorát na univerzitě Princetonu. Jeho školitelem byl Emil Artin. V současnosti J. Tate bydlí se svou manželkou Carol v Cambridge ve státě Massachusetts. Je otcem tří dcer.



Obr. 1. John Tate (foto Charlie Fondville), viz [18].

Prof. Tate se proslavil zejména svými pracemi z algebraické teorie čísel a algebraické geometrie. Pokud by se měřil výkon matematika počtem matematických termínů, které jsou po něm pojmenovány, pak by John Tate mohl být překonán snad jedině Gaussem. Jeho jméno totiž nese Tateova kohomologie, Tateova věta o dualitě, Barsottiovy–Tateovy grupy, Tateův motiv, Tateův modul, Tateova křivka, Tateův cyklus, Hodgeův–Tateův rozklad, Tateův algoritmus, Néronova–Tateova výška, Mumfordovy–Tateovy grupy, Tateova izogenní věta, Hondaova–Tateova věta pro abelovské variety nad konečnými tělesy, Serreova–Tateova deformační teorie, Serreův–Tateův parametr, Tateova stopa, Lubinova–Tateova grupa, Tateovy–Shafarevichovy grupy, Satoova–Tateova domněnka aj.

Tateovy výsledky jsou také jádrem některých samoopravných kódů, které umožňují mírně poškozenou informaci opravit. Toho se využívá při ochraně CD disků před poškrábáním, při přenosu SMS zpráv, které jsou rušeny různými rádiovými signály apod. John Tate produkuje skvělé matematické výsledky už více než šest desetiletí. Na University of Texas v Austinu přešel v roce 1990. Předtím učil 36 let na Harvard University. Teprve nedávno odešel do důchodu.

Prof. Tate měl zvanou přednášku na Mezinárodním matematickém kongresu ve Stockholmu v roce 1962 a pak ještě v Nice v roce 1970. Během života získal mnoho

dalších ocenění. Již v roce 1956 dostal Coleovu cenu od Americké matematické společnosti za vynikající výsledky z teorie čísel. Od Americké matematické společnosti také obdržel Leroy P. Steele Prize v roce 1995 za celoživotní dílo. Za zmínku stojí i Wolfova cena z let 2002–2003.

John Tate byl v roce 1969 zvolen do National Academy of Sciences, v roce 1992 byl jmenován zahraničním členem francouzské Académie des Sciences a čestným členem Londýnské matematické společnosti se stal v roce 1999.

3. Velice stručně o teorii čísel

Teorie čísel je jednou z nejstarších vědních disciplín. Avšak teprve ve 20. století matematici objevili obrovské množství praktických aplikací, např. při tvorbě samoopravných kódů, digitálního podpisu, algoritmech rychlého násobení, generování pseudonáhodných čísel či šifrování tajných zpráv (viz [5]). Poznatky z teorie čísel také podstatně přispívají ke zvyšování informační bezpečnosti internetu.

Teorie čísel se zabývá zejména vlastnostmi množiny přirozených čísel

$$\mathbb{N} = \{1, 2, 3, \ldots\}.$$

Připomeňme, že přirozené číslo se nazývá *prvočíslo*, jestliže má právě dva různé dělitele (každé prvočíslo je tak dělitelné pouze sebou samým a jednou). Už Eukleides (4.–3. stol. př. n. l.) uměl dokázat následující tvrzení:

Věta (Eukleidova). *Prvočísel je nekonečně mnoho.*

Každé přirozené číslo větší než jedna může být jednoznačně vyjádřeno (až na pořadí) jako součin prvočísel. Prvočísla 2, 3, 5, 7, ... tak tvoří základní stavební jednotky přirozených čísel větších než jedna, podobně jako atomy tvoří molekuly.

Za zakladatele moderní teorie čísel je považován francouzský matematik Pierre de Fermat (viz [14]). Jeho nejčastěji používaný výsledek, který má i velké množství praktických aplikací (viz [5]), lze zformulovat takto:

Malá Fermatova věta. *Jestliže $a \in \mathbb{N}$ a p je prvočíslo, pak p dělí $a^p - a$.*

Dalším významným francouzským matematikem, který podstatně ovlivnil rozvoj teorie čísel, je Marin Mersenne.[3]) Studoval mj. čísla tvaru

$$M_p = 2^p - 1,$$

kde p je prvočíslo, která se po něm nazývají *Mersennova čísla*. Požadavek prvočíselnosti exponentu ilustruje následující věta.

Věta. *Je-li $2^p - 1$ prvočíslo, pak p je také prvočíslo.*

[3]) M. Mersenne (1588–1648) je též považován za duchovního otce vzniku francouzské Akademie věd (viz [5, s. 110]).

Největší známé prvočíslo je v současnosti Mersennovo číslo $2^{43112609}-1 \approx 10^{12978188}$. Pro srovnání uveďme, že počet atomů v pozorovatelné části vesmíru je přibližně jen 10^{80}, což je téměř o 13 miliónů řádů menší číslo než $M_{43112609}$.

Jedním z nejkrásnějších a zároveň nejpřekvapivějších výsledků poslední doby je následující tvrzení z roku 2004 (podrobnosti viz [4]).

Věta (Greenova–Taova). *Pro každé $k \in \mathbb{N}$ množina prvočísel obsahuje aritmetickou posloupnost délky k.*

Více než 150 dalších zajímavých vět z teorie čísel je uvedeno v [5].

4. Eliptické křivky

Eliptické křivky jsou algebraické křivky v $\mathbb{R}^2$ (popř. v $\mathbb{C}^2$) dané rovnicí

$$y^2 = x^3 + Ax^2 + Bx + C, \tag{2}$$

kde koeficienty A, B, C jsou racionální čísla taková, že polynom $x^3 + Ax^2 + Bx + C$ nemá násobný kořen. Je patrné, že žádná eliptická křivka nemůže být elipsou. Jejich název pouze souvisí s užitím těchto křivek pro výpočet délky eliptického oblouku. Poznamenejme, že řešením rovnic typu (2) s celočíselnými koeficienty se zabýval již řecký matematik Diofantos právě pro jejich zajímavé vlastnosti.

Popišme si nyní grupu, kterou se John Tate intenzivně zabýval a která byla později použita při důkazu Velké Fermatovy věty. Připomeňme, že *grupa* G je množina, na které je definována asociativní binární operace $\circ : G \times G \to G$ s neutrálním prvkem n a v níž ke každému prvku $g \in G$ existuje právě jeden prvek inverzní $g^{-1} \in G$ tak, že $g \circ g^{-1} = g^{-1} \circ g = n$.

V jedné části důkazu Velké Fermatovy věty (srov. (1) a [8]) se pracuje se speciálními grupami bodů na eliptických křivkách tvaru $y^2 = x(x - a^p)(x + b^p)$ (kde vhodnou lineární substitucí lze „vynulovat“ koeficient u x^2). Abychom se blíže seznámili s těmito grupami, zabývejme se pro jednoduchost jen jedinou křivkou $\mathcal{C}$ danou vztahem

$$y^2 = x^3 - x + \tfrac{1}{4}, \tag{3}$$

jejíž graf se skládá ze dvou částí (viz obr. 2).

Na této křivce budeme definovat grupu bodů. Pro každý bod $U = (x, y) \in \mathcal{C}$ nejprve definujme inverzní prvek

$$\ominus U = (x, -y), \tag{4}$$

který opět leží na $\mathcal{C}$, jak plyne z (3). Graf na obr. 2 je tak symetrický podle osy x. Pokuste se nyní předem odhadnout, kde se nalézá neutrální prvek (za chvíli vám to prozradíme).

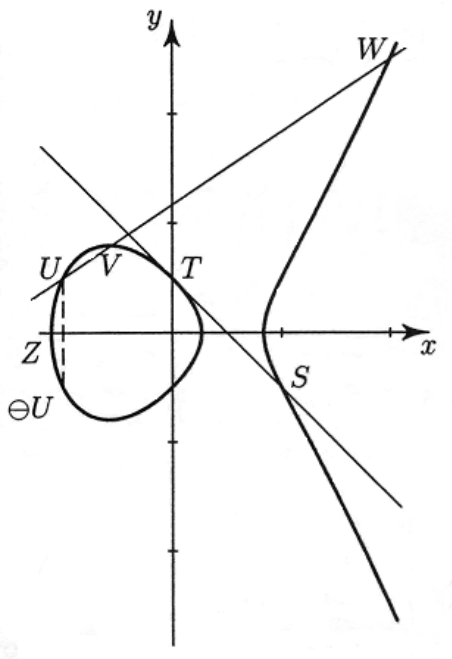
Nyní popíšeme, jak budeme definovat binární grupovou operaci $\oplus$. Nechť $U, V \in \mathcal{C}$ jsou dva různé body ležící na přímce $y = kx + q$. Potom z (3) dostáváme kubickou rovnici

$$(kx + q)^2 = x^3 - x + \tfrac{1}{4}, \tag{5}$$

která má dvě různá reálná řešení (x-souřadnice bodů U a V). Třetí kořen rovnice tedy musí být také reálný.

a) Pokud je tento kořen jednoduchý, potom na přímce $y = kx + q$ leží také bod $W \in \mathcal{C}$, jehož x-ová souřadnice je právě třetím kořenem rovnice (5) a $U \neq W \neq V$.

b) Pokud je tento kořen dvojnásobný, potom přímka $y = kx + q$ je v jednom bodě tečnou ke křivce $\mathcal{C}$, tj. $W \equiv U$ anebo $W \equiv V$.



Obr. 2. Grupa na eliptické křivce.

Body $U, V, W \in \mathcal{C}$ jsou tedy kolineární (tj. leží na jedné přímce) a alespoň dva z nich jsou navzájem různé. Na množině všech bodů křivky $\mathcal{C}$ definujme grupovou operaci $\oplus$ předpisem

$$U \oplus V = \ominus W. \tag{6}$$

Je ihned patrné, že tato operace je komutativní. Pomocí (3), (4), (5) a (6) si můžete sami ověřit, že např. pro bod $T = (0, \frac{1}{2})$ na obr. 2 platí

$$\begin{aligned} T \oplus T &= (1, \tfrac{1}{2}) = \ominus S, \\ T \oplus T \oplus T &= (-1, -\tfrac{1}{2}) = \ominus U, \\ T \oplus T \oplus T \oplus T &= (2, -\tfrac{5}{2}) = \ominus W. \end{aligned}$$

V (4) jsme definovali inverzní prvky k libovolnému bodu křivky $\mathcal{C}$. Je zřejmé, že involutorními prvky (tj. inverzními samy k sobě) jsou všechny průsečíky křivky $\mathcal{C}$

s osou x (např. na obrázku 4 bod $Z = \ominus Z$). Jaký bod je ale neutrálním prvkem vyšetřované grupy? Musí to být takový bod $N \in \mathcal{C}$, že pro libovolné $U \in \mathcal{C}$ platí

$$U \oplus N = U. \tag{7}$$

Co to konkrétně geometricky znamená? Podle (6) body U, $\ominus U$ a N leží na jedné přímce, která je rovnoběžná s osou y. Protože však (7) platí pro libovolný bod $U \in \mathcal{C}$, „leží" neutrální prvek N na každé přímce rovnoběžné s osou y, tj. N je nevlastním bodem nacházejícím se v nekonečnu, který vlastně na křivce C neleží.

Abychom dokázali, že body křivky (3), k nimž je doplněn neutrální prvek N, tvoří grupu s operací $\oplus$ definovanou v (6), zbývá ještě dokázat asociativitu grupové operace. Takový důkaz ale není snadný a přesahuje rámec tohoto článku.

Poznamenejme ještě (srov. [8]), že rovnici (6) lze ekvivalentně zapsat takto

$$U \oplus V \oplus W = N.$$

Diofantské rovnice jsou rovnice s celočíselnými koeficienty, jejichž řešení se hledá mezi celými, popř. racionálními čísly. Tento název je odvozen od již zmíněného Diofanta, který žil v Alexandrii ve 3. století našeho letopočtu a zabýval se řešením rozličných úloh z teorie čísel.

Lze ukázat, že rovnice

$$y^2 = x^3 - 43x + 166 \tag{8}$$

má právě 6 racionálních řešení (x, y): $(3, \pm 8)$, $(-5, \pm 16)$ a $(11, \pm 32)$, která jsou shodou okolností všechna celočíselná. Všimněte si, že leží na dvou přímkách $y = 3x - 1$ a $y = -3x + 1$. Přidáme-li k těmto bodům ještě neutrální prvek, dostaneme konečnou grupu, která je izomorfní cyklické grupě $\mathcal{C}_7$.

Na druhé straně rovnice

$$y^2 = x^3 - 2$$

má nekonečně mnoho racionálních řešení (např. $(3, \pm 5)$). Jedna z klíčových otázek řešení rovnic typu (2) je tedy:

Která z těchto rovnic má konečný počet racionálních řešení a která jich má nekonečný počet?

A byl to právě John Tate, který vyvinul sofistikovanou metodu, jež pomáhá překonávat záhady eliptických křivek a rozhodovat, zda odpovídající diofantské rovnice mají konečný či nekonečný počet racionálních řešení. Na každé eliptické křivce existuje jen konečně mnoho celočíselných bodů, ale grupa racionálních bodů je typicky nekonečná,[4]) i když je vždy konečně generována (Mordellova věta).

Málokdo ví, že aritmetika eliptických křivek je implementována v mobilních telefonech, platebních kartách, dopravních kontrolních systémech apod. V takových kódech je např. číslo vaší kreditní karty konvertováno na bod na eliptické křivce. K zašifrování informace se použije jistá důmyslná transformace, která posune tento bod na jiný bod eliptické křivky.

[4]) Existují však výjimky – viz např. (8).

Obr. 3. V rodišti Pierra de Fermata (Beaumont-de-Lomagne) v říjnu 1996: *Velká Fermatova věta byla tedy skutečně dokázána?* ptají se vesničané A. Wilese.

5. Závěr

John Tate se v roce 1950 ve své doktorské disertaci [15] zabýval Fourierovou analýzou v číselných tělesech. Tím vytyčil zcela ojedinělou cestu k moderní teorii automorfních forem. Vyškolil přes 20 Ph.D. studentů v teorii čísel. Mnozí z nich se později velice proslavili, např. Joe Buhler, Joseph Silverman, Benedict Gross či Kenneth Ribet. Posledně jmenovaný ukázal, že Velká Fermatova věta plyne z Taniyamaovy–Šimurovy domněnky,[5]) a tím pomohl A. Wilesovi s R. Taylorem k nalezení důkazu Velké Fermatovy věty. Domněnka byla v plné obecnosti dokázána až v roce 2001 v článku [3], kde je R. Taylor spoluautorem.

Další Tateův student, Carl Pomerance, ve své disertaci dokázal, že každé liché dokonalé číslo má alespoň 7 prvočinitelů. Později Pomerance vyvinul známé kvadratické síto (angl. *the quadratic sieve algorithm*), což je hojně používaná faktorizační metoda [9], spolupodílel se na efektivní metodě pro testování prvočíselnosti (spoluautoři Adleman a Rumely) a na důkazu, že Carmichaelových čísel je nekonečně mnoho [5]. Prof. Tate tak měl podstatný vliv na rozvoj moderní teorie čísel prostřednictvím svých studentů.

Sám Tate má velké množství publikací v prestižních matematických časopisech, např. v Annals of Mathematics [2], [6], [11] a [16]. Přitom práci [11] napsal s Jean-Pierrem Serrem, který získal Abelovu cenu za matematiku jako vůbec první. J. Tate

[5]) Viz např. PMFA 42 (1997), 169–187.

se svým bývalým školitelem Emilem Artinem napsali hojně citovanou monografii [1], v níž je představen nový pohled na teorii číselných těles. V pořadí již osmá Abelova cena je tedy jistě ve správných rukou. Bez Tatea a jeho studentů by A. Wiles Velkou Fermatovu větu jen těžko dokázal (viz obr. 3).

Poděkování. Autoři děkují doc. RNDr. Martinu Klazarovi, Dr., za cenné připomínky. Článek byl podpořen výzkumným záměrem MSM 0021620839 a grantem IAA 100190803 GA AV ČR.

L i t e r a t u r a

[1] Artin, E., Tate, J.: *Class field theory.* AMS Chelsea Publ. 1967, 2009.
[2] Brauer, R., Tate, J.: *On the characters of finite groups.* Ann. of Math. *62* (1955), 1–7.
[3] Breuil, C., Conrad, B., Diamond, F., Taylor, R.: *On the modularity of elliptic curves over Q: wild 3-adic exercises.* J. Amer. Math. Soc. *14* (2001), 843–939.
[4] Klazar, M.: *Prvočísla obsahují libovolně dlouhé aritmetické posloupnosti.* PMFA *49* (2004), 177–188.
[5] Křížek, M., Somer, L., Šolcová, A.: *Kouzlo čísel: Od velkých objevů k aplikacím.* Edice Galileo, sv. 39, Academia, Praha 2009.
[6] Lubin, J., Tate, J.: *Formal complex multiplication in local fields.* Ann. of Math. *81* (1965), 380–387.
[7] Mlýnek, J.: *Informační bezpečnost.* PMFA *51* (2006), 89–98.
[8] Nekovář, J.: *Modulární křivky a Fermatova věta.* Math. Bohem. *119* (1994), 79–96.
[9] Pomerance, C.: *Vyprávění o dvou sítech.* PMFA *43* (1998), 9–29.
[10] Ribenboim, P.: *Fermat's Last Theorem for amateurs.* Springer, New York 1999.
[11] Serre, J.-P., Tate, J.: *Good reduction of abelian varieties.* Ann. of Math. *88* (1968), 462–517.
[12] Singh, S.: *Velká Fermatova věta.* Academia, Praha 2000.
[13] Skula, L.: *Některé historické aspekty Fermatova problému.* PMFA *39* (1994), 318–330.
[14] Šolcová, A., Křížek, M., Mink, G. (eds.): *Matematik Pierre de Fermat.* Cahiers du CEFRES, No. 28, Praha 2002.
[15] Tate, J.: *Fourier analysis in number fields and Hecke's zeta functions.* Ph.D. Thesis, Princeton Univ., 1950, Reprinted in Cassels, J. W. S., Frölich, A. (eds): *Algebraic number theory.* Academic Press, London 1967, 305–347.
[16] Tate, J.: *The higher dimensional cohomology groups of class field theory.* Ann. of Math. *56* (1952), 294–297.
[17] Taylor, R., Wiles, A.: *Ring-theoretic properties of certain Hecke algebras.* Ann. of Math. *141* (1995), 553–572.
[18] `http://www.abelprisen.no/en/`
[19] `http://www.dtc.umn.edu/~odlyzko`