Pokroky matematiky, fyziky a astronomie

Michal Křížek; Lawrence Somer

Abelova cena v roce 2016 udělena za důkaz Velké Fermatovy věty

Pokroky matematiky, fyziky a astronomie, Vol. 61 (2016), No. 3, 169–188

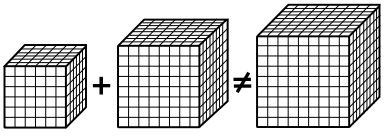
Persistent URL: http://dml.cz/dmlcz/145844

Abelova cena v roce 2016 udělena za důkaz Velké Fermatovy věty

Michal Křížek, Praha, Lawrence Somer, Washington, DC

Cubum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos, et generaliter nullam in infinitum ultra quadratum potestatem in duos eiusdem nominis fas est dividere[1]*...*

Pierre de Fermat



Abstrakt. Abelovu cenu za matematiku získal v roce 2016 britský matematik sir Andrew Wiles za svůj senzační důkaz Velké Fermatovy věty. V článku popisujeme, jakým způsobem k důkazu dospěl.

1. Úvod

Abelova cena je vedle Fieldsovy medaile nejvyšší mezinárodní ocenění za vynikající výsledky na poli matematiky zahrnující i matematické aspekty výpočetní matematiky, matematické fyziky, pravděpodobnosti, numerické matematiky, vědeckých výpočtů, statistiky a aplikované matematiky.

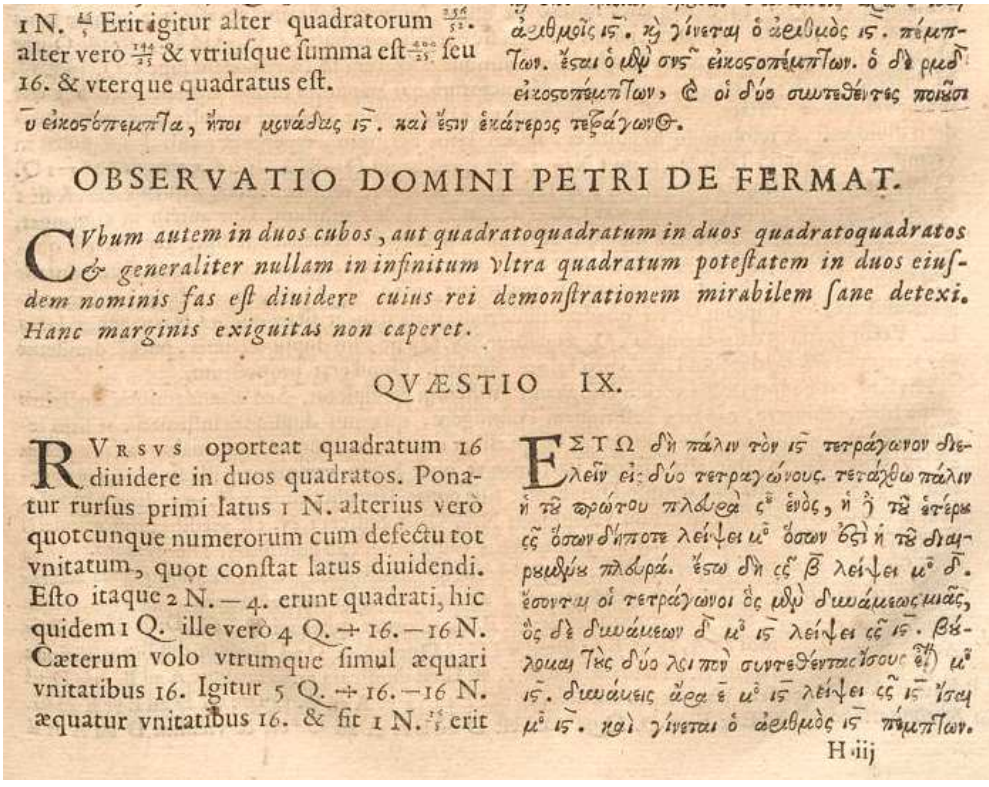
Dne 15. března 2016 prezident Norské akademie věd Ole M. Sejersted oznámil, že Abelovu cenu za rok 2016 obdrží britský matematik Andrew Wiles za svůj senzační důkaz Velké Fermatovy věty pomocí modulární domněnky pro semistabilní eliptické křivky a za otevření nové epochy výzkumu v teorii čísel [39].

Francouzský matematik Pierre de Fermat (1601–1665) si v roce 1637 připsal na okraj svého exempláře[2] Bachetova vydání Diofantovy *Aritmetiky* [2] poznámku,

[1] Je nemožné napsat třetí mocninu jako součet dvou třetích mocnin, nebo čtvrtou mocninu jako součet dvou čtvrtých mocnin, či obecně jakékoliv číslo, které samo je mocninou větší než dva, nelze napsat jako součet dvou stejných mocnin... [Míní se jen mocniny přirozených čísel.]

[2] V roce 1670 Samuel de Fermat, syn Pierra de Fermata (1601–1665), publikoval ve francouzském Toulouse Diofantovu *Aritmetiku* [2] rozšířenou právě o poznámky svého otce, viz obr. 1.

Prof. RNDr. Michal Křížek, DrSc., Matematický ústav AV ČR, v. v. i., Žitná 25, 115 67 Praha 1, e-mail: krizek@cesnet.cz, prof. Lawrence Somer, Ph.D., Department of Mathematics, Catholic University of America, Washington, DC 20064, U.S.A., e-mail: somer@cua.edu



1 N. $\frac{44}{7}$ Erit igitur alter quadratorum $\frac{256}{529}$. alter vero $\frac{144}{529}$ & vtriusque summa est $\frac{400}{529}$ seu 16. & vterque quadratus est.

ἀριθμοῖς ις̄. καὶ γίνεται ὁ ἀριθμὸς ις̄. πέμπτων. ἔσται ὁ μὲν εἷς εἰκοσιπέμπτων. ὁ δὲ μεδ' εἰκοσιπέμπτων, ἃ οἱ δύο συντεθέντες ποιοῦσι τὸν εἰκοσιπέμπτα, ἤτοι μονάδας ις̄. καὶ ἔστιν ἑκάτερος τετράγωνος.

OBSERVATIO DOMINI PETRI DE FERMAT.

CVbum autem in duos cubos, aut quadratoquadratum in duos quadratoquadratos & generaliter nullam in infinitum vltra quadratum potestatem in duos eiusdem nominis fas est diuidere cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet.

QVÆSTIO IX.

RVRSVS oporteat quadratum 16 diuidere in duos quadratos. Ponatur rursus primi latus 1 N. alterius verò quotcunque numerorum cum defectu tot vnitatum, quot constat latus diuidendi. Esto itaque 2 N. — 4. erunt quadrati, hic quidem 1 Q. ille verò 4 Q. + 16. — 16 N. Cæterum volo vtrumque simul æquari vnitatibus 16. Igitur 5 Q. + 16. — 16 N. æquatur vnitatibus 16. & fit 1 N. $\frac{32}{5}$ erit

ΕΣΤΩ δὴ πάλιν τὸν ις̄ τετράγωνον διελεῖν εἰς δύο τετραγώνους. τετάχθω πάλιν ἡ τῆ πρώτου πλευρὰ ς̄ ἑνός, ἡ δὲ τῆ ἑτέρᾳ ς̄ ὅσων δήποτε λείψει μ̄ ὅσων ὑπὸ ἡ τῆ διαιρουμένῃ πλευρά. ἔστω δὴ ς̄ β̄ λείψει μ̄ δ̄. ἔσονται οἱ τετράγωνοι ὁ μὲν δυνάμεως καὶ, ὁ δὲ δυνάμεων δ̄ μ̄ ις̄ λείψει ς̄ ις̄. βάλλομαι τὰς δύο ἴσας πὸν συντεθέντας ἴσους εἶ μ̄ ις̄. δυνάμεις ἄρα ε̄ μ̄ ις̄ λείψει ς̄ ις̄ ἴσαι μ̄ ις̄. καὶ γίνεται ὁ ἀριθμὸς ις̄ πέμπτων.

H iij

Obr. 1. Ukázka z rozšířeného vydání Diofantovy *Aritmetiky* se slavnou poznámkou Pierra de Fermata

kterou uvádíme v záhlaví našeho článku. Za ní pak připsal: ... *cuius rei demonstrationem mirabilem sane detexi. Hanc marginis exiguitas non caperet*, což volně přeloženo znamená: *Mám skutečně nádherný důkaz tohoto tvrzení.*[3] *Avšak tento okraj je příliš úzký na to, abych jej zde uvedl.* Tento výrok nedal spát mnoha generacím matematiků. Většinou je formulován takto:

Věta 1 (Velká Fermatova věta). *Neexistují přirozená čísla $n \geq 3$, x, y a z taková, že*

$$x^n + y^n = z^n. \tag{1}$$

Matematikům trvalo celých 358 let, než Andrew Wiles našel v roce 1995 způsob, jak větu 1 dokázat pro všechny exponenty $n \geq 3$.

V úterý dne 24. května 2016 A. Wiles převzal Abelovu cenu z rukou norského korunního prince Haakona v hlavní aule na Univerzitě v Oslu (viz obr. 2 a 3). Další den pak následovaly abelovské přednášky v auditoriu 1 uprostřed univerzitního kampusu. V úvodním slovu rektor univerzity Ole Petter Ottersen zdůraznil nutnost základního výzkumu v matematice. Prezident Norské akademie věd ve svém projevu mj. pozna-

[3] Ve Fermatově pozůstalosti zmíněný důkaz nalezen nebyl.

Obr. 2. Hlavní aula Univerzity v Oslu se nachází v blízkosti královského paláce a sochy N. H. Abela (foto S. Korotov).

menal, že Alfred Nobel[4] nezřídil Nobelovu cenu za matematiku údajně proto, že matematika je jen málo praktická disciplína.

Dopolední program uváděl předseda výběrové komise John Rognes z Univerzity v Oslu. První přednášku proslovil sám laureát Abelovy ceny, sir Andrew Wiles z Univerzity v Oxfordu, a to na téma *Fermat's Last Theorem: abelian and non-abelian approaches*. Posluchače seznámil s hlavními myšlenkami svého důkazu, že každá racionální semistabilní eliptická křivka je modulární. Pro větší názornost se omezil jen na případ $n = 3$.

Henri Darmon (viz obr. 4 a [6]) z McGillovy univerzity svoji přednášku nazval *Andrew Wiles' marvelous proof* jako narážku na Fermatovo výše uvedené prohlášení z roku 1637, že má skutečně nádherný důkaz věty 1. H. Darmon posluchačům vysvětlil koncept Heckeho algeber, který byl k důkazu použit (viz [36]).

Bývalý Wilesův doktorand a nositel Fieldsovy medaile za rok 2014, Manjul Bhargava z Univerzity v Princetonu, proslovil přednášku *What is the Birch–Swinnerton-Dyer Conjecture, and what is known about it?* Tato domněnka patří mezi tzv. 7 Millennium Prize Problems. Na vyřešení každého z nich vypsal Clayův matematický ústav

[4] A. Nobel nebyl nikdy ženatý ani neměl děti. Proto ve své závěti rozhodl, že jeho obrovský majetek bude vložen do fondu, z něhož bude každoročně udělována cena za významné vědecké objevy, literární tvorbu a zásluhy o mír ve světě.

Obr. 3. Sir Andrew Wiles (vlevo) a norský korunní princ Haakon Magnus (vpravo) při předávání Abelovy ceny (zdroj `http://www.abelprize.no/`)

odměnu 1 000 000 dolarů. BSD domněnka zhruba řečeno tvrdí,[5] že pro eliptickou křivku E hodnosti r je $\prod_{p\le x} N_p/p \sim c(\log x)^r$, kde N_p označuje počet bodů na E (mod p). Wiles ji společně se svým školitelem Johnem Coatesem dokázal v roce 1977 ve speciálním případě pro eliptické křivky tvaru $y^2 = x^3 + Ax$ a $y^2 = x^3 + B$ (srov. (13) níže).

Závěrečnou popularizační přednášku *From Fermat's Last Theorem to Homer's Last Theorem* přednesl Simon Singh, autor mnoha úspěšných populárně-naučných bestsellerů, viz např. [32]. Během svého vystoupení zdůraznil, že jediná diofantická rovnice $x^2 + y^2 = z^2$ má nekonečně mnoho řešení (srov. (8) níže), zatímco nekonečně mnoho diofantických rovnic $x^n + y^n = z^n$ pro $n \ge 3$ nemá žádné řešení.

Poté následovalo promítání Singhova dokumentárního filmu BBC o Velké Fermatově větě, kde Wiles živě popisuje svou vlastní zkušenost s matematickým výzkumem, který trefně přirovnává k cestě neprozkoumaným zámkem plným temných komnat: *Vstoupíte do první komnaty a tam je tma. Naprostá tma. Klopýtáte kolem, vrážíte do nábytku, postupně však poznáváte, kde se jednotlivé kusy nábytku nacházejí. Nakonec,*

[5] Ve 4. kapitole se budeme věnovat grupě racionálních bodů na eliptických křivkách. Hodnost takové křivky je maximální počet nezávislých bodů $V_1, \dots, V_r$ nekonečného řádu. Zhruba řečeno, pokud $n_1V_1 \oplus \cdots \oplus n_rV_r = V_0$, kde $n_1, \dots, n_r$ jsou celá nezáporná čísla a V_0 je neutrální prvek vyšetřované grupy, pak platí $n_1 = \cdots = n_r = 0$ (podrobnosti viz [31]). Nejvyšší známá hodnost je v současnosti 28. Body konečného řádu se nazývají *torzní*, protože po konečném počtu sčítání dostaneme neutrální prvek V_0.

Obr. 4. Přednášející zleva: Simon Singh, sir Andrew Wiles, Manjul Bhargava a Henri Darmon (foto M. Křížek)

po nějakých šesti měsících najdete vypínač, stisknete jej a náhle se vše osvětlí. Víte jasně, kde se nacházíte. Pak přejdete do sousední místnosti a strávíte dalších šest měsíců v temnotě. Tak každý z těch objevů — někdy se zdají být dílem okamžiku, někdy jde o jeden či dva dny — je ve skutečnosti vyvrcholením mnoha měsíců tápání ve tmě. A bez tápání by nemohl vzniknout ...

2. Stručný životopis A. Wilese

Sir Andrew John Wiles se narodil Patricii Wilesové (roz. Mowllové) a Maurici Franku Wilesovi dne 11. dubna 1953 v Cambridgi. Otec byl profesorem teologie na Univerzitě v Oxfordu. V letech 1952–1955 působil též jako kaplan v Cambridgi. Malý Andrew navštěvoval nejprve královskou kolejní školu a později Leysovu školu v Cambridgi. V roce 1974 získal titul bakaláře na Mertonově koleji v Oxfordu. V letech 1977–1980 byl Wiles odborným asistentem na Harvardově univerzitě, kde se začínal zabývat modulárními formami. Doktorskou dizertační práci *Reciprocity Laws and the Conjecture of Birch and Swinnerton-Dyer* obhájil v roce 1980 na koleji Clareové v Cambridgi a získal vědeckou hodnost Ph.D.

Po stáži v Ústavu pro pokročilá studia v New Jersey, USA, Andrew Wiles získal již v roce 1981 titul profesora na Univerzitě v Princetonu a působil zde až do roku 2010.

V letech 1985–1986 se stal Guggenheim Fellow v Institut des hautes études scientifiques v blízkosti Paříže a na École normale supérieure. Od roku 1988 do 1990 byl na přechodnou dobu Royal Society Research Professor na Univerzitě v Oxfordu a tento post opětovně získal v roce 2011.

Sám A. Wiles uvádí, že se zajímal o Velkou Fermatovu větu už od svých deseti let. Jednou se po cestě ze školy zastavil v místní veřejné čítárně na Milton Road, kde nalezl knihu *The Last Problem* od Erica Templea Bella zmiňující onu větu. Byl doslova fascinován její jednoduchou formulací a tím, že větu ještě nikdo nedokázal. Už tehdy úplně propadl teorii čísel a předsevzal si, že to bude právě on, kdo ji první dokáže. Brzy však zjistil, že jeho znalosti jsou na to zatím příliš omezené. Wilesův klukovský sen se začal naplňovat, až když mu bylo 33 let. Tehdy se seznámil s důkazem tzv. ε-domněnky[6] pocházející od Kennetha Alana Ribeta z roku 1986, kterou již předtím Gerhard Frey spojil se slavnou Fermatovou rovnicí (1), viz kap. 6. Od té doby se na 7 let dobrovolně uzavřel do izolace a veškerý svůj čas věnoval důkazu Velké Fermatovy věty. Žádnému profesionálnímu matematikovi se o svém snažení nezmiňoval[7] a jen své manželce Nadě se občas svěřoval o svých dílčích úspěších.

Ve dnech 21. až 23. června 1993 se v Ústavu Isaaca Newtona pro matematické vědy v Cambridgi konal pracovní seminář s názvem *L-funkce a aritmetika*, který spoluorganizoval Wilesův bývalý školitel J. Coates. Sjelo se tam přes 60 specialistů na teorii čísel z celého světa. Coates přidělil Wilesovi hned dva přednáškové bloky. Pak ale zjistil, že Wiles potřebuje ještě třetí blok, a tak se Coates vzdal své vlastní přednášky v jeho prospěch. Celý Wilesův přednáškový cyklus měl prostý název *Eliptické křivky, modulární formy a Galoisovy reprezentace*. Až v závěrečné přednášce Wiles oznámil, že má důkaz Velké Fermatovy věty. Coates to pak komentoval slovy: *Věděl jsem, že se Wiles chystá oznámit nějaký velký výsledek, ale neměl jsem představu, jaký.*

Wiles pak zaslal svůj dvousetstránkový důkaz do časopisu *Inventiones Mathematicae*, jehož redaktor Barry Mazur z Harvardovy uviverzity zvolil hned šestici recenzentů, aby řádně zaručil, že je vše v pořádku. Na drobné připomínky recenzentů Wiles v průběhu recenzního řízení okamžitě reagoval a drobné chybičky stačil neprodleně opravovat. Jenomže v srpnu 1993 jeden z recenzentů, Nick Katz, objevil ve Wilesově důkazu podstatnou chybu. Andrew Wiles tak zaplatil vysokou daň za to, že o svých výsledcích s nikým nediskutoval, neboť bylo dosti pravděpodobné, že se nějaká závažná chyba objeví. Po více než roce usilovné práce, když už chtěl Wiles odstraňování chyby vzdát, jej dne 19. září 1994 napadla hlavní myšlenka, jak důkaz opravit. Tehdy požádal o pomoc svého bývalého studenta Richarda Taylora[8]. Přepracovaný důkaz („jen“ 130 stránek) pak vyšel v květnu 1995 ve dvou článcích [38] a [36] jako speciální číslo renomovaného časopisu *Annals of Mathematics*.

Během svého života Andrew Wiles získal celou řadu významných ocenění. Jmenujme kupříkladu Whiteheadovu cenu (1988), Schockovu cenu (1995), Fermatovu

[6]Této domněnce se dnes říká Ribetova věta, viz věta 4. Opírá se o Galoisovy reprezentace odpovídající modulárním formám (viz kap. 5). Jako první ji zformuloval Jean-Pierre Serre, pozdější nositel první Abelovy ceny.

[7]A. Wiles k otázce práce v utajení prohlásil: *I realized that anything to do with Fermat's Last Theorem generates too much interest. You can't really focus yourself for years unless you have undivided concentration, which too many spectators would have destroyed.*

[8]R. Taylor obhájil Ph.D. v roce 1988 na Univerzitě v Princetonu. Byl také jedním ze šestice recenzentů původního chybného Wilesova důkazu.

cenu (1995), Wolfovu cenu (1995/96), Coleovu cenu (1997), Wolfskehlovu cenu[9] (1997), stříbrnou plaketu Mezinárodní matematické unie (1998), Pythagorovu cenu (2004) a Shawovu cenu (2005). Budova Univerzity v Oxfordu, v níž sídlí matematický ústav, byla pojmenována Andrew Wiles a asteroid č. 9999 nese od roku 1999 jméno Wiles. V roce 1989 se A. Wiles stal Fellow of the Royal Society a v roce 2000 byl povýšen na rytíře Řádu Britského impéria (angl. Knight Commander of the Order of the British Empire). Jeho podrobný životopis je uveřejněn v knize Simona Singha [32].

3. Historické aspekty řešení Fermatova problému

S Velkou Fermatovou větou je spojeno nesčetné množství pozoruhodných příběhů. O tomto asi nejslavnějším matematickém problému všech dob byla proto napsána celá řada monografií, viz např. [5], [13], [21], [24], [26], [27], [32]. Také v *PMFA* byla tomuto tématu věnována velká pozornost, viz [11], [16], [22], [33] a [34].

Exponent $n \geq 3$ ve větě 1 je zřejmě buď dělitelný lichým prvočíslem, nebo je n mocninou 2. Ukážeme nejprve, že větu stačí dokázat, jen je-li exponent n liché prvočíslo nebo $n = 4$. Pokud by totiž měla rovnice (1) řešení pro nějaké $n = pq$, kde p je liché prvočíslo a $q > 1$, pak

$$x^{pq} + y^{pq} = \left(x^q\right)^p + \left(y^q\right)^p = \left(z^q\right)^p = z^{pq}. \tag{2}$$

Tudíž stačí položit $x' = x^q$, $y' = y^q$, $z' = z^q$ a vidíme, že rovnice (1) má řešení i pro $n = p$.

Podobně zjistíme, že pokud by existovalo nějaké řešení rovnice (1) pro $n = 2^k$, kde $k > 2$, pak by muselo existovat řešení i pro $n = 4$, neboť

$$x^{2^k} + y^{2^k} = \left(x^{2^{k-2}}\right)^4 + \left(y^{2^{k-2}}\right)^4 = \left(z^{2^{k-2}}\right)^4 = z^{2^k}. \tag{3}$$

Sám Fermat dokázal neexistenci řešení (1) jen pro $n = 4$, z čehož podle (3) okamžitě plyne, že rovnice (1) nemá řešení ani pro $n = 8, 16, 32, \ldots$ Použil k tomu svoji oblíbenou metodu nekonečného sestupu (franc. *descente infinie*).

Věta 2 (Fermatova). *Bikvadratická rovnice*

$$x^4 + y^4 = z^4 \tag{4}$$

nemá řešení v množině přirozených čísel, tj. věta 1 platí pro $n = 4$.

Důkaz. Stačí ukázat, že jiná bikvadratická rovnice $w^2 + y^4 = z^4$ nemá řešení v množině přirozených čísel $\mathbb{N}$. Kdyby totiž existovalo nějaké řešení (4), pak by existovalo též řešení rovnice $w^2 + y^4 = z^4$ pro $w = x^2$, což ale chceme vyvrátit.

Budeme postupovat sporem. Předpokládejme tedy, že existuje řešení rovnice

$$w^2 = z^4 - y^4 \tag{5}$$

v množině přirozených čísel. Nechť navíc řešení rovnice (5) je takové, že $z \in \mathbb{N}$ je nejmenší možné číslo. Takové z zřejmě existuje, neboť množina přirozených čísel je

[9] V roce 1908 německý průmyslník Paul Wolfskehl vypsal odměnu 100 000 zlatých marek tomu, kdo první dokáže Velkou Fermatovu větu.

dobře uspořádaná, tj. každá její neprázdná podmnožina má minimální prvek. Pak pro největší společný dělitel čísel y a z platí

$$\gcd(y, z) = 1. \tag{6}$$

Kdyby totiž nějaké prvočíslo p dělilo y i z, pak bychom mohli rovnici $(p^2w')^2 = (pz')^4 - (py')^4$, kde $w' = w/p^2$, $z' = z/p$ a $y' = y/p$, vydělit p^4 a dostali bychom spor s minimalitou z.

Uvažujme rozklad $w^2 = (z^2 + y^2)(z^2 - y^2)$. Pak $d = \gcd(z^2 + y^2, z^2 - y^2)$ musí dělit součet i rozdíl obou činitelů, což lze zapsat jako $d \mid 2z^2$ a $d \mid 2y^2$. Podle (6) je $d \in \{1, 2\}$. Rozlišíme dva případy.

Případ 1: $\gcd(z^2 + y^2, z^2 - y^2) = 1$.

Protože součin $z^2 + y^2$ a $z^2 - y^2$ dvou nesoudělných čísel je čtvercem, je každé z nich také čtvercem, tj. existují nesoudělná čísla $s > t$ tak, že

$$z^2 + y^2 = s^2, \qquad z^2 - y^2 = t^2.$$

Obě čísla s a t musí být lichá, protože

$$2z^2 = s^2 + t^2 \qquad \text{a} \qquad \gcd(s, t) = 1.$$

Existují tedy $u, v \in \mathbb{N}$ tak, že

$$u = \frac{s + t}{2}, \qquad v = \frac{s - t}{2}.$$

Protože s a t jsou lichá, platí

$$\gcd(u, v) = 1. \tag{7}$$

Jelikož $uv = (s^2 - t^2)/4 = y^2/2$, máme $y^2 = 2uv$. Odtud podle vztahu (7) tedy existují $j, m \in \mathbb{N}$ tak, že platí buď

$$u = 2j^2, \qquad v = m^2,$$

anebo

$$u = j^2, \qquad v = 2m^2.$$

Budeme uvažovat jen první alternativu, protože druhou lze vyšetřit analogicky.

Číslo u je tedy sudé, $\gcd(u, v, z) = 1$ a

$$u^2 + v^2 = \frac{(s + t)^2 + (s - t)^2}{4} = \frac{s^2 + t^2}{2} = z^2.$$

Protože $\langle u, v, z\rangle$ je pythagorejská trojice nesoudělných čísel (tzv. primitivní pythagorejská trojice), existují nesoudělná přirozená čísla $k > \ell$ tak, že (viz např. [17, s. 54])

$$2j^2 = u = 2k\ell, \quad m^2 = v = k^2 - \ell^2, \quad z = k^2 + \ell^2. \tag{8}$$

Jelikož $j^2 = k\ell$, existují nesoudělná přirozená čísla d a e tak, že

$$k = d^2, \quad \ell = e^2,$$

a podle (8) tedy platí $m^2 = d^4 - e^4$. Ukázali jsme, že čísla $d, e, m \in \mathbb{N}$ rovněž splňují rovnici (5), což je ve sporu s minimalitou z, neboť $0 < d < k < z$.

Případ 2: $\gcd(z^2 + y^2, z^2 - y^2) = 2$.

Nyní je tedy w sudé a y, z jsou lichá. Podle (5) a (6) je $\langle w, y^2, z^2 \rangle$ pythagorejská trojice nesoudělných čísel. Podobně jako v (8) existují nesoudělná přirozená čísla $k > \ell$ tak, že

$$w = 2k\ell, \quad y^2 = k^2 - \ell^2, \quad z^2 = k^2 + \ell^2.$$

Tudíž $y^2 z^2 = k^4 - \ell^4$ pro $0 < k < z$, což je opět spor s minimalitou z. □

Důsledek 1. *Neexistuje pythagorejský trojúhelník, jehož obsah je čtvercem přirozeného čísla.*

Důkaz. Nechť $a, b \in \mathbb{N}$ jsou délky odvěsen pythagorejského trojúhelníka a nechť jeho obsah $ab/2 = j^2$ pro nějaké přirozené číslo $j \in \mathbb{N}$. Pak

$$(a + b)^2 = c^2 + 4j^2, \quad (a - b)^2 = c^2 - 4j^2,$$

kde $c^2 = a^2 + b^2$. Tedy $(a^2 - b^2)^2 = c^4 - (2j)^4$. Z předchozího důkazu ale víme, že rovnice (5) nemá celočíselné řešení, což je spor. □

Další překvapivý důsledek zformulovali ve vzájemných dopisech sir Kenelm Digby a Pierre de Carcavi již v 17. století.

Důsledek 2. *Neexistuje pravoúhlý trojúhelník s racionálními délkami stran a jednotkovým obsahem.*

Důkaz. Nechť naopak existují čísla $a, b, c, q, r, s \in \mathbb{N}$ taková, že

$$\left(\frac{a}{q}\right)^2 + \left(\frac{b}{r}\right)^2 = \left(\frac{c}{s}\right)^2 \qquad \text{a} \qquad \frac{1}{2}\frac{a}{q}\frac{b}{r} = 1.$$

Pak $(ars)^2 + (bqs)^2 = (cqr)^2$ a $\frac{1}{2}(ars)(bqs) = (qrs)^2$, což podle důsledku 1 nemůže nastat. □

Fermat používal metodu nekonečného sestupu s nadšením i k důkazům jiných hypotéz. Tato metoda je příbuzná známé metodě matematické indukce. O století později použil metodu nekonečného sestupu k důkazu Velké Fermatovy věty též Leonhard Euler pro $n = 3$. V jeho důkazu z roku 1770 však byla nalezena mezera, kterou se naštěstí později podařilo zaplnit (viz [27, s. 30]). Případu $n = 3$ se věnovali i Christian Huygens, Karel Rychlík a mnoho dalších autorů[10], viz např. [12], [21, s. 86], [26, s. 39], [37, s. 90].

Věta 3 (Fermatova–Eulerova). *Kubická rovnice*

$$x^3 + y^3 + z^3 = 0 \tag{9}$$

nemá řešení v množině nenulových celých čísel.

[10] Vlastní elegantní důkaz nedávno předložil středoškolský student Vojtěch Suchánek [35]. Jeho důkaz se opírá o vlastnost, že právě jedno číslo z trojice x, y, z je dělitelné třemi, pokud tuto trojici tvoří nesoudělná čísla splňující (1) pro $n = 3$. Je-li totiž $x \equiv r \pmod 9$, kde $r \in \{0, 1, \ldots, 8\}$, pak $x^3 \equiv 0$ nebo $\pm 1 \pmod 9$, což implikuje onu vlastnost.

Důkaz. Předpokládejme naopak, že existují po dvou nesoudělná čísla x, y, z, pro něž platí (9), kde bez újmy na obecnosti jsou x a y lichá, z je sudé a $|z|$ je nejmenší možné. Pak

$$x + y = 2a, \qquad x - y = 2b,$$

kde a, b jsou nenulová nesoudělná celá čísla rozdílné parity. Pokud by tomu tak nebylo, tak snadno dojdeme ke sporu. Tudíž

$$-z^3 = x^3 + y^3 = (a+b)^3 + (a-b)^3 = 2a(a^2 + 3b^2). \tag{10}$$

Jelikož a a b mají rozdílnou paritu, je $a^2 + 3b^2$ liché, 8 dělí $2a$ a b je liché. Tedy $\gcd(2a, a^2 + 3b^2)$ dělí $4a^2 - a^2 - 3b^2 = 3(a-b)(a+b)$. Protože

$$\gcd(a, b) = 1,$$

dostáváme, že $\gcd(2a, a^2 + 3b^2) = 1$ nebo 3. Rozlišujme dva případy.

Případ 1: $\gcd(2a, a^2 + 3b^2) = 1$.
Podle (10) jsou $2a$ a $a^2 + 3b^2$ třetí mocniny

$$2a = r^3, \qquad a^2 + 3b^2 = s^3,$$

kde s je liché. Podle Eulera [7] pak existují[11] celá čísla u, v taková, že platí (viz [26, s. 40–42])

$$s = u^2 + 3v^2, \qquad a = u(u^2 - 9v^2), \qquad b = 3v(u^2 - v^2).$$

Protože b je liché, je v rovněž liché. Dále pak $u \neq 0$, u je sudé, 3 nedělí u (tj. $3 \nmid u$), $\gcd(u, v) = 1$ a

$$r^3 = 2a = 2u(u - 3v)(u + 3v).$$

Poznamenejme, že $2u$, $u - 3v$ a $u + 3v$ musí být po dvojicích nesoudělná čísla, a tak musí být třetími mocninami

$$2u = -k^3, \qquad u - 3v = \ell^3, \qquad u + 3v = m^3,$$

kde celá čísla k, ℓ, m jsou nenulová (protože 3 nedělí u). Tedy

$$k^3 + \ell^3 + m^3 = 0,$$

kde k je sudé. Protože navíc $b \neq 0$ a $3 \nmid u$, z (10) dostaneme

$$|z^3| = |2a(a^2 + 3b^2)| = |k^3(u^2 - 9v^2)(a^2 + 3b^2)| \geq 4|k^3| > |k^3|,$$

jelikož $|u^2 - 9v^2| \geq 1$ a $a^2 + 3b^2 \geq 1 + 3$. To je však ve sporu s minimalitou $|z|$.

Případ 2: $\gcd(2a, a^2 + 3b^2) = 3$.
Nechť $a = 3c$. Protože $4 \mid a$, platí $4 \mid c$, $3 \nmid b$, $4 \nmid b$ a podle (10) máme

$$-z^3 = 6c(9c^2 + 3b^2) = 18c(3c^2 + b^2),$$

[11] Položíme-li $M = \{a^2 + 3b^2 \mid a, b \in \mathbb{Z}\} = \{0, 1, 3, 4, 7, 9, 12, 13, 16, 19, 21, 25, 27 = 3^3, \dots\}$, pak M je uzavřená množina vzhledem k násobení, protože $(a^2 + 3b^2)(c^2 + 3d^2) = (ac + 3bd)^2 + 3(ad - bc)^2 = (ac - 3bd)^2 + 3(ad + bc)^2$. Jinými slovy, M je komutativní monoid. Euler již kolem roku 1760 dokázal (viz [26, s. 39]), že pokud $s^3 = a^2 + 3b^2 \in M$ pro nesoudělná čísla a a b, pak samotné s je stejného tvaru $s = u^2 + 3v^2 \in M$.

kde $18c$, $3c^2+b^2$ jsou nesoudělná, $3c^2+b^2$ je liché a není násobkem 3. Pak $18c$ a $3c^2+b^2$ jsou třetí mocniny celých čísel

$$18c = r^3, \qquad 3c^2 + b^2 = s^3,$$

kde s je liché. Podobně jako v případě 1 je $s = u^2 + 3v^2$, kde u, v splňují

$$b = u(u^2 - 9v^2), \qquad c = 3v(u^2 - v^2).$$

Tedy u je liché, v je sudé, $v \neq 0$, $\gcd(u, v) = 1$ a $2v$, $u + v$ a $u - v$ jsou po dvojicích nesoudělná čísla. Z rovnosti

$$\left(\frac{r}{3}\right)^3 = 2v(u + v)(u - v)$$

plyne, že

$$2v = -k^3, \qquad u + v = \ell^3, \qquad u - v = -m^3.$$

Tudíž $k^3 + \ell^3 + m^3 = 0$, kde k, ℓ, m jsou nenulová a k sudé. Konečně tak dostáváme

$$|z|^3 = 18|c|(3c^2+b^2) = 54|v(u^2-v^2)|(3c^2+b^2) = 27|k|^3|u^2-v^2|(3c^2+b^2) \geq 27|k|^3 > |k|^3,$$

což je opět ve sporu s minimalitou $|z|$. □

Francouzská matematička Sophie Germainová [10] v roce 1819 dokázala, že rovnice (1) nemá řešení, jestliže součin xyz není dělitelný exponentem $n \geq 3$ a jestliže n a $2n + 1$ jsou prvočísla. Byl to vlastně první výsledek, který se týkal nekonečně mnoha prvočíselných exponentů. V roce 1825 G. P. L. Dirichlet a o tři roky později i A. M. Legendre dokázali Velkou Fermatovu větu pro exponent $n = 5$ včetně případu, že n dělí xyz, který S. Germainová neuvažovala. Důkaz pro exponent $n = 7$ představili G. Lamé a V. A. Lebesgue v roce 1840.

V roce 1847 německý matematik Ernst Eduard Kummer viz ([18], [19], [20]) dokázal Velkou Fermatovu větu v případě, že daný prvočíselný exponent p (srov. (2)) nedělí žádného čitatele Bernoulliových čísel $B_0, B_1, \ldots, B_{p-3}$ (viz též [34]). Taková prvočísla se nazývají *regulární*. Postupně se tedy začaly vylučovat další a další exponenty. Jenomže existují prvočísla, která nejsou regulární (nejmenší jsou 37, 59, 67), a dodnes není známo, zda jich je konečně či nekonečně mnoho. Pro ně žádná úspěšná metoda tehdy nebyla známa. Od vzniku počítačů byly též spotřebovány miliony hodin strojového času k nalezení řešení diofantické rovnice (1).

V roce 1983 Gerd Faltings [8] dokázal slavnou Mordellovu domněnku (viz [26, s. 214], [34, s. 318]) z roku 1922, která tvrdí, že rovnice (1) má pro každý exponent $n \geq 3$ jen konečně mnoho řešení takových, že x, y, z nemají společného dělitele. Podrobný historický přehled obsahující řadu dalších speciálních tvrzení, která se týkají řešení rovnice (1), je podán v článku [37].

Bylo nutno najít nějakou zcela novou metodu, která by zahrnovala všechny prvočíselné exponenty v (1) současně. V následujících třech kapitolách se stručně seznámíme se základními ingrediencemi Wilesova důkazu.

4. Eliptické křivky

Předem je nutno upozornit, že název eliptická křivka je poněkud zavádějící, protože se nejedná o elipsu.

Eliptická křivka je množina všech řešení $x, y \in \mathbb{R}$ rovnice

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \tag{11}$$

kde koeficienty a_i jsou racionální čísla.[12] Studiu těchto křivek se matematikové věnují už dlouho, protože se mj. používají k vyjádření délky eliptických oblouků[13] (např. při vyšetřování trajektorií planet). Pro jejich zajímavé vlastnosti se speciálními případy eliptických křivek zabývali již staří Řekové a též Niels Henrik Abel.

Pomocí lineární substituce $y \mapsto y - a_1x/2 - a_3/2$ lze rovnici (11) zjednodušit na tvar

$$y^2 = x^3 + b_2x^2 + 2b_4x + b_6, \tag{12}$$

kde b_i jsou vhodná racionální čísla. Pomocí další substituce $x \mapsto x - b_2/3$ reprezentující jen posunutí lze rovnici (12) zjednodušit na tvar (podobně jako při řešení kubických rovnic [25, s. 39])

$$y^2 = x^3 + Ax + B. \tag{13}$$

Odpovídající diskriminant

$$\Delta = -\left(\frac{A}{3}\right)^3 - \left(\frac{B}{2}\right)^2 = -(4A^3 + 27B^2)/108$$

má pěknou geometrickou interpretaci, která některými vlastnostmi připomíná diskriminant při řešení kvadratických rovnic. Je-li $\Delta = A = 0$, pak má křivka $y^2 = x^3$ bod vratu, tj. singularitu typu *cusp* (viz obr. 5 vlevo). Je-li $\Delta = 0$ a $A \neq 0$, pak eliptická křivka (13) protíná sama sebe (viz obr. 5 uprostřed). Pokud $\Delta \neq 0$, pak má monický polynom $p(x) = x^3 + Ax + B$ tři různé kořeny; v opačném případě má vícenásobný kořen. Je-li $\Delta < 0$, pak existuje jeden reálný a dva komplexně sdružené kořeny a eliptická křivka je souvislá (např. $y^2 = x^3 + 2$). Je-li $\Delta > 0$, pak existují jen reálné kořeny a eliptická křivka má dvě komponenty (viz obr. 5 vpravo).

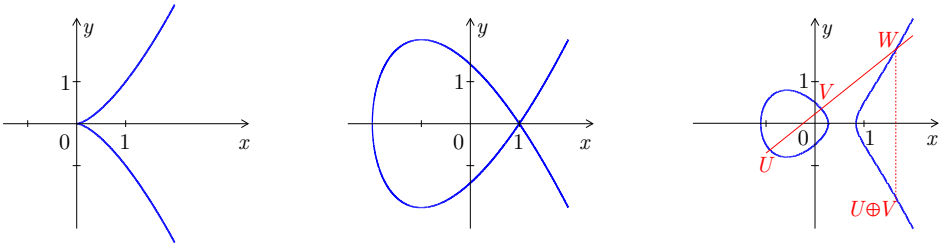
Na bodech eliptické křivky (13) lze pro $\Delta \neq 0$ definovat grupu s operací $\oplus$ (viz obr. 5 vpravo) a s neutrálním prvkem v nekonečnu. Inverzní prvek k danému bodu eliptické křivky je definován jako jeho zrcadlový obraz vzhledem k ose x. Více podrobností o této abelovské grupě uvádíme v [16].

Je velice obtížné stanovit všechna celočíselná řešení $(x, y) \in \mathbb{Z}^2$ rovnice (11), viz [16, s. 94]. Na konkrétním příkladě si nyní ukážeme, jak lze eliptické křivky charakterizovat. Uvažujme eliptickou křivku

$$x^3 - x^2 = y^2 + y. \tag{14}$$

[12] Jako definiční obor pro x, y se často uvažují též množiny $\mathbb{Z}$, $\mathbb{Q}$ nebo $\mathbb{C}$.

[13] Vznik termínu eliptická křivka má spletitou historii. Výpočet délky eliptického oblouku $f(x) = b\sqrt{a^2 - x^2}/a$ s poloosami a a b vede na tzv. eliptický integrál z funkce $\sqrt{1 + (f'(x))^2}$, který však nemá analytické vyjádření pomocí elementárních funkcí. Invertováním eliptických integrálů dostaneme tzv. eliptické funkce, které se používají k parametrizaci eliptických křivek, podrobnosti viz [4] a [30].



Obr. 5. Eliptické křivky $y^2 = x^3$, $y^2 = x^3 - 3x + 2 = (x-1)^2(x+2)$ a $y^2 = x^3 - x + \frac{1}{4}$. Na poslední křivce lze definovat grupovou operaci $\oplus$ tak, jak je nakresleno na obrázku vpravo, tj. prvek W je inverzní k $U \oplus V$.

Její celočíselná řešení jsou

$$x = 0,\ y = 0 \qquad \text{a} \qquad x = 1,\ y = 0,$$

ale nevíme, zda jsou to všechna řešení. V modulární aritmetice ale další řešení existují. Například v aritmetice modulo 5 je kongruence

$$x^3 - x^2 \equiv y^2 + y \pmod 5 \tag{15}$$

navíc splněna pro

$$x = 0,\ y = 4 \qquad \text{a} \qquad x = 1,\ y = 4.$$

Snadno lze ověřit, že kongruence (15) má právě 4 výše uvedená řešení a žádná jiná, což zapíšeme jako

$$E_5 = 4.$$

Podobně zjistíme, že existují právě 4 řešení $(0,0)$, $(1,0)$, $(0,2)$ a $(1,2)$ v aritmetice modulo 3, tj. $E_3 = 4$. Eliptické křivce (14) tak můžeme jednoznačně přiřadit nekonečnou posloupnost

$$E_2 = 4,\ E_3 = 4,\ E_4 = 8,\ E_5 = 4,\ E_6 = 16,\ E_7 = 9,\ E_8 = 16, \ldots \tag{16}$$

Protože většinou nejsme schopni určit, kolik má konkrétní rovnice řešení v množině $\mathbb{Z}^2$, hledají se její řešení alespoň v modulární aritmetice. Posloupnost $\{E_j\}$ pak jistým způsobem charakterizuje uvažovanou eliptickou křivku a pro pevné j příslušná řešení patří do konečné grupy.

Dále se budeme zabývat jen eliptickými křivkami tvaru (13) s $\Delta \neq 0$. Jejich definiční obor pro x a y zúžíme jen na množinu racionálních čísel $\mathbb{Q}$, přičemž bod v nekonečnu také zahrneme do této křivky. Budeme jim říkat *racionální eliptické křivky*. Mají-li body $U = (u_1, u_2)$ a $V = (v_1, v_2)$ pro $u_1 \neq v_1$ na eliptické křivce racionální souřadnice, pak směrnice přímky, která jimi prochází, je také racionální číslo. Lze ukázat, že tato přímka protíná eliptickou křivku v dalším bodě W (viz obr. 5 vpravo), který má rovněž racionální souřadnice.

Je ale velice obtížné stanovit, zda má daná eliptická křivka konečně či nekonečně mnoho bodů s racionálními souřadnicemi (viz monografie [31], jejímž spoluautorem

je další nositel Abelovy ceny John Tate). Podle již zmíněné Mordellovy domněnky, kterou dokázal G. Faltings, je ale grupa všech racionálních bodů na eliptické křivce vždy jen konečně generovaná.

Eliptické křivky našly v poslední době i řadu praktických uplatnění. Používají se např. pro stanovení veřejného šifrovacího klíče v kryptografii, při testování prvočíselnosti velkých přirozených čísel nebo jejich rozkladu na prvočinitele.

5. Modulární formy

Modulární formy jsou mnohem abstraktnější matematické objekty než eliptické křivky. Jsou to jistá zobrazení vykazující neuvěřitelně mnoho symetrií (viz např. (18) a (19) níže). Označme $SL_2(\mathbb{Z})$ multiplikativní grupu matic typu 2×2

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix},$$

kde a, b, c, d jsou celá čísla a

$$\det g = ad - bc = 1.$$

Inverzní prvek této neabelovské grupy je zřejmě dán vztahem

$$g^{-1} = \begin{pmatrix} d & -b \\ -c & a \end{pmatrix}.$$

Pro $g \in SL_2(\mathbb{Z})$ a $z \in \mathbb{C}$ definujme tzv. *akci* gz pomocí komplexní racionální funkce (viz např. [14, s. 98])

$$gz = \frac{az + b}{cz + d}. \tag{17}$$

Nechť dále $H = \{z \in \mathbb{C} \,|\, \mathrm{Im}\ z > 0\}$. Pak snadno zjistíme, že pro libovolné $g \in SL_2(\mathbb{Z})$ se horní Gaussova polorovina H zachovává, tj. že $\mathrm{Im}\ z > 0$ implikuje $\mathrm{Im}\ gz > 0$. Platí totiž

$$\mathrm{Im}\ gz = \mathrm{Im}\frac{az + b}{cz + d} = \mathrm{Im}\frac{(az + b)(c\overline{z} + d)}{|cz + d|^2} = |cz + d|^{-2}\mathrm{Im}(adz + bc\overline{z}),$$

kde $\overline{z}$ je číslo komplexně sdružené se z. Protože

$$\mathrm{Im}(adz + bc\overline{z}) = (ad - bc)\mathrm{Im}\ z = \det g\ \mathrm{Im}\ z = \mathrm{Im}\ z,$$

dostaneme

$$\mathrm{Im}\ gz = |cz + d|^{-2}\mathrm{Im}\ z \quad \forall g \in SL_2(\mathbb{Z}).$$

Každému prvku grupy $g \in SL_2(\mathbb{Z})$ lze tedy pomocí (17) přiřadit transformaci $H \to H$.

Definice. Nechť $k \in \mathbb{Z}$ a nechť funkce f meromorfní[14] v horní polorovině H splňuje vztah

$$f(gz) = (cz + d)^k f(z) \quad \forall g \in SL_2(\mathbb{Z}). \tag{18}$$

[14] Komplexní funkce se nazývá *meromorfní*, jestliže je holomorfní na otevřené souvislé podmnožině komplexní roviny $\mathbb{C}$ až na body v množině izolovaných pólů.

Předpokládejme navíc, že f je meromorfní v nekonečnu.[15] Pak se f nazývá *modulární forma s vahou k grupy $SL_2(\mathbb{Z})$*.

Ze vztahu (18) je patrná vysoká symetrie modulárních forem. Zvolíme-li např. $g = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$, pak

$$f(z+1) = f(z). \tag{19}$$

Podobně pro $g = \left(\begin{smallmatrix} 0 & 1 \\ -1 & 0 \end{smallmatrix}\right)$ dostaneme

$$f(-1/z) = (-z)^k f(z). \tag{20}$$

V padesátých letech minulého století japonský matematik Yutaka Taniyama[16] vyslovil domněnku o souvislosti eliptických křivek a modulárních forem. Další japonský matematik Goro Šimura mu ji pak pomohl zpřesnit. Proto se jí dnes většinou říká Taniyamova–Šimurova.

Taniyamova–Šimurova domněnka. *Každá racionální eliptická křivka je modulární.*

Podle této domněnky lze každou racionální eliptickou křivku ztotožnit s jistou modulární formou.[17] Ztotožnění probíhá následovně. V předchozí kapitole jsme ukázali, že dané eliptické křivce lze jednoznačně přiřadit posloupnost $\{E_j\}$, srov. (16). Y. Taniyama podobně každé modulární formě jednoznačně přiřadil jakousi posloupnost přirozených čísel $\{M_j\}$. Když se podíval na několik prvních členů určité modulární formy, zjistil, že souhlasí s několika prvními členy posloupnosti $\{E_j\}$ jisté eliptické křivky. Pak spočítal několik dalších členů obou posloupností a zjistil, že se shodovaly. A tak jej napadlo, že by každá modulární forma mohla mít svou odpovídající eliptickou křivku. To byl úžasný objev. Nikdo ale nevěděl, jak rovnost $E_j = M_j$ dokázat pro všechna $j = 2, 3, \ldots$ Tak vznikla Taniyamova–Šimurova domněnka.[18]

6. Wilesova–Taylorova věta

Propojení mezi Taniyamovou–Šimurovou domněnkou a Velkou Fermatovou větou vzniklo, když německý matematik Gerhard Frey na konferenci v Oberwolfachu v roce 1985 prohlásil: Pokud by platilo

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

pro nějaká přirozená čísla a, b, c a prvočíselný exponent $p \geq 5$ (srov. (1) a (2)), potom by racionální eliptická křivka, tzv. *Freyova křivka*[19] tvaru (12),

$$y^2 = x(x - a^p)(x + b^p) \tag{21}$$

dávala protipříklad na Taniyamovu–Šimurovu domněnku.

[15] To znamená, že Fourierova řada $f(z) = \sum_{m\in\mathbb{Z}} a_m q^m$, kde $q = \exp(2\pi \mathrm{i} z)$, má jen konečně mnoho nenulových koeficientů a_m pro $m < 0$. Přitom f má pól v ∞, jestliže $f(1/z)$ má pól v nule.

[16] Y. Taniyama spáchal ve svých nedožitých 31 letech sebevraždu, a tak se rozřešení své domněnky nedožil. O pár dní později jej následovala i jeho dívka. G. Šimura po rozřešení domněnky vystoupil v BBC, viz [33].

[17] K téže domněnce později, leč nezávisle dospěl i francouzský matematik André Weil, a proto občas v odborné literatuře nese i jeho jméno, viz [6].

[18] Vztahům mezi eliptickými křivkami a modulárními formami je věnována monografie [14] z roku 1984.

[19] Tuto křivku uvedl předtím ve své doktorské dizertaci Yves Hellegouarch. Případnému řešení diofantické rovnice (1) tak přiřadil zcela jiný matematický objekt: eliptickou křivku.

Ve stejném roce Jean-Pierre Serre podal částečný důkaz toho, proč Freyova křivka nemůže být modulární. Jinými slovy, pokud by platila Taniyamova–Šimurova domněnka, pak by Freyova křivka (21) byla tak bizarní, že by nemohla existovat, tj. množina racionálních řešení rovnice (21) by byla prázdná. Kenneth Ribet pak v roce 1990 v článku [28] podal úplný důkaz toho, že Frey měl pravdu.

Věta 4 (Ribetova). *Jestliže platí Taniyamova–Šimurova domněnka, pak platí Velká Fermatova věta pro* $p \geq 5$.

Díky této větě získali matematici zcela nový přístup, jak Fermatův problém atakovat. Robert Langlands z Ústavu pro pokročilá studia v Princetonu byl již od šedesátých let minulého století svědkem rozmachu Taniyamovy–Šimurovy domněnky. Byla to vlastně část jeho grandiózního schématu sjednocujícího veškerou matematiku (tzv. Langlandsův program). Byl přesvědčen, že existují mosty mezi jednotlivými zdánlivě nesouvisejícími matematickými disciplínami a ty je třeba hledat. A právě Andrew Wiles takový most našel. Dokázal sice jen restringovanou (omezenou) Taniyamovu–Šimurovu domněnku pro tzv. semistabilní eliptické křivky[20], ale naštěstí tento speciální případ v sobě stále ještě zahrnuje Velkou Fermatovu větu.

Věta 5 (Wilesova–Taylorova). *Každá semistabilní racionální eliptická křivka je modulární.*

K důkazu Wiles použil Iwasawovu teorii společně s Kolyvaginovou–Flachovou metodou [32, s. 161]. Semistabilní eliptické křivky vyjádřil pomocí Galoisových reprezentací[21] a ukázal, že se shodují s Galoisovými reprezentacemi příslušných modulárních forem.

V roce 1995 zveřejnil v *Annals of Mathematics* (viz [38]) úplný důkaz věty 5, ze kterého Velká Fermatova věta vyplývá, přičemž část důkazu je ve společném článku [36] s Richardem Taylorem. Předložený důkaz se ale opírá o celou řadu dalších netriviálních tvrzení publikovaných jinde (viz např. [8], [28]). Metody, které Wiles použil, jsou podrobně vysvětleny např. v knize [13] či v článku [23].

Úplný důkaz Taniyamovy–Šimurovy domněnky i pro nesemistabilní eliptické křivky později provedli Christophe Breuil, Brian Conrad, Fred Diamond a Richard Taylor v obsáhlém článku [3].

Věta 6 (modulární). *Každá racionální eliptická křivka je modulární.*

Každé racionální eliptické křivce tak lze přiřadit posloupnost čísel, která ji definuje, a stejná posloupnost pak bude definovat odpovídající modulární formu. Oba termíny jsou tudíž koncepčně ekvivalentní.

[20] Tyto křivky mají bezkvadrátový konduktor. To je jistý invariant, který dělí diskriminant. Na obr. 5 vlevo je příklad křivky, která není semistabilní. Zbývající dvě křivky semistabilní jsou. Podrobnosti viz [31].

[21] Galoisovou reprezentací se obvykle rozumí homomorfismus absolutních Galoisových grup do grupy čtvercových matic nad tělesem reálných či komplexních čísel. A. Wiles uvažoval eliptickou křivku nad komplexními čísly a na ní množinu $E(p)$ tzv. p-torzních bodů, kde p je prvočíslo. Použil homomorfismus z $E(p)$ do multiplikativní grupy $GL_2(F_p)$ matic typu 2×2 nad konečným tělesem F_p charakteristiky p. Podrobnosti viz [1].

Obr. 6. Abelova cena (zdroj `http://www.abelprize.no/`)

7. Závěr

Před rokem 1995 se někteří matematikové domnívali, že Fermatova hypotéza je nerozhodnutelné tvrzení. Sir Andrew Wiles však našel způsob, jak Velkou Fermatovu větu[22] dokázat. Její důkaz je bez nadsázky považován za „důkaz století“ a za jeden z největších triumfů současné matematiky [9]. Metodu, kterou Andrew Wiles a Richard Taylor použili, však Pierre de Fermat nemohl znát, neboť řada pojmů (jako např. eliptické křivky, modulární formy, grupy) tehdy nebyla ještě zavedena. Předpoklad $p \geq 5$ v Ribetově větě 4 (viz [28, s. 120, 128]) není omezující, neboť jej vtipně doplňují Fermatova věta 2 a Fermatova–Eulerova věta 3. Vzhledem ke vztahům (2) a (3) tak Velká Fermatova věta 1 platí pro všechny exponenty $n \geq 3$.

[22] V anglicky mluvících zemích se pro Velkou Fermatovu větu používá termín *Fermat's Last Theorem* naznačující, že jde o poslední (až do nedávna) nevyřešený problém, který nám Fermat zanechal. Dodnes ale není vyřešen jiný závažný problém, zda posloupnost Fermatových čísel $F_m = 2^{2^m} + 1$ pro $m = 0, 1, 2, \ldots$ obsahuje jen konečně mnoho prvočísel [15].

Jen málo matematických výsledků má tak bohatou a dramatickou historii jako Velká Fermatova věta. Jejím důkazem však příběh nekončí. Existuje totiž celá řada podobných problémů, které jsou stále otevřené. Například Američan Andrew Beal formuloval následující domněnku, na jejíž vyřešení je vypsána vysoká finanční odměna (viz [22]).

Bealova domněnka. *Rovnice*

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

nemá řešení v přirozených číslech k, m, n, x, y a z, kde k, m a n jsou větší než 2 a čísla x, y a z jsou vzájemně nesoudělná.

Předpoklad, že všechny tři exponenty jsou větší než 2, je podstatný, jak plyne z identit $2^5 + 7^2 = 3^4$, $7^3 + 13^2 = 2^9$ apod.

Během osmdesátých let 20. století formulovali David Masser a Joseph Oesterlé diofantickou nerovnost známou pod názvem *domněnka abc*. Její rozřešení by mělo mnoho aplikací (např. pro důkaz Bealovy domněnky).

Domněnka abc. *Ke každému reálnému číslu $\varepsilon > 0$ existuje konstanta $C > 1$ taková, že pro každá dvě vzájemně nesoudělná přirozená čísla a a b a jejich součet $c = a + b$ platí*

$$c \leq Cr^{1+\varepsilon},$$

kde r je součin všech různých prvočinitelů abc.

Smysl předchozí nerovnosti je zhruba tento.[23] Pokud $a = 2^m$ i $b = 3^n$ pro velká m a n, pak domněnka říká, že c musí mít velký prvočíslený dělitel nebo velké množství prvočinitelů tak, aby r bylo velké.[24]

V případě Velké Fermatovy věty (1) stačí zvolit $\varepsilon = \frac{1}{2}$. Pak podle domněnky abc je $z^n < Cr^{3/2}$, kde

$$r = \prod_{p \mid x^n y^n z^n} p = \prod_{p \mid xyz} p \leq xyz \leq z^3,$$

a tedy $z^n < Cz^{9/2}$. Odtud plyne existence n_0 takového, že by Velká Fermatova věta byla splněna pro všechny exponenty $n > n_0$.

Poděkování. Na některé zajímavé materiály nás upozornil Jon Eivin Vatne z Bergen University College. S obrázky nám pomohli Hana Bílková a Filip Křížek. Drobné úpravy textu nám navrhli Ľubomíra Dvořáková, Pavla Pavlíková, Antonín Slavík, Jana Žďárská a anonymní recenzent. Jim všem patří náš velký dík. Článek byl podpořen RVO 67985840 České republiky.

[23] Nedávno japonský matematik Shinichi Mochizuki oznámil, že domněnku abc dokázal. Jeho důkaz však čítá kolem 500 stránek, a tak je stále ještě prověřován odborníky na teorii čísel.

[24] Existuje nekonečně mnoho případů, kdy $r < c$ (např. pro $a + b = 3 + 5^3 = 2^7 = c$ je $r = 2 \cdot 3 \cdot 5 = 30 < 128 = c$). Jiná verze domněnky abc ale praví, že pro libovolné $\varepsilon > 0$ existuje jen konečně mnoho případů, kdy $r^{1+\varepsilon} < c$.

[1] Ash, A., Gross, R.: *Fearless symmetry: Exposing the hidden patterns of numbers*. Princeton Univ. Press, 2008.

[2] Bachet, C. -G.: *Diophanti Alexandrini arithmeticorum*. Sebastiani Cramoisy, Paris, 1621.

[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] Brown, E.: *Three Fermat trails to elliptic curves*. College Math. J. *31* (2000), 162–172.

[5] Casti, J. L.: *Mathematical mountaintops. The five most famous problems of all times*. Oxford Univ. Press, 2001.

[6] Darmon, H.: *A proof of the Shimura–Taniyama–Weil conjecture is announced*. Notices Amer. Math. Soc. *42* (1995), 1397–1401.

[7] Euler, L.: *Supplementum quorundam theorematum arithmeticorum quae in nonnullis demonstrationibus supponuntur*. Novi Comm. Acad. Sci. Petrop. *8* (1760/1763), 105–128; též Opera Omnia, Ser. I, vol. II, 556–575, Teubner, Leipzig, 1915.

[8] Faltings, G.: *Finitness theorems for abelian varieties over number fields (German)*. Invent. Math. *73* (1983), 349–366.

[9] Faltings, G.: *The proof of Fermat's Last Theorem by R. Taylor and A. Wiles*. Notices Amer. Math. Soc. *42* (1995), 743–746.

[10] Germain, S.: *Œuvres philosophiques* (ed. H. Spurny). P. Ritti, Paris, 1879, 298–302, 363–364.

[11] Granville, A.: *Recenze pořadu Horizon stanice BBC „Fermatova poslední věta“*. PMFA *42* (1997), 184–187.

[12] Hardy, G. H., Wright, E. M.: *An introduction to the theory of numbers*. Clarendon Press, Oxford, 4th edition, 1960; other editions: 1938, 1945, 1954, 1979.

[13] Hellegouarch, Y.: *Invitation to the mathematics of Fermat-Wiles*. Academic Press, London, 2002.

[14] Koblitz, N.: *Introduction to elliptic curves and modular forms*. Springer, New York, 1984.

[15] Křížek, M., Luca, F., Somer, L.: *17 lectures on Fermat numbers: From number theory to geometry*. CMS Books in Mathematics, vol. 9. Springer-Verlag, New York, 2nd edition, 2011.

[16] Křížek, M., Somer, L.: *John Tate získal Abelovu cenu za rok 2010*. PMFA *55* (2010), 89–96.

[17] Křížek, M., Somer, L., Šolcová, A.: *Kouzlo čísel: Od velkých objevů k aplikacím*. Edice Galileo, sv. 39. Academia, Praha, 2. vydání, 2011.

[18] Kummer, E. E.: *Extrait d'une lettre de M. Kummer à M. Liouville*. J. Math. Pures Appl. *12* (1847), 136.

[19] Kummer, E. E.: *Beweis des Fermatschen Satzes der Unmöglichkeit von* $x^\lambda + y^\lambda = z^\lambda$ *für eine unendliche Anzahl Primzahlen* λ. Monatsber. Akad. d. Wiss., Berlin (1847), 132–139, 140–141, 305–319.

[20] Kummer, E. E.: *Allgemeiner Beweis des Fermat'schen Satzes dass die Gleichung* $x^\lambda + y^\lambda = z^\lambda$ *durch ganze Zahlen unlösbar ist, für alle diejenigen Potenz-Exponenten* λ*, welche ungerade Primzahlen sind und in die Zählern der ersten* $\frac{1}{2}(\lambda-3)$ *Bernoulli'schen Zahlen als Factoren nicht Vorkommen*. J. Reine Angew. Math. *40* (1850), 130–138.

[21] Lepka, K.: *Historie Fermatových kvocientů*. Dějiny matematiky, sv. 14. Prometheus, Praha, 2000.

[22] Mauldin, R. D.: *Zobecnění Velké Fermatovy věty: Bealova domněnka a problém o cenu*. PMFA *43* (1998), 104–107.

[23] Nekovář, J.: *Modulární křivky a Fermatova věta*. Math. Bohem. *119* (1994), 79–96.

[24] van der Poorten, A.: *Notes on Fermat's Last Theorem*. John Wiley, New York, 1996.

[25] Rektorys, K.: *Přehled užité matematiky I*. Prometheus, Praha, 1995.

[26] Ribenboim, P.: *13 lectures on Fermat's last theorem*. Springer, New York, 1979.

[27] Ribenboim, P.: *Fermat's last theorem for amateurs*. Springer, New York, 1999.

[28] Ribet, K. A.: *From the Taniyama-Shimura conjecture to Fermat's last theorem*. Ann. Fac. Sci. Toulouse Math. *11* (1990), 116–139.

[29] Ribet, K. A.: *Wiles proves Taniyama's conjecture; Fermat's last theorem follows*. Notices Amer. Math. Soc. *40* (1993), 575–576; český překlad: Math. Bohem. *116* (1994), 75–78.

[30] Rice, A., Brown, E.: *Why ellipses are not elliptic curves*. Math. Mag. *85* (2012), 163–176.

[31] Silverman, J. H., Tate, J.: *Rational points on elliptic curves*. Springer-Verlag, 1992.

[32] Singh, S.: *Velká Fermatova věta*. Academia, Praha, 2000.

[33] Singh, S., Millson, R.: *Velká Fermatova věta (Pořad Horizon stanice BBC)*. PMFA *42* (1997), 169–183.

[34] Skula, L.: *Některé historické aspekty Fermatova problému*. PMFA *39* (1994), 318–330.

[35] Suchánek, V.: *Důkaz Velké Fermatovy věty pro $n = 3$*. SOČ, Brno, 2015, 1–20.

[36] Taylor, R., Wiles, A.: *Ring-theoretic properties of certain Hecke algebras*. Ann. of Math. *141* (1995), 553–572.

[37] Terjanian, G.: *Velká Fermatova věta*. Cah. CEFRES *28* (2002), 87–106.

[38] Wiles, A.: *Modular elliptic curves and Fermat's last theorem*. Ann. of Math. *141* (1995), 443–551.

[39] `http://abelprisen.no/en/c67107/seksjon/vis.html?tid=671088&struk_tid=67107`